STORMSHIELD

Yearbook

2019

2019: a busy year for news

Relive the year's highlights with the different awareness-building content produced by Stormshield.

Une année 2019 riche en actualités

Revivez les temps forts de cette année à travers les différents contenus de sensibilisation signés Stormshield.

Pierre-Yves Hentzen

CEO of Stormshield

In an ever-changing world, in which technologies evolve as fast as the threats which accompany them, strategic thinking about cybersecurity needs to cover many different and complex areas. Such thinking is critically important, as it enables us as individuals to question our relationships with digital hygiene and our awareness of cyber risks.

Asking key questions and raising awareness is an integral part of Stormshield's mission. It provides a practical shape for the role we have to play in a fragile, vulnerable world, and our involvement in creating a durable, stable, healthy cyberspace environment. This concept of a "mission" is one which is very dear to us because, as we see it, it is not restricted to simply designing cybersecurity projects — which is, after all, only a means rather than an end. In addition to providing protection for computing resources or data, and thereby protecting people and our institutions, our mission is also to question, analyse, understand and share. In this way, we can create the confidence and peace of mind people need to start a company, to do business and to grow.

That's why, for more than two years, we have been enhancing our efforts to produce Stormshield-branded content. A great initiative... but it doesn't stop there. Our strategic thinking is effective because it is the fruit of teamwork and shared expression — with complementary and contradictory points of view. We combine internal expert studies from our various departments with as much real-world raw data as possible. This provides a mix of opinions and ideas from our R&D and Security Intelligence teams, but also from sales and pre-sales staff, our marketing and human resources teams. In addition, we seek to involve an increasing number of external stakeholders from the world of cybersecurity, including partners, customers, universities, researchers, etc.

The content we produce identifies weak signals which anticipate the trends of tomorrow, and responds to strong signals created by current cyber-events. And because cybersecurity maturity levels can vary according to profession, company, region and even experience, we realised the importance of devising content covering several different levels. That's why we produce contents to educate and raise awareness, more expert papers, professional perspectives and forward-looking projections — as a practical demonstration of our innovative vision and foresight.

This 2019 Yearbook looks back on a year which has been particularly rich in headlines and content. Structured around four key themes and several internal sub-areas, it provides a fluid, logical read which moves between the year's various trends — from cyberattacks against the world of industry through to the construction of a new relationship with cybersecurity. It will enhance your own strategic thinking, and help to raise awareness.

TABLE OF CONTENTS
SOMMAIRE

You'll find original versions on the website www.stormshield.com

CYBER CULTURE IN CORPORATIONS, A LONG JOURNEY FULL OF PITFALLS

THE SLOW EVOLUTION OF IT PROFESSIONS

THE CYBER REGULATIONS JUNGLE

BUILDING A NEW RELATIONSHIP WITH CYBERSECURITY

CYBERSECURITY AS PART OF THE DAILY LIVE

THE TOPIC OF CYBERSECURITY TRAINING AND EXCHANGES

THE MATTER OF CYBERSECURITY STAFFING

#1

Cyber threats, the industrial world in the hurricane's eye

L'industrie, dans l'œil du cyclone des cyberattaques

What cyber challenges does industry face in 2019?

Quels défis cyber doit relever l'industrie en 2019 ?

By Robert Wakim – March 26, 2019

The dawn of the industry 4.0 poses new risks with regard to cybersecurity. Whether these risks come from competitors, criminal organisations or even hostile States, the threats weighing heavily on this ultra-connected industry are numerous and need to be pre-empted at all levels.

In the family of industrial malware, I'm requesting the latest: "Triton". Also known as "Trisis" or "HatMan", it is the most recent of its kind and leaves an even greater mark on the history of industrial cyberattacks. At the end of 2017, this impressive attack was carried out against an industrial plant located in the Middle East, the identity of which has not been revealed. Even though this cyberattack would appear to have failed, it was able to cause great operational disruption to the plant.

Since then, cyberattacks against industrial infrastructures throughout the world have continued; their official number only increasing with public announcements. Over the course of December 2018 alone, two major attacks were identified: the first was a variant of the Shamoon malware, and infected the IT system of the Italian petrol giant, Saipem; and the second delayed the distribution of several large American newspapers,

L'avènement de l'industrie du futur ouvre de nouveaux risques en matière de cybersécurité. Qu'elles viennent de concurrents, d'organisations criminelles, voire d'États hostiles, les menaces qui pèsent sur cette industrie hyper connectée sont multiples et réclament une anticipation à tous les niveaux.

Dans la famille des malwares industriels, je demande le petit dernier : « Triton ». Aussi appelé « Trisis » ou « HatMan », il est le plus récent de son espèce et marque davantage l'histoire des cyberattaques industrielles. Fin 2017, cette attaque impressionnante était menée contre un site industriel situé au Moyen-Orient, dont l'identité n'a pas été révélée. Même si cette cyberattaque semblerait avoir échoué, elle aurait pu causer de très fortes perturbations opérationnelles de l'installation.

Depuis, les cyberattaques contre des infrastructures industrielles à travers le monde n'ont pas cessé ; leur nombre officiel n'augmentant qu'au rythme des annonces publiques. Au cours du seul mois de décembre 2018, on recensait deux attaques majeures : la première, variante du malware Shamoon, a infecté le système d'information du géant italien du pétrole Saipem ; la seconde a retardé la distribution de plusieurs grands journaux américains, comme le Los Angeles Times. En mars 2019, c'est Norsk Hydro, l'un des plus

such as the Los Angeles Times. More recently, in March 2019, Norsk Hydro, one of Europe's largest aluminium producers, suffered a major cyber attack, attributed so far to LockerGoga ransomware.

And there is nothing to indicate that the risks are going to decrease. On the contrary. At a time when the industry 4.0, development of the Industrial Internet of Things (IIoT), the digitisation of factories, and artificial intelligence technology are making industrial networks (OT) more and more connected and communicative, particularly with regard to IT networks (company information systems), this ultra-connection exposes them to more threats.

The strength of the cybersecurity chain is only equal to the strength of its weakest link

The rise in machine-to-machine communication, requiring no human intervention, or the development of digital twins (digital replicas of a piece of equipment or system), are also participating **in the increase of industrial attack surfaces**. It is worth remembering that the strength of the cybersecurity chain is only equal to the strength of its weakest link. The multiplication of entry points therefore requires an increased securing of interconnections between these different networks. It thus becomes a strategic challenge to protect sensitive industrial environments effectively.

Facing up to the major sources of attack against industry in 2019

The main sources of attack against the industrial sector come from within three groups: its own stakeholders, via the game of industrial spying; cybercriminals at the origin of mass attacks (such as WannaCry); and hostile states, through cyberwarfare. The first are looking to obtain a competitive advantage, the second to make money, and the third to weaken the country in which industrialist is attacked.

When faced with its own competitors, industry at least has the option to level the playing field. This is because an industrial attacker usually has good knowledge of the equipment used by its competitors — as it uses it itself — and therefore has the information necessary to lead its criminal company.

grands producteurs d'aluminium en Europe, qui a subi à son tour une cyberattaque majeure, imputée à ce jour au ransomware LockerGoga.

Et rien ne permet de penser que les risques vont diminuer. Bien au contraire. À l'heure de l'industrie du futur, le développement de l'internet industriel des objets (IIoT), de la numérisation des usines, et des technologies d'intelligences artificielles rendent les réseaux industriels (OT) de plus en plus connectés et communicants, notamment vers les réseaux IT (systèmes d'information de l'entreprise) ; cette hyper-connexion les expose toujours plus aux menaces.

L'essor de la communication machine to machine, se passant d'intervention humaine, ou encore le développement des jumeaux numériques (des répliques numériques d'un équipement ou d'un système), participent également ***à l'accroissement des surfaces d'attaque des industriels****. Or, il ne faut pas oublier que la force de la chaîne de cybersécurité est égale à la force de son maillon le plus faible. La multiplication des points d'entrée nécessite donc une sécurisation accrue des interconnexions entre ces différents réseaux. Elle devient alors un enjeu stratégique pour protéger efficacement les environnements industriels sensibles.*

Faire face aux sources majeures d'attaques contre l'industrie en 2019

Les principales sources d'attaques contre le secteur industriel trouvent leurs origines au sein de trois groupes : ses propres acteurs, via le jeu de l'espionnage industriel ; les cybercriminels à l'origine d'attaques de masse (de type WannaCry) ; et les États hostiles, au travers de la cyberguerre. Les premiers cherchent à obtenir un avantage concurrentiel, les seconds à gagner de l'argent et les derniers à affaiblir le pays dans lequel est attaqué l'industriel.

Face à ses propres concurrents, l'industriel a au moins la possibilité de jouer à armes égales. C'est d'ailleurs parce qu'un industriel-attaquant a généralement une bonne connaissance des équipements utilisés par ses concurrents – les utilisant lui-même – qu'il dispose des informations nécessaires pour mener son entreprise délictueuse.

Le cybercriminel, lui, ne disposant pas de ces informations ne vise pas une cible mais l'équipement le plus massivement

A cybercriminal does not have this information and so does not aim at a target but at the most widely used equipment which contains a security flaw (e.g.: Windows XP, IP cameras, routers, etc.). With the rise of the IIoT and the digital, connected equipment of the industry 4.0, it is very tempting to choose the latest, state-of-the-art device. **However, it is always prudent to choose the one that ensures the best cyber protection**.

With regard to the threat from hostile states, this remains the most difficult to comprehend by industrialists. Faced with an attacker that has both financial and human means that are generally greater than those of its target, it is complicated to integrate this statistically very low risk. Especially when an industrialist's security and cybersecurity teams are used to classifying and managing risks depending on their probability of triggering an incident.

Implementing the appropriate procedures

Once the potential stakeholders involved in industrial cyberattacks, their motivation, and their means of action have been identified, the industrial business just needs to follow a few basic rules and:

- Place itself in a position whereby it thinks that this doesn't just happen to others,
- Be aware that every system is weak, and that this weakness only increases over time,
- Draw up a map of its devices and the communication means between them,
- Train all employees, without exception, and make them aware of all the different types of cyberattack in order to make them potential whistle-blowers,
- Identify critical areas and potential attack scenarios,
- Implement response procedures to identified attacks,
- Ensure compliance with the different regulations or, in the event that the regulations do not directly apply, become familiar with them and use them as a guide to good practice.

Finally, the best thing to do is to form a cybersecurity entity, bringing together security and cybersecurity experts in the same team. The business then has operational knowledge in addition knowledge of the abuse and associated risks. ¶

déployé dans le secteur, et qui contient une faille de sécurité (ex. : Windows XP, caméras IP, routeurs…). Avec l'essor de l'IIoT et des équipements numérisés et connectés de l'industrie du futur, la tentation est grande de choisir un nouvel équipement dernier cri. ***La prudence pourtant est de toujours choisir celui qui assure la meilleure cyber-protection****.*

Quant à la piste étatique, elle reste la plus difficile à appréhender par les industriels. Devant un agresseur aux moyens financiers et humains généralement bien supérieurs à ceux de sa cible, il est compliqué d'intégrer ce risque statistiquement très faible. Surtout quand les équipes de sûreté et de cybersécurité d'un industriel sont habituées, elles, à classifier et traiter les risques en fonction de leur probabilité à déclencher un incident.

Mettre en place les bonnes procédures

Une fois identifiés les acteurs potentiels de cyberattaques industrielles, leurs motivations et leurs moyens d'action, reste à l'entreprise industrielle à suivre quelques règles de base :

- *se mettre en situation de penser que cela n'arrive pas qu'aux autres,*
- *savoir que tout système est faillible, et que cette faillibilité ne cesse de croître avec le temps,*
- *réaliser une cartographie de ses équipements et des moyens de communication entre eux,*
- *former et sensibiliser tous les collaborateurs, sans exception, à tous les types de cyberattaques, afin d'en faire d'éventuels lanceurs d'alerte,*
- *identifier les zones critiques et les scénarios d'attaques possibles,*
- *mettre en place des procédures de réaction aux attaques identifiées,*
- *se mettre en conformité avec les différentes réglementations, ou dans le cas où elle ne s'applique pas directement, en prendre connaissance et de le prendre comme un guide de bonnes pratiques.*

Enfin, l'idéal est de former une entité de cyber sûreté regroupant, au sein d'une même équipe, des experts de la sûreté et des experts de la cybersécurité. L'entreprise dispose ainsi de la connaissance opérationnelle et de la connaissance des malveillances et de leurs risques associés. ¶

Industrial networks

Les réseaux industriels

In a series of three webinars, Stormshield shares its experience of the industrial world.

Au travers d'une série de trois webinaires, Stormshield partage son expérience du monde industriel.

IT-OT networks: why convergence is delicate, yet crucial

By Khobeib Benboubaker – July 27, 2019

Emerging industries 4.0 are turning convergence between industrial networks (OTs) and information networks (IT) into a hot topic in industrial world. This phenomenon highlights the specific characteristics of this infrastructure and reveals certain risks, particularly with regard to cybersecurity.

Predictive maintenance, goods and services that precisely satisfy consumer demand: there are a proliferation of promises offered by this Industry 4.0, related to information and industrial networks. However, the task of reconciling these two very different types of infrastructure is more complex than it seems.

"The industry 4.0 brings the extra dimension of data, collected by machines or from users. With the convergence of IT/OT networks, this data can be used to reduce maintenance time, predict failures and reduce environmental costs," explains Stéphane Prévost, Product Marketing Manager at Stormshield.

Réseaux IT-OT : les raisons d'une convergence délicate

Portée par l'industrie du futur, la convergence des réseaux industriels (OT) et des réseaux informatiques (IT) est à l'œuvre dans le monde industriel. Ce phénomène met en lumière les spécificités de ces infrastructures et dévoile certains risques, notamment en matière de cybersécurité.

Maintenance prédictive, production au plus près des attentes des consommateurs, les promesses de cette industrie du futur liées à la convergence des réseaux informatiques et industriels abondent. Or, le rapprochement de ces deux types d'infrastructures très différents est plus complexe qu'il n'y paraît.

Two-speed development of IT and OT infrastructure

For a number of years now, industry has watched as the boundaries between IT and OT start to blur. Computer technology, which is updated at regular intervals on control workstations in workshops, rubs shoulders with a pool of machines offering greatly increased lifespans and amortisation periods. Much like the USB/RS232 converter enabling a machine speaking one language (USB for a PC) to be understood by a different one (RS232 for an industrial machine), **the challenge for OT teams was to find a way of reconciling these worlds with their different development priorities.**

"Industrial tools have their own pace and methodology for making connections between the various active components of the network: the fieldbus. This was created during the second Industrial Revolution, and made mass production methods possible. It then survived the third industrial revolution, which ushered in the age of automation... but its relationship with the information age is rather more complicated," Stéphane Prévost points out. Indeed, with the advent of the Internet, commands for the industrial protocols that are now ubiquitous in workshops and consoles are now conveyed via TCP/IP.

Information networks and industrial networks: diametrically opposed design concepts

The fundamental differences in how IT and OT networks are secured originate in how they are each designed.

The purpose of information networks is to transport large quantities of data. As they were created in an open environment, interaction lies at the heart of how they operate, and secure versions of their protocols are available. Conversely, industrial networks are intended to transfer commands to ensure industrial processes

"The convergence of IT/OT networks can be used to reduce maintenance time, predict failures and reduce environmental costs"

Stéphane Prévost, Product Marketing Manager, Stormshield

« L'industrie du futur vient rajouter une dimension de données, collectées par les machines ou auprès des utilisateurs. La convergence des réseaux IT/OT permet de les utiliser pour réduire les temps de maintenance, anticiper les pannes ou encore diminuer les coûts environnementaux », expose Stéphane Prévost, Product Marketing Manager Stormshield.

Une évolution des infrastructures IT et OT à deux vitesses

Depuis plusieurs années déjà, l'industrie a vu s'estomper la frontière entre IT et OT. L'informatique, régulièrement renouvelée dans les postes de contrôle au sein des ateliers, côtoie un parc de machines à la durée de vie et d'amortissement beaucoup plus élevées. À l'image du convertisseur USB/RS232 qui permettait à une machine qui parle un langage (USB pour un PC) d'être comprise par une autre (RS232 pour la machine industrielle), ***le défi des équipes OT était donc d'arriver à relier ces deux mondes qui n'évoluent pas au même rythme****.*

« L'outil industriel a son propre tempo et son propre système pour connecter les différents éléments actifs du réseau : le bus terrain. Il a été créé lors de la deuxième révolution industrielle et a permis la production de masse. Il a ensuite survécu à la troisième révolution industrielle, celle qui a permis l'automatisme, mais la cohabitation avec l'ère informatique est plus compliquée », explique Stéphane Prévost. En effet, à l'heure d'Internet, les commandes des protocoles industriels toujours présents dans les ateliers et sur les consoles requièrent désormais un transfert par TCP/IP.

Réseaux informatiques et réseaux industriels : des contextes de conception aux antipodes

Les divergences fondamentales en matière de sécurisation des réseaux IT et OT remontent à leur conception.

Les réseaux informatiques ont vocation à transporter des données en grande quantité. Nés dans un environnement

are managed correctly. As they are generally designed independently from one workshop to another, these networks have not been specifically secured, having been deemed to be isolated and thus already protected by the respective security policies of the factories that house them.

"From the outset, information technology has made use of secure data protocols (https for web browsing, SMTPS for email exchanges, etc.), whereas for operational networks, security has been implemented at industrial site level: there seemed to be no advantage to adding a protection layer to networks developed in a confined, secure environment," adds Stéphane Prévost.

Industrial networks: singular management

Until recently, industries had no need to centralise the management of their OT infrastructure: these networks, operating independently of one another and having little exposure from a cybersecurity perspective, "just somehow worked" thanks to the ingenuity of the on-site teams!

As convergence gains speed, the risk increases, leading to greater awareness. Many industrial companies are implementing governance systems to provide a better overview of their networks. This is especially important as every industrial network is unique.

"The bespoke nature of industrial networks makes it more complex to implement a shared security policy," continues Stéphane Prévost.

Lastly, the main challenge regarding convergence of IT and OT networks is a human one: how can information and operational teams learn to understand one another and adapt to the other's constraints? Dialogue between IT teams, with their experience in cybersecurity, and OT teams, with their specialist skills in their own industrial network, is the real key to better security of the overall infrastructure.

Together, they can take responsibility for better identifying and analysing risks, and for facilitating the implementation of a comprehensive IT/OT security policy. ¶

ouvert, l'interaction est au cœur de leur fonctionnement et leurs protocoles disposent de version sécurisée. À l'inverse, les réseaux industriels sont dédiés à l'acheminement des commandes pour assurer la bonne gestion du processus industriel. Généralement conçus de façon autonome d'un atelier à un autre, ces réseaux n'ont pas fait l'objet d'une sécurisation spécifique car ils étaient considérés comme isolés et déjà protégés par la politique de sécurité des usines qui les abritent.

« L'informatique s'est dotée dès le départ de protocoles de données sécurisés (https pour la navigation internet, SMTPS pour les échanges d'emails, etc.) alors que dans le cas des réseaux opérationnels, la sécurité a été pensée au niveau du site industriel : il n'a pas été jugé utile de rajouter une couche de protection à des réseaux développés dans un environnement confiné et sécurisé », complète Stéphane Prévost.

Réseaux industriels : une gestion singulière

Jusque récemment, les industries n'avaient pas besoin de centraliser la gestion de leur infrastructure OT : ces réseaux, indépendants les uns des autres et peu exposés d'un point de vue cybersécurité, « tombaient en marche » grâce à l'ingéniosité des équipes sur le terrain !

À mesure que la convergence progresse, le risque augmente et provoque une prise de conscience. Beaucoup d'industriels mettent en place une gouvernance pour bénéficier d'une meilleure visibilité sur leurs réseaux. C'est d'autant plus important que chaque réseau industriel est unique. « La singularité des réseaux industriels complexifie la mise en place d'une politique de sécurité commune », résume Stéphane Prévost.

Finalement, le principal défi de la convergence des réseaux IT et OT est d'ordre humain : comment les équipes informatiques et opérationnelles peuvent-elles apprendre à se comprendre et s'adapter à leurs contraintes respectives ? Le dialogue entre les équipes IT, fortes de leur expérience en cybersécurité, et les équipes OT, spécialistes de leur réseau industriel, est en effet la clé d'une meilleure sécurité de l'infrastructure globale.

Charge à elles, ensemble, de mieux identifier, analyser les risques et faciliter la mise en place d'une politique de sécurité globale IT/OT. ¶

Top 5 most dangerous industrial cyberattacks

By Khobeib Benboubaker
– August 19, 2019

In addition to the financial losses they cause, industrial cyberattacks are feared due to the threat they pose for the environment, human lives, as well as the sovereignty of the country affected. We review five — or almost five — of the most dangerous threats that industry has faced up to now.

Top 5 des cyberattaques les plus dangereuses pour les industries

Au-delà des pertes financières qu'elles engendrent, les cyberattaques industrielles sont redoutées car elles présentent un risque pour l'environnement, les vies humaines voir la souveraineté du pays impacté. Retour sur les cinq menaces les plus dangereuses qu'ait connues l'industrie à ce jour – ou presque.

5 SHAMOON

NEARLY CAUSES A POLLUTION EVENT

Though it didn't get very far into the industrial system, this malware paralysed Aramco, the Saudi Arabian national hydrocarbon company, for more than 15 days in 2012. With nearly 35,000 computers rendered unusable, the company found itself disconnected from the world. It lost control of its supervision consoles and production process, which could have led to a large-scale explosion and pollution event. In 2018, the Italian petrol company Saipem was also reportedly impacted by an attack linked to Shamoon.

LA POLLUTION EN RÉPERCUSSION

Sans aller très loin dans le système industriel, ce logiciel malveillant a paralysé Aramco, la société nationale saoudienne d'hydrocarbures, pendant plus de 15 jours en 2012. Avec près de 35 000 ordinateurs inutilisables, l'entreprise se retrouve déconnectée du monde. Elle perd le contrôle de ses consoles de supervision et de son processus de production, faisant courir un risque de pollution et d'explosion à grande échelle. En 2018, le pétrolier italien Saipem aurait à son tour été impacté par une attaque basée sur Shamoon.

4 INDUSTROYER

SHORT CIRCUITS POWER GRIDS

Since 2015, multiple attacks by multiple versions of the malware Industroyer have come on the scene, affecting at least one country, Ukraine. Its speciality? Attacking electrical generation systems. Industroyer gives the attacker complete control of the targeted system, without the victim's knowledge. The possibilities for malfeasance are almost endless: cutting power to a district, city or region; changing the frequency of a power grid; overloading a plant grid; or even interfering with the global power network.

FAIT DISJONCTER LES RÉSEAUX ÉLECTRIQUES

Depuis 2015, plusieurs versions et attaques du malware Industroyer se sont succédées et ont notamment frappé un pays comme l'Ukraine. Sa particularité ? S'attaquer aux systèmes de production d'électricité. Coupures de courant, changement de fréquence du réseau électrique, Industroyer donne à l'assaillant le contrôle total du système attaqué et ce, sans connaissance particulière préalable. À la clé, des possibilités presque infinies : couper le courant d'un quartier, d'une ville ou d'une région, surcharger le réseau d'une usine ou bien encore interférer avec le réseau électrique mondial…

3 TRITON

A MALWARE WITH ENVIRONMENTAL CONSEQUENCES

First detected in 2017, when it was targeting the Saudi Arabian petrol company Petro Rabigh, this malware could have caused enormous harm, including marine pollution, a spike in petrol prices, and even deaths due to explosion. Its MO? Reprogramming the controllers of the Triconex Safety Instrumented System (SIS). According to the latest reports on this cyberattack, Triton went unnoticed for three years before being detected. An unsettling piece of news, now that the malware seems to have resurfaced in April 2019.

UN MALWARE AUX CONSÉQUENCES ENVIRONNEMENTALES

Détecté en 2017 alors qu'il visait la société pétrolière Petro Rabigh, en Arabie saoudite, ce logiciel malveillant aurait pu provoquer d'énormes dégâts : morts en cas d'explosion, pollution maritime, ou encore flambée du prix du baril... Son mode opératoire ? Reprogrammer les contrôleurs du système instrumenté de sécurité (SIS) Triconex. Selon les derniers rapports sur cette cyberattaque, Triton serait passé inaperçu pendant trois ans avant d'être détecté. Une donnée inquiétante, alors que le malware semble avoir refait surface au cours du mois d'avril 2019.

2 STUXNET

RAISES THE SPECTRE OF NUCLEAR FALLOUT

As described in the documentary "Zero Days", Stuxnet is a 2010 cyberattack that targeted centrifuges at the Natanz uranium enrichment site in Iran. Its goal? To halt or slow down production. A warning sign that raises the spectre of an even larger attack, this time with nuclear consequences.

LAISSE PLANER LA MENACE DE RADIOACTIVITÉ

Décrite dans le documentaire « Zero Days », la cyberattaque Stuxnet de 2010 s'en prend aux centrifugeuses du site d'enrichissement d'uranium de Natanz en Iran. L'objectif ? Ralentir voire stopper la production. Un avertissement qui laisse planer la menace d'une attaque de plus grande ampleur dont les conséquences seraient radioactives.

1 ?

AN AS-YET UNIDENTIFIED ATTACK

The fifth most dangerous industrial cyberattack could already be happening right now, without anyone's knowledge. As we saw with Triton and Stuxnet, several years may go by between a malware's first move and its subsequent detection. That's why cybersecurity remains one of the biggest challenges for industry in 2019.

UNE ATTAQUE ENCORE NON IDENTIFIÉE

La cinquième cyberattaque industrielle la plus dangereuse pourrait bien être déjà en cours, sans pour autant avoir été identifiée. Comme dans les exemples de Triton et Stuxnet, plusieurs années s'écoulent parfois entre le premier mouvement du malware et sa découverte. C'est pourquoi la cybersécurité reste un des principaux défis à relever pour l'industrie en 2019.

Taking action: The primary challenge facing industry

L'action, principal défi du monde industriel

At the centre of the digital transformation, SCADA systems represent a double-edged sword, as they become more vulnerable when they are exposed to the outside world. In order to tackle this challenge, industry players have no choice but to take action.

Au cœur de la transformation numérique, la connexion des systèmes SCADA est à double tranchant. En s'ouvrant au monde extérieur, ils deviennent plus vulnérables. Pour y faire face, les industriels n'ont plus le choix : il faut passer à l'action.

By Khobeib Benboubaker – July 18, 2019

SCADA systems are currently at the centre of a profound shift in the digital transformation. Despite the promises in store for the industrial sector, the recent raft of high-profile cyberattacks against these systems attests to their poor cybersecurity protections. When it comes to this issue, the primary challenge facing industry today is the need to take action. **The question is not whether it should protect itself, but how.**

Les systèmes SCADA sont aujourd'hui au cœur d'une profonde mutation avec la transformation numérique. Malgré les promesses de l'industrie du futur, la médiatisation des cyberattaques impactant ces systèmes témoigne de leur faible niveau de cybersécurité. Le principal défi du monde industriel en la matière est aujourd'hui l'action. ***La question n'est pas de savoir s'il faut se protéger, mais comment.***

The difficult task of incorporating cybersecurity into industry

Companies that have already begun their digital transformation will need to redefine their deployment procedures in order to incorporate cybersecurity. The goal in this case is to expand the operational infrastructure timetable by seamlessly introducing deployment phases for security solutions — a process made all the more difficult by the fact that OT systems (ICS/SCADA) lack the same constrains as conventional information systems (IT). Other companies, on the other hand, will be able to take a "Cybersecurity by design" approach to their digital transformation. Here, the central goal is to incorporate security solutions more efficiently.

In addition to incorporating cybersecurity into the deployment planning process, a second fundamental mechanism for effectively securing SCADA systems is to educate employees about the issues at hand. This is best accomplished by getting IT and OT staff to communicate and share experiences with one another. Indeed, while technicians, operators and production managers are needed to handle the specific demands of SCADA systems — due in no small part to the design of the facilities and their operational requirements — it is also true that cybersecurity has traditionally been the purview of the team responsible for office communication systems. As such, dialogue and a good understanding of both approaches are key to successfully securing industrial facilities. ¶

La difficile intégration de la cybersécurité dans l'industrie

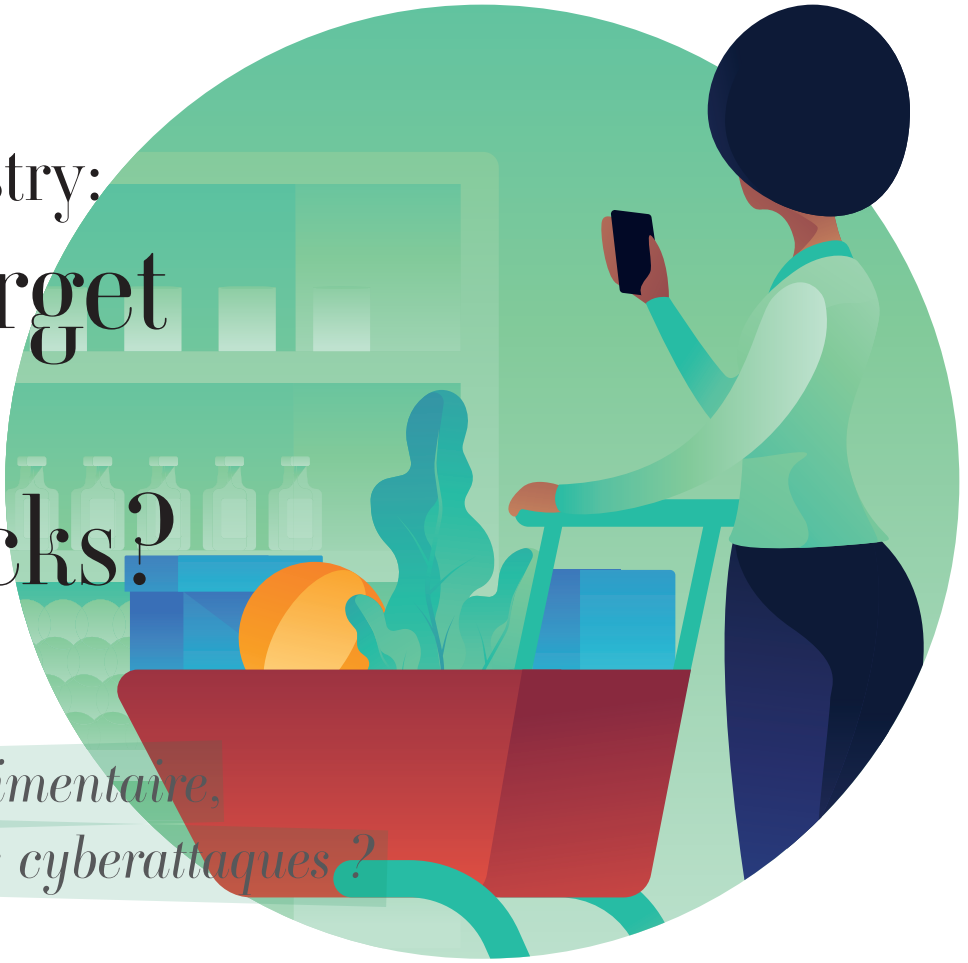
Pour les entreprises ayant déjà entamé leur transformation numérique, elles devront redéfinir leurs procédures de déploiement pour y intégrer la cybersécurité. L'enjeu étant ici d'inclure de manière fluide les différentes phases de déploiement de solutions de protection, dans le planning des infrastructures opérationnelles. Une intégration d'autant plus difficile que les systèmes OT (ICS/SCADA) n'ont pas les mêmes contraintes que les systèmes d'information classiques (IT). Les autres entreprises auront la possibilité d'appréhender leur transformation digitale sous le prisme du cybersecurity-by-design. Une intégration plus efficace des solutions de protection est ici au cœur des enjeux.

À côté de l'intégration de la cybersécurité dans la planification des déploiements, la sensibilisation des équipes constitue la seconde clé fondamentale pour sécuriser efficacement les systèmes SCADA. Elle doit s'appréhender sous l'angle de la communication et du partage d'expériences entre les équipes IT et OT. En effet, d'un côté, la singularité des systèmes SCADA, de par la conception des installations ou de leurs opérations, requiert la connaissance des techniciens, opérateurs et responsables de production. De l'autre côté, la cybersécurité est traditionnellement sous la responsabilité d'une équipe du réseau bureautique. C'est donc dans le dialogue et la compréhension des deux approches que l'on va trouver l'une des principales clés de réussite de la sécurisation des installations industrielles. ¶

The food industry

L'industrie agro-alimentaire

The food industry: A new target for cyberattacks?



L'industrie agroalimentaire, nouvelle cible des cyberattaques ?

By Stéphane Prévost – October 8, 2019

The cyberattack against Fleury Michon in France seems to support what had previously been suspected: that agri-food industries are the new targets for cyberattackers. And this is no coincidence, given their strategic nature. Issues, risks and counter-measures: we review the situation.

The date is April 15th, 2019 and, on a Spring Monday, Fleury Michon is gradually finding its feet again following a cyberattack that brought production to a halt for five days. "During the night of April 10th to 11th, Fleury Michon's computer systems were hit by an electronic virus. As a precautionary measure, all systems were disconnected to prevent it from spreading. Our factories and our logistics unit were shut down on last Thursday, April 11, at 2:00pm", the group revealed in a statement.

No more information is available about the origins of this virus, or how it managed to get into Fleury Michon's computer system. Nor do we know the financial cost to the business of a five-day plant shutdown. So

La cyberattaque contre Fleury Michon en France semble étayer ce qui était pressenti : les industries agro-alimentaires sont de nouvelles cibles pour les cyberattaquants. Et ce n'est pas un hasard tant ces industries sont stratégiques. Enjeux, risques et parades : tour d'horizon de la situation.

Nous sommes le 15 avril 2019 et en ce lundi de printemps, Fleury Michon reprend peu à peu pied après une cyberattaque qui a immobilisé sa production pendant cinq jours. « Dans la nuit du 10 au 11 avril, les systèmes informatiques de Fleury Michon ont été touchés par un virus informatique. Par mesure de précaution, l'ensemble des systèmes ont été déconnectés, pour éviter la propagation. Les usines, ainsi que notre unité logistique, ont été mises à l'arrêt jeudi dernier, 11 avril, à 14h00 », dévoile le groupe dans un communiqué.

On n'en saura pas plus sur l'origine de ce virus ni la façon dont il s'est introduit dans le système informatique de Fleury Michon. Pas plus que le montant du préjudice après un arrêt de cinq jours des usines. Fin de l'histoire ? Pas tout à fait. Cette cyberattaque confirme l'avertissement lancé en début

does the story end there? Not quite. This cyberattack is a vindication of the warning issued at the start of the year by Kaspersky: agri-food industries are the new targets for cyberattackers... and the consequences could be serious.

Professional, organised cyberattackers

Forget about script kiddies. The cyberattackers targeting the agri-food industry are on a different level. "The parties attacking this industry are no more amateurs. Given the underlying economic, health and governance issues, we're more likely dealing with a group of well-coordinated hackers, or perhaps even a mafia-style or state organisation", warns Robert Wakim, Stormshield Offers Manager.

With very specific motivations. "An attack can have consequences on multiple levels: disrupting the continuity of service, damaging consumer trust, harming the company's image, financial consequences on profitability, impeding innovation and directly hitting competitiveness", points out Tiphaine Leduc, Cybersecurity Leader at Bretagne Développement Innovation.

Where there used to be a pair of human eyes on guard, nowadays the front line is manned by a machine. If a silo's measurement sensor is sufficiently compromised, for example, it could be made to feedback incorrect information about the quantity of wheat it contains. And this raises several possible scenarios: a silo that is thought to be empty — but isn't — will prompt a reduction in production for the time the wheat order takes to arrive, but will also have an effect on deliveries, as the lorry (which is unable to unload) will then leave full and cannot continue its rounds. Conversely, a silo that is wrongly believed to be full will cause production machines to run while empty, and wear out — because, with no product to process, they may overheat and seize up the entire production line. Results: major losses in revenue, but also a loss of credibility.

To say nothing of attacks which could take control of machines to change a product's recipes or quality. "If someone changes the recipe of my fizzy drink and it tastes different, people will stop buying it. If they alter a probe to prevent it from detecting an allergen or harmful substance, I'm putting consumers at risk.

d'année par Kaspersky : les industries agroalimentaires seraient les nouvelles cibles des cyberattaquants. Et c'est plutôt inquiétant.

Des cyberattaquants professionnels et organisés

Oubliez les script kiddies ici. Les cyberattaquants qui visent l'industrie agroalimentaire sont d'un autre niveau. « Ce ne sont pas les débutants qui s'attaquent à cette industrie. Vu les enjeux économiques, sanitaires et de gouvernance qu'il y a derrière, on a plutôt affaire à un groupe de pirates informatiques bien coordonnés, voire une organisation mafieuse ou étatique », avertit Robert Wakim, Offers Manager Stormshield.

Avec des motivations bien précises. « Les conséquences d'une attaque peuvent être de plusieurs ordres : perturber la continuité de service, affaiblir la confiance des consommateurs, nuire à l'image de l'industriel, avoir des conséquences financières sur la rentabilité, freiner l'innovation et impacter directement la compétitivité », énumère Tiphaine Leduc, cheffe de mission cybersécurité chez Bretagne Développement Innovation.

Là où avant il y avait un humain qui contrôlait à l'œil, c'est désormais une machine qui veille. Si on dérègle suffisamment le capteur de mesure d'un silo, on peut, par exemple, lui faire remonter de mauvaises informations sur la quantité de blé qu'il contient. Et c'est un engrenage qui peut suivre plusieurs logiques : un silo que l'on pense vide – mais qui ne l'est pas – va provoquer une réduction de la production, le temps que la commande de blé arrive, mais également un impact sur les livraisons puisque le camion, qui ne peut pas décharger, repart donc à plein et ne peut pas poursuivre sa tournée. A contrario, à cause d'un silo que l'on pense plein, à tort, les machines de production peuvent se retrouver à tourner à vide et se dégrader – car, sans produit à transformer, elles risquent la surchauffe et un blocage de toute la chaîne de production. Résultats : pertes sèches de revenus, mais aussi perte de crédibilité.

Sans parler des attaques permettant de prendre le contrôle des automates pour modifier les recettes ou la qualité d'un produit. « Si demain quelqu'un change la recette de mon soda et qu'il n'a plus le même goût, les gens vont arrêter de l'acheter. Si on modifie une sonde et qu'elle n'est plus capable de détecter un allergène ou un produit nocif, je mets mes consommateurs en danger. Et si ma chaîne de production est réduite ou à l'arrêt, je ne pourrai plus répondre à la demande », explique Robert Wakim.

And if my production lines are slowed or halted, I may not be able to meet demand", Robert Wakim explains.

But that's not all. Cyberattackers may also benefit from market speculation on food stocks or commodities. "It isn't out of the question that some parties may have been betting on falls in Eurofins shares following a cyberattack", he continues. "A new form of insider trading."

Agri-food: a highly strategic industry

"There's nothing new about attempts to cause damage using agriculture or food. For decades now, we have seen attacks using biological or chemical contamination against cattle, plantations, fruit and vegetables", explains Florian Bonnet, Stormshield's Director of Product Management. "However, for a long time, the fairly unspectacular nature of such attacks meant that they raised no particular concern."

That is, until Allied forces uncovered thousands of scientific documents on US agriculture among the papers of a certain... Osama bin Laden. Post 9/11 America is now aware that attacks on the agri-food sector could have terrible consequences on human lives and on the country's economy. The concept of agro-terrorism, born almost a century ago, is now entering the era of cyber-terrorism.

Some foodstuffs are even considered "critical". In France, water and food management are part of 12 sectors of vital importance listed in the French Military Planning Act. And could the 249 identified Operators of Vital Importance (OVIs) potentially include a number of agriculturalists? Given that the healthcare sector is a major consumer of starch (from potatoes), anything is possible.

"The industry is critically important to our survival. But it's also a globalised, hyper-competitive industry, with very large sums of money at stake. These are the characteristics that increase its exposure than any other", emphasises Robert Wakim. Attacks on this industry

"It's possible to weaken an entire country by attacking its agri-food industry"

Robert Wakim
Offers Manager, Stormshield

Mais ce n'est pas tout. Les cyberattaquants peuvent aussi tirer profit des spéculations boursières sur les valeurs alimentaires ou les matières premières. « Il n'est pas impossible que certaines personnes aient parié contre Eurofin à la baisse suite à la cyberattaque, poursuit-il. Une nouvelle forme de délit d'initié. »

L'agroalimentaire, une industrie hautement stratégique

« La volonté de nuire par le biais de l'agriculture ou de l'alimentation n'est pas nouvelle. Depuis des dizaines d'années, des attaques via des contaminations biologiques ou chimiques ont eu lieu sur du bétail, des plantations, des fruits ou légumes, recontextualise Florian Bonnet, Directeur du Product Management Stormshield. Pourtant, pendant longtemps, parce qu'elles n'étaient pas très spectaculaires, ces attaques n'ont pas suscité d'inquiétude particulière. »

Jusqu'à ce que les forces alliées découvrent des milliers de documents scientifiques portant sur l'agriculture aux États-Unis dans la cache d'un certain… Oussama Ben Laden. L'Amérique post 11-Septembre comprend alors que des attaques visant le secteur agroalimentaire auraient des conséquences terribles sur les vies humaines et sur l'économie du pays. L'agro-terrorisme, né il y a près d'un siècle, entre maintenant dans l'ère du cyber-terrorisme.

Certaines denrées alimentaires sont même considérées comme "critiques". En France, la gestion de l'eau et l'alimentation font ainsi partie des 12 secteurs d'importance vitale listés dans la Loi de programmation militaire. Et parmi les 249 Opérateurs d'Importance Vitale (OIV) recensés, qui sait si certains agriculteurs ne seraient pas présents ? Quand on sait que le domaine de la santé est un grand consommateur d'amidon (issu de la pomme de terre), tout est possible.

« C'est une industrie fondamentale à notre survie. Mais c'est aussi une industrie mondialisée, hyper concurrentielle, avec de très grosses sommes d'argent en jeu. Ce sont des caractéristiques qui l'exposent plus qu'une autre », souligne Robert Wakim. Attaquer cette industrie, c'est aussi attaquer un pays. « On peut affaiblir un pays en réduisant ses capacités

are also attacks against a country itself. “It’s possible, for example, to weaken a country by compromising its ability to produce a particular foodstuff, he continues. This helps to weaken the health of the entire country; firstly nutritionally, but also economically — especially if the targeted agriculture is vitally important to the population or to GDP.”

This is a logical moment to stop and take a deep breath. Yes, the cybersecurity risks faced by the sector are truly staggering. But now, what can we do to protect this industry without curbing its activity?

Secure the whole chain

Like any industry, agri-food has specific issues to deal with: “remaining a competitive industry in a globalised market, in which innovation is an everyday fact of life and food safety is the absolute priority”, Tiphaine Leduc warns.

Like any industry, it is weakened by its chain-like structure. Between the producer and the consumer lie a series of overlapping players (from harvesting to processing, via distribution), with varying levels of cybersecurity. The problem is: each link in the chain is responsible for its own cybersecurity. If any link fails, the entire chain could be compromised.

“The supply chain concentrates risks: automation introduces new gateways that, if not clearly identified from the start, may become back doors”, adds Robert Wakim. Speaking in 2018 through Patrick Bigeard, its delegate for digital security in the Île de France region, at an event hosted by antivirus producer ESET, France’s ANSSI cybersecurity agency noted a drop in attacks targeting OVIs and a rise in attacks targeting... their suppliers!

Strengthening workstation protection

Systems for protecting workstations, networks and even data are essential. Indeed, OVIs are even subject

à produire telle denrée par exemple, poursuit-il. Cela contribue à affaiblir toute la santé du pays, nutritionnelle d’abord mais aussi économique, surtout si l’agriculture visée est vitale pour la population ou le PIB. »

C’est logiquement le moment de prendre une profonde inspiration par le ventre. Oui, les enjeux du secteur en matière de cybersécurité sont vertigineux. Maintenant que pouvons-nous faire pour protéger cette industrie sans freiner son activité ?

Sécuriser toute la chaîne

Comme toutes les industries, l’agroalimentaire doit composer avec des enjeux propres : « rester une industrie compétitive, dans un marché globalisé, où l’innovation fait partie du quotidien et où la sécurité alimentaire est la priorité absolue », rappelle Tiphaine Leduc.

Comme toutes les industries, elle est fragilisée par son organisation chaînée. Du producteur au consommateur, s’entrecroisent différents acteurs (de la récolte à la transformation, en passant par la distribution) aux niveaux de cybersécurité variés. Problème : chaque maillon de la chaîne est le garant de sa propre cybersécurité. Si l’un d’eux fait défaut, c’est toute la chaîne qui peut être compromise.

« La supply chain concentre les risques : l’automatisation amène de nouvelles portes d’entrée qui, si elles n’ont pas clairement été identifiées dès le début, peuvent devenir des portes dérobées », souligne encore Robert Wakim. Par la voix de son délégué à la sécurité numérique Île de France, Patrice Bigeard, lors d’un événement organisé par l’éditeur d’antivirus ESET, l’ANSSI a ainsi noté en 2018 une baisse des attaques en direction des OIV et une augmentation des attaques en direction de... leurs prestataires !

Renforcer les protections des postes

Des systèmes de protection sur les postes de travail, les réseaux ou même les données sont indispensables. Pour les OIV, il existe même une obligation de protection spéciale.

to a special protection requirement. “The first protection is to improve your digital hygiene”, insists Robert Wakim. “This primarily takes the form of updates to systems and good habits within companies. Apart from the development of a corporate cybersecurity culture, the protection of workstations — especially those which are exposed to non-internal personnel, such as providers — must be improved. And of course, there needs to be network protection around functionalities such as segmentation, filtering and order control...”

Some players have decided to take the lead. Having been targeted by “incidents” (which were halted in time), agricultural co-operative Triskalia recently embarked on a preventive cybersecurity strategy affecting all of its employees, business lines and factories. “All staff, participating farmers, suppliers and customers have received awareness training”, says Denis Saout, CISO for the co-operative, which employs 4,800 staff.

After all, we need to bear in mind the universal cybersecurity problem: an attack will always target the weakest link. “All security levels need to be increased at more or less the same speed”, insists Robert Wakim. “There’s no point in putting an armoured door on a wire fence. Cyberprotection lies in the ability to strengthen your defences from all sides.”

Although the subject may provoke anger or fear, industry needs to face up to the fact that one day it may be the target of a cyberattack. Florian Bonnet believes that “the next step is to work on your cyber-resilience; that is, the ability to recover from an attack and resume your business activity as quickly as possible. This calls for considerable efforts in background auditing of your existing equipment (condition, age, internal security level).”

And don’t forget to get your entire ecosystem on board, insisting that your providers operate the same level of cybersecurity that you do. Because in a cybersecurity protection chain, the weakest link is the one that will be attacked first. ¶

« La première protection, c’est d’augmenter son hygiène numérique, insiste Robert Wakim. Cela passe notamment par les mises à jour des outils et de bonnes habitudes en interne. Outre le développement d’une culture de la cybersécurité dans l’entreprise, les protections des postes – notamment des postes qui sont exposés à des personnes non internes comme des prestataires – doivent être renforcées. Et bien évidemment, prévoir une protection réseau autour de fonctionnalités telles que la segmentation, le filtrage ou encore le contrôle des commandes… »

Certains acteurs ont décidé de prendre les devants. Cible d’« incidents », stoppés à temps, la coopérative agricole Triskalia a récemment engagé une stratégie préventive de cybersécurité qui concerne l’ensemble de ses collaborateurs, tous ses métiers et ses usines. « Tous les collaborateurs, les agriculteurs adhérents, les fournisseurs et les clients sont sensibilisés », précise Denis Saout, RSSI du groupe coopératif composé de 4 800 collaborateurs.

Car il faut bien garder à l’esprit la problématique générale de la cybersécurité : une attaque passera toujours par le maillon le plus faible. « Il faut augmenter tous les niveaux de sécurité à peu près à la même vitesse, insiste Robert Wakim. Ça ne sert à rien de mettre une porte blindée sur une clôture de champ. La cyberprotection est dans la capacité de renforcer ses défenses de tous les côtés. »

Même si le sujet fâche ou fait peur, les industriels doivent accepter l’idée d’être un jour la cible d’une cyberattaque. Pour Florian Bonnet, « l’étape d’après, c’est de penser sa cyber-résilience, soit la capacité de se remettre d’une attaque pour reprendre son activité le plus vite possible. Cela demande un gros travail de fond d’audit des équipements qui sont en fonction (état, âge, niveau de sécurité interne). »

Et n’oubliez pas d’embarquer tout votre écosystème et d’imposer à vos prestataires d’avoir le même niveau de cybersécurité que le vôtre. Parce que dans une chaîne de protection de cybersécurité, c’est le maillon le plus faible qui sera attaqué le premier. ¶

The energy sector

Les acteurs de l'énergie

Why the connectivity of power grids increases their exposure to cyberattacks

Pourquoi la connectivité des réseaux d'électricité augmente leur exposition aux cyberattaques

By Victor Poitevin – February 11, 2019

Whilst the trend towards ever more interconnected power grids is understandable from an efficiency point of view, it also increases the risks of cyberattacks. Risks which many players in this market continue to underestimate.

From science fiction to reality

A total blackout. Fifteen years have passed since the disappearance of all forms of electrical energy and populations who have gone back to living off the land are being terrorised by militia. This scenario from the NBC series Revolution, which was broadcast from 2012 to 2014, undoubtedly belongs to the realm of science fiction. But it hints at a real threat.

"Imagine the consequences of an attack on a country's energy grids. Let's not be under any illusions, there are teams, countries, armies out there working towards exactly that objective in anticipation of future conflicts. It's not science fiction any more." Words from the mouth of Guillaume Poupard, the Director General of France's National Cybersecurity Agency (ANSSI), in a speech to the French Foreign Affairs, Defence and Armed Forces Committee on October 2018.

It's true that these threats to power grids are now increasing. Not just because the hackers are becoming more skilful but also, and most of all, because of ever greater connectivity. "Technology has caught up with us, says Robert Wakim, Offers Manager at Stormshield. From the production to the transmission and consumption of electricity, Smart Grids use considerable communication bridges to enable more effective management." This makes protecting the whole chain, from the power station to the smart meter, critical.

> **"Technology has caught up with us"**
>
> **Robert Wakim**
> **Offers Manager, Stormshield**

La tendance à rendre les réseaux d'électricité toujours plus connectés entre eux, bien que compréhensible d'un point de vue efficacité, augmente les risques de cyberattaques. Des risques qui restent encore sous-estimés par de nombreux acteurs de ce marché.

De la science-fiction à la réalité

Un black-out total. Quinze ans après la disparition de toute forme d'énergie électrique, des milices terrorisent les populations retournées vivre de l'agriculture. Le scénario de la série Revolution, diffusée de 2012 à 2014 sur NBC, appartient sans nul doute à la science-fiction. Mais il révèle un danger bien réel.

« Imaginez les conséquences d'une attaque sur les réseaux de distribution d'énergie d'un pays. Ne nous leurrons pas, tel est l'objectif d'un certain nombre d'équipes, de pays, d'armées, pour anticiper les conflits de demain. Ce n'est plus de la science-fiction. » Un discours qui sort bien de la bouche de Guillaume Poupard, Directeur général de l'ANSSI. Il tenait ce discours à la Commission française des Affaires Étrangères, de la Défense et des Forces Armées en octobre 2018.

Aujourd'hui en effet, ces risques pour les réseaux d'énergie se multiplient. Pas seulement parce que les hackers montent en compétences, mais aussi, et principalement, à cause d'une connectivité de plus en plus importante. « Nous avons été rattrapés par la technologie, affirme Robert Wakim, Offers Manager Stormshield. De la production à la consommation en passant par le transport d'électricité, les Smart Grids déploient des ponts de communication très forts pour permettre une gestion plus efficace. » Ainsi, la protection de l'ensemble de la chaine, de la centrale au compteur intelligent, devient de ce fait critique.

Cette course à la technologie est visible de deux côtés de la frontière, chez les acteurs de la filière comme chez les acteurs

This technology race is visible on both sides, amongst industry players as well as malicious parties. Take for example the malware Industroyer, which is capable of exploiting this interconnectivity in power grids. "This malware is capable of communicating through four electrical communication protocols, Robert Wakim explains. It's pretty much the only malware that specialises in the energy sector." It's possible to get hold of Industroyer on the darknet and target any facility.

Widespread attacks... since 2010

Shamoon, Stuxnet, BlackEnergy... other malware has struck the energy sector. But unlike Industroyer, this other malware needs to really know the infrastructure before attacking it, meaning it makes do with less network connectivity. Stuxnet, in particular, made people "sit up and take notice", as Gabrielle Desarnaud, a researcher at the French International Relations Institute, puts it in her study Cyberattacks and energy systems, published in January 2017. Although it was uncovered in 2010, in 2017 the researcher still rated Stuxnet as "the most advanced attack ever on a nuclear infrastructure". The malware caused damage in uranium enrichment centrifuges in the Natanz complex in Iran for years.

In Saudi Arabia, Shamoon affected 30,000 computers and blocked the oil company Saudi Aramco's trucks in 2012. "The attack started with a phishing email, recalls Robert Wakim. A secretary clicked on an email. But her infected PC continued to behave normally. This meant the attacker was able to discretely take control of the computer from the inside and go deep into the servers."

The BlackEnergy virus that was the source of the first wave of attacks on the Ukrainian power grid in December 2015, also started with a phishing campaign. This is good news and bad news: as in other industries, cyberattacks on power grids often rely on human error.

A feeling of invulnerability?

But **this human vulnerability is also due to a failure to recognize the risks at the highest corporate levels**. "Clients usually approach us out of the need to comply with regulations, rather than the fear of being the target of an attack", points out Robert Wakim. Why is there such a lack of awareness? "The problem, the expert continues, is that operators underestimate the effect of an attack. They see their facility as insignifi-

malveillants. À l'image du malware Industroyer, capable de tirer profit de cette interconnectivité dans les réseaux d'électricité. « Ce maliciel est capable de communiquer à travers quatre protocoles de communication électrique, détaille Robert Wakim. C'est quasiment le seul malware spécialisé dans l'énergie. » Sur le darknet, il est possible de se procurer Industroyer et ainsi viser n'importe quelle installation.

Des attaques répandues… depuis 2010

Shamoon, Stuxnet, BlackEnergy... d'autres malwares ont frappé le secteur de l'énergie. Mais, à la différence d'Industroyer, ces autres malwares nécessitent de bien connaître l'infrastructure avant d'attaquer et s'accommodent donc d'une connectivité moindre des réseaux. Stuxnet, en particulier, a constitué « une prise de conscience », selon les mots de Gabrielle Desarnaud, chercheuse à l'IFRI (Institut Français des Relations Internationales), dans son étude Cyberattaques et systèmes énergétiques, publiée en janvier 2017. Bien qu'il fut découvert dès 2010, la chercheuse qualifiait Stuxnet – en 2017 – « d'attaque la plus avancée à laquelle une infrastructure nucléaire ait été confronté ». Pendant des années, le malware a causé des avaries dans les centrifugeuses d'enrichissement d'uranium, dans le complexe de Natanz en Iran.

En Arabie saoudite, Shamoon a touché 30 000 ordinateurs et bloqué les camions de l'entreprise pétrolière Saudi Aramco en 2012. « L'attaque a commencé par un email de phishing, se rappelle Robert Wakim. Une secrétaire a cliqué sur un email. Mais son PC infecté se comportait normalement. L'attaquant a alors pris discrètement le contrôle de l'ordinateur d'à côté et ainsi de suite jusqu'à descendre profondément dans les serveurs. »

De même, le virus BlackEnergy, à l'origine de la première vague d'attaques contre le réseau électrique ukrainien, en décembre 2015, a été amorcé par une campagne de phishing. C'est une bonne et une mauvaise nouvelle : comme ailleurs, les cyberattaques contre les réseaux d'énergie profitent bien souvent des failles humaines.

Un sentiment d'invulnérabilité ?

*Mais **cette vulnérabilité humaine provient aussi d'un défaut de prise de conscience des risques dans les plus hauts échelons des entreprises**. « Ce sont plutôt les réglementations qui poussent nos clients à nous contacter, plus que la crainte d'être attaqué », argumente Robert Wakim. Pourquoi ce manque de prise de conscience ? « Le problème, reprend l'expert, c'est que les opérateurs sous-estiment l'effet d'une attaque, pensant que leur le poids de leur installation*

cant in relation to the grid as a whole, and so imagine it wouldn't be a worthwhile target."

Another reason for this feeling of invulnerability has to do with the fact that many facilities, such as nuclear power stations, are not connected to the internet. "But this is an illusion, claims Robert Wakim. A connection is essentially a communication, an exchange of data, even if it is only activated briefly once a year. A risk arises the moment I connect to an object that is itself connected, or use a USB stick."

To date, two of the main motivations behind cyberattacks like this have been the domino effect and competitive advantage. The first would include an attack designed to disrupt the network enough to have consequences on a national level. "And the specific characteristics of this type of attack mean it is capable of causing a domino effect, or in other words, having the maximum effect with minimum effort", explains Robert Wakim. "The best illustration of this is the impact on French oven clocks of an electricity shutdown in Kosovo". An example of the second type would be an attack by a smaller competitor on the market being targeted. Corrupting, limiting or even stopping the production or transmission of electricity will give them a not inconsiderable competitive advantage, regardless of size, on the market of the company being targeted.

An increasingly connected future

And how does the future look for these power grids? Apart from installations of one or more megawatts, the future lies in lower-power, renewable energy facilities: wind and solar farms, even solar panels on private homes… These individual producers will be linked and organised by aggregators or as Gabrielle Desarnaud calls them, "virtual power plants".

The future of energy therefore lies in a larger number of production points and interconnections. A development which will increase attack surfaces all the more, but also heighten the risks for all of the players. And whilst to date there is no legal framework in place that provides for this increase in the number of players, we still need to protect the whole. Although setting up virtual power plants is a very good thing for resilience in terms of production for the market overall, it is imperative that we understand the cyber threat to these new players ahead of time. And in so doing, prepare for a safer energy future. ¶

est négligeable dans le poids total du réseau, et par conséquent qu'il n'y aurait aucun intérêt à les attaquer ».

Une autre raison à ce sentiment d'invulnérabilité réside dans la non connexion à internet de nombreuses installations, comme les centrales nucléaires. « Mais c'est un mirage, affirme Robert Wakim. Une connexion est avant tout une communication, c'est-à-dire un échange de données, même s'il n'est activé brièvement qu'une fois dans l'année. Le risque existe dès que je me connecte à un objet lui-même connecté, ou que j'utilise une clé USB. »

À ce jour, l'effet domino et l'objectif concurrentiel sont deux des principales raisons derrière de telles cyberattaques. Dans le premier cas, il s'agit par exemple d'une attaque à visée nationale, en venant suffisamment perturber le réseau. « Et parce que celui-ci possède des propriétés particulières, il est possible de provoquer un effet domino, ou en ayant un effort minimum, on peut avoir un effet maximum, explique Robert Wakim. La meilleure démonstration de cet effet est l'impact sur les horloges des fours Français à la suite d'un arrêt de production électrique au Kosovo ». Dans le deuxième cas, il s'agit par exemple d'une attaque venant d'un concurrent plus petit sur le marché visé. Venir corrompre, limiter ou même arrêter la production ou le transport d'électricité lui donnera un avantage concurrentiel non négligeable, et ce quelle que soit la taille sur le marché de l'entreprise ciblée.

Un futur de plus en plus connecté

Et quel futur pour ces réseaux d'électricité ? Au-delà des installations d'un ou plusieurs mégawatts, le futur passera par des dispositifs de moindre puissance en énergies renouvelables : des parcs éoliens, des fermes solaires ou même quelques panneaux chez des particuliers… Ces producteurs individuels seront reliés et organisés par des agrégateurs, « des centrales électriques virtuelles », comme les appelle Gabrielle Desarnaud.

L'avenir de l'énergie réside donc dans la multiplication des points de production et des interconnexions. Une évolution qui augmentera d'autant plus les surfaces d'attaques mais aussi les risques pour l'ensemble des acteurs. Et alors qu'aucun cadre législatif ne prend à ce jour en compte cette augmentation des acteurs, il est pourtant essentiel de sécuriser l'ensemble. Si la création de ces centrales électriques virtuelles est une très bonne chose pour la résilience en terme de production pour l'ensemble du marché, il est impératif d'appréhender en amont la menace cyber sur ces nouveaux acteurs. En ainsi préparer un avenir énergétique plus sûr. ¶

#2 Other cyberattacks of the year, between expected targets and emerging trends

Les autres cyberattaques de l'année, entre cibles attendues et tendances émergences

What cybersecurity trends will 2019 bring?

Quelles tendances en cybersécurité pour 2019 ?

By Victor Poitevin – January 30, 2019

What does 2019 have in store for us? In 2018, the world of cybersecurity certainly saw its share of surprise cyberattacks, Zero-day attacks, and other methods ranging from the new to the familiar. In an attempt to forecast the trends for 2019, we've gathered information on weak signals, combined with the latest industry analyses and the opinions of our experts. We've managed to identify four trends in the form of scenarios which are likely to shape cybersecurity over the coming year. No need for a crystal ball...

Que nous réserve l'année 2019 ? En 2018 déjà, l'univers de la cybersécurité a connu son lot de cyberattaques surprises, des nouveautés, d'attaques Zero-day et d'autres méthodes connues mais revisitées. Pour tenter de prévoir 2019, nous nous sommes penchés sur certains signaux faibles, sur les dernières analyses du secteur ainsi que sur les convictions de nos experts. Nous en avons ressortis quatre tendances, sous la forme de scénarios plausibles, qui devraient façonner la cybersécurité pour cette nouvelle année. Un papier garanti sans boule de cristal.

Trend 1:
Cybercrime as a new social phenomenon

The situation in 2018...
In early 2018, two researchers discovered significant vulnerabilities at petrol stations in the United States, which had enabled criminals to deactivate petrol pumps, redirect payments and steal customers' card numbers. This technique was repeated in other cases, such as in the north of France, where an individual was caught red-handed in October 2018.

What 2019 could bring...
What if tomorrow's hackers target everyday consumer goods and widely-used services? Citizens' solutions to issues such as recent rises in costs of living and energy may well fall outside legal frameworks. Using petrol pumps for free could then become a far more frequent activity than it is today.

Meanwhile, and similarly to the Sciences Po hack in France, prestigious schools entrance exams or mid-year university exams could become sources of profit. Administrative bodies and examiners would not be engaging in corruption, but more and more candidates would be preparing to hack servers where model answers are stored. These would likely not involve sophisticated hacking operations, but students who have mastered the art of social engineering. This new generation of hackers may be able to access tests, by combing through the online lives of their victims or simply via phishing operations, before selling them to the highest bidder.

Tendance 1 :
La cybercriminalité comme nouveau fait divers de société

Ce qu'il s'est déjà passé en 2018…
En début d'année 2018, deux chercheurs ont découvert des vulnérabilités dans des stations-services aux États-Unis qui permettaient de désactiver les pompes à essence, de détourner des paiements et de voler des numéros de carte. Une technique reproduite sur des pompes à essence du nord de la France, où un individu a été pris en flagrant délit en octobre de la même année.

Ce qu'il pourrait se passer en 2019...
Et si les piratages informatiques de demain visaient des biens de consommation courante ou des services répandus ? Face aux coûts de la vie et d'accès à l'énergie qui augmentent, les réponses citoyennes pourraient bien s'affranchir d'un cadre légal. Et se servir gratuitement à la pompe à essence deviendrait une activité plus fréquente qu'aujourd'hui.

En parallèle, et dans la continuité du hack de Sciences Po, les examens d'entrée dans les Grandes Écoles ou les partiels des universités se monnayeront. Les directions et les examinateurs n'auraient pas versé subitement dans la corruption, mais de plus en plus de candidats s'organiseront pour pirater les serveurs où sont stockés les corrigés des épreuves. Il ne s'agira pas ici de techniques de hack sophistiquées mais bien de candidats, passés maîtres dans l'art de l'ingénierie sociale. Ces pirates d'un nouveau genre parviendront à accéder aux épreuves, en épluchant la vie en ligne de leurs victimes ou plus simplement via des campagnes de phishing, avant de les mettre en vente au plus offrant.

Trend 2:
A corrupted update on a reliable server

What's happened so far...
In 2018, two researchers demonstrated how to compromise corporate networks by hacking into Windows Server Update Services and replacing security patches with malware. Facebook and Google were also affected in 2018 by major security breaches, reinforcing their image of IT giants with feet of clay.

In May 2018, fake Android mobile applications for the Fortnite game were launched, carrying malware such as bitcoin mining applications.

By 2017, certain sources were already suggesting that the ransomware NotPetya had initially been spread via updates for the accounting software MeDoc, available on the server of the solution's Ukrainian publisher.

What 2019 could bring...
For optimal protection, it is recommended to always have the latest available version of a software or application. But what if this update is itself corrupt? Responding to this new cybersecurity recommendation, hackers may create a new form of malware: a sophisticated, silent ransomware, capable of bypassing sandbox mechanisms before infecting an update for a universally trusted server such as the App Store or the Google Play Store. After some deliberation they might choose an application to which 1.3 billion users have arguably become addicted: "Messenger".

After several hours, the Facebook, Apple and Google teams would realise and provide users with a patch. But the hackers might have already thought to integrate a function into their ransomware that disables the application in the event of any updates. Internet users, by in an emotional strain caused by the fear of missing out, might then find themselves paying the ransom to continue receiving their daily notifications...

Tendance 2 :
Une mise à jour corrompue sur un serveur fiable

Ce qu'il s'est déjà passé…
En 2018, deux chercheurs ont montré comment compromettre les réseaux d'entreprise en piratant Windows Server Update Services et en proposant des logiciels malveillants à la place des correctifs de sécurité. En parallèle, Facebook et Google ont également été impactés en 2018 par des failles de sécurité importantes, renforçant cette image des géants informatiques aux pieds d'argile.

En mai 2018, des fausses applications mobile Android du jeu Fortnite ont vu le jour, comprenant des malwares comme des applications de minage de bitcoin par exemple.

En 2017, déjà, certaines sources avaient avancé que le ransomware NotPetya se serait propagé initialement par le biais de mises à jour du logiciel de comptabilité, MeDoc, à disposition sur le serveur de l'éditeur ukrainien de cette solution.

Ce qu'il pourrait se passer en 2019…
Pour une protection optimale, il est recommandé de toujours avoir la dernière mise à jour disponible d'un logiciel ou d'une application. Et si cette mise à jour était en fait corrompue ? En se basant sur cette maxime de cybersécurité, des hackers vont imaginer un nouveau genre de malware : un ransomware sophistiqué et silencieux, capable de passer les épreuves de sandboxing, infectant une mise à jour sur un serveur dans lequel tout le monde a confiance, comme l'App Store ou le Google Play Store. Et ils choisiront avec soin une application à laquelle 1,3 milliard d'utilisateurs sont devenus accros : la messagerie « Messenger ».

Après quelques heures, les équipes de Facebook, Apple et Google s'en rendraient compte et proposeraient un patch correctif. Mais les pirates auraient pensé à intégrer dans leur ransomware une fonction qui désactive l'application en cas de nouvelle mise à jour. Les internautes, alors en panique à l'idée de manquer quelque chose, se retrouveraient alors à payer la rançon pour continuer à recevoir leurs notifications quotidiennes...

Trend 3:
Botnets at the service of artificial intelligence

What happened in 2018...
In 2018, hackers used botnets not only to conduct conventional denial-of-service (DoS) attacks, but also to hack into information systems. Other hackers created a system of three botnets designed to generate fake traffic on fake websites, through which they were able to earn real advertising revenue — and scam Google in the process.

Meanwhile, late 2018 was marked by numerous data breaches, with those experienced by Facebook (with a breach of more than 200 million users) and Marriott (500 million) ranking among the top ten largest data breaches of the year. Finally, 2018 also saw a surge in the prevalence of artificial intelligence, which has been drawing a great deal of attention in cyberspace. And the IBM adverts of November 2018 seem to have finally transformed it from a mere buzzword into a genuine opportunity.

What 2019 could bring...
What if the major botnets of the future aren't used to for destructive purposes, at least not immediately? To exist, artificial intelligence must be provided with a continuous and exponentially-growing amount of data. In the case of artificial intelligence used for malicious purposes, this data could be samples of behaviour of the targeted company's employees. Faced with the problem of retrieving this data, what could be better than a botnet capable of scanning large numbers of servers, email exchanges, and other digital networks of employees connected via their workstations?

Hackers will no longer necessarily seek a place in the rankings of the largest data breaches of the year, instead aiming to make the greatest use of the smallest amounts of data. Tomorrow's botnets could then be used to provide malicious artificial intelligence with data, and thus teach them to better exploit and influence these behaviours, with the cyberattacks of the future becoming increasingly automated as a result. After having copied the behaviour of certain members of the management committee, email exchanges with the CEO or a chat session with the company's financial director could convince even the most sceptical of minds. Phishing operations thus have the potential to become more efficient than ever...

Tendance 3 :
Des botnets pour alimenter une intelligence artificielle

Ce qu'il s'est déjà passé en 2018...
En 2018, des hackers ont utilisé des botnets, non seulement pour mener des attaques traditionnelles par déni de services (DDoS), mais aussi pour pirater des systèmes d'informations. D'autres ont créé un système de trois botnets destinés à générer du faux trafic sur de faux sites internet, et ainsi gagner de vrais revenus publicitaires – arnaquant Google au passage.

En parallèle, la fin d'année 2018 a été marquée par de nombreux scandales de fuites de données. Facebook (avec une fuite de données de plus de 200 millions d'utilisateurs) et Marriott (500 millions) se classant ainsi dans le top 10 des plus grosses fuites de données de l'année. Enfin, l'année 2018 a également été marquée par l'intelligence artificielle, qui suscite beaucoup de passion dans le cyber espace. Et les annonces d'IBM de novembre 2018 semblent enfin la faire passer de simple buzzword à une réelle opportunité.

Ce qu'il pourrait se passer en 2019...
Et si le nouveau botnet majeur de demain n'était pas utilisé pour détruire ? Tout du moins, pas tout de suite. Pour exister, une intelligence artificielle doit se nourrir d'un nombre exponentiel et constant de données. Dans l'optique d'une intelligence artificielle malveillante, ces données pourraient être des samples de comportements de collaborateurs d'une entreprise ciblée. Et face à la problématique de les récupérer, quoi de mieux qu'un botnet pouvant scanner en masse les serveurs, échanges d'emails et autres réseaux sociaux des collaborateurs connectés depuis leur poste ?

Plus question de s'assurer une place dans le classement des plus grosses fuites de données de l'année, mais bien d'utiliser la moindre donnée à disposition. Les botnets de demain serviront alors à alimenter des intelligences artificielles malveillantes et ainsi mieux apprendre comment exploiter et détourner ces comportements, en automatisant toujours plus les cyberattaques. Et après avoir copié le comportement de certains membres du Comité de Direction, des échanges d'emails avec le PDG ou encore une session chat avec le Directeur Financier de l'entreprise pourront convaincre même les esprits les plus alertes. Les campagnes de phishing promettent alors d'être plus efficaces que jamais...

Trend 4:
Blurring the distinction between the digital and the physical

What happened in 2018...
With the emergence of the Internet of Things, hackers are increasingly carrying out attacks on individuals. In 2018, the extent of data breaches reached new heights. Ranging from login details to medical data and biometrics, the quantity of stolen data now measures in the hundreds of millions, if not billions.

In January 2018, the physical dimension and relevance of this data shocked the general public after a sports application revealed the geolocation of American military bases in the Middle East.

What could happen in 2019...
Throughout recent data breaches such as those that marked 2018, hackers have been directly using Big Data and drawing inspiration from the marketing rules of targeted advertising to heighten the effectiveness of their attacks. 'Spearphishing' thus enables increasingly targeted and precise cyberattacks. And with connected objects, this information is no longer solely digital, as it takes on an undeniably physical nature. Information such as email addresses and credit card details will increasingly be replaced by physical data, ranging from real-time location and daily commutes to one's heart rate — information that enables individuals' lives to be systematically profiled and their privacy compromised.

Hackers may then acquire the ability to analyse data in large groups and identify activities that are dubious in nature (such as adultery or visits to pornographic sites), if not illegal. With this information, all they will need to do is blackmail their victims. Far from phishing emails that may border on parody, ransom requests (which could become physical in nature) will be substantiated and well-documented. 2019 indeed has the potential to be the year of blackmailing 2.0. ¶

Tendance 4 :
Vers la disparition de la frontière numérique-physique

Ce qu'il s'est passé en 2018…
Avec l'émergence de l'Internet des Objets, les hackers s'attaquent de plus en plus aux individus. En 2018, l'envergure des fuites de données a ainsi atteint de nouveaux records. Que ce soit de simples identifiants, des données médicales ou encore biométriques, les données dérobées se comptent désormais en centaines de millions, voire en milliards.

En janvier 2018, la dimension physique de ces données avait frappé le grand public après qu'une application de sport ait exposé la géolocalisation des bases militaires américaines au Moyen-Orient.

Ce qu'il se pourrait se passer en 2019…
Avec les fuites de données massives de l'année 2018, les pirates informatiques se servent directement dans le Big Data et s'inspirent des règles marketing du ciblage publicitaire pour affiner leurs attaques. Le spearphishing permet ainsi des cyberattaques toujours plus ciblées et précises. Et avec les objets connectés, les informations ne sont plus que numériques ; elles sont également (re)devenues physiques. Il n'est plus question d'adresse email ou de code de carte bleue, mais bien de données physiques comme la localisation en temps réel, des trajets journaliers ou la fréquence cardiaque… Des informations qui permettraient de profiler la vie des individus et de sérieusement mettre à mal leur vie privée.

La nouvelle compétence des hackers serait alors leur capacité à analyser ces faisceaux d'indices et identifier des activités pour le moins douteuses (comme des adultères ou des visites de sites pornographiques), voire illégales. Avec ces informations, il ne leur restera plus qu'à faire chanter leurs victimes. Loin des emails de phishing proches de la caricature, les demandes de rançons (pouvant être physiques cette fois-ci) seront étayées et documentées. Et si l'année 2019 était celle des maîtres-chanteurs 2.0 ? ¶

The supply chain

La chaîne logistique

When the supply chain is subjected to cyberattacks

By Victor Poitevin – November 4, 2019

Now that large companies have greater awareness of security, hackers are increasingly targeting contractors to achieve their goals. This "weakest link" strategy requires greater collaboration throughout the supply chain. We explain.

The supply chain: a priority target for hackers

The largest companies are tending to reach a certain digital maturity regarding cyber threats, between greater protections and generally greater awareness. They seem to be completely prepared, but this completely hides these giants' Achilles tendon: their suppliers and service providers.

Supplier components, their assembly into production lines, storing finished products or moving them into distribution networks are all vulnerable stages that

La chaîne logistique à l'épreuve des cyberattaques

Confrontés à une prise de conscience de la sécurité dans les grandes entreprises, les pirates informatiques ciblent de plus en plus les sous-traitants pour atteindre leurs objectifs. Une stratégie du « maillon faible » qui nécessite une collaboration accrue sur l'ensemble de la chaîne logistique. Décryptage.

La chaîne logistique, cible privilégiée des hackers

Face à la menace cyber, les plus grandes entreprises tendent à atteindre une certaine maturité numérique – entre protections accrues et sensibilisation des collaborateurs généralisée. Une préparation qui semble donc complète, mais qui occulte totalement les pieds d'argile de ces colosses : les fournisseurs et prestataires de services.

Les composants des fournisseurs, l'assemblage de ceux-ci dans les lignes de production, le stockage des produits finis ou encore le passage dans les réseaux de distribution sont pourtant autant d'endroits vulnérables et de moments propices à une contamination malveillante. Qui va se méfier

are opportunities for malicious contamination. Who would suspect a parcel delivered by their usual delivery person? Similarly, who would suspect software provided by their traditional service provider? Instead of attacking large companies head on, hackers are now targeting this other, more vulnerable stakeholder who can open the door to large companies' computer network and devices. As they are generally smaller in size, the issue of cybersecurity and digital hygiene is unfortunately not a priority for them, making them a perfect target for cyberattacks.

In 2013, American distributor Target was attacked via a sub-contractor in charge of...air conditioning. In the end, several million pieces of confidential data were stolen. In 2018, 50,000 students, parents and teachers in an American school also saw their personal data leaked because of a contractor.

Cyber-risks from subcontracting are nearer than we think... "What about companies where computers come back from repair and are directly handed back to employees without checking if malware was installed during repair or transport?", says Florian Bonnet, Stormshield's Director of Product Management.

And there can be many objectives at each link in the logistics chain: gather secrets in manufacturing and intellectual property, steal client and partner data, or simply seize up the manufacturing chain. Late fees, loss of turnover, and a tarnished reputation can be expected. A 2018 study by the Vanson Bourne Institute showed that the pharmaceutical, biotechnological, hotel, media, entertainment and IT service sectors are the most targeted. Software publishers may also be concerned, as their applications seen as reliable can reach many companies unhindered, as evidenced by the Ukrainian financial software MEDoc, the starting point of NotPetya in 2017.

The temptation to underestimate risk

For hackers, even the smallest businesses – whose activity may not seem like a major prize at first glance – can be a choice target. Nevertheless, "most small businesses do not feel like this concerns them", notes Stéphane Prévost, Product Marketing Manager at Stormshield. "Since they don't have a war chest or sensitive information in their networks, they don't always put in place the appropriate measures. It's like with insurance: pointless until the day we need them".

d'un colis délivré par son livreur habituel ? Et de la même manière, qui va se méfier d'un logiciel fourni par son prestataire de service classique ? Plutôt que de s'attaquer frontalement à des grandes entreprises, les hackers s'en prennent désormais à cette autre partie-prenante, plus vulnérable et qui peut leur ouvrir en grand les portes du réseau informatique et des terminaux des grandes entreprises. Généralement de taille plus modeste, la question de la cybersécurité ou de l'hygiène numérique ne fait malheureusement pas partie de leurs priorités et les transforme donc en cibles de choix pour des cyberattaques.

En 2013 déjà, la chaîne de distribution américaine Target a été attaquée à travers un sous-traitant chargé de… la climatisation. Au final, plusieurs millions de données confidentielles dérobées. En 2018, 50 000 élèves, parents et enseignants d'un groupe scolaire – américain également – ont eux-aussi vu leurs données personnelles fuiter à cause d'un prestataire.

Les cyber-risques liés à la sous-traitance sont donc bien plus proches de nous qu'il n'y paraît… « Que dire d'entreprises où des ordinateurs qui reviennent de réparation, sont directement distribués aux collaborateurs sans vérifier si un malware n'a pas été introduit au cours de la réparation ou lors du transport ? », glisse Florian Bonnet, Directeur du Product Management Stormshield.

Et les objectifs peuvent s'avérer multiples pour tous les maillons de la chaîne logistique : récupérer des secrets de fabrication et de propriété intellectuelle, subtiliser des données clients et partenaires ou simplement gripper la chaîne de fabrication. À la clé, pénalités de retard, perte de chiffre d'affaires, atteinte à la réputation sont à prévoir. Une étude de l'Institut Vanson Bourne de 2018 avançait que les secteurs pharmaceutiques, biotechnologiques, hôteliers, des médias, du divertissement et des services informatiques seraient les plus ciblés. Les éditeurs de logiciels peuvent aussi être concernés ici, puisque leurs applications – réputées fiables – permettent d'atteindre de nombreuses entreprises sans encombre. Comme en témoigne le cas du logiciel financier ukrainien MEDoc, point de départ de NotPetya en 2017.

La tentation de sous-estimer le risque

Pour les hackers, même des TPE – dont l'activité ne représente pas à première vue d'enjeu majeur – peuvent constituer une cible de choix. Pour autant, « la plupart de ces petites structures ne se sentent pas assez concernées », constate Stéphane Prévost, Product Marketing Manager Stormshield. « Puisqu'elles ne détiennent pas de trésor de guerre ou d'in-

This attitude leads to a sort of taboo when an incident occurs. In this way, ANSSI's message for 2019 – "All connected, all involved, all responsible" – is meaningful. "Now that systems are all connected to the Internet and, therefore, with each other, we must involve everyone in thinking about cybersecurity. Teams must communicate with each other to ensure global security", says Alain Dupont, Stormshield's General Manager and Customer Service Director.

Only one solution: work together

Current protection techniques, such as detecting incidents through abnormal behaviour or simulations of attack, no longer seem to be sufficient for companies' new scope. The reach of these tools is limited if they are only considered for the scope of the organisation itself without a connection to its ecosystem. "A chain's level of security is that of its weakest link", Florian Bonnet reminds us. Thus, for each company, the challenge is to raise awareness among its contractors as it does for its teams.

With the possibility of a better, more secure sharing of information between subcontractors and purchasers, the latter are in a position to play a decisive role. "For example, during calls for bids, by making sure that subcontractors fulfil certain cybersecurity criteria", says Alain Dupont.

This change is vital since, in the current model of massive outsourcing through alliances, the only companies that will survive are those able to guarantee the integrity of all their processes and data, including those that they do not control directly.

This ambition requires us to rigorously select our partners, to continue automating all flows, and above all to instil a spirit of cooperation from one end of the chain to the other. And what about you: are you ready? ¶

"A chain's level of security is that of its weakest link"

Florian Bonnet, Product Management Director, Stormshield

formations sensibles directement dans leurs réseaux, elles ne mettent pas toujours en place les mécanismes adaptés. C'est la même logique qu'avec les assurances : inutile jusqu'au jour où on en a besoin ».

Cette attitude entraîne une forme d'omerta lorsqu'un incident survient. À ce titre, le message de l'ANSSI pour l'année 2019 – « tous connectés, tous impliqués, tous responsables » – est donc éloquent. « Maintenant que les systèmes deviennent tous reliés avec Internet et donc connectés, il faut intégrer tout le monde dans la réflexion de cybersécurité. Les équipes doivent communiquer entre elles, pour arriver à une sécurité globale », traduit Alain Dupont, Directeur du Service Clientèle & Directeur Général Délégué Stormshield.

Une seule solution : jouer collectif

Les techniques actuelles de protection, telles que la détection d'incidents basée sur les comportements anormaux ou encore les simulations d'attaque, ne semblent aujourd'hui pas suffisantes par rapport au nouveau périmètre des entreprises. La portée de ces outils reste en effet limitée s'ils sont envisagés à la seule échelle de la seule organisation, sans lien avec son écosystème. « Le niveau de sécurité d'une chaîne est celui du maillon le plus faible », rappelle en effet Florian Bonnet. Ainsi, pour chaque entreprise, tout l'enjeu consiste à sensibiliser ses sous-traitants au même titre que ses équipes.

Dans la perspective d'un meilleur partage sécurisé de l'information entre sous-traitants et donneurs d'ordre, ces derniers sont en capacité de jouer un rôle déterminant. « Par exemple lors des appels d'offres, en s'assurant que le sous-traitant remplit certains critères de cybersécurité », estime Alain Dupont.

Une évolution indispensable puisque, dans le modèle actuel d'externalisation massive sous forme d'alliances, ne survivront que les entreprises capables de garantir l'intégrité de tous leurs processus et données, y compris ceux qu'elles ne contrôlent pas directement.

Cette ambition exige de sélectionner rigoureusement ses partenaires, d'automatiser encore et toujours les flux, mais surtout d'insuffler un esprit de coopération d'un bout à l'autre de la chaîne. Et vous, êtes-vous prêt ? ¶

The public sector

Les administrations publiques

RobbinHood ransomware: Why Baltimore ends up in the spot lights?

Ransomware RobbinHood : pourquoi Baltimore se retrouve sous les projecteurs ?

By Matthieu Bonenfant – June 12, 2019

Since the beginning of May 2019, computer networks in the city of Baltimore (United States) have been paralyzed. This was due to a ransomware attack that locked down the government's 10,000 computers on site and is being investigated as a major cyberattack.

After Atlanta and San Antonio in 2018, the cyberattack on Baltimore confirms that cities are now targets like any other industry, as are businesses and public administrations. But then, why are we talking so much about Baltimore? How is it different from the others?

Depuis début mai 2019, les réseaux informatiques de la ville de Baltimore (États-Unis) sont paralysés. La cause : un ransomware qui a verrouillé les 10 000 ordinateurs du gouvernement sur place.

Après Atlanta et San Antonio en 2018, la cyberattaque de Baltimore confirme que les villes sont désormais des cibles comme les autres, au même titre que les entreprises et les administrations publiques. Mais alors, pourquoi parle-t-on autant de Baltimore ? En quoi est-ce différent des autres cyberattaques ?

A high ransom amount

Firstly, because of the ransom amount; about $100,000. An important symbolic step, far from the $300 requested at the beginning of the WannaCry ransomware in 2017. Amounts that have therefore increased dramatically. The reasons? A higher level of organization and sophistication to these attacks than general ransomware campaigns and a trend towards cyberattacks on large organizations that cannot afford the luxury of business interruption. Sensitive industrial sectors, public services or hospitals are then on the front line. The latest industry figures estimate the average amount of ransoms paid per incident in the first quarter of this year at $13,000, compared to $7,000 in the last quarter of 2018.

A high cyberattack cost

Secondly, this RobbinHood ransomware in Baltimore is also making headlines following initial feedback on the total cost of the cyberattack. Latest estimates are up to $18 million and could increase even more. This is above the average of the figures from the latest international study by Accenture Security and the Ponemon Institute, which estimated the average cost of a cyberattack at $13 million. This figure is up 27% compared to last year and 72% compared to five years ago. It should be noted that this is indeed an average; around the world, cases of cyberattacks affecting large groups have been in the news since 2017 — with amounts that make heads turn. Maersk, Mondelez and Saint-Gobain, affected by NotPetya, reported losses of $300 million, $100 million and €80 million respectively. Closer to home, at the beginning of 2019, Norsk Hydro and Altran were also losing $40 million and €20 million due to the LockerGoga ransomware infection.

A doubt concerning the ransom payment

Could these costs then justify the decision of some companies to pay the ransom demanded by cybercriminals? This is the third point that draws attention to Baltimore's current events — since the city's mayor,

$13,000

the average amount of ransoms paid per incident in the first quarter of this year

Un montant de rançon élevé

Premièrement, à cause du montant de la rançon ; environ 100 000 $. Une étape symbolique importante, loin des 300 $ demandés au début de WannaCry en 2017. Les raisons de cette augmentation spectaculaire ? Une plus grande préparation et surtout sophistication des cyberattaques ainsi qu'une tendance contre les grandes organisations – qui ne peuvent se permettre le luxe d'interrompre leurs activités. Les secteurs industriels sensibles, les services publics ou encore les hôpitaux sont alors en première ligne. Selon les derniers chiffres du secteur, le montant moyen des rançons versées par incident au premier trimestre de cette année est de 13 000 $, en forte hausse par rapport aux 7 000 $ du dernier trimestre de 2018.

Une cyberattaque qui coûte cher

Deuxièmement, ce ransomware RobbinHood à Baltimore fait également la Une des journaux suite aux premières estimations sur le coût total de la cyberattaque. Qui irait jusqu'à 18 millions de dollars et pourrait augmenter encore davantage. Un chiffre bien supérieur à la moyenne des ceux issus de la dernière étude internationale réalisée par Accenture Security et le Ponemon Institute, qui ont estimé le coût moyen d'une cyberattaque à 13 M$. Un chiffre lui-même en hausse de 27% par rapport à l'année dernière et de 72% par rapport à il y a cinq ans. Attention, il convient de noter qu'il s'agit en effet d'une moyenne ; partout dans le monde, des cas de cyberattaques touchant de grands groupes font la Une des journaux depuis 2017 – avec des montants qui font tourner les têtes. Maersk, Mondelez et Saint-Gobain, affectés par NotPetya, ont enregistré des pertes respectives de 300 M$, 100 M$ et 80 M€. Plus près de chez nous, début 2019, Norsk Hydro et Altran perdaient également 40 M$ et 20 M€ suite à l'infection par le ransomware LockerGoga.

Un doute sur le paiement de la rançon

Ces coûts exorbitants pourraient-ils alors justifier la décision de certaines entreprises de payer la rançon exigée par les cybercriminels ? C'est le troisième point qui attire l'attention sur l'actualité de Baltimore, puisque le maire de la ville, Bernard C. Young, semble hésiter sur la question. « Pour l'instant, je dis non », déclarait-il fin mai. « Mais pour faire avancer

Bernard C. Young, seems to be hesitant on the issue. "Right now, I say no," he said at the end of May. "But in order to move the city forward? I might think about it. But I have not made a decision yet." And yet, giving in to ransom demands does not seem to be the best idea – for several reasons. First, as authorities such as the FBI in the United States, or ANSSI in France, specify paying a ransom encourages malicious acts. By contributing to the financing of cybercriminals' activities, paying companies also contribute to the development of ransomwares. In addition, paying a first time may give you a "good customer" label in these cybercriminal minds or "cash cow", it depends. Finally, those who pay the ransoms do not systematically recover their data: in 20% of cases, they are destroyed as soon as they are encrypted. After-sales service is not a priority for cybercriminals.

A successful spread

Finally, it is the (successful) spread of this ransomware that makes people talk about it – since the New York Times mentions the number of 10,000 computers affected. As well as the long period of blocking the information system. So how can we effectively protect ourselves against these massive ransomwares? Basic security and digital hygiene measures exist. Starting with regular installation of updates, use of endpoint protection software, avoid opening attachments from suspicious emails or unknown senders, and regular backup to an external storage system or in the cloud. By exploiting remote vulnerabilities, some ransomwares can spread themselves automatically within internal networks and infect thousands of computer in short period of time. To limit this kind of propagation, it is necessary to implement next-generation firewalling systems, offering granular filtering of connections and threat detection capabilities, at the edge and the core of the infrastructure.

To defend against the increasing sophistication of cybercriminals, it is time for companies – privates and public ones – to equip themselves accordingly. ¶

la situation ? Je vais peut-être y réfléchir. Je n'ai pas encore pris de décision. » Pourtant, céder aux demandes de rançon ne semble pas être la meilleure idée – et ce, pour plusieurs raisons. Tout d'abord, les autorités comme le FBI aux États-Unis ou l'ANSSI en France le précisent bien : le paiement d'une rançon encourage les actes malveillants. En contribuant au financement des activités des cybercriminels, les entreprises payantes contribuent également au développement d'autres ransomwares. De plus, payer une première fois peut vous coller une étiquette de « bon client » dans l'esprit des cybercriminels. Voire de potentielle « vache à lait », c'est selon. Enfin, ceux qui paient les rançons ne récupèrent pas systématiquement leurs données : dans 20% des cas, celles-ci sont en fait détruites dès qu'elles sont chiffrées. Le service après-vente n'est décidément pas une priorité pour les cybercriminels.

Une propagation réussie

Enfin, c'est la diffusion (réussie) de ce ransomware qui fait parler de lui – puisque le New York Times mentionne le nombre de 10 000 ordinateurs concernés. Ainsi que la longue période de blocage du système d'information. Alors, comment se protéger efficacement contre ces demandes de ransomwares qui se multiplient ? Il existe des mesures de sécurité et d'hygiène numérique de base. Commencez par l'installation régulière de mises à jour et l'utilisation d'un logiciel de protection Endpoint, évitez d'ouvrir des pièces-jointes à partir d'emails suspects ou d'expéditeurs inconnus et sauvegardez régulièrement vos données sur un système de stockage externe ou dans le cloud. En parallèle, en exploitant les vulnérabilités à distance, certains logiciels de ransomwares peuvent se répandre automatiquement dans les réseaux internes et infecter des milliers d'ordinateurs en peu de temps. Pour limiter ce type de propagation, il est nécessaire de mettre en place des systèmes de pare-feu de nouvelle génération, offrant un filtrage granulaire des connexions et des capacités de détection des menaces, en périphérie et au cœur de l'infrastructure.

Pour se défendre contre la sophistication croissante des cybercriminels, il est temps pour les entreprises – comme pour les administrations publiques – de s'équiper en conséquence. ¶

Customer case

Vichy Community: a solution for remote site management

Cas client

Communauté d'agglomération de Vichy : une solution pour administrer des sites distants

Public administrations: How should you choose your cybersecurity solution?

Administrations publiques : comment choisir votre solution de cybersécurité ?

By Raphaël Granger – July 8, 2019

The digital transformation has unleashed a storm of cyberattacks that are undermining public administrations and their information systems. Faced with the multitude of firewall options on the market, how can you select the most appropriate cybersecurity solution? A three-part response.

What kinds of regulatory obligations are imposed on the public sector?

The public sector is subject to a variety of different cybersecurity regulations. As such, each administration must first determine which regulations apply to it. For example, France's regulatory framework consists of three pillars with varying degrees of strictness. The Military Planning Law (MPL) requires that public administrations under its jurisdiction use ANSSI-qualified solutions, while the General Security Baseline (GSB) merely recommends it. For its part, the Security Policy on Government Information Systems (SPGIS) describes it as good practice, alongside the use of certified solutions. This national framework is complemented at the European level by the GDPR and the Cybersecurity Act.

La transformation numérique et son lot de cyberattaques fragilisent les administrations publiques et leurs systèmes d'informations. Et face à la multiplicité des solutions de pare-feu qui existent, comment sélectionner la solution de cybersécurité la plus adéquate ? Réponse en trois actes.

Quelles sont les obligations à respecter en matière de cybersécurité dans le secteur public ?

La cybersécurité appliquée au secteur public se traduit par de nombreux textes réglementaires. Chaque administration doit donc en premier lieu déterminer quelles règlementations la concernent. Par exemple, le cadre règlementaire français repose sur trois piliers plus ou moins contraignants. La loi de programmation militaire (LPM) impose aux administrations qui y sont soumises le recours à une solution qualifiée par l'ANSSI, tandis que le référentiel général de sécurité (RGS) le recommande seulement. De son côté, la politique de sécurité des systèmes d'information de l'État (PSSIE) le liste parmi les bonnes pratiques avec l'utilisation de solutions certifiées. Ce cadre national est complété au niveau européen par le RGPD et le Cybersecurity Act.

At present, Stormshield Network Security (SNS) is the only firewall solution qualified as "Standard" by the ANSSI. Why is this important?

It is the result of a complex process that goes beyond certification and attests to the reliability of our product. It's also a sign of the ANSSI's trust in us: qualification is bestowed after six to eight months of testing by the agency, which also examines the solution's source code.

What other criteria should be taken into account when selecting a cybersecurity solution for a public administration?

It is very important to:

- Focus on the essential features needed to meet your firewall requirements and comply with your regulatory obligations. Instead of choosing a product based on a myriad of proposed features that won't really be used, it's more important to select a product that will perfectly meet the needs of your public administration.

- Make sure the solution is a good fit for the needs and architecture of your information system (IS).

- Choose a reliable vendor that specialises in protecting the information systems of public administrations. This is the case for Stormshield, which does a lot its business in the public sector (local governments, core ministries, etc.).

- Choose a local partner. Through its distribution network, Stormshield has cultivated a regional presence and a European footprint—two complementary assets that will ensure it will always be by your side. ¶

À ce jour, Stormshield Network Security est la seule solution de type firewall qualifiée au niveau Standard par l'ANSSI. En quoi est-ce important ?

C'est le résultat d'un processus complexe, qui va au-delà de la certification et qui atteste de la fiabilité de notre produit. Et de la confiance de l'ANSSI : la qualification intervient en effet après six à huit mois de tests par l'autorité, qui contrôle également le code source de la solution.

Quels autres critères sont à prendre en compte dans la sélection d'une solution de cybersécurité pour une administration publique ?

Il est très important de :

- *Se concentrer sur les fonctionnalités essentielles pour répondre aux besoins firewall et se conformer aux exigences réglementaires. Plutôt que choisir un produit sur la base d'une myriade de fonctionnalités proposées, qui ne seront pas réellement utilisées, il est en effet important d'en sélectionner un qui saura répondre parfaitement aux problématiques de votre administration publique.*

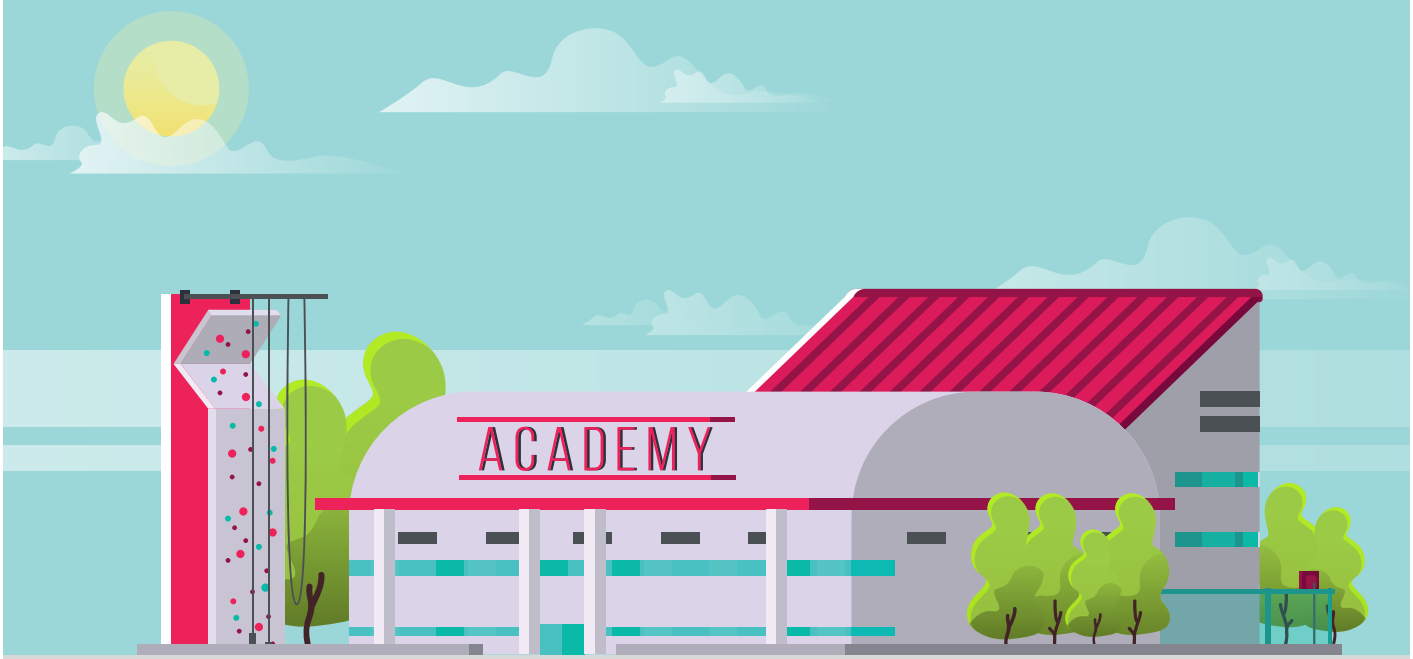
- *Vérifier l'adéquation de la solution avec les besoins et l'architecture du système d'information (SI).*

- *S'appuyer sur un fournisseur fiable, spécialiste de la protection des SI des administrations. C'est le cas de Stormshield qui réalise une part importante de son chiffre d'affaires dans le secteur public (collectivités locales, territoriales, ministères régaliens, etc.).*

- *S'appuyer sur un partenaire local. Pour cela, notre présence régionale et notre ancrage européen, aux côtés de notre réseau de distribution, sont deux atouts complémentaires dans une optique de proximité. ¶*

The world of education

Le monde de l'éducation



Cyberattacks: Why the education sector is not immune

Cyberattaques : Pourquoi le monde de l'enseignement n'est pas à l'abri

By Florian Bonnet – October 15, 2019

From schools to universities or research labs, the whole education sector is a huge pool of sensitive data. It therefore needs to be protected. However, the education sector is struggling to get to grips with the subject of cybersecurity. Background.

In addition to the classic ransom attacks as seen at the University of Corsica in May 2019, the theft of sensitive data is a key motivation behind cyberattacks against educational establishments. This summer, in France, the Epitech IT School noted that personal data had been posted to the web belonging to several students and partners. Last year, in Florida, an attack on a

Des écoles aux universités en passant par les laboratoires de recherche, c'est tout le monde de l'enseignement qui entretient un réservoir de données sensibles gigantesque. Et donc à protéger. Pourtant, le secteur de l'enseignement peine à prendre le sujet de la cybersécurité à bras le corps. Mise au point.

Au-delà des cas classiques de demande de rançon comme en a connu l'université de Corse en mai 2019, le vol de données sensibles est une motivation majeure dans les cyberattaques d'établissements scolaires. Cet été, l'école d'informatique Epitech n'a pu que constater la fuite sur le web de données

schools group affected more than 50,000 people: pupils and alumni, parents, teachers and non-teaching staff, whose names, dates of birth, contact details, login details, academic information and even health data had fallen into the wrong hands…

Educational establishments are also becoming a theatre for economic and military conflicts through their research laboratories. Using phishing to obtain innovative technology or a mass spoofing campaign to connect to online libraries, hackers will try anything to access personal data.

Prime targets, but insufficiently protected

Guillaume Rénier, IT and Information Systems director at Cergy-Pontoise university, explains that "it's our job to protect the privacy of users, especially students, who leave a considerable trail behind them online". But also that of other researchers working on strategic and confidential matters and who often need to communicate using collaborative tools. However, **it can be difficult to get these experts interested in a subject as abstract as cybersecurity**. For this reason, the university has prioritised the deployment of a Wi-Fi network rather than using the external 4G network and is working on securing the use of existing solutions (like Dropbox for example). Working with Stormshield, the university is currently examining a multiple encryption solution for this resource

"We are starting to see greater awareness within educational establishments"

Xavier Prost, Training Manager, Stormshield

There is also an internal risk which is just as dangerous as any external threat. Some students may be tempted to try and gain access to exam papers or to falsify grades. A security audit involving 400 British schools revealed that 20% of them had been hacked by their own pupils! Robert Wakim, Offers Manager at Stormshield, summed up the problem in the following terms: "We find ourselves faced with millions of people who are either potential hackers or people who are unaware of the challenges of cybersecurity. Both groups are equally dangerous".

personnelles de plusieurs étudiants et partenaires. En Floride l'année dernière, une attaque sur un groupe scolaire a touché plus de 50 000 personnes : élèves et anciens élèves, parents, professeurs et personnel non-enseignant dont le nom, la date de naissance, les coordonnées, les informations de connexion ainsi que des données académiques et même de santé se sont retrouvées entre de mauvaises mains…

De plus en plus, les établissements deviennent également le théâtre de guerres commerciales et militaires à travers leurs laboratoires de recherche. Phishing pour s'approprier des technologies innovantes ou campagne massive de spoofing afin de se connecter aux bibliothèques en ligne, tout est bon pour avoir accès à des données sensibles.

Des cibles de choix, mais insuffisamment protégées

*Pour Guillaume Rénier, Directeur Informatique et des Systèmes d'Information de l'Université de Cergy-Pontoise, « notre travail est de protéger la vie privée des usagers, surtout les étudiants, qui laissent de nombreuses traces en ligne ». Mais aussi des chercheurs qui travaillent sur des sujets stratégiques et confidentiels, avec un fort besoin de communiquer via des outils collaboratifs. Mais **ces experts restent difficiles à mobiliser sur un sujet aussi abstrait que la cybersécurité**. Pour cette raison, l'université a privilégié le déploiement d'un réseau Wi-Fi plutôt que l'utilisation du réseau 4G extérieur et travaille à sécuriser l'utilisation des outils existants (comme Dropbox par exemple). L'établissement étudie actuellement, avec Stormshield, une solution de surchiffrement pour cet outil.*

Il existe aussi un risque interne, tout aussi dangereux qu'une menace extérieure. En effet, des étudiants peuvent tenter d'accéder à des épreuves ou de falsifier des notes. Ainsi, un audit de sécurité auprès de 400 écoles britanniques révèle que 20% d'entre elles ont été piratées par leurs propres élèves ! Robert Wakim, Offers Manager chez Stormshield, résume le casse-tête : « nous sommes face à des millions de personnes qui sont soit des pirates potentiels, soit des personnes peu conscientes des enjeux de cybersécurité. Deux populations tout aussi dangereuses l'une que l'autre ».

How can we improve cybersecurity in our schools?

At a time when connected resources are being increasingly used in classrooms, the education sector needs to face up to new challenges when it comes to securing networks, workstations and sensitive data. With educational establishments increasingly being grouped together under the same IT department, managing these interconnections has become vital.

The initial objective is to ensure that workstations are not infected — for example through the use of USB flash drives brought in by students. However, if one of them did get contaminated, effective network segmentation then plays a key role in avoiding any possible mass contagion. Finally, effective management also means installing virtual vaults, making it possible to encrypt data to limit access to it to only teaching staff or authorised students.

The need to raise awareness

In the education sector just like elsewhere, cybersecurity is largely a people thing. However, some teachers see the IT network is merely a secondary resource: "If it's not working, that doesn't fundamentally prevent them from doing their jobs so they don't pay the same attention to it as a company would", explains Robert Wakim.

"We're starting to see greater awareness within educational establishments", observes Xavier Prost, head of training and documentation services at Stormshield. Stormshield supports teachers and students through this awareness-building process with SecNum*edu* recognised and quality-labelled training courses provided by the ANSSI. "However, it is often limited to specialised post-baccalaureate courses". With this in mind, how is it possible to reach a larger number of education teams and students? What if cybersecurity was taught at school? ¶

Comment améliorer la cybersécurité dans nos écoles ?

Alors que les outils connectés se multiplient dans les classes, le monde de l'enseignement doit relever de nouveaux défis autour de la sécurisation des réseaux, des postes de travail et des données sensibles. Avec le contexte actuel de regroupements croissants d'établissements scolaires sous la même direction informatique, la maîtrise de ces interconnexions est un point-clé.

Dans un premier temps, l'objectif est notamment de s'assurer que les terminaux de travail ne soient pas infectés – par exemple via des clés USB d'étudiants. Mais si l'un d'entre eux venait à se faire contaminer, la segmentation des réseaux joue alors un rôle fondamental pour éviter d'éventuelles contagions massives. Enfin, la maîtrise passe également par l'installation de coffres forts virtuels, permettant de chiffrer les données pour en restreindre l'accès uniquement aux chercheurs, professeurs ou autres étudiants autorisés.

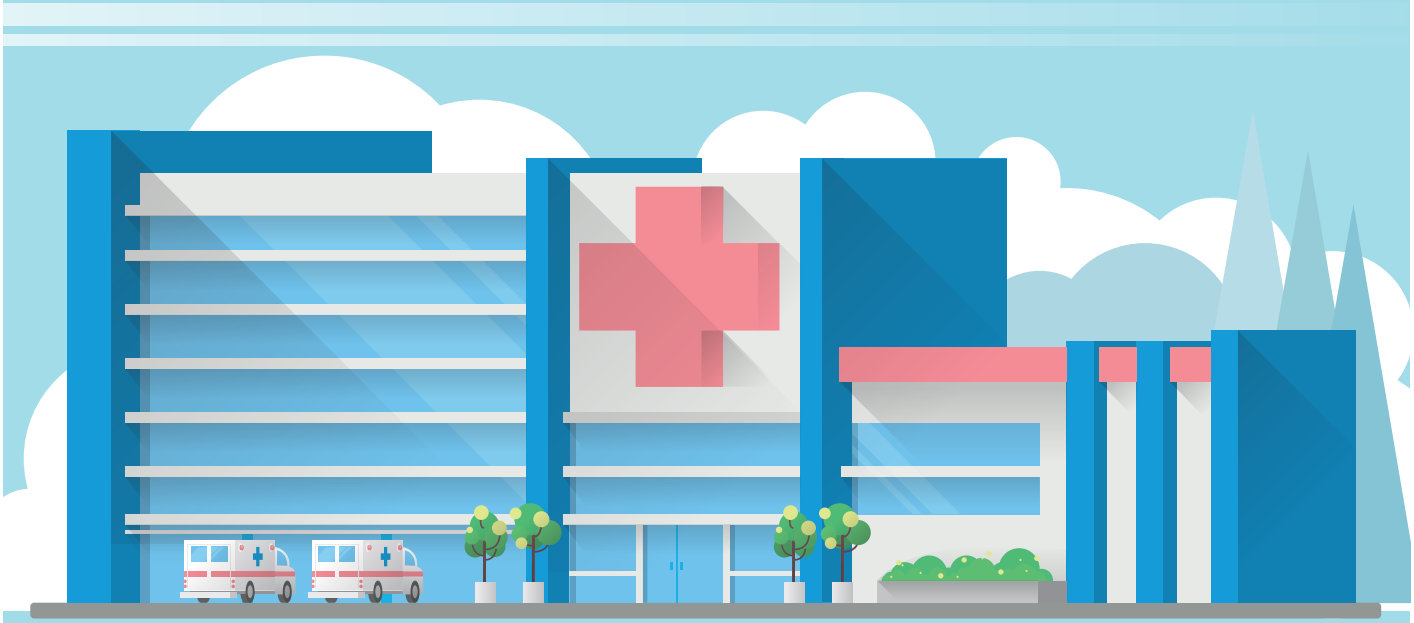
Une question de sensibilisation

Dans l'éducation comme ailleurs, la cybersécurité passe largement par l'humain. Or, pour certains enseignants, le réseau informatique n'est qu'un outil secondaire : « s'il ne fonctionne pas, cela ne les empêche pas fondamentalement de travailler ; alors peut-être ne lui accordent-ils pas la même attention qu'en entreprise », analyse Robert Wakim.

« La sensibilisation commence à se développer au sein des établissements », observe Xavier Prost, en charge des services formation et documentation chez Stormshield. Avec des formations labellisées et reconnues SecNumedu - Formation continue par l'ANSSI, Stormshield accompagne professeurs et étudiants dans cette approche. « Mais elle reste trop souvent cantonnée dans des cursus spécialisés post-Bac. » Dès lors, comment toucher un plus grand nombre d'équipes pédagogiques et d'étudiants ? Et si la cybersécurité devait s'enseigner dès l'école ? ¶

Healthcare institutions

Les établissements de santé



Top 5 cyberattacks against the health care industry

By Marco Genovese
— August 28, 2019

The healthcare industry, and hospitals in particular, are the number one target of ransomware attacks. By 2020, these attacks are expected to quadruple, according to CSO Online. We review the five most noteworthy examples of cyberattacks against the healthcare industry. These incidents are a reminder of the importance of educating employees – including healthcare professionals – on good cybersecurity practices.

5 BLUE CROSS

PAYS THE PRICE FOR HUMAN ERROR

While these malicious attacks are impressive, incidents can sometimes be the result of negligence or a lack of information. Such was the case in April 2018, when an employee of Independence Blue Cross, an American health insurer, accidentally posted a file containing the personal and medical info of nearly 17,000 patients online. It took two months for the company to detect this human error

FAIT LES FRAIS D'UNE ERREUR HUMAINE

Si ces attaques malveillantes sont impressionnantes, les incidents sont parfois les résultats de négligences ou d'un manque d'informations. Ainsi en avril 2018, un employé de l'organisme américain d'assurance maladie Independence Blue Cross met en ligne par erreur un fichier contenant les données personnelles et médicales de près de 17 000 patients. Une erreur humaine que la société va mettre deux mois à détecter.

4 A PHISHING ATTACK

AGAINST A MONTPELLIER MEDICAL CENTRE

Phishing is the most widespread cyberthreat, according to the Corporate Cybersecurity Barometer published by the CESIN. An employee of the Montpellier university medical centre found this out the hard way in March 2019, when he opened an email containing a virus that went on to infect more than 600 computers. Fortunately, the hospital was using independent internal networks, which prevented the virus from spreading to all of its 6,000 machines.

HAMEÇONNAGE AU CHU DE MONTPELLIER

L'hameçonnage, ou phishing, est la menace la plus répandue selon le Baromètre de la Cybersécurité des entreprises publié par le CESIN. Un employé du CHU de Montpellier en a fait la malheureuse expérience en mars 2019 : l'email qu'il a ouvert contenait un virus qui a infecté plus de 600 ordinateurs. Heureusement, l'utilisation de réseaux internes indépendants a permis d'éviter la propagation à l'ensemble du parc de 6 000 machines.

Top 5 des cyberattaques qui ont marqué le secteur de la santé

Le secteur de la santé, hôpitaux en tête, est la première cible des attaques de ransomwares. D'ici à 2020, elles devraient quadrupler selon CSO Online. Retour sur cinq exemples de cyberattaques en milieu hospitalier parmi les plus marquantes. De quoi rappeler l'importance de la sensibilisation aux bonnes pratiques de cybersécurité… même pour les professionnels de santé.

3
RESPIRATORS AND ANAESTHESIA MACHINES

AT RISK OF "MEDJACKING"

Technology is increasingly common in health care institutions. This growing prevalence increases the risk of "medjacking", or medical device hijacking, as demonstrated by the security flaw that researchers discovered in General Electric respirators and anaesthesia machines. This vulnerability, which the US Department of Homeland Security says is easily exploitable, has yet to be corrected by GE.

FACE AU RISQUE DE « MEDJACK »

La technologie est de plus en plus présente dans les structures de santé. Avec elle, le risque de « medjack » ou de piratage d'appareils médicaux augmente comme l'illustre la faille de sécurité découverte par des chercheurs dans des produits respiratoires et d'anesthésie de General Electric. Cette vulnérabilité, facilement exploitable d'après le Département de la Sécurité intérieure des États-Unis, n'a pour l'instant pas été corrigée par le groupe industriel américain.

2
BOSTON CHILDREN'S HOSPITAL

TARGETED BY A DDOS ATTACK

In 2014, a hacker launched a DDoS (Distributed Denial of Service) attack against Boston Children's Hospital. The hospital, whose donations page was shut down by the attack, is estimated to have lost 300,000 dollars on repairs to its computer system.

VICTIME D'UNE ATTAQUE DDOS

In 2014, c'est via une attaque DDoS qu'un hacker s'en était pris à l'hôpital pour enfants de Boston. Le manque à gagner pour l'établissement, dont la page de dons était indisponible, s'élevait à 300 000 dollars. Soit la somme dépensée pour réparer le système informatique.

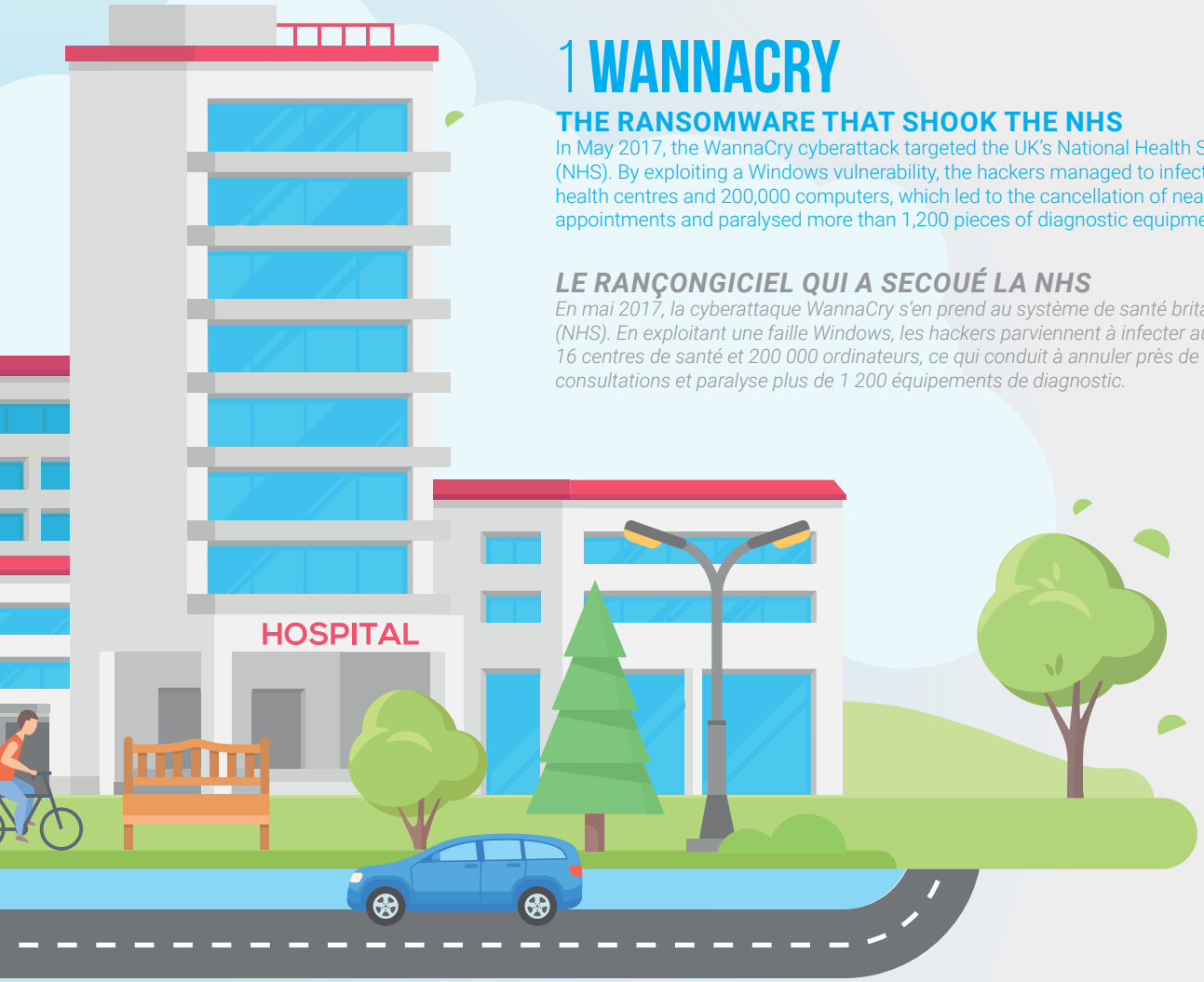
1 WANNACRY

THE RANSOMWARE THAT SHOOK THE NHS

In May 2017, the WannaCry cyberattack targeted the UK's National Health Service (NHS). By exploiting a Windows vulnerability, the hackers managed to infect at least 16 health centres and 200,000 computers, which led to the cancellation of nearly 20,000 appointments and paralysed more than 1,200 pieces of diagnostic equipment.

LE RANÇONGICIEL QUI A SECOUÉ LA NHS

En mai 2017, la cyberattaque WannaCry s'en prend au système de santé britannique (NHS). En exploitant une faille Windows, les hackers parviennent à infecter au moins 16 centres de santé et 200 000 ordinateurs, ce qui conduit à annuler près de 20 000 consultations et paralyse plus de 1 200 équipements de diagnostic.



The hospital sector: Critical systems, highly sensitive to cyberattacks

By Marco Genovese – November 7, 2019

It's a terrifying paradox: despite the fact that trust and confidence is a central aspect in the relationship between hospitals and their users, 80% of health organisations have suffered a successful attack between 2016 and 2018 according to an article by Orange Cyberdefense and Orange Healthcare. How can we explain this vulnerability and above all how can it be countered?

Data and critical operations make the hospital sector a prime target

Health organisations are particularly attractive to hackers because they process ultra-sensitive data concerning patients. Ransomware, denial of service attacks, "medjacking", or botnets, hackers will try anything to compromise access to this sensitive information or to get their hands on it. However, data isn't the only thing of interest to cyberattackers. Because disrupting the different activities carried out in these healthcare establishments, putting lives at risk, offers a powerful means of blackmail enabling them to get what they want.

How can it be that systems which are so sensitive – and which are known to be under threat – can still be so vulnerable? It all comes down to a complete mishmash of failings.

The permeability of front-line networks

In hospital environments, it's by no means rare to find several networks with different privacy levels existing side-by-side. For example, from a Wi-Fi hotspot, it's easy to connect to the patients' network. From there, it's possible to intercept the medical network and from

Milieux hospitaliers :

Des systèmes hyper sensibles aux cyberattaques

C'est un paradoxe qui peut effrayer : alors que la confiance est au cœur de la relation entre l'hôpital et ses usagers, 80% des organisations de santé auraient subi une attaque réussie entre 2016 et 2018 d'après une tribune d'Orange Cyberdefense et Orange Healthcare. Comment expliquer une telle vulnérabilité et, surtout, comment y remédier ?

Données et criticité font du milieu hospitalier une cible de choix

Parce qu'elles traitent des données ultra-sensibles, relatives aux patients, les structures de santé attirent particulièrement les hackers. Ransomwares, attaques par déni de service, « medjack », ou encore botnets, tous les moyens sont bons pour compromettre l'accès à ces informations sensibles ou mettre la main dessus. Mais la data n'est pas la seule motivation des cyber-attaquants. Car réussir à bloquer l'activité de ces établissements, dans lesquels des vies sont en jeu, représente un levier de chantage particulièrement puissant pour arriver à leurs fins.

Comment expliquer que des systèmes à ce point sensibles – et que l'on sait être menacés – restent encore si vulnérables ? Par un cocktail de défaillances multiples.

La perméabilité des réseaux en première ligne

Il n'est pas rare dans le milieu hospitalier que plusieurs réseaux aux niveaux de confidentialité différents coexistent. Depuis un hotspot wifi, il est par exemple facile de se connec-

there to access the administrative network. Where it exists, this lack of segmentation constitutes the first flaw in the system, which can be exploited by hackers.

Emergencies take priority

Hospitals and other health organisations have an obligation to ensure business continuity. This means that they cannot interrupt treatments in progress. For this reason, when their IT infrastructure changes, most of them are reluctant to switch into maintenance mode or to switch off certain devices, even briefly. This way of working often leads them to make do with older solutions rather than view the IT system as an all-embracing project with its own governance. To appreciate the problem at first hand, the next time you visit a hospital, have a quick look at the browsers or applications used. After WannaCry, the British National Audit Office (NAO) examined the impact on the National Health Service (NHS). At the time, "most of the infected NHS equipment used supported versions of Windows 7, which hadn't been patched". At the same time, working under emergency conditions also results in basic security measures being neglected on a daily basis, such as closing your session when away from the workstation. The information contained in the patient's record then becomes accessible and administrative access may also be compromised in some cases.

Very few in-house cybersecurity experts

In addition to insufficient governance, another problem is simply the absence of IT security experts in health establishments. However, this problem may soon be a thing of the past as the sector is now making a considerable effort to catch up.

BYOD: a common but uncontrolled practice

Another factor increasing the vulnerability of hospital environments is directly linked to the way the doctors work: many split their time between a private practice and the hospital, but use the same computer and smartphone. As this equipment has not been supplied by the hospital, it does not always comply with the security measures the hospital has put in place.

New and relatively insecure medical technologies

Connected medical devices are becoming increasingly common in the best-resourced hospitals. However, the attention paid to security when designing these devices is still insufficient, leaving an open door to "medjacking".

ter au réseau des patients. Et de là, il est possible d'intercepter le réseau médical puis d'accéder au réseau administratif. Un défaut de segmentation qui, lorsqu'il existe, constitue une première faille exploitable par les hackers.

Priorité à l'urgence

Les hôpitaux et autres organisations de santé sont contraints par une obligation de continuité de service. Concrètement, ils ne peuvent se permettre d'interrompre les soins. C'est pourquoi, lorsque leur infrastructure informatique évolue, ils sont peu nombreux à basculer en mode maintenance – ou à éteindre, même brièvement, certains appareils. Cette façon de fonctionner les conduit souvent à composer avec l'ancien, plutôt que d'appréhender le système d'information comme un projet global, avec une gouvernance propre. Petit exercice pratique : lors d'une prochaine visite à l'hôpital, jetez un œil aux navigateurs ou applications utilisées. Après WannaCry, le bureau national d'audit britannique, le National Audit Office (NAO), s'est penché sur l'impact auprès du National Health Service (NHS). À l'époque, « la majorité des équipements du NHS infectés utilisaient des versions supportées de Windows 7 sur lesquelles les correctifs n'avaient pas été appliqués ». En parallèle, l'urgence se traduit aussi au quotidien par un oubli des principes de base de sécurité comme verrouiller sa session lorsque l'on quitte un poste de travail. Les informations contenues dans le dossier du patient restent alors accessibles, ainsi que potentiellement certains accès administratifs.

Peu d'experts cybersécurité en interne

Au-delà de ce déficit de gouvernance, c'est tout simplement l'absence d'experts en sécurité informatique qui est souvent à déplorer au sein des établissements de santé. Mais cette phrase devrait être bientôt à employer au passé, tant le secteur réalise des efforts considérables pour se (re)mettre au niveau.

Une pratique courante mais incontrôlée du BYOD

Un autre facteur aggravant la vulnérabilité des milieux hospitaliers tient directement au mode d'exercice des médecins : beaucoup partagent leur temps entre un cabinet privé et l'hôpital, mais utilisent le même ordinateur et le même smartphone. Ce matériel n'étant pas fourni par l'hôpital, il ne respecte pas toujours les règles de sécurité mises en place par celui-ci.

Des nouvelles technologies médicales peu sécurisées

Au sein des hôpitaux aux moyens les plus importants, les appareils médicaux connectés se répandent. Or, l'attention portée à la sécurité lors de leur conception est encore faible, ce qui constitue une porte ouverte au « medjack ».

The increasing use of technical management systems for buildings

Among other things, technical management systems in buildings make it possible to remotely control equipment such as the air conditioning systems, fire detection systems or the lifts. If such a system gets hacked, this can result in the forced evacuation of the hospital for example. Designed based on "physical" security standards, these systems are not sufficiently resilient from a digital security viewpoint.

How can the hospital sector become more resilient to cyberattacks?

The first necessity is to fully appreciate the vulnerability of these health establishments and to make cybersecurity a key concern within the organisation, with everything this entails in terms of investments (human resources, governance, equipment, and dedicated budget, etc.).

Use certified and qualified security solutions for networks and hardware

At a more practical level, it's vital to use solutions designed to secure networks, to protect them against intrusions and to guarantee business continuity, but also to guarantee the security of workstations. These solutions must be compulsory for all equipment involved in patient care, whether the organisation owns this equipment or not.

Raising awareness among staff

To convince health staff to comply with best practices in the cybersecurity field, it's vital to regularly remind them of just what is at stake and to clarify the different procedures with them. With this in mind, the Pays de la Loire's e-health healthcare cooperation group (GCS) worked with Orange Cyberdefense on the creation of an escape game known as Sant'escape–Digital Security. Its principle? To explain and apply good practices in the health sector through participation in the game!

Hospitals and the health sector in general are today caught between the need to cut costs and the need to fully exploit the potential offered by digital technology, such as for example the launch of new services like teleconsultation. However, the insufficient security offered by their IT systems can have a particularly severe impact on privacy and security for patients. Unless cybersecurity is treated as a health-related priority in its own right. ¶

Généralisation des systèmes de gestion technique des bâtiments

Les systèmes de gestion technique des bâtiments permettent, entre autres, le contrôle à distance d'équipements comme l'air conditionné, la détection incendie ou les ascenseurs. Le piratage d'un tel dispositif peut conduire à l'évacuation forcée de l'hôpital par exemple. Conçus selon les normes de sécurité « physique », ces systèmes ne sont pas suffisamment armés du point de vue de la sécurité numérique.

Comment le milieu hospitalier peut-il développer sa résilience aux cyberattaques ?

La première mesure consiste à prendre conscience de la vulnérabilité de ces structures de santé et à faire de la cybersécurité une préoccupation majeure de l'organisation, avec ce que cela implique en termes d'investissements (ressources humaines, gouvernance, matériel, budget dédié…).

Utiliser des solutions de sécurité réseau et matériel certifiées et qualifiées

D'un point de vue plus concret, il est impératif de recourir à des solutions sécurisant les réseaux, pour les protéger contre les intrusions et garantir une continuité de service, mais aussi les postes de travail. Avec, comme obligation, de les imposer à l'ensemble du matériel impliqué dans le traitement des patients, que la structure en soit propriétaire ou non.

Sensibiliser le personnel

Pour convaincre les personnels de santé de se conformer aux bonnes pratiques de la cybersécurité, il est indispensable d'en rappeler régulièrement les enjeux et de clarifier avec eux les procédures. C'est dans cet esprit que le groupement de coopération sanitaire e-santé Pays de la Loire (GCS) a travaillé avec Orange Cyberdefense à l'élaboration d'un escape game baptisé Sant'escape – Sécurité numérique. Le principe ? Expliquer et appliquer les bonnes pratiques dans le secteur de la santé par le biais du jeu !

Aujourd'hui, les hôpitaux et le secteur de la santé en général sont pris entre la nécessité de réduire leurs coûts et celle d'exploiter tout le potentiel du numérique avec par exemple de nouveaux services comme la téléconsultation. Or, le déficit de sécurité de leurs systèmes d'information pourrait avoir un prix particulièrement élevé pour la confidentialité et la sécurité des patients. À moins que la cybersécurité ne devienne une priorité de santé à part entière. ¶

Why telemedicine represents a cybersecurity risk

By Marco Genovese – October 1, 2019

It's been a little over a year since French social security services started reimbursing remote consultations. And although the practice offers numerous benefits, some cyber-security risks need to be considered in advance. Here's why.

Telemedicine means no more having to travel: your appointment with the GP takes place through a TV screen in between you. Thanks to telecommunications, the remote delivery of medical services (appointments, consultancy, monitoring, assistance) is growing. And such advances are providing easier access to care for everyone, everywhere.

"Digital technology has disrupted our society; and so, logically, we need to rethink how our care journeys work", says Lydie Canipel, Secretary-General of the Société Française de Télémédecine. "This needs to be done by mutual agreement between doctor and patient, but telemedicine is a great way to fight against geographical gaps in the medical map."

This method of consultation is also particularly well suited to following up chronic diseases. "These are difficult, expensive illnesses that require close monitoring. Having two remote consultations in between

Pourquoi la télémédecine représente un risque pour la cybersécurité

Voilà un peu plus d'un an que la téléconsultation est remboursée par la sécurité sociale en France. Or, si l'exercice présente de nombreux avantages, certains risques liés à la cybersecurité doivent être anticipés. Décryptage.

Avec la télémédecine, plus besoin de vous déplacer : votre rendez-vous avec le généraliste se déroule par écran interposé. L'exercice de pratiques médicales à distance (consultation, expertise, surveillance, assistance) se développe grâce aux télécommunications. Une avancée qui facilite l'accès aux soins partout et pour tous.

« Le numérique a bouleversé notre société, il est normal de repenser nos parcours de soins en conséquence, analyse Lydie Canipel, Secrétaire Générale de la Société Française de Télémédecine. Cela doit se faire d'un commun accord entre le médecin et le patient, mais la télémédecine est un excellent moyen de lutter contre les déserts médicaux. »

Ce mode de consultation est aussi particulièrement adapté dans le suivi de maladies chroniques. « Ce sont des pathologies lourdes et chères qui nécessitent un suivi rapproché. Bénéficier de deux téléconsultations entre ses rendez-vous

your annual appointments with the cardiologist makes your life easier as a patient. Digital technology has enabled us to get back to proximity-based monitoring", she adds.

Faster, fairer and more efficient... telemedicine has many advantages. But how secure is it?

Cyberattacks and their various motives

Telemedicine involves risks inherent to the technologies it is based on. A computerised medical instrument, such as a smart morphine pump, may experience a technical malfunction; but more importantly, it comes with increased cyber risk. And when it comes to remote operations, such risks are vital issues which must be directly factored in.

There are many possible motivations: resale of personal data (including health data), elimination of a competitive advantage, increased bargaining power, and even military sabotage. "All scenarios are possible, including the hijacking of a telemedicine instrument to monitor an individual or threaten their life", adds Robert Wakim, Offers Manager at Stormshield. The six categories of risk apply perfectly to telemedicine: data integrity, confidentiality, availability, authentication, traceability of transactions and attribution of acts. "It has recently been shown that it is possible for a hacker to modify test results, resulting in a misdiagnosis. But hackers can also block access to patient records or paralyse health equipment – in this case, to obtain a ransom". Returning again to remote operations, hackers could attempt to disrupt the connection with the doctor's computer, or even switch it off or take control of it...

Teleradiology is, for example, a domain requiring an awareness of these issues. Robert Wakim details a few possible attack scenarios. "In real time, attackers could alter data being sent from the health device to the doctor's computer; they could also change how commands are interpreted directly at instrument level and

> **"It is essential to educate about the new risks and symptoms of a cyberattack"**
>
> **Robert Wakim**
> **Offers Manager, Stormshield**

annuels chez le cardiologue, c'est moins lourd pour le patient. Grâce au numérique, on a pu réinjecter du suivi de proximité », abonde-t-elle.

Plus rapide, plus pratique, plus équitable, la télémédecine présente nombre d'avantages. Mais est-elle si sûre ?

Des cyberattaques aux motivations diverses

La télémédecine comporte par nature des risques liés aux technologies sur lesquels elle repose. Un instrument médical informatisé, par exemple une pompe à morphine connectée, peut rencontrer un dysfonctionnement technique, mais surtout, il augmente les cyber risques. Et quand il s'agit d'opérations à distance, ce sont directement des enjeux vitaux qui rentrent en ligne de compte.

Et les motivations se révèlent diverses : revente des données personnelles, dont celles de santé, anéantissement d'un avantage concurrentiel, augmentation d'un pouvoir de négociation, voire sabotage opération militaire. « Nous pouvons tout imaginer, comme détourner un instrument de télémédecine pour surveiller un individu ou atteindre à sa vie », complète Robert Wakim, Offers Manager de Stormshield. Les six catégories de risques s'appliquent parfaitement à la télémédecine : l'intégrité des données, la confidentialité, la disponibilité, l'authentification, la traçabilité des échanges et l'imputation des actes. « Récemment il a été démontré qu'il est possible pour un hacker de modifier des résultats d'analyse, conduisant à un mauvais diagnostic. Mais il peut également bloquer l'accès aux dossiers des patients ou paralyser le matériel de santé – cette fois-ci pour obtenir une rançon. » Toujours dans le cadre d'opérations à distance, des hackers pourraient tenter de perturber la connexion de l'ordinateur du médecin, voire de l'éteindre ou d'en prendre les commandes…

La téléradiologie est, par exemple, un domaine qui permet de prendre conscience de ces enjeux. Robert Wakim détaille plusieurs scénarii d'attaques possibles. « L'attaquant peut modifier en temps réel les données envoyées depuis l'instrument de santé vers l'ordinateur du médecin ; il peut également changer l'interprétation de la commande directement

change the viewing angle; and lastly, they could take control of the doctor's computer and change the result displayed on the screen". In all of these cases, the test results would be wrong. And the diagnosis would be unreliable.

So how can we ensure that telemedicine can offer its benefits while at the same time protecting patients, health personnel and their data?

Multiple solutions against attacks

Faced with cyber threats, **health professionals must consider the four components of the system: the communication, the instrument, the computer and the human being**. Here, "communication" refers to the exchanged data enabling the instrument to be manipulated using electronic control systems.

In terms of systems, Stormshield has a full range of solutions to provide optimum assistance to health professionals, as Robert Wakim explains. "A solution such as Stormshield Endpoint Security protects end workstations and ensures they remain healthy. As for Stormshield Network Security (SNS) and its VPN system, data exchange confidentiality can be increased by creating an encrypted "private" virtual tunnel. SNS is also able to perform protocol verification; i.e. ensuring that transiting data complies with exchange standards. Once the data has reached the servers or the end workstations, solutions such as Stormshield Data Security are useful for protecting it in line with GDPR requirements."

But the first and last line of defence is, of course, the practitioner, as the party best placed to realise that something is wrong and raise the alarm at the slightest doubt. "It is essential to educate medical and telemedicine professionals about the new risks and symptoms of a cyberattack," Robert Wakim points out.

"Just like hygiene in the health sector, digital hygiene needs to be an instinctive reaction for health professionals"

Bernard Cassou-Mounat
Health sector co-ordinator, ANSSI

dans l'instrument et modifier l'angle de prise de vue ; ou enfin, il peut prendre le contrôle de l'ordinateur du médecin et modifier le résultat affiché à l'écran. » Dans tous les cas, les résultats d'analyse seront erronés. Et le diagnostic faussé.

Dans ces conditions, comment permettre à la télémédecine d'apporter ses bénéfices tout en protégeant les patients, les personnels de santé et leurs données ?

Des solutions multiples pour contrer les attaques

Face aux cyber menaces, ***les professionnels de santé doivent ainsi considérer les quatre composantes du système, à savoir la communication, l'instrument, l'informatique et l'humain****. La communication correspondant aux échanges de données qui permettent la manipulation de l'instrument à travers les outils informatiques de contrôle.*

Côté outils, Stormshield possède une offre complète de solutions pour aider au mieux les professionnels de santé, comme le détaille Robert Wakim. « Une solution comme Stormshield Endpoint Security protège les postes d'extrémité et garantit qu'ils soient sains. Quant à Stormshield Network Security (SNS) et son système de VPN, on accroît la confidentialité des échanges en créant un tunnel chiffré "privé" et virtuel. SNS est également capable de faire de la vérification protocolaire, c'est-à-dire s'assurer que les données qui transitent respectent les normes d'échange. Une fois sur les serveurs ou sur les postes d'extrémité, des solutions comme Stormshield Data Security sont utiles pour protéger les données conformément au RGPD. »

Mais le premier et dernier rempart est bien le praticien ; qui est le mieux placé pour se rendre compte que quelque chose ne va pas et d'alerter au moindre doute. « Il faut absolument sensibiliser les professionnels de la médecine et télémédecine aux nouveaux risques et symptômes d'une cyberattaque » rappelle souligne Robert Wakim.

Because cybersecurity is also about habits and practices: "the health system needs to be fully informed about the telemedicine solution. In particular, it must ensure it has fully understood how the data are transmitted, processed and stored, and whether regular updates are being made", he urges.

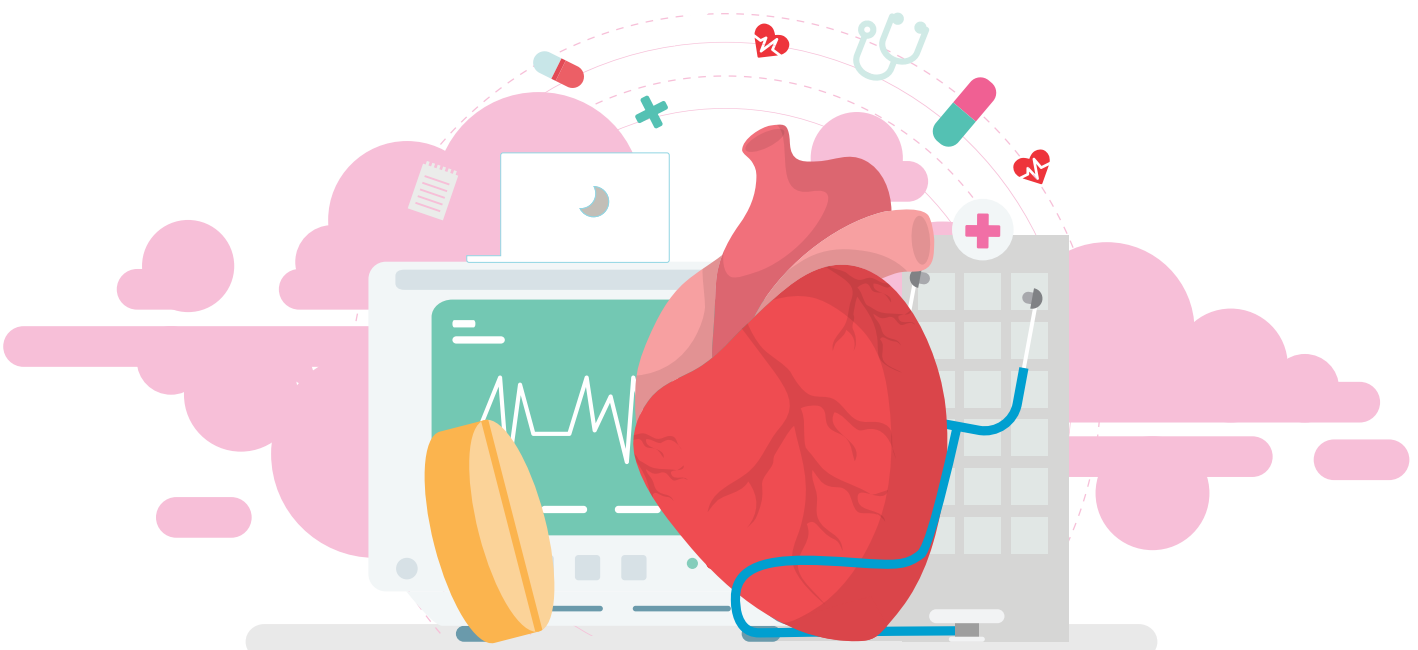
It's a message that Lydie Canipel also promotes when training health professionals: "No-one is ever safe from the threat of a cyberattack. It's vital to comply with ASIP Santé technical frameworks and CNIL data protection standards regarding secure messaging, CE marks and health data hosting. These regulations were designed with patient security in mind". This message was echoed at a morning session focusing on the issue of health data protection, at which Bernard Cassou-Mounat, a health sector co-ordinator at the French ANSSI cybersecurity agency, explained, "Just like hygiene in the health sector, digital hygiene needs to be an instinctive reaction for health professionals"

And lastly, industrialists also need to change their habits, as shown in a proposal by France's Agence nationale de sécurité de médicament (ANSM) drug safety agency, which is expected to result in the issuing of recommendations to manufactures of medical equipment by the end of the year. When it does, improved telemedicine security will be one step closer. ¶

Car la cybersécurité est aussi une affaire de réflexes et d'usages : « la structure de santé doit se renseigner sur sa solution de télémédecine. Elle doit notamment s'assurer de bien comprendre comment les données sont transmises, traitées, stockées et si des mises à jour régulières sont faites », rappelle l'expert.

Un message que passe également Lydie Canipel lorsqu'elle forme des professionnels de santé : « Nous ne sommes jamais à l'abri d'une cyberattaque. Il faut respecter les référentiels techniques de l'ASIP Santé ou les normes de la CNIL en matière de messagerie sécurisée, de marquage CE ou encore d'hébergeur de données de santé. Ces textes ont été pensés pour la sécurité du patient. » Un message repris à l'occasion d'une matinée organisée autour de la question de la protection des données de santé, Bernard Cassou-Mounat, Coordonnateur du secteur Santé à l'ANSSI, expliquait que « comme l'hygiène sanitaire, l'hygiène numérique doit rentrer dans les mœurs des professionnels de santé ».

Enfin, les industriels aussi doivent changer leurs habitudes comme en atteste le projet de l'Agence nationale de sécurité de médicament (ANSM) qui devrait aboutir en fin d'année par l'envoi de recommandations aux fabricants de dispositifs médicaux. Un pas supplémentaire vers une télémédecine plus sûre. ¶



#3 Cyber culture in corporations, a long journey full of pitfalls

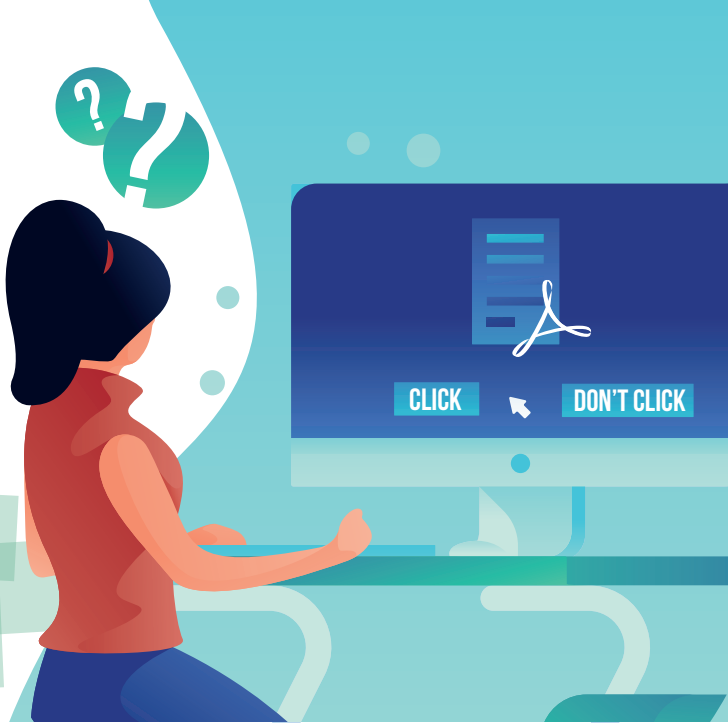
La culture cyber en entreprise, un long parcours semé d'embuches

The slow evolution of IT professions

La lente évolution des métiers de l'IT

Instilling a cybersecurity culture in the company

Comment insuffler une culture de cybersécurité dans l'entreprise ?



By Victor Poitevin – February 4, 2019

Looking beyond the fundamental protective tools, we can sum up the key to a successful cybersecurity policy in just one word: people. However, educating and training staff in IT risks involves more than just applying a few basic rules. You also need to develop an internal "cybersecurity culture".

According to the 2018 Cybersecurity Study by Deloitte, employees are responsible for 63% of internal security incidents. Yet, as shown by ISACA and the CMMI Institute in the 2018 Cybersecurity Culture Report, many organisations rely heavily on technology for their cybersecurity and fail to invest sufficiently in what should be their first line of defence: their workforce.

The need to develop an in-house culture of cybersecurity

Cybercriminals are skilled in identifying the weakest links in a company. Often, they look no further than the personal information shared publicly on social media. An employee's interests, the birthdays of their children or the name of the family pet can all be used in spear phishing attacks or provide clues for hacking passwords.

"People are the greatest point of vulnerability when it comes to cybersecurity. The breach may be accidental (mistakes, forgetting or failing to respect instructions), or it might result from data compromise (unwittingly enabling malicious intrusion) or premeditation

Au-delà des indispensables outils de protection, la clé de la réussite en matière de cybersécurité se résume en un mot : l'humain. Mais sensibiliser et former ses équipes aux risques informatiques ne se limite pas à l'application de quelques règles élémentaires. Il s'agit également d'arriver à développer une véritable « culture de cybersécurité » en interne.

Selon l'étude « Enjeux cyber 2018 » du cabinet Deloitte, 63% des incidents de sécurité dont les organisations sont victimes proviennent d'un de leurs employés. Or, comme le constate l'ISACA et l'institut CMMI dans « The 2018 cybersecurity culture report », de nombreuses organisations basent leur cybersécurité sur la technologie, mais sous-investissent ce qui devrait être leur première ligne de défense : leurs collaborateurs.

L'impérative acculturation des collaborateurs aux enjeux de la cybersécurité

Les cybercriminels excellent dans l'identification des maillons faibles au sein des entreprises, en exploitant notamment des informations personnelles affichées publiquement sur les réseaux sociaux. Les centres d'intérêt d'un employé, la date de naissance de ses enfants ou encore le petit nom de son chien sont autant d'éléments pour enrichir des emails de phishing ciblés ou d'indices pour casser ses mots de passe.

« L'humain est de fait le principal point de vulnérabilité en matière de cybersécurité que ce soit par accident (erreur, non-respect ou oubli des consignes…), par compromission (vecteur à son insu d'une intrusion malveillante) ou par pré-

(causing intentional harm for a variety of reasons.)," says Franck Nielacny, Chief Information Officer at Stormshield.

The risk of data compromise, in particular, is increasing. "All companies and all employees can be threat vectors. This is true for mass attacks, as in the case of the WannaCry ransomware in 2017, but also for highly targeted attacks, where they are unwitting players," warns Stéphane Prévost, Product Marketing Manager at Stormshield.

Corporate cybersecurity: everybody's business

Even when everybody has understood the need to place people at the core of the corporate cybersecurity policy, you still have to persuade employees that cybersecurity is everybody's business. To successfully develop a shared in-house cybersecurity culture, five key players need to be involved, according to Franck Nielacny: "management, employee representatives, HR, the head of IT security and the IT director".

Employees are responsible for 63% of internal security incidents

The process is far from simple, for a number of (good) reasons. First, the new security processes are generally viewed by employees as yet another constraint. At the same time, many companies have a siloed organisation that is not necessarily favourable to teamwork. A shared culture cannot develop effectively with only minimal cooperation between departments. As a result, it appears difficult to collect practical real-time feedback on each company's vulnerabilities and to find a way to address them quickly.

The cybersecurity culture needs to place even greater emphasis on integrating security from an early stage, in the business software development cycle. This is one of the best ways to educate all corporate departments on managing sensitive data! With the GDPR, "Security by design" has even become a standard, ensuring that the software itself does not become the weakest link in the security process. Often, however, it is the lack of qualified in-house staff that hampers efforts to deploy an ongoing information policy on IT risk.

méditation (démarche intentionnelle de nuire pour diverses raisons…) », souligne Franck Nielacny, Directeur des Systèmes d'Information Stormshield.

La compromission notamment est un risque de plus en plus grand. « Toutes les entreprises et tous les employés peuvent devenir vecteurs de menace. Que ce soit via des attaques de masse comme pour le ransomware WannaCry en 2017, mais aussi involontairement au travers d'attaques de plus en plus ciblées », prévient Stéphane Prévost, Product Marketing Manager Stormshield.

Cybersécurité de l'entreprise : l'affaire de tous

Mais une fois acquise la conviction que l'humain doit être au centre de la politique de cybersécurité de l'entreprise, reste à convaincre chacun que celle-ci est l'affaire de tous. Pour installer dans les meilleures conditions une culture de cybersécurité partagée par tous au sein de l'entreprise, il est indispensable, selon Franck Nielacny, de s'appuyer sur cinq acteurs clés : « la direction, des représentants des collaborateurs, les RH, le responsable de la sécurité des systèmes d'information et enfin la DSI ».

Et une telle démarche n'est pas simple – et ce, pour plusieurs (bonnes) raisons. La première raison tient au fait que, ces nouveaux process de sécurité sont généralement perçus comme une contrainte supplémentaire par les collaborateurs. En parallèle, le fonctionnement en silos d'un certain nombre d'entreprises ne favorise pas toujours ce travail d'équipe puisqu'une collaboration minimaliste ne permet pas de diffuser de façon efficace une culture partagée. Ainsi, il semble difficile de collecter en temps réel des retours concrets sur les vulnérabilités de l'entreprise et de trouver comment les résoudre rapidement.

Cette culture de la cybersécurité devrait insister de manière encore plus importante sur l'intégration de la sécurité en amont, dans le cycle de développement des logiciels métiers. Un des meilleurs moyens de sensibiliser tous les services de l'entreprise à la gestion des données sensibles ! Avec le RGPD, le « security-by-design » est même devenu une norme pour empêcher que le logiciel ne devienne lui-même le maillon faible en matière de sécurité. Mais souvent, c'est le manque d'équipes qualifiées en interne qui freine ce travail

Also, the emergence of a cybersecurity culture can also be hindered by an approach that is too top-down. Getting employees on board requires active involvement from senior management as well as middle management. As a result, the end user and his/her needs must always be the key concern. For cybersecurity to be effective, it needs to become part of everyday practices. At Stormshield, one of the measures put in place to instill a cybersecurity culture involves 'punishment by pastry'. If an employee leaves its workstation unlocked when he is not at its desk, its email client is 'hacked' and he has to buy croissants for the whole office. This method has proved to be highly effective.

Implement protective solutions tailored to business use

However, not all companies are immersed in these issues to the same extent. Many have a far more distant relationship with cybersecurity. For these companies, the urgent need to educate employees is clear. "A relatively well-informed user is already able to avoid a significant number of risks," points out Matthieu Bonenfant, Chief Marketing Officer at Stormshield. Particularly as the threat can frequently be traced back to employees who are careless or unlucky, rather than truly ill-intentioned.

Franck Nielacny adds, "it's essential right from the start to understand how employees use tools and critical data, to ensure that appropriate solutions are put in place". One of the problems to be addressed in the way employees use IT tools is shadow IT. This is when employees use new apps for business purposes without consulting the IT department first. Another key requirement is to make sure that "all security procedures are a smooth fit with the business processes of each department," he adds.

Last, we also need to take account of mobile working. "With the development of mobile working, connected objects and external ERP systems, it no longer makes sense to maintain an internal security perimeter. Today, companies can build a reinforced security policy based on greater segmentation of the data flow, for example. By designing the system as a zero trust network, they can contain threats and prevent propagation," concludes Stéphane Prévost. ¶

de déploiement d'une politique récurrente d'information sur les risques informatiques.

Enfin, l'émergence d'une culture de cybersécurité peut également souffrir d'un mode de diffusion trop descendant. L'adhésion des collaborateurs passe par une forte implication de la direction mais aussi du middle management, ce qui implique de placer en permanence l'utilisateur final et ses besoins au centre des préoccupations. C'est par les usages au quotidien que la cybersécurité sera la plus efficace. Chez Stormshield, une de ces mesures d'acculturation passe par une « sanction » à base de viennoiseries : quand un collaborateur laisse son poste ouvert alors qu'il n'est pas à son poste, il se fait « hacker » sa boite email et doit payer sa tournée de croissants aux équipes. Redoutablement efficace.

Proposer des solutions de protection adaptées aux usages métiers

Mais toutes les entreprises ne baignent pas dans un tel contexte et beaucoup ont un rapport plus distant à la cybersécurité. Pour ces entreprises, la sensibilisation des collaborateurs est autant une évidence qu'une urgence. « Un utilisateur relativement averti peut à lui seul éviter beaucoup de risques », rappelle Matthieu Bonenfant, Directeur Marketing Stormshield. D'autant que les menaces sont plus souvent liées à des collaborateurs imprudents ou malchanceux, qu'à des employés véritablement malveillants.

Selon Franck Nieclany, « il est essentiel de bien comprendre au préalable ce que les collaborateurs font des outils et des données critiques, afin d'adapter au mieux les solutions mises en place ». L'un des problèmes notamment à ne pas négliger dans l'usage que font les salariés des outils informatiques étant le shadow IT, cette propension des employés à utiliser de nouvelles applications à des fins professionnelles sans consulter la direction informatique. Autre impératif majeur : s'assurer que « toutes les procédures de sécurité s'intègrent harmonieusement dans le process métier de chaque direction », ajoute le Directeur des Systèmes d'Information de Stormshield.

Enfin, il faut également tenir compte du travail en mobilité. « Le périmètre de sécurité intra-entreprise n'ayant plus de sens à l'heure du travail nomade, des objets connectés ou des ERP externalisés, les entreprises peuvent aujourd'hui construire une politique de sécurité renforcée en recourant par exemple à une segmentation plus fine des flux de données. Celle-ci, conçue selon le principe du « zero trust network », permet de confiner une menace et d'éviter qu'elle se propage », conclut Stéphane Prévost. ¶

Top 5 myths about data encryption

By Jocelyn Krystlik – March 11, 2019

Numerous preconceptions still prevent companies from adopting encryption solutions to protect their data. Yet this reluctance could prove costly if it results in massive data leaks... We take a closer look at five common myths surrounding data encryption.

N°1

"Encrypting my data is a waste of money"

Data encryption is a bit like an insurance contract — you only really notice its usefulness when problems arise. But the figures speak for themselves. According to the 2018 study 'Cost of a Data Breach Study: Global Overview', conducted by Ponemon Institute for IBM, the cost of data theft in France averages at €3.54 million, an increase of 8.2% from 2017.

As highlighted in Stormshield's white paper 'Digital transformation of companies; where does security fit in?', a host of potential sources of vulnerability are emerging that we cannot afford to ignore, including employee nomadism, cloud-based document sharing services and the emergence of connected objects.

« Chiffrer ses données, ça coûte mais ne rapporte rien »

Le chiffrement de ses données, c'est un peu comme un contrat d'assurance. C'est lorsqu'on a un problème qu'on en perçoit vraiment l'utilité. Et pourtant, les chiffres parlent d'eux-mêmes. Selon l'étude de 2018 « Cost of data breach study : global overview » menée par Ponemon Institute pour IBM, le coût d'un vol de données s'élève en moyenne à 3,54 millions d'euros en France, soit une hausse de 8,2% par rapport à 2017.

Comme le souligne notre livre blanc de 2018, « Transformation numérique des entreprises : et la sécurité dans tout ça ? », le nomadisme des salariés, les services de partage de documents dans le cloud et l'émergence des objets connectés sont autant de sources potentielles de nouvelles vulnérabilités à ne pas négliger. Et qui peuvent, elles, coûter très cher.

N°2

"Encryption is too complicated to set up"

Middleware, PKI, cryptographic cards, a variety of other certification policies... Until a few years ago, the complexity of data protection procedures was enough to discourage even the most determined of potential customers.

But today, publishers offer solutions that no longer require the implementation of an ultra-complex infrastructure. Whether for end users or administrators, these new solutions have made implementing and managing encryption systems noticeably more transparent. SaaS mode, for example, has enabled significantly lower infrastructure and maintenance costs.

« Le chiffrement, c'est trop compliqué à mettre en œuvre »

Middleware, PKI, carte cryptographique et autre politique de certification... Il y a encore quelques années, la complexité des procédures de protection des données avait de quoi décourager les plus téméraires.

Mais aujourd'hui, les éditeurs proposent des solutions ne nécessitant plus la mise en œuvre d'une infrastructure ultra-complexe. Que ce soit pour l'utilisateur final ou l'administrateur, ces nouvelles solutions permettent de rendre plus transparente la mise en place et la gestion d'un système de chiffrement. Comme par exemple en mode SaaS, avec des coûts d'infrastructures et de maintenance encore plus sensiblement allégés.

Top 5 des idées reçues sur le chiffrement des données

Bon nombre de préjugés empêchent encore les entreprises d'adopter des solutions de chiffrement pour protéger leurs données. Une réticence qui peut coûter cher à l'heure des fuites de données massives ! Retour sur cinq mythes récurrents autour du chiffrement des données.

N°3

"There are other solutions that are just as effective as encryption"

The concept of encryption is often associated with the implementation of virtual private networks (VPNs), useful for protecting data in transit over the Internet. Yet these protection systems do not guarantee the data's integrity in situations such as the theft of the terminal.

On the other hand, beyond VPNs, firewalls and access rights, hard-drive encryption on terminals is becoming an increasingly viable solution. Here, the terminal itself – and not the data – is protected, in response to the threat of theft in particular.

These additional solutions can and should be considered alongside a data encryption solution, forming the 'holy trinity' of an information security policy. This way, regardless of who has access to the workstation, server or network- or cloud-based sharing system, only the user with decryption rights can use the data in question.

« Face au chiffrement, il existe d'autres solutions aussi efficaces »

Souvent, la notion de chiffrement est associée à la mise en place de réseaux privés virtuels (VPN) – utiles pour protéger les flux de données en transit sur Internet. Cependant, une telle protection ne garantit pas leur intégrité, comme par exemple en cas de vol du terminal.

D'autre part, au-delà des VPN, firewall et droits d'accès, le chiffrement de surface des terminaux s'avance comme une autre piste possible. Ici, c'est bien le terminal qui est protégé, pour répondre notamment à cette problématique de vol. Mais non plus les données échangées.

Ces solutions, complémentaires, peuvent et devraient être envisagées aux côtés d'une solution de chiffrement des données, comme véritable triptyque d'une politique de sécurité informatique. Dès lors, peu importe qui a accès au poste, au serveur, au partage de réseau ou de cloud : seul l'utilisateur ayant le droit de déchiffrement pourra les exploiter.

N°4

"I don't need encryption, cyberattacks never happen to me"

"I'm not at risk." "I don't have sensitive data that needs protecting." These kinds of remarks are more common than you would think, and not only within local associations or authorities. But it's not only the responsibility of sectors handling sensitive information to protect the data they manage. The General Data Protection Regulation (GDPR) reminds those who may be in doubt that everyone is responsible for protecting individuals' data.

In France, CNIL's decision to fine Optical Center €250,000 in June 2018 for failing to secure its customers' data is proof that negligence itself can be costly. And the threat is ever-present – even recently, the technology consulting giant Altran was the victim of a cyberattack

« Pas besoin du chiffrement, les cyberattaques n'arrivent qu'aux autres »

« Je ne suis pas concerné », « Je n'ai pas de données sensibles à protéger »... Ce type de remarque est plus courante qu'on ne le croit et pas seulement au sein des associations ou collectivités locales. Il n'incombe pas aux seuls secteurs sensibles de protéger les données qu'ils gèrent. Le RGPD rappelle ainsi à ceux qui en doutaient encore que tout le monde est responsable des données de quelqu'un.

L'amende de 250 000 € infligée en juin 2018 par la CNIL à Optic Center pour avoir insuffisamment sécurisé les données de ses clients témoigne que la négligence peut aussi avoir un coût.

N°5

"If I encrypt my data, I might never get it back"

Many people still fear that they might lose their data after forgetting their password, or if an employee leaves the company without passing on theirs. But certain technologies can help to avoid this kind of inconvenience, such as data recovery, which provides one or two people within a company with access in case of urgent need. The key escrow technique is another possibility, whereby a database – itself encrypted, of course! – is used to store all of a company's encryption keys.

« Si je chiffre mes données, je risque de ne pas les récupérer »

Reste une crainte récurrente, celle de perdre des données parce que l'on a oublié son mot de passe ou qu'un collaborateur a quitté la société sans transmettre le sien. Des technologies permettent d'éviter ce genre de désagrément, tels que le recouvrement de données qui autorise une ou deux personnes dans l'entreprise à y avoir accès en cas de besoin impérieux. Ou encore la technique du séquestre, une base de données (chiffrée, bien entendu !) de toutes les clés de chiffrement de la société.

Data protection solutions:

Towards a seamless deployment?

Data protection solutions: toward deployment without constraints?

To improve their agility, more and more organisations have decided to move away from "classic" workstations – with their many cumbersome clients – in favour of thin clients or virtual computers. This increasing reliance on applications delivered on a SaaS basis is forcing the publishers of security solutions to innovate, including by performing data encryption directly in the browser. This is one of the benefits of Stormshield Data Security.

Solutions de protection des données : vers un déploiement sans contrainte ?

Pour être plus agiles, de plus en plus d'organisations ont décidé de délaisser les postes de travail « classiques » – avec leurs nombreux clients lourds – au profit de clients légers ou de postes virtuels. Ce recours de plus en plus courant aux applications en mode SaaS oblige alors les éditeurs de solutions de sécurité à innover en intégrant notamment le chiffrement des données, directement dans le navigateur. C'est l'une des promesses de Stormshield Data Security.

Shadow IT: A real challenge for IT departments

Le shadow IT : un véritable défi pour les DSI

By Victor Poitevin – March 18, 2019

***Shadow IT* is a real threat for IT services. But where does it come from? What risks does it pose for businesses? What can be done about it? We asked five experts to discuss this important challenge, at a time when the cloud promises to revolutionise business practices.**

The IT departments are usually at the forefront when it comes to measuring the impact of these changes on employee practices. However, recent years have seen the emergence of new unsafe practices. One of these is "Shadow IT"; the use of applications and services, often cloud-based, in parallel with the "official" SaaS offered by the IT department. This practice is currently increasing in pace with the exponential growth of cloud services and connected objects. In a recent report, another cybersecurity player estimates that businesses currently employ, on average, 1,935 cloud services. This figure climbs by 15% year on year. As for "Shadow IT", it is difficult to quantify the threat thanks to its diffuse and temporary nature. Nonetheless, a 2015 PwC survey indicated that 15 to 30% of IT expenses were incurred outside of the official budget. And there is little doubt that this tendency has continued to grow in the meantime.

"The greatest risk is not from a massive direct attack but rather the employees themselves"

Emmanuel Dupont
Chief Security Officer, Oxya

New practices, new risks

"Shadow IT means that part of the company's information assets do not come within the control of the IT

Le « shadow IT » constitue une véritable menace pour les services informatiques. Mais d'où vient ce phénomène ? Quels risques fait-il peser sur l'entreprise ? Quelles réponses y apporter ? Nous avons sollicité five experts pour évoquer cet enjeu crucial, à l'heure où les promesses du cloud bouleversent les usages au sein des entreprises.

Les DSI sont en général aux avant-postes pour mesurer l'impact de ces transformations sur les pratiques des collaborateurs. Or, ces dernières années, de nouvelles pratiques à risque ont émergé. Parmi elles, le shadow IT ; l'utilisation d'applications et de services, souvent localisés dans le cloud, en parallèle des SaaS « officielles » proposés par la direction IT. Aujourd'hui, cette pratique se développe à mesure que les services cloud et le nombre d'objets connectés explosent. Dans un rapport récent, un autre acteur de la cybersécurité estime ainsi que les entreprises ont recours, en moyenne, à 1 935 services de cloud aujourd'hui. Un chiffre qui grimpe de 15% chaque année. Quant au shadow IT, il est très compliqué de quantifier la menace, tant celle-ci est diffuse et conjoncturelle. Néanmoins, une enquête PwC de 2015 notait déjà que 15 à 30% des dépenses informatiques se faisaient en dehors du budget officiel. Et il y a fort à parier que cette tendance a continué d'évoluer depuis.

Nouveaux usages, risques nouveaux

« Avec le shadow IT, c'est une partie du patrimoine informationnel de l'entreprise qui échappe au contrôle de la DSI », explique Emmanuel Dupont, Global Chief Security Officer de Oxya (groupe Hitachi). Fuites de données, failles de sé-

department", according to Emmanuel Dupont, Global Chief Security Officer at Oxya (Hitachi Group). Whether it's about data leaks, security breaches or exposure to malware, this partial loss of control is not without its significant risks. "When information is transferred outside of the boundaries defined by IT, the risk is also transferred but not with the protective measures established by the company. Today, the greatest risk is not from a massive direct attack but rather the employees themselves," says Emmanuel Dupont. "When they use tools without the knowledge of the IT department they become privileged and defenceless targets."

A member of Stormshield's Security Intelligence team reckons that this practice has been boosted by the emergence of new business models. In more flexible and open organisations, the itinerant nature of staff conditions can sometimes lead to them using their own digital equipment (laptop, personal phone, connected watch or voice assistants) in their professional capacity. "When personal devices are used, the usual data circuits are bypassed and secure VPNs are sidestepped. But, if employees have fluid locations, it is difficult to systematically monitor where and how they connect."

Financial factor and time factor

Our experts agree that the growth of Shadow IT is a direct consequence of corporate cost reduction policies. "In-house IT has long been considered as a cost centre," says Denis Lechevin, CISO at Worldline. "The business lines have therefore placed the services offered by IT departments in competition with external services, whose declared costs are lower." And this, without necessarily weighing up the risks incurred.

And, in many cases, the IT departments are slow to react. "This lack of agility on the part of the IT departments goes a long way to explaining the growth of Shadow IT," says Johanne Ulloa, NoLimitSecu podcast host. "If employees needs a resource but the unwieldiness of the process means that the IT department are slow to provide it, they will go through a third party." Thus, the time factor plays a pivotal role. But IT departments often seem to be like a "steamroller that starts off but reacts too slowly," points out Denis Lechevin. But this impression is exacerbated by the fact that the company often brings in the IT department too late in the process. "It is the ease of access and timely deployment of external solutions that leads to this discrepancy. And the urgency of business practice then finds

curité, vulnérabilité aux logiciels malveillants… Cette perte de contrôle partielle n'est pas sans faire peser des risques importants. « Lorsque l'on déporte l'information en dehors du périmètre balisé par l'IT, on y déporte également le risque, mais sans les moyens de protection mis en place par l'entreprise. Aujourd'hui, le principal risque ce n'est pas la grosse attaque directe massive, c'est l'employé lui-même », indique Emmanuel Dupont. « Lorsqu'il utilise des outils dont la DSI n'a pas connaissance, il devient une cible privilégiée et sans défense. »

Pour un membre de l'équipe de Security Intelligence de Stormshield, cette pratique se trouve également renforcée par l'avènement de nouveaux modèles d'entreprises. Dans ces organisations plus flexibles et ouvertes, le nomadisme des employés les amène parfois à utiliser leur propre matériel informatique (ordinateur portable, téléphone personnel, montre connectée ou assistants vocaux) dans un cadre professionnel. « Lorsque l'on utilise ses équipements personnels, on ne passe plus par les mêmes circuits de données, on contourne les VPN sécurisés. Mais dans le cas où les salariés sont très mobiles, il devient compliqué de contrôler systématiquement où ils se connectent et comment. »

Facteur financier et facteur temps

Pour nos experts, le développement du shadow IT est la conséquence directe des politiques de réduction des coûts en entreprise. « L'informatique interne a longtemps été considérée comme un centre de coûts », souligne Denis Lechevin, RSSI chez Worldline. « Les métiers ont donc mis les services proposés par la DSI en concurrence avec des services externes, dont les coûts annoncés sont moins importants. » Sans prendre nécessairement la mesure des risques encourus.

Et dans de nombreux cas, les DSI réagissent avec du retard. « Ce manque d'agilité des DSI explique en grande partie le développement du shadow IT », note Johanne Ulloa, animateur du podcast NoLimitSecu. « Si un collaborateur a besoin d'une ressource, mais que la lourdeur du process fait que la DSI met du temps à la lui fournir, alors on passe par un service tiers ». Le facteur temps joue alors un rôle décisif. Mais souvent, les DSI donnent l'impression d'un « rouleau compresseur qui se met en branle et donne sa réponse trop tard », souligne Denis Lechevin. « Mais cette impression est accentuée par le fait que, souvent, c'est l'entreprise qui sollicite trop tard les DSI. » Face à la facilité d'accès et rapidité de déploiement de solutions externes, c'est ce décalage qui créé un hiatus. Et l'urgence liée à l'usage métier entre alors en contradiction avec le besoin de structurer des services in-

itself at odds with the need to structure IT services in the long term. "Too often, the IT departments are seen as in-house service suppliers, in competition with external suppliers," reckons Denis Lechevin.

However, "third-party solutions without prior approval from the IT department are never long-term solutions," says Franck Nielacny, Chief Information Officer at Stormshield. "Even if the device works and is adopted by the staff, it can prove very complicated to incorporate it retrospectively into the company's official Information System. Network changes, access policies and even security requirements are all potential sticking points. The same applies to personal equipment."

Awareness rather than force

So, what can IT departments do to stem the growth of Shadow IT? "There are three types of response. Prevention, cure and force," says Johanne Ulloa. In the first example, the IT departments are the guarantors of employee awareness. They must draw attention to bad practices to avoid and good practices to adopt. "The CIO must find a way to "slip" into conversations and projects between business units, in order to optimise the security of these exchanges," according to Franck Nielacny. And it must be done as subtly as possible. Because, very often, "the security layers that are added are seen as awkward," says the member of Stormshield's Security Intelligence team. "The challenge, then, is to implement resources in a way that they become a normal part of day-to-day staff routines. "The UX (User eXperience) aspect and the integration of IT into development projects play an essential role here, so that they use IT-validated solutions rather than third-party applications.

As part of a curative policy, the IT department would try to "determine if such services are already being used by the company, using mainly technical methods such as a study of log files," explains Johanne Ulloa.

The last approach would be the use of force. With the introduction of GDPR, some companies have already tightened their policies. "There is a real regulatory challenge," he adds. "The use of third-party applications or services, leads to a risk of non-compliance with GDPR guidelines, especially as regards the management of personal data. "Nevertheless, in the latter case, raised awareness will always be preferable to force. ¶

formatiques sur le long terme. « Trop souvent, les DSI sont considérées comme des fournisseurs de service interne, que l'on peut mettre en concurrence avec des fournisseurs externes », conclut Denis Lechevin.

Pourtant, « les solutions tierces qui ne sont pas validées a priori par le service IT ne sont jamais des solutions de long terme », nuance Franck Nielacny, Directeur des Systèmes d'Information Stormshield. « Même si l'outil fonctionne et est adopté par les équipes, il peut s'avérer très compliqué de l'intégrer a posteriori dans le SI officiel de l'entreprise. Évolutions du réseau, règles d'accès, ou encore exigences de sécurité sont en effet autant de points de blocage potentiels. Il en va de même s'il s'agit de matériel personnel. »

Sensibilisation plus que coercition

Dès lors, quelles solutions s'offrent aux DSI pour enrayer le développement du shadow IT ? « Il y a trois types de réponses. Un axe préventif, un axe curatif et un axe coercitif », pointe Johanne Ulloa. Dans le premier cas, les DSI sont les garants de la sensibilisation des collaborateurs. Ils doivent communiquer sur les mauvaises pratiques à éviter, et les bonnes conduites à adopter. « L'art du SI est donc de parvenir à se « glisser » dans les conversations et les projets entre métiers, pour optimiser la sécurité de ces échanges », explique Franck Nielacny. De la manière la plus subtile possible. Car souvent, « les couches de sécurité que l'on vient rajouter sont perçues comme gênantes », souligne le membre de l'équipe Security Intelligence. « Tout l'enjeu est donc de parvenir à implémenter des moyens qui seront parfaitement insérés dans le quotidien des collaborateurs. » L'aspect UX (User eXperience) et l'intégration de l'IT dans les projets de développement jouent ici un rôle essentiel, de manière à ce que ces derniers utilisent des solutions validées par l'IT, plutôt que des applications tierces.

Dans le cadre d'une politique curative, la DSI essaiera de « déterminer si de tels services sont d'ores et déjà utilisés par l'entreprise, en utilisant principalement des moyens techniques, tel que l'étude des fichiers de logs », explique Johanne Ulloa.

Le dernier axe est coercitif. Avec la mise en place du RGPD, certaines entreprises ont d'ores et déjà durci leur politique. « Il y a en effet un véritable enjeu règlementaire », poursuit-il. « En utilisant des applications ou services tiers, on s'expose à un risque de non-conformité avec les principes du RGPD dans la gestion des données personnelles notamment. » Néanmoins, pour ce dernier, la sensibilisation vaudra toujours mieux que la coercition. ¶

The IT Department: A leading force in cyber development?

DSI : Un métier en pleine évolution cyber ?

By Victor Poitevin – April 24, 2019

After years of being seen as a mere provider of IT services to business units, the IT Department is now at the vanguard of corporate digital transformation. Its role is now to advise, evangelise and instil a healthy IT culture at all levels. And its central role is lent added prominence by growing cybersecurity issues and risk.

Switching on your computer at work, connecting to the internet, saving your documents... none of these simple everyday tasks would be possible without your company's Information Systems Department. The IT department is responsible for the company's IT infrastructure, handling all the hardware and software it comprises, whether application, data and infrastructure for storage, backups, printing and telecommunications.

Longtemps considérée comme un simple fournisseur de services IT pour les pôles métiers, la DSI est aujourd'hui aux avant-postes de la transformation numérique des entreprises. Face à l'hyperconnexion, charge à elle désormais de conseiller, d'évangéliser et d'insuffler une culture d'hygiène informatique à tous les étages. Un rôle central renforcé par la montée des enjeux et des risques de cybersécurité.

Allumer votre ordinateur au travail, vous connecter à internet, sauvegarder vos documents… Tous ces petits gestes du quotidien seraient impossibles sans la DSI de votre entreprise. En charge du parc informatique de l'entreprise, la DSI s'occupe de l'ensemble des matériels et des logiciels qui le compose, qu'il s'agisse des applications, des données et des infrastructures nécessaires au stockage, aux sauvegardes, aux impressions ou encore aux télécommunications.

The IT Department: a strategic role

In other words, the IT department acts as the interface between people and machines. Long regarded as a mere provider of IT services to business units, the IT department is now at the vanguard of corporate digital transformation, driven by new work practices and technologies. The result: this key position, at the crossroads of technology, project management, general management, security and strategy, has developed to incorporate new roles and new skills. "It's not so much about technical skills, more the ability to communicate and listen, notes Franck Nielacny, Chief Information Officer at Stormshield. You have to be able to converse with an accountant, a logistics expert, an HR manager ... to be familiar with their roles and their vocabulary. In short, you need a "business partner" philosophy. This is critically important, because business units are increasingly involved in IT decisions."

The IT department has moved from being an operational function to a strategic role supporting the company's major projects. "The IT department is increasingly expected to be conversant with technological developments, anticipate the requirements expressed by business units, and able to co-ordinate the two coherently," Franck Nielacny points out. "Previously, IT had to keep step with business strategy. With digital transformation, the opposite is now true," comments Frédéric Lau, Mission Director at Cigref.

Today, the growing challenges of corporate cybersecurity require not only security solutions resources, but also employee awareness. The IT department's role is now to advise, evangelise and instil a healthy IT culture at all levels. This calls for no small amount of teaching work. "At Stormshield, for example, all employees have a strong digital culture and a good awareness of security issues. But no-one can afford to be complacent in terms of accidents or mistakes, which means awareness training is a constant necessity, in conjunction with the CISO and HR," confirms Franck Nielacny.

> **"It's not so much about technical skills, more the ability to communicate and listen"**
>
> **Franck Nielacny**
> **Chief Information Officer, Stormshield**

DSI, un rôle stratégique

La DSI assure donc l'interface entre les hommes et les machines. Longtemps considérée comme un simple fournisseur de services IT pour les pôles métiers, la DSI est aujourd'hui aux avant-postes de la transformation numérique des entreprises, poussée par les nouveaux usages et les nouvelles technologies. Résultat : ce poste-clé, à la croisée de la technique, de la gestion de projet, du management, de la sécurité et de la stratégie, a su évoluer pour intégrer de nouvelles missions, et de nouvelles compétences. « Ce sont moins des compétences techniques que des capacités à communiquer et à écouter, note Franck Nielacny, Directeur des Systèmes d'Information Stormshield. Il faut être capable de discuter facilement avec un comptable, un logisticien, un DRH... de connaître les métiers et leur vocabulaire. Bref, d'être dans un esprit de business partner. C'est fondamental car les directions métier sont de plus en plus impliquées pour les choix IT. »

D'exécutant opérationnel, la DSI a pivoté vers un poste stratégique d'accompagnement des grands projets de l'entreprise. « De plus en plus, on attend du DSI qu'il soit au courant des évolutions technologiques, qu'il anticipe le besoin exprimé par les directions métier et qu'il soit capable de coordonner les deux avec cohérence », souligne Franck Nielacny. « Avant, l'IT devait s'aligner sur la stratégie business. Avec la transformation numérique, c'est l'inverse qui se produit », analyse de son côté Frédéric Lau, directeur de mission au Cigref.

Aujourd'hui, les enjeux grandissants de cybersécurité des entreprises imposent autant un équipement en matière de solutions de sécurité qu'une prise de conscience des collaborateurs. La DSI a désormais la charge de conseiller, d'évangéliser et d'insuffler une culture d'hygiène informatique à tous les étages de l'entreprise. Ce qui suppose une bonne dose de pédagogie. « Chez Stormshield par exemple, tous les collaborateurs ont une forte culture du numérique et une bonne sensibilité à la sécurité. Mais on n'est jamais à l'abri d'un accident ou d'une erreur, donc il y a toujours des actions de pédagogie à mener, en collaboration avec le RSSI et les RH », confirme Franck Nielacny.

As the CIO of France's CEA atomic and alternative energies commission, Louis Arrivet places a strong emphasis on awareness training. "Researchers are a unique group: their job is to seek out, research, develop and innovate. Consequently, they sometimes make use of exotic protocols which aren't always right for integrating into a secure IT. I have teams whose job is solely and constantly to raise awareness within the whole CEA," he explains.

Cybersecurity: a daily preoccupation for IT departments

When we think about cybersecurity, we have an image of large-scale attacks, destructive malware and media security flaws. But this is only the tip of the iceberg; for an IT department, the cybersecurity arena covers everything that is unseen. "Cybersecurity affects every company employee and department, emphasises Franck Nielacny. It's an issue of daily concern which requires monitoring and control work, and updates to devices to protect the company."

> **"Between a quarter and a third of all daily tasks are related to cybersecurity"**
>
> **Louis Arrivet**
> **Chief Information Officer, CEA**

Louis Arrivet estimates that between a quarter and a third of daily tasks relate to cybersecurity. "All our projects have a cybersecurity element at one point or another, regardless of the application in question. Cybersecurity inputs form a key part of our thinking even before the design phase. When I discuss a requirement with a department, we start raising security questions even at the earliest stages of the project." And every CIO knows they are expected to answer such questions. "Cybersecurity's importance among the IS Department's business processes is rising exponentially. In the United States, experts estimate a shortage of nearly 200,000 cybersecurity experts. In 10 years' time, that figure will be 500,000," says Emmanuel Dupont, Global Chief Security Officer at oXya.

SaaS and new technologies, IT Department challenges

But the paradigm shift in security in the IT department is also affecting the world outside of the company. In

DSI du CEA (Commissariat à l'Énergie Atomique et aux énergies alternatives), Louis Arrivet mise beaucoup sur la pédagogie. « Les chercheurs sont une population particulière : c'est leur métier de farfouiller, de chercher, de développer et d'innover. Du coup, ils déploient parfois des protocoles exotiques, pas toujours à intégrer dans un SI sécurisé. J'ai des équipes dont le boulot consiste à faire de la pédagogie auprès de tout le CEA, tout le temps », confie-t-il.

La cybersécurité, une préoccupation quotidienne des DSI

Quand on parle de cybersécurité, on y associe donc attaques d'envergure, malwares destructeurs et failles de sécurité médiatiques. Mais ce n'est que la partie émergée de l'iceberg ; pour une DSI, la cybersécurité se joue sur tout ce que l'on ne voit pas. « La cybersécurité concerne tous les collaborateurs et tous les services de l'entreprise, souligne Franck Nielacny. C'est une préoccupation quotidienne qui engendre des actions de surveillance, de contrôle et de mise à jour des dispositifs pour protéger l'entreprise. »

Louis Arrivet évalue entre un quart et un tiers le nombre d'actions quotidiennes consacrées à la cybersécurité. « Tous nos projets ont une dimension cybersécurité à un moment ou à un autre, quelle que soit l'application que l'on déploie. Les inputs de cybersécurité sont intégrés dans nos réflexions, avant la phase de conception. Lorsque j'échange avec une direction sur un besoin, on évoque déjà les questions de sécurité alors que nous sommes au stade le plus amont du projet. » Et chaque DSI se sait attendue sur ces questions. « La part de la cybersécurité dans les métiers de la DSI augmente de façon exponentielle. Aux États-Unis, les experts estiment qu'il manque déjà 200 000 experts cybersécurité. Dans 10 ans, ce sera 500 000 », souligne Emmanuel Dupont, Global Chief Security Officer chez oXya.

SaaS et nouvelles technologies, challenges des DSI

Mais le changement de paradigme de la DSI vis-à-vis de la sécurité concerne aussi l'extérieur de l'entreprise. DSI depuis 17 ans, Louis Arrivet a observé cette évolution « Il y a 20 ans, on était dans la sécurité périmétrique. On parlait de

his 17 years as CIO, Louis Arrivet has seen this change: "20 years ago, perimeter security was the name of the game. We talked in terms of the IT objective. We designed fortresses and thought that putting up walls would keep people out. Now, everything is centred on data: we've realised that what matters is not the information system, but the information itself." The days of developing on your own physical in-house server are gone. Today's approach is to virtualise, to outsource; everything gives way to the SaaS model, driven by new practices. In short, opening up is the norm. But not without due precautions. The IT department is also responsible for the security of any company information processed externally. Delegating technical control of a system in SaaS mode? Yes. Delegating the responsibility for protecting company information stored in that system? Out of the question.

"We're in an area in which everything moves very quickly, and so one thing is obvious... our business is changing. But the basics still remain the same, insists Louis Arrivet. Today, just like 20 years ago, the role of the IT department is to exercise control over its company's information system. And the same will be true tomorrow, even if technologies change."

And what will tomorrow be like?

Blockchain, IoT, cloud computing, serverless computing, machine learning… The electronic playing field on which the IT department operates will change rapidly in future. "In the very short term, the challenge comes from the cloud: IT departments need to ensure that the chosen solutions are reliable and compatible with user requirements, but also sufficiently secure and able to be incorporated in to the information system," notes Franck Nielacny.

"My feeling is that companies will push SaaS providers to host infrastructure and applications at their own premises, but in a way that ensures data remains within the company", is Louis Arrivet's analysis. Alternatively, suppliers will have to provide an absolute guarantee that the companies will retain full control over their information, make their own decisions as to what is and is not sensitive, and what they do and do not want to share. "Outsourcing doesn't have to mean losing your understanding of these mechanisms and how to control them, he continues. If you let that happen, you really put yourself at risk. A company that loses control of its information is in great danger. In future,

l'objet informatique. On concevait une forteresse et on pensait qu'en mettant des murailles, les gens ne rentreraient pas. Désormais, on est data centrics : on a compris que ce qui compte, ce n'est pas le système d'information, mais l'information elle-même. » Fini le développement sur serveur chez soi, "en dur". Aujourd'hui, on virtualise, on externalise, on se plie à la mode SaaS, un peu poussé par les nouveaux usages. Bref, on s'ouvre. Mais pas à n'importe quelle condition. La DSI est aussi la garante de la sécurité des informations de l'entreprise traitées en externe. Déléguer la maîtrise technique d'un système en mode SaaS, oui. Déléguer la maîtrise de la protection des informations de l'entreprise stockées dans ce système, hors de question.

« On est dans un domaine où tout bouge très vite, de facto le métier change, c'est sûr. Mais les fondamentaux ne changent pas, soutient Louis Arrivet. Il y a 20 ans comme aujourd'hui, le rôle de la DSI est d'avoir la maîtrise du système d'information de son entreprise. Ce sera pareil demain, même si les technologies changent. »

Et demain ?

Blockchain, IoT, cloud computing, serverless computing, machine learning… Demain, le terrain de jeu cyber de la DSI changera rapidement. « À très court terme, le défi est celui du cloud : les DSI doivent s'assurer que les solutions choisies sont fiables et compatibles avec les besoins des utilisateurs, mais aussi suffisamment sécurisées et qu'elles s'intègrent dans le système d'information », note Franck Nielacny.

« Mon sentiment, c'est que les entreprises vont pousser les fournisseurs de SaaS à héberger les infrastructures et le logiciel chez eux, mais en faisant en sorte que les données restent dans l'entreprise », analyse de son côté Louis Arrivet. À défaut, les fournisseurs devront apporter l'absolue garantie que les entreprises conservent la maîtrise de leurs informations, qu'elles pourront décider elles-mêmes de ce qui est sensible ou pas, et ce qu'elles veulent partager ou pas. « Ce n'est pas parce qu'on externalise qu'il faut perdre la compréhension de ces mécanismes et leur maîtrise, poursuit-il. Si on fait ça, on s'expose dangereusement. Une entreprise qui perd la maîtrise de son information est en grand danger. Tout chef d'entreprise aura encore besoin demain d'un DSI capable de lui garantir cette maîtrise. »

Idem avec l'intelligence artificielle. « Avec l'apparition d'outils basés sur l'IA et le machine learning, on passe d'un modèle de raisonnement numérique à un modèle de raisonnement « humain » par analogie. L'IA va permettre une détection plus fine des anomalies, elle pourra inventer des

company directors everywhere will still need an IT department which is able to deliver this control."

And the same applies to artificial intelligence. "With the advent of tools based on AI and machine learning, there is – by analogy – a shift from a digitally-centred model to a "human"-centred one. AI will enable more precise detection of anomalies, and will be able to invent scenarios to respond to threats, maintains Emmanuel Dupont. And it will enable the IT department-to be ready. "IT departments always lag a little behind. We're often playing catch-up. AI should help to remedy that situation," continues Emmanuel Dupont. But then you have to consider AI-driven attacks that target AI-based systems."

Although AI is supposed to make IT more efficient and easier, it isn't (yet) ready to replace the IT department. "It will continue to fulfil the role of an interface between a business need (such as sales/care/production) and a range of technologies being offered to markets and companies, concludes Franck Nielacny. The task of combining these two will always require a human being." ¶

scénarios pour répondre aux menaces », juge Emmanuel Dupont. Et permettre à la DSI d'anticiper. « Les DSI ont toujours un petit temps de retard. On fait souvent du réactif. L'IA pourrait permettre de palier à cela, poursuit Emmanuel Dupont. Mais on peut aussi envisager des attaques à base d'IA pour déjouer les systèmes basés sur l'IA ».

Si l'IA devrait rendre l'IT plus efficace et plus facile, elle n'est pas (encore) prête à remplacer la DSI. « Son rôle restera de faire en sorte de relier d'un côté un besoin métier (comme vendre / soigner / produire) à un panel de technologies mis à la disposition des marchés et des entreprises, conclut Franck Nielacny. Il faudra toujours un humain pour concilier les deux. » ¶

The cyber regulations jungle

La jungle des règlementations cyber

Confidence: More than Just a Word in the World of Cybersecurity

By Matthieu Bonenfant – February 25, 2019

The notion of confidence finds itself at the centre of many current debates in the cybersecurity sector. Its strategic dimension ties it to a wide variety of ongoing issues, and geopolitical tensions, which were clearly visible in 2018, have had significant repercussions in the world of cyberspace. There is certainly no shortage of examples.

In addition to suspicions surrounding the presence of nation states behind major cyberattacks, and the opening of cyber-espionage 'schools' in certain countries, 2018 was marked by the announcement of an embargo against certain suppliers following concerns over espionage-related activities, as well as new suspicions regarding the introduction of backdoors into foreign technologies. **Such issues raise doubts concerning the reliability and integrity of software products, particu-**

La confiance : Plus qu'un simple mot dans le monde de la cybersécurité

La notion de confiance est aujourd'hui au centre de nombreux débats dans le secteur de la cybersécurité. Elle revêt une dimension stratégique qui amène sans cesse de nouvelles questions et les tensions géopolitiques, fortement perceptibles en 2018, ont eu de nouvelles répercussions dans le cyberespace. Les exemples ne manquent pas à ce sujet.

Outre les soupçons sur l'origine étatique de cyberattaques majeures ou l'ouverture d'écoles de cyber-espionnage dans certains pays, l'année 2018 a été marquée par l'annonce d'embargo contre certains fournisseurs pour risque d'espionnage, ou encore de nouvelles suspicions sur la présence de backdoors dans des technologies étrangères. ***Ce contexte crée le doute en matière de fiabilité et d'intégrité des produits logiciels, notamment en ce qui concerne les***

larly in terms of cybersecurity solutions. In fact, these solutions are particularly sensitive due to their function as 'guardians of the temple': maintaining control over protection systems means direct access to protected resources. The choice of cybersecurity partner has never been such a crucial issue for companies and institutions.

Positions taken by nation states on thorny issues such as backdoors and the weakening of encryption mechanisms vary. Russia has already introduced legislation to force publishers to provide authorities with a means of accessing encrypted communications. The member states of the Five Eyes alliance* also wish to impose the implementation of weaknesses in software. The primary, and official, objective is to be able to decipher exchanges that could be tied to terrorist activities, and to share information between the various intelligence services.

Of course, the fight against terrorism is a priority. Yet we can question the appropriateness of creating back doors, which might in fact provide an indirect way of accessing sensitive information belonging to private companies or individuals. All kinds of scenarios then become conceivable: nation-state espionage, access to trade secrets, infringements on civil liberties, and so on. Entirely separate to the war on terror, these developments could seriously undermine the ability of businesses and institutions to protect their information assets.

As has been mentioned, these backdoors have not received universal approval. Europe in particular is clearly opposed to their implementation and advocates end-to-end encryption in communications in order to guarantee complete security. In 2017, the Vice-President of the European Commission stressed this position by highlighting the threat posed by the use of backdoors that might eventually be exploited by cybercriminals. Weaknesses in protection or encryption systems could well be discovered and exploited for malicious purposes, providing the perfect opportunity for criminal activity.

The choice of cybersecurity partner has never been such a crucial issue for companies and institutions.

***solutions de cybersécurité**. En effet, ces dernières sont particulièrement sensibles de par leur fonction de « gardien du temple ». Avoir le contrôle sur les systèmes de protection, c'est obtenir un accès direct aux ressources protégées. C'est pourquoi, le choix des partenaires cybersécurité n'a jamais été aussi crucial pour les entreprises et les institutions.*

Sur l'épineuse question des portes dérobées ou de l'affaiblissement des mécanismes de chiffrement, les positions prises par les États diffèrent. La Russie a déjà légiféré pour obliger les éditeurs à fournir aux autorités un moyen d'accéder à des communications chiffrées. Les États membres de l'Alliance des Five Eyes souhaitent également imposer l'introduction de faiblesses dans les logiciels. L'objectif principal et officiel est de pouvoir déchiffrer certains échanges qui pourraient être liés à des activités terroristes et de partager l'information entre les services de renseignement.

Bien entendu, lutter contre le terrorisme est une cause prioritaire. On peut cependant s'interroger sur le bien-fondé de cette volonté de créer des backdoors qui pourraient être un moyen détourné d'accéder aux informations sensibles des entreprises ou des particuliers. Tous les scénarii sont alors envisageables : espionnage étatique, accès à des secrets industriels, atteinte aux libertés individuelles, etc. Autant d'éléments qui ne sont en aucun cas liés à la guerre contre le terroriste et qui pourraient nuire gravement à la protection du patrimoine informationnel des entreprises et des institutions.

Comme évoqué précédemment, ces backdoors ne font pas l'unanimité. L'Europe notamment se positionne très clairement contre leur mise en place et préconise un chiffrement de bout en bout dans les communications afin d'en garantir une totale sécurité. Déjà en 2017, le Vice-Président de la Commission Européenne martelait cette position en mettant en avant la menace induite par l'utilisation de portes dérobées qui peuvent être exploitées par la cybercriminalité. En effet, l'affaiblissement d'un système de protection ou de chiffrement pourrait tout à fait être découvert puis utilisé par des personnes malintentionnées, leur offrant ainsi une voie royale pour réaliser leurs méfaits.

This demonstrates once again that the notion of digital confidence goes well beyond purely technological and functional considerations, often taking on a highly geopolitical nature. An understanding of the origins of digital technologies, particularly those used to manipulate or protect sensitive data, is central to digital confidence. Businesses must also incorporate this strategic information into their reasoning before entrusting suppliers with the keys to securing their information systems. In this sense, continuous awareness-raising efforts among private and public organisations is required. We should also welcome the work carried out to support digital confidence on a European level and by various governmental agencies such as ANSSI. The French agency's system of qualifying security products, for instance, requires a review of source codes to ensure that the protection functions are sufficiently robust and that backdoors are not present. We would wager that this initiative will be taken up more broadly within the future European certification framework, for which ENISA has been mandated. ¶

Ce constat montre encore une fois que la notion de confiance numérique va bien au-delà de considérations purement technologiques et fonctionnelles pour intégrer une dimension éminemment géopolitique. L'origine des technologies numériques, et notamment celles qui manipulent ou protègent des données sensibles, est un pilier de cette confiance numérique. Les entreprises doivent prendre en compte cette donnée stratégique dans leur raisonnement avant de confier les clés de la sécurisation de leur système d'information à un fournisseur. En ce sens, un travail de sensibilisation continue est nécessaire auprès des organisations privées et publiques. On peut également se féliciter des travaux en faveur de la confiance numérique entrepris à l'échelle européenne et par différentes agences gouvernementales à l'image de l'ANSSI. La qualification de produits de sécurité portée par l'agence française impose, par exemple, une revue de code source pour s'assurer du niveau de robustesse des fonctions de protection et de l'absence de portes dérobées. Gageons que cette initiative sera reprise plus largement dans le futur cadre de certification européen pour lequel a été mandaté l'ENISA. ¶

Why your cybersecurity strategy shouldn't depend (only) on a probe

Pourquoi votre stratégie de cybersécurité ne peut pas reposer (que) sur une sonde

By Florian Bonnet – August 28, 2019

Since the ANSSI qualified two detection probes in April 2019, people in the cybersecurity world have talked of little else. Could they be the silver bullet of network protection? This does not seem to be the case. Here's why.

Over the last few months, much has been made of security probes as the latest front in the fight against cyberthreats, especially in the industrial sector. This past April, the ANSSI qualified some "Made in France" probes from Thales and its rival Gatewatcher, intensifying the hostility within the cybersecurity market. On an international level, well-positioned start-ups are on the rise, including Sentryo, a French gem that was recently approached by Cisco. At the same time, there have been several big fund-raisers, notably for the Swiss-Italian company Nozomi and its Israeli competitor, Claroty.

However, the qualification of these first probes did not happen instantaneously. It took the ANSSI four years to quality the first sovereign probes, starting when this term first appeared in the 2015 Military Planning Act (Loi de programmation militaire, or LPM). Primarily intended for Operators of Vital Importance (OVI) — as well as Operators of Essential Services (OES), and based on the November 2018 European Network and Information System Security (NIS) directive —, these probes were tested for two qualities: robustness and the ability to guarantee confidentiality. But not everything that's called a "probe" has the same uses.

Depuis la qualification de deux sondes de détections en avril 2019 par l'ANSSI, le monde de la cybersécurité n'a que ce mot à la bouche. Serait-ce la solution miracle annoncée pour protéger son réseau ? Rien n'est moins sûr ; explications.

Depuis quelques mois, les sondes de sécurité sont présentées comme un nouveau rempart face aux cybermenaces, en particulier dans le monde industriel. En avril dernier, la qualification par l'ANSSI des sondes made in France de Thales et de son rival Gatewatcher a renforcé les hostilités sur le marché de la cybersécurité. Sur la scène internationale, les start-ups positionnées sur le marché ont le vent en poupe, comme Sentryo, pépite française approchée par Cisco. En parallèle, les levées de fonds abondent, notamment pour l'entreprise italiano-suisse Nozomi et son concurrent israélien, Claroty.

Pour autant, la qualification des premières sondes ne s'est pas faite en un jour. Il a fallu quatre ans à l'ANSSI pour qualifier les premières sondes souveraines depuis l'apparition de ce terme dans la Loi de programmation militaire (LPM) de 2015. Destinées prioritairement aux Opérateurs d'Importance Vitale (OIV) – ainsi qu'aux Opérateurs de Services Essentiels (OSE), issus de la directive européenne Network and Information System Security (NIS) de novembre 2018 –, ces sondes ont été testées autour de deux axes : la robustesse et la capacité à garantir la confidentialité. Mais tout ce qui porte le terme « sonde » ne remplit pas les mêmes usages.

What is a probe?

"It's a bit of a catch-all term that's used in many different ways," warns Stormshield Offers Manager Robert Wakim, before adding: "In terms of cybersecurity, we need to talk about network monitoring probes. These are passive tools that monitor network traffic and report information or raise alerts based on where they are installed".

This equipment should be able to detect the weak signals created by a cyberattack. Unlike an anti-virus program or a firewall, these probes let all data pass by them unrestricted.

For it to work, the network monitoring probe needs to be installed transparently, using port mirroring with a listening port, rather than restricting data flows. This means creating supplementary networks: each data flow is duplicated and sent to the probe. If there is an attack on the original network, the probe will identify and report it in the anomaly log.

If a network probe detects an anomaly, one of two things will happen. If your company has an SOC (Security Operations Center). Alerted by the probe (after it has taken the time to calculate the probability that infection has taken place), the SOC will take charge of the situation and halt the attack as quickly as possible. But what if you don't have an SOC? The good news is that the probe informed you that your network has been attacked. The bad news? If the aim of the attack was to destroy your infrastructure, it's already too late.

"Ticks are a good metaphor for talking about how network monitoring probes work. When a tick bites you, you may receive that information from several sources – either your fingers finding a little bump that wasn't there before, your skin beginning to itch, or you may spot it with your eyes. However, none of these alerts can prevent diseases from entering your blood. It's exactly the same thing with a probe. They cannot contain or quarantine infected machines," insists Robert Wakim.

"Probes cannot contain or quarantine infected machines"

Robert Wakim
Offers Manager, Stormshield

Une sonde, c'est quoi ?

« C'est un terme un peu fourre-tout qui est souvent mis à toutes les sauces », prévient Robert Wakim, Offers Manager Stormshield, avant d'ajouter : « En matière de cybersécurité, il faut parler de sonde de détection réseau. C'est un équipement passif qui va écouter le flux d'un réseau et faire remonter des informations et des alertes en fonction de son point d'installation ».

Cet équipement doit être capable de repérer les signaux faibles générés par une cyberattaque. Contrairement à un antivirus ou un firewall, elle laisse passer l'ensemble des flux de données librement.

Pour fonctionner, une sonde de détection réseau doit être installée de façon transparente, en port d'écoute (port mirroring) – en opposition à une installation en coupure. Cette utilisation consiste à créer des réseaux supplémentaires : chaque flux est dupliqué et renvoyé vers la sonde. En cas d'attaque sur le réseau original, la sonde va l'identifier et la remonter au travers de logs d'anomalies.

En cas de détection d'anomalie par une sonde réseau, deux cas de figure se présentent. Dans le premier, votre entreprise possède un SOC. Alerté par la sonde (en prenant en compte le temps de calcul de la sonde pour estimer s'il y a infection ou non), il va prendre la main pour juguler l'attaque dans la limite de sa capacité de réaction. Dans l'autre cas de figure, vous n'avez pas de SOC. La bonne nouvelle ? C'est que la sonde vous indique que votre réseau a été attaqué. La mauvaise ? Si l'attaque vise à détruire votre infrastructure, il est déjà trop tard.

« Le parallèle avec une tique est approprié pour parler des sondes de détection réseau. Lorsque vous vous faites mordre par une tique, l'information peut venir de plusieurs facteurs – que ce soit vos doigts qui rencontrent une aspérité qui n'était pas là avant, votre peau qui vous démange, ou vos yeux qui la repèrent. Mais pour autant, aucun ne pourra empêcher la propagation des maladies dans votre sang. C'est exactement la même chose avec une sonde. Elle ne peut pas contenir l'infection de la machine ni la mettre en quarantaine », souligne Robert Wakim.

Detection vs. Protection

Probes have also received good press, especially in the industrial sector, because they can be installed easily into a listening port. Even as recently as a few years ago, many industrial networks went unprotected because they were isolated from the outside world and its threats. With the rise of Industry 4.0, however, IT-OT Convergence has led to industrial networks being connected with the outside world. Now facing cyber-threats, they needed to install appropriate security measures.

If an attack on the network is detected, it may shut down production entirely, leading to serious economic consequences. The risk with security equipment that restricts data flows is that it may have a negative impact on production, not because of a cyberattack, but because an anomaly or "false positive" is found, i.e. a network behaviour that is falsely believed to be part of a cyberattack. "Probes are reassuring for industrial clients because they only detect, there's not risk of shutting down production," shares Julien Paffumi, Product Management Leader at Stormshield. "In an ideal world, you would have a data-blocking firewall with an integrated IPS to block detected cyberattacks with certainty and a parallel network probe to identify and signal suspected threats."

The need for a qualified firewall

With the LPM in France, and the European NIS directive, OVIs in France have a regulatory obligation, and OESs in Europe are strongly recommended to implement qualified probe solutions. However, the ideal toolkit for companies and municipalities also includes qualified firewalls alongside these probes. Alongside detection, which is a probe's primary purpose, they also offer concrete protection for networks by blocking cyberattacks.

But how can such equipment be installed using a data-blocking connection? Some, like our SNi40 firewall, can operate in IPS/IDS mode: if there is a significant failure, they let data flows pass (fail-safe). Finally, "there's always a solution to counterbalance the inconvenient aspects of data-blocking equipment" highlights Julien Paffumi, "for example, there are High Availability boxes that are synced and that establish backup connections if there is a problem". ¶

Détection vs. Protection

Les sondes ont également bonne presse, grâce à leur intégration en simple port d'écoute, notamment dans le monde industriel. Il y a encore quelques années, les réseaux industriels n'étaient pas du tout protégés car isolés du monde extérieur et de ses menaces. Mais avec l'avènement de l'industrie du futur, la convergence IT-OT instaure une connexion des réseaux industriels vers le monde extérieur. Face à ces cyber-menaces, il faut donc désormais mettre en place les solutions de sécurité adéquates.

En cas d'attaque détectée sur le réseau, c'est toute la production qui peut être arrêtée – avec des conséquences économiques importantes. Et le risque avec un équipement de sécurité dit-de coupure est de bloquer la production non pas à cause d'une cyberattaque mais à cause d'une anomalie ou d'un « faux positif », c'est-à-dire un comportement sur le réseau considéré à tort comme participant à une cyberattaque. « La sonde a ce côté rassurant pour les industriels, car comme elle ne fait que de la détection, il n'y pas de risque d'arrêt de production », indique Julien Paffumi, Product Management Leader Stormshield. « Dans un monde idéal, on aurait un firewall en coupure avec un IPS intégré pour bloquer les cyberattaques détectées de façon certaine et une sonde réseau en parallèle pour identifier et alerter sur les suspicions de menaces ».

Le nécessaire firewall qualifié

Avec la LPM en France et la NIS à l'échelle européenne, il existe une obligation réglementaire pour les OIV en France et une forte recommandation pour les OSE en Europe autour du déploiement de solutions de sondes qualifiées. Mais dans la trousse à outils idéale de ces entreprises et collectivités, aux côtés de ces sondes, il ne faut pas oublier les firewalls qualifiés. En parallèle de la détection, mission première de la sonde, ils sont en charge de la protection concrète des réseaux, en bloquant les cyberattaques.

Mais comment intégrer un tel équipement en coupure ? Certains d'entre eux, à l'image de notre firewall SNi40, peuvent fonctionner en mode IPS/IDS : en cas de défaillance importante, ils laissent passer le flux (fail-safe). Enfin, « il y a toujours une solution pour mitiger les inconvénients des équipements mis en coupure, souligne Julien Paffumi, comme les boîtiers en Haute Disponibilité, qui sont synchronisés et qui prennent le relais entre eux en cas de problème ». ¶

Critical infrastructure: Complex yet vital compliance

Infrastructures critiques :

Une conformité délicate, mais cruciale

By Julien Paffumi – October 21, 2019

Cyberattacks targeting critical infrastructure entail extremely high risks. Hence the complexity of the legislation needed to combat them. Faced with the challenges of securing such infrastructure, no one can afford to skimp when it comes to understanding and complying with this legal framework.

"Critical infrastructure" plays a central role in the way our societies work.

Behind this expression, we find abbreviations such as OVI (Organisme d'Importance Vitale – Organisation of vital importance) for France or OES (Operator of Essential Services) for Europe, but this isn't all. More generally, the expression refers to all public and private infrastructure, the continuous operation of which is vital to the satisfactory operation of the State or of society.

Les cyberattaques visant les infrastructures critiques comportent des risques au niveau de criticité très élevé. D'où la complexité de leur réglementation. Au vu des enjeux de sécurité à l'œuvre, nul ne peut faire l'économie de connaître et de se conformer à ce cadre législatif.

L'« infrastructure critique », au cœur du fonctionnement de la société

Derrière la formule, se cachent des sigles tels qu'OIV (Organisme d'Importance Vitale) pour la France ou encore OSE (Opérateur de Services Essentiels) pour l'Europe, mais pas seulement. L'expression désigne plus largement toutes les structures, privées ou publiques, dont la continuité de l'activité est indispensable au bon fonctionnement de l'État et de la société.

Stéphane Prévost, Stormshield Product Marketing Manager, explains that: "It generally refers to organisations operating in the telecommunications, transport, energy or health sectors. Any organisation for which an interruption of their services following a breakdown of the IT infrastructure would have dramatic consequences".

Prime targets for cyber-attackers

Ensuring the satisfactory operation of these structures is therefore vital to the day-to-day running of our societies and the security of our people. However, this means that such infrastructure becomes a prime target for terrorist acts or acts of sabotage perpetrated through cyberattacks. It was after the 9/11 terror attacks that people began giving thought to this notion of critical infrastructure in France.

To avoid such attacks occurring via their IT systems, the managers of critical infrastructure must strive for maximum security, as specified in a jungle of different directives, versions and regulatory texts both at a national and European level.

The legislation is particularly dense and not always very clear

As Stéphane Prévost explains, the critical nature of this infrastructure has led to the member states of the European Union adopting laws, regulations and directives to ensure that this infrastructure can resist cyberattacks. "Although we may be unable to prevent cyberattacks, we need to do everything possible to successfully block them or at least to restore the affected services as quickly as possible".

In France, organisations operating in the health sector for example are subject to at least four European directives or regulations (such as the GDPR, the NIS or the PCI-DSS), to two French laws or directives (the Public Health Code and interministerial instruction number 901) and potentially to two standards (Common Criteria and ISO27000). And that's before we even get to the good practices guides. This framework naturally includes recommended solutions, such as the "decree concerning the health sector of the French Military Planning Law which makes it compulsory to use cybersecurity solutions recommended by the French state", adds Stéphane Prévost.

Stéphane Prévost, Product Marketing Manager Stormshield, précise : « Ce sont généralement des acteurs des télécommunications, du transport, de l'énergie ou encore de la santé… Tout organisme dont l'interruption de service, suite à une mise en défaillance de l'infrastructure informatique, aurait des conséquences dramatiques. »

Des cibles de choix pour les cyberattaquants

La bonne marche de ces structures se révèle donc indispensable au quotidien de nos sociétés et à la sécurité des populations. Mais ce statut en fait les cibles privilégiées d'actes terroristes ou de sabotages réalisés au moyen de cyberattaques. C'est d'ailleurs après les attentats du 11 septembre 2001 qu'une réflexion sur cette notion d'infrastructure critique a émergé en France.

Pour se prémunir de telles attaques via leurs systèmes informatiques, les infrastructures critiques doivent adopter un niveau de sécurité maximal, décrit par une jungle de directives, de versions et de textes réglementaires au niveau national ainsi qu'européen.

Une législation dense, pas toujours explicite

Comme l'explique Stéphane Prévost, la nature critique de ces infrastructures pousse les États membres de l'Union européenne à se doter de lois, de règlements et de directives pour faire en sorte que celles-ci soient résilientes face aux cyberattaques. « Si nous ne pouvons pas empêcher la cyberattaque, il faut tout faire pour réussir à la bloquer ou a minima à rétablir le service au plus vite ».

En France, une organisation du secteur de la santé est par exemple soumise à au moins quatre directives ou règlements européens (comme le RGPD, la NIS ou le PCI-DSS), deux lois ou directives françaises (Code de la santé publique et l'instruction interministérielle n°901) et potentiellement deux standards (Critères Communs et ISO27000). Sans parler des guides de bonnes pratiques. Ce cadre tend bien sûr à recommander des solutions, comme « l'arrêté relatif au secteur de la Santé de la Loi de programmation militaire française qui impose le recours à des solutions de cybersécurité recommandées par l'État français », complète Stéphane Prévost.

Adopting the right habits: qualification, compliance and protection

These good habits in the cybersecurity field first and foremost include choosing products approved by the ANSSI (National Cybersecurity Agency of France). An approved solution is compliant with the regulatory framework and offers added peace of mind as it has been tested to very demanding levels.

"The challenge is to deploy the cybersecurity solution while at the same time taking full account of the business processes and the various constraints specific to this infrastructure, such as availability or continuity of service for example", adds Houari Rachedi, Stormshield Project Manager.

This sometimes means trialling even a minor update in a test environment to avoid the risk of modifying the ecosystem for the workstation or network or affecting a business-critical product. "We try to anticipate in as far as this is possible, by notifying the product managers of these constraints to ensure that they are taken into account right from the design stage. Our consultants then get involved, supporting our clients through the deployment and configuration stages", he continues.

Fortunately, critical infrastructure is today managed by teams who are increasingly competent when it comes to guaranteeing the security of their IT systems. A good first step towards ensuring compliance is to choose solutions recommended and/or approved by the ANSSI. However, support from specialists can also come in handy to help you get the most from solutions implemented in a restricted environment. ¶

"The challenge is to deploy the cybersecurity solution while at the same time taking full account of the business processes and the various constraints specific to this infrastructure"

Houari Rachedi
Project Manager, Stormshield

Les bons réflexes : qualification, conformité et protection

Le premier réflexe en matière de cybersécurité est d'opter pour des produits qualifiés par l'ANSSI. La solution qualifiée s'illustre ainsi par sa conformité au cadre règlementaire et l'assurance d'être testée au plus haut niveau d'exigences.

« Le défi est de déployer la solution de cybersécurité tout en respectant les processus métier et les contraintes spécifiques à ces infrastructures comme par exemple la disponibilité ou la continuité de service », complète Houari Rachedi, Project Manager Stormshield.

Cela implique parfois pour une mise à jour même mineure de passer par un environnement de test pour ne pas risquer de modifier l'écosystème du poste ou du réseau ou encore d'influer sur un produit métier sensible. « Nous anticipons au maximum en faisant remonter ces contraintes aux responsables produit pour qu'elles soient prises en compte dès la conception. Nos consultants interviennent ensuite pour accompagner nos clients dans le déploiement et le paramétrage », poursuit-il.

Heureusement, les infrastructures critiques disposent aujourd'hui d'équipes de plus en plus compétentes pour assurer la sécurité de leurs systèmes informatiques. Choisir des solutions recommandées et/ou qualifiées par l'ANSSI constitue une première étape, celle de la mise en conformité. Toutefois, l'accompagnement par des spécialistes peut également s'avérer utile pour tirer le meilleur parti des solutions implémentées dans un cadre contraint. ¶

Cybersecurity Act: An initial signal sent by Europe

Cybersecurity Act : Un premier signal envoyé par l'Europe

By Stéphane Prévost – November 12, 2019

With the adoption of the Cybersecurity Act a few months ago, Europe was taking a new step forward in cybersecurity by adopting a common framework. Strengthening the powers of the European Network and Information Security Agency (ENISA), European certification... what can we expect from these regulations?

More restrictive than the existing recognition agreements (Common Criteria Certification (CCRA), SOG-IS agreement or "EU Restricted" Certification), this new framework strengthens the European Union's position on cybersecurity issues. This will enable its Member States to stand united against the cyber-attacks they are undergoing.

Laying the foundations for a common future for security

In addition to the weight given to the European Network and Information Security Agency (ENISA), the

Avec l'adoption du Cybersecurity Act il y a quelques mois, l'Europe franchissait un nouveau cap en matière de cybersécurité, en se dotant d'un cadre commun. Renforcement des pouvoirs de l'Agence européenne de la sécurité des réseaux et de l'information (ENISA), certification européenne… que peut-on attendre de ce règlement ?

Plus contraignant que les accords de reconnaissance existants (Certification Critères Communs (CCRA), accord SOG-IS ou la Certification « Restreint UE »), ce nouveau cadre vient renforcer le positionnement de l'Union européenne sur les questions de cybersécurité. Ses États membres pourront ainsi faire front commun face aux cyberattaques qu'ils subissent.

Poser les bases d'un futur commun pour la sécurité

En complément du poids donné à l'Agence européenne de la sécurité des réseaux et de l'information (ENISA), le Cyber-

Cybersecurity Act will improve the overall level of security across Europe by setting common certification rules. A company that has obtained certification in Italy will now be able to use this "European label" in France, Spain or Germany without taking any further steps in these countries.

These certifications are accompanied by a shared frame of reference with three security levels: basic, substantial and high. These three levels reflect a dimension of trust in IT solutions or services, including connected objects – whether consumer or more technical (such as connected medical devices, for example).

Differentiating between IT and security solutions

In contrast, national certifications – such as ANSSI in France – focus on the level of trust in cybersecurity solutions, such as smart cards, digital certificates or other cybersecurity products. Nuance is paramount when distinguishing between IT solutions and cybersecurity solutions. Since European certifications are designed for a broader scope than cybersecurity alone, their level of requirement is necessarily lower. This is enough to generate some reservations at the present time.

In France, the leading country in terms of digital security, the main concern is that the highest level of European certifications would correspond to the lowest level of French certifications. A blur that could represent a real risk to cybersecurity, favouring less reliable solutions than others. To protect against this, each country of the European Union will be able to maintain sovereign national levels in parallel with European certification. In particular, France, through ANSSI, maintains – beyond certification – its own qualification levels (basic, standard, enhanced), required to operate in national critical infrastructures such as OVIs (Operators of Vital Importance). In short, the solutions already certified by ANSSI – such as those of Stormshield – would therefore already correspond to a level of certification higher than or equal to the European requirement.

While some details related to the implementation of the Cybersecurity Act still need to be refined, this regulation is a good indicator for European cybersecurity. Beyond short-term harmonisation, this legislation will help to shape a more secure digital future. ¶

security Act améliorera le niveau de sécurité global à travers l'Europe en fixant des règles de certification communes. Une entreprise ayant obtenu une certification en Italie pourra désormais faire valoir ce « label européen » en France, en Espagne ou encore en Allemagne sans entamer de démarches supplémentaires dans ces pays.

Ces certifications s'accompagnent d'un référentiel partagé de trois niveaux de sécurité : élémentaire, substantiel et élevé. Ces trois niveaux témoignent d'une dimension de confiance envers des solutions ou services informatiques, et notamment les objets connectés – qu'ils soient grand public ou plus techniques (comme des dispositifs médicaux connectés par exemple).

Faire la différence entre solutions informatiques et solutions de sécurité

En regard, les certifications nationales – type ANSSI en France – portent sur le niveau de confiance envers des solutions dédiées à la cybersécurité, comme des cartes à puce, des certificats numériques ou autres produits de cybersécurité. Entre solutions informatiques et solutions de cybersécurité, la nuance est primordiale. Puisque les certifications européennes sont pensées pour un périmètre plus large que la seule cybersécurité, leur niveau d'exigence est forcément moindre. De quoi susciter aujourd'hui quelques réserves.

En France, pays moteur en matière de sécurité numérique, la principale crainte tient au fait que le niveau le plus élevé des certifications européennes correspondrait au niveau le plus bas des certifications françaises. Un flou qui pourrait représenter un risque réel pour la cybersécurité, en favorisant des solutions moins fiables que d'autres. Pour s'en prémunir, chaque pays de l'Union européenne pourra conserver des niveaux nationaux souverains en parallèle de la certification européenne. En particulier, la France, par l'intermédiaire de l'ANSSI, maintient – au-delà des certifications – ses niveaux de qualification propres (élémentaire, standard, renforcée), requis pour opérer dans les infrastructures critiques nationales comme les OIV. En résumé, les solutions déjà qualifiées auprès de l'ANSSI – comme celles de Stormshield – correspondraient donc déjà à un niveau de certification supérieur ou égal à l'exigence européenne.

Si certains détails liés à l'implémentation du Cybersecurity Act restent à affiner, ce règlement est un bon signal pour la cybersécurité européenne. Au-delà de l'harmonisation à court terme, cette législation permettra de façonner un avenir numérique plus sécurisé. ¶

Cybersecurity compliance:

Which regulations apply to your organization?

Which cyber regulations apply to your organization?

In a world of increasing cyber threats, every organization – large and small, public and private – is required to comply with cybersecurity regulations relevant to their market. But the regulatory landscape is complicated and constantly evolving, in line with the threats and risks organizations are likely to face. Answering that question is the purpose of this interactive guide designed for Chief Information Officers, Chief Information Security Officers and IT managers.

Quelles réglementations cyber s'appliquent à votre organisation ?

Dans un monde de plus en plus en proie aux cybermenaces, chaque organisation (grande ou petite, publique ou privée) doit se conformer aux réglementations en matière de cybersécurité applicables à son marché. Toutefois, l'environnement réglementaire est complexe et en constante évolution, tout comme les menaces et risques auxquels les organisations sont susceptibles d'être exposées. Répondre à cette question est l'objectif de notre guide interactif destiné aux Directeurs des Systèmes d'Information, aux Directeurs de la sécurité informatique et aux responsables informatiques.

Should individual and corporate liability be invoked in cybersecurity issues?

Vers une responsabilité des collaborateurs et de l'entreprise en matière de cybersécurité ?

By Victor Poitevin – September 25, 2019

In cases of data theft or leaks, liability – as applied to individual employees, directors or the company itself – is increasingly being presented as a regulatory tool. So will the war against poor digital hygiene soon be waged with mandatory sanctions?

Does the name "Equifax" ring any bells? In July 2017, it was publicly announced that this US credit rating and analysis company had committed serious breaches of its cybersecurity obligations. A hack against the company had resulted in the leaking of the personal data of 143 million Americans. And this negligence wasn't even the company's first time. The year before, in 2016, the company had already been issued a warning for insufficient guards against cyber risks.

The risks of poor digital hygiene

It cannot be stated often enough: threat levels have never been so high. Nor has the need to instil a genuine cybersecurity culture at corporate level been so critical. Indeed, the Moody's rating agency, known as a major influencer in market capitalisation, has chosen to incorporate a cyber risk component into its evaluation criteria. In fact, it is now given as a rating criterion. In other words, companies without sufficient protection

Dans les affaires de vol ou de fuite de données, la responsabilité des collaborateurs, des dirigeants ou de l'entreprise elle-même est de plus en plus brandie comme un outil de régulation. La lutte contre la mauvaise hygiène numérique passera-t-elle bientôt systématiquement par la sanction ?

Vous souvenez-vous de l'affaire Equifax ? Cette société américaine de notation et d'analyse de solvabilité avait été publiquement mise en cause en juillet 2017 pour des manquements graves à ses obligations en matière de cybersécurité. Victime d'une intrusion, la société avait ainsi laissé fuiter les données personnelles de 143 millions d'américains. Cette négligence n'était d'ailleurs pas la première. L'année d'avant, en 2016, la société avait déjà été mise en garde pour ses manquements face au risque cyber.

Les risques d'une mauvaise hygiène numérique

On ne cesse pourtant de le répéter, le risque n'a jamais été aussi haut. Et l'enjeu d'insuffler une véritable culture de la cybersécurité en entreprise aussi crucial. À tel point que l'agence de notation Moody's, connue comme principale influenceuse des capitalisations boursières, a décidé d'intégrer le paramètre du risque cyber dans ses critères d'évaluation. Désormais, il s'agit même d'un critère de notation. En

against this threat might potentially see their scores lowered – or could even be held liable for their failings, as was the case with Equifax.

At the same time, France's Cour de Cassation appeals court had already given a verdict in March 2018 regarding the liability of a customer in respect of a phishing email. Citing "the customer's serious negligence in retaining and conserving data", the French Court of Justice declared that the individual was liable, and quashed their claim for damages.

Although these two cases – one of which held a company to be liable, while the other found against an individual – are still fairly isolated, they can nonetheless be seen as a weak signal. Are we heading towards a world in which poor digital hygiene could result in mandatory sanctions?

d'autres termes, les sociétés insuffisamment protégées face à cette menace peuvent voir leur note dégradée. Voire être reconnues responsables de leurs manquements, comme cela a été le cas pour Equifax.

En parallèle, la Cour de Cassation en France s'est déjà prononcée en mars 2018 sur la responsabilité d'un client face à un e-mail de phishing. En reconnaissant « la négligence grave du client dans la garde et la conservation de ses données », la Cour de justice a pointé du doigt la responsabilité de l'individu et a annulé sa demande de remboursement du préjudice.

Si ces deux affaires mettant en jeu la responsabilité d'une entreprise d'une part, et celle d'un individu d'autre part, sont encore relativement isolées, elles n'en constituent pourtant pas moins un signal faible. Se dirige-t-on vers un monde où une mauvaise hygiène numérique serait désormais passible de sanctions systématiques ?

Sanctions provided for under the GDPR

Since May 2018, the General Data Protection Regulation (GDPR) has provided a framework for an arsenal of sanctions which can be applied to companies and public bodies in the fight against compliance failures. Article 58 of the European Regulation gives France's CNIL data protection authority the power to implement such deterrents, and Article 83 lists the conditions under which it could apply an administrative sanction – of up to 4% of world turnover.

Des sanctions prévues par le RGPD

Depuis mai 2018, le règlement général sur la protection des données (RGPD) prévoit un arsenal de sanctions qui peuvent être appliquées aux entreprises et administrations, pour lutter contre les défauts de conformités. L'article 58 du règlement européen donne à la CNIL en France le pouvoir de mettre en place ces moyens dissuasifs et l'article 83 liste les conditions qui lui permettent d'appliquer une sanction administrative – pouvant aller jusqu'à 4% du chiffre d'affaires mondial.

And some companies are already paying the (high) price. In France, the CNIL also imposed an administrative sanction of 50 million euros on Google in January 2019, while in the United Kingdom, the Information Commissioner's Office (ICO) data protection authority announced its intention to sanction the airline British Airways with a fine of over 200 million euros. And others will no doubt follow.

Prevention mechanisms still weak

To avoid such possible scenarios, companies already have access to a variety of tools. "Systems are already being put in place to protect access to networks, messaging services, web browsing and workstations and mobile devices," emphasises Matthieu Bonenfant, Chief Marketing Officer at Stormshield. But this is not enough. "More than ever, with new, disruptive changes such as the increase in teleworking and mobility, the weak link is now the employee, especially in cases where those employees are using business devices outside of the company's scrutiny. Regardless of whether they believe they are harming the company."

In addition to purely technical solutions, another critically important factor is that of educating staff and raising their awareness. And this involves the use of significant legal tools. Such as electronic charters, for example, which are intended to provide a framework for best practice and identify "the fundamental rules of appropriate behaviour to be adopted by all users when using computing and electronic communication resources and, therefore, their own rights", says Sylvie Blondel, Human Resources Director at Stormshield. But all too often, such charters, rules of conduct and digital hygiene guides no longer seem to suffice. If you want proof, consider the fact that ransomware is doing a roaring trade. Phishing attempts are paying off handsomely. And cybercrime is becoming more and more costly for organisations... and their leaders. So what if, along with stepping up our awareness campaigns, we also decided to crack down harder with potential sanctions?

More frequent use of individual sanctions?

In 2014, having been held responsible for the massive data leak that affected his company, the manager of the Target company was promptly given his marching orders. More recently, the director of Equifax was also

Et les (gros) montants commencent à tomber. En France, cette même CNIL infligeait une sanction administrative de 50 millions d'euros à Google en janvier 2019, alors qu'au Royaume-Uni, l'autorité de protection des données du Royaume-Uni (ICO – Information Commissioner's Office) a annoncé son intention d'infliger à la compagnie aérienne British Airways une amende de plus de 200 millions d'euros. En attendant les prochains. Moins connu, l'article 84 du RGPD prévoit également de mettre en place des sanctions pénales. À ce jour, sans exemple connu…

Des mécanismes de prévention encore faibles

Pour éviter d'en arriver là, de nombreux outils sont déjà à la disposition des entreprises. « On met déjà en œuvre des outils pour protéger les accès aux réseaux, les services de messagerie, la navigation sur Internet ou encore les postes de travail et terminaux mobiles », souligne Matthieu Bonenfant, Directeur Marketing de Stormshield. Mais cela ne suffit pas. « Avec les bouleversements d'usage comme l'augmentation du télétravail et de la mobilité, c'est le collaborateur qui est plus que jamais le maillon faible, notamment lorsque ses terminaux professionnels se trouvent hors du champ de vision de l'entreprise. Même s'il n'a pas l'impression de nuire à son entreprise. »

Au-delà des outils techniques, le volet de sensibilisation et d'éducation des collaborateurs est fondamental. Et implique de premiers outils juridiques. Comme des chartes informatiques, par exemple, qui doivent encadrer les bonnes conduites et recenser « l'ensemble des règles fondamentales de bon comportement que doit adopter tout utilisateur en matière d'utilisation des ressources informatiques et de communication électronique et, par là même, leurs droits », précise Sylvie Blondel, Directrice des Ressources Humaines de Stormshield. Mais bien souvent ces chartes, ces règles de bonne conduite et ces guides sur l'hygiène numérique ne semblent pas non plus suffire. La preuve en est que les ransomwares se portent très bien. Les tentatives de phishing prospèrent. Et la cybercriminalité coûte de plus en plus cher aux organisations... tout comme à leurs dirigeants. Et si, en parallèle d'une intensification de la sensibilisation, il fallait être plus ferme sur d'éventuelles sanctions ?

Vers un recours plus fréquent à la sanction individuelle ?

En 2014, jugé responsable de la fuite massive de données qui a touché son entreprise, le dirigeant de la société Target a été diligemment poussé vers la porte de sortie. Plus récemment,

dismissed by the company's shareholders. And the reason for this punitive action? The scale of the damage inflicted and the impact on the brand provided justification for invoking the director's personal liability on behalf of the company he represented.

The use of such sanctions for negligence, irresponsible actions or poor digital hygiene could increase in the years to come. And they could be aimed at any employee, regardless of status in the company. In March 2018, the financial director of the Netherlands subsidiary of the Pathé Group was dismissed after falling victim to a high-level scam. "Depending on the case, penalties could range from suspension or termination of employment through to criminal proceedings," points out Matthieu Bonenfant. "But it would be the employer's responsibility to assess the wrongdoing and its severity in respect of its own business activity and the employee's level of responsibility, experience and any other prior incidents, says Sylvie Blondel. And in the event of any criminal action, the employer could join the proceedings as a private party, attempt to prove the harm suffered and assert its rights."

Framework, case law and regulation

As we have seen, a company can be held liable for offences committed on its behalf, and it can itself even invoke the liability of any of its employees or directors. But a number of unknowns remain: what about the liability of subcontractors in the event of negligence or fault? Or supplier liability?

Today, there is still a lack of evidence to allow us to assess such legal questions. But it is safe to assume that regulatory frameworks, legal theory and the law will see major changes in coming years. Do desperate times call for desperate measures? ¶

le dirigeant de la société Equifax a lui-même été révoqué par ses actionnaires. Motif de la sanction ? L'ampleur des dégâts infligés et l'impact sur la marque justifiaient que la responsabilité individuelle du dirigeant soit engagée, au nom de l'entreprise qu'il représente.

Ce recours à la sanction pour négligence, irresponsabilité ou mauvaise hygiène numérique pourrait se développer dans les années à venir. Et concerner n'importe quel collaborateur, quel que soit son niveau hiérarchique. En mars 2018, le directeur financier de la filiale du groupe Pathé aux Pays-Bas s'est ainsi fait licencier après l'« arnaque au Président » dont il a été victime. « En fonction des cas, la sanction pourrait aller de la mise à pied, de la rupture du contrat de travail jusqu'au recours pénal », souligne Matthieu Bonenfant. « Mais il reviendrait à l'employeur d'évaluer la faute et sa gravité au regard de son activité propre, du niveau de responsabilité du collaborateur, de son expérience ou de ses antécédents éventuels, précise Sylvie Blondel. Et s'il y a recours pénal, l'employeur pourrait se porter partie civile, tenter de prouver le préjudice subi et faire valoir ses droits. »

Encadrement, jurisprudence et régulation

On l'a vu, une entreprise peut être tenue pour responsable des infractions commises pour son compte, et elle peut elle-même engager la responsabilité de l'un de ses salariés ou de son dirigeant. Mais plusieurs inconnues demeurent : quid de la responsabilité des sous-traitants en cas de négligence ou de faute ? Et celle des fournisseurs ?

Aujourd'hui, le recul sur les façons d'appréhender cette question juridique est encore insuffisant. Mais gageons que l'encadrement par la régulation, la jurisprudence et le droit devraient prendre de l'ampleur dans les années à venir. Aux grands maux, les grands remèdes ? ¶

#4 Building a new relationship with cybersecurity

La construction d'un nouveau rapport à la cybersécurité

Cybersecurity as part of the daily live

La cybersécurité, dans le quotidien des individus

Illegal streaming: beware of the backlash

Streaming illégal : gare au retour de bâton

By Victor Poitevin – May 2, 2019

Streaming via illegal websites is spreading at break-neck speed. In addition to the legal aspects, streaming is particularly risky for individuals and companies alike.

La consommation de streaming via des sites illégaux se répand à vitesse grand V. Au-delà des aspects légaux, cette pratique s'avère particulièrement risquée pour les particuliers comme pour les entreprises.

On April 14, 2019, the release of the final season of the cult TV series, Game of Thrones, once again provided the opportunity for millions of fans to resort to illegal streaming. When it comes to computer security, the risks are often underestimated. Closing pop-ups and not downloading false Adobe applications does not make you immune to threats.

La sortie, le 14 avril 2019, de l'ultime saison de la série TV culte Game of Thrones a été une nouvelle fois l'occasion pour des millions de fans de recourir au streaming illégal. Une pratique dont les risques sont souvent sous-estimés en matière de sécurité des postes. Car ce n'est pas en fermant les pop-ups et en ne téléchargeant pas les fausses applications Adobe que l'on peut espérer être invulnérable.

As a reminder, streaming, which enables you to listen to and watch programmes online without having to download them is not illegal in itself. Major web platforms, such as YouTube, Deezer, Netflix, etc., use it. However, a vast number of other platforms are providing the public with programmes, films and TV series without permission. According to the MUSO report published in March 2018, in 2017, France recorded no less than 10.5 billion visits on piracy websites and illegal streaming platforms. Mainland France is therefore the European champion of this fraudulent practice ahead of Germany and the United Kingdom.

Pour rappel, le streaming, qui permet d'écouter ou de visionner des programmes en ligne sans avoir à les télécharger, n'est pas illégal en soi : les plus grandes plateformes du web l'utilisent, à l'image de YouTube, Deezer, Netflix… Mais une multitude d'autres plateformes mettent à disposition du public des programmes, des films et des séries TV sans autorisation. Selon le rapport MUSO publié en mars 2018, la France a enregistré pas moins de 10,5 milliards de visites en 2017 sur des sites de piratage et des plateformes de streaming illégal. L'Hexagone est ainsi le champion européen de cette pratique frauduleuse devant l'Allemagne et le Royaume-Uni.

Streaming, a key vector in the dissemination of malware

Le streaming, vecteur majeur de diffusion de malwares

However, beyond a possible fine for receiving stolen goods, if downloading is involved, the risks for users are not without consequences. By clicking on misleading adverts, the web user exposes his terminal to be infected by a computer virus. "Illegal streaming sites are effectively insufficiently protected. Lacking time, resources and awareness of cybersecurity issues, these platforms are the preferred playground for malicious acts", points out Adrien Brochot, Endpoint Security Product Leader at Stormshield

Pourtant, au-delà de l'éventuelle amende pour recel dans le cas d'un téléchargement, les risques pour les utilisateurs ne sont pas anodins. Via notamment l'intrusion de publicités abusives sur lesquelles il aurait cliqué, l'internaute risque en effet de voir son terminal infecté par un virus informatique. « Les sites de streaming illégaux sont en effet mal protégés. Manquant de temps, de ressources et de sensibilité aux problématiques de cybersécurité, ces plateformes sont un terrain de jeu privilégié pour des actes malveillants », illustre Adrien Brochot, Product Leader Endpoint Security Stormshield.

According to a report by the Association of Internet Security Professionals, 97% of these platforms would

Selon un rapport de l'Association of Internet Security Pro-

in fact more or less be infected. Furthermore, the warning to users of pirated content from the British agency against audiovisual piracy, is clear: "You are 28 times more likely to be infected by malicious software when using illegal streaming!"

The threat is even greater if streaming is performed by a company employee who uses their business PC to watch an episode of their favourite series via this type of illegal site. You can hardly blame them: who has never used their business computer at home during the evening to watch the rerun of their favourite team's match? Or even quickly watching an episode during your lunch break? So it is really important to draw attention to the fact that employees are therefore much more likely to make it easy for viruses to infect their company's servers or networks. This is not without the subsequent damages that we are well aware of.

You are 28 times more likely to be infected by malicious software when using illegal streaming!

Highly varied attack mechanisms

Cybercriminal techniques are abundant via illegal streaming sites. You can be exposed to a phishing action by logging on to a streaming site that looks exactly the same as the original site (same design, same typography, similar or even identical connection url, etc.) and that will in fact try to steal your personal data. Similarly, by downloading a free streaming viewing or peer-to-peer application, you could expose your computer to the intrusion of malware or cryptomining software – an action aimed at using the power of a regular computer, which will run without your knowledge, in order to generate cryptocurrency. Big names like Cacaoweb or PopCorn Time have often been singled out and are always the subject of much debate in the cyber community.

Another risk that should not be ignored is the use of a Flash player. The multiple flaws found on this multimedia player are known to enable malicious hackers to infect your computer, before using it to send spam to other internet users, or even steal documents or install ransomware. Now banned from Apple or Microsoft ecosystems, this technology has been replaced with HTML5, WebP or even WebM – deemed to be more

fessionals, 97% de ces plateformes seraient en effet plus ou moins infectées. D'ailleurs, l'avertissement de l'agence britannique contre le piratage audiovisuel aux utilisateurs de contenus piratés est clair : « vous avez 28 fois plus de chances d'être infecté par un logiciel malveillant en consommant du streaming illégal ! ».

Et la menace est d'autant plus grande quand il s'agit du collaborateur d'une entreprise, qui utilise un PC professionnel pour visionner un épisode de sa série préférée sur ce genre de sites illégaux. Difficile de lui jeter la pierre : qui n'a jamais utilisé son ordinateur professionnel chez lui le soir pour regarder la retransmission du match de son équipe favorite ? Ou même lors d'une pause déjeuner pour se lancer rapidement un épisode ? Il faut quand même alerter sur le fait que le collaborateur a alors de fortes chances de favoriser ainsi l'infection des réseaux et serveurs de son entreprise. Avec les dommages que l'on connaît derrière.

Des mécanismes d'attaque très variés

Via les sites de streaming illégaux, les techniques cybercriminelles ne manquent pas. Vous pouvez être exposé à une action de phishing en vous connectant à un site de streaming qui ressemble en tout point à l'original (même design, même typo, url de connexion approchante voire identique…) et qui cherchera en fait à subtiliser vos données personnelles. De même, en téléchargeant une application gratuite de visionnage en streaming ou en peer-to-peer, vous pourriez exposer votre poste à l'introduction de malwares ou de logiciels de cryptomining – action visant à utiliser la puissance d'un ordinateur lambda, qui va tourner sans que vous le sachiez, afin de générer de la cryptomonnaie. Régulièrement pointés du doigt, des grands noms comme Cacaoweb ou PopCorn Time suscitent toujours autant de débats dans la communauté cyber.

Autre risque qu'il ne fallait pas négliger : l'utilisation d'un player Flash. Les multiples failles relevées sur ce lecteur multimédia sont connues pour permettre à des hackers malveillants d'infecter votre ordinateur, avant de l'utiliser pour envoyer des spams à d'autres internautes, voire de dérober des documents ou d'installer un ransomware. Désormais bannie au sein des écosystèmes Apple ou Microsoft, cette technologie est remplacée par des formats HTML5, WebP ou encore

secure. And then subsequently, on top of that other vulnerabilities have been discovered…

Even more cunning is the technique of false track that makes you click on a pop-up inciting you to download security software. "The principle is clever" explains a member of Stormshield's Security Intelligence team. "These false error messages lead you to believe that you have a technical problem and incite you to download an antivirus".

Lastly, there is a fine line between streaming and downloading – some streaming applications even suggest downloading episodes or programmes on your computer. In this case you need to be very careful as very often the files that you are about to install on your computer may contain adware or downloader type programs. In addition to receiving a poorly focused version with almost zero quality, you could be receiving all kinds of malware.

What measures need to be put in place in professional settings?

The business world is therefore not spared from this illegal streaming phenomenon. By watching their programmes on their business computer, employees are exposing their company to a number of risks.

"To limit these risks, installing a UTM solution provides a first level of network protection. Based on a firewall, this solution, in particular, provides a URL filtering function that blocks these streaming sites via dynamic classification in the Cloud. In addition, other functions provide further protection against infections disseminated by some of these sites. This is the case of sandboxing that will run programs in a sandbox environment, of the IP reputation, which assigns scores to IP addresses or even of traffic reports that analyse bandwidth usage", advises Julien Paffumi, Product Management Leader at Stormshield.

Solutions for protecting against the exploitation of vulnerabilities on browsers are not to be overlooked. "HIPS bricks effectively detect malicious behaviour that deviates from the normal behaviour expected by employees", explains Adrien Brochot. However, the best defence is still raising awareness with users, who have to understand that illegal streaming of course constitutes breaking the law, but is above all dangerous. ¶

WebM – censés être plus sécurisés. Et puis ensuite, d'autres vulnérabilités ont été découvertes dessus…

Plus sournois encore, la technique de la fausse piste qui vous fait cliquer sur un pop-up vous incitant à télécharger un logiciel de sécurité. « Le principe est habile, expose un membre de l'équipe de Security Intelligence de Stormshield. Ces faux messages d'erreur vous font croire que vous avez un problème technique et vous incitent à télécharger un antivirus ».

Enfin, la frontière est fine entre streaming et téléchargement – certaines applications de streaming vous proposant même de télécharger les épisodes ou programmes sur votre ordinateur. Attention dans ce cas : bien souvent, les fichiers que vous vous apprêtez à déposer sur votre ordinateur peuvent contenir des programmes de type adware ou téléchargeur. En plus de récupérer une version mal cadrée et dans une qualité proche du néant, vous pourriez ainsi bien récupérer des malwares en tout genre.

Quelles parades en milieu professionnel ?

Ce phénomène de streaming illégal n'épargne donc pas le monde de l'entreprise. En visionnant ses programmes sur son ordinateur professionnel, le collaborateur expose ainsi son entreprise à de nombreux risques.

« Pour les limiter, la mise en place d'une solution UTM amène une première protection au niveau du réseau. Basée sur un pare-feu, cette solution fournit notamment une fonction de filtrage URL qui assure le blocage de ces sites de streaming grâce à une classification dynamique dans le Cloud. Et complément, d'autres fonctions assurent une protection supplémentaire contre les infections véhiculées par certains de ces sites. C'est le cas du sandboxing qui va lancer les programmes dans un environnement de bac à sable, de l'IP reputation qui attribue des scores aux adresses IP ou encore des rapports de trafic qui analysent l'utilisation de la bande passante », conseille Julien Paffumi, Product Management Leader Stormshield.

Sans oublier les solutions de protection contre l'exploitation de vulnérabilités sur les navigateurs. « Des briques HIPS permettent en effet de détecter des comportements malveillants, qui dévient des comportements normaux attendus des collaborateurs », explique Adrien Brochot. Mais la meilleure parade reste encore la sensibilisation des utilisateurs, qui doivent comprendre que le streaming illégal est hors-la-loi, certes, mais surtout dangereux. ¶

Sextortion: are we heading towards a trade in shame?

Sextorsion : vers un marketing de la honte ?

By Victor Poitevin – June 26, 2019

Each month, several billion visitors flock to pornographic sites. These are figures that stimulate the imagination of cybercriminals, who are delighted with these fresh, vulnerable targets that can be easily and ruthlessly blackmailed.

After the giants Google, YouTube and Facebook, pornographic sites are among the most visited platforms in the world. According to SimilarWeb, on April 1, 2019, Pornhub was in 7th position with more than 3 billion monthly visits followed by Xvideos in 8th and Xnxx in 11th, with more than 2 billion visits each. These are figures that are sure to have cybercriminals blushing... with pleasure!

Cyberattacks linked to pornographic content almost tripled in 2018, according to Kaspersky. In 2017, Russian cybercriminals were already using fake pornographic applications to extort more than $890,000 through one million targeted Android phones. And on computers, there are more than 300,000 pieces of pornographic malware...

Chaque mois, plusieurs milliards de visiteurs se ruent sur les sites pornographiques. Des chiffres qui stimulent l'imaginaire des cybercriminels, ravis de ces nouvelles cibles fragiles et faciles à faire chanter, sans modération.

Après les géants Google, YouTube et Facebook, les sites pornographiques comptent parmi les plateformes les plus visitées dans le monde. D'après SimilarWeb, au 1er avril 2019, Pornhub se positionnait ainsi en 7ème position avec plus de 3 milliards de visites mensuelles suivi de Xvideos 8ème et Xnxx 11ème, pour plus de 2 milliards de visites chacun. Des chiffres à faire rougir de plaisir… les cybercriminels !

En effet, les cyberattaques liées à un contenu pornographique ont presque triplé en 2018 d'après Kaspersky. En 2017, des cybercriminels russes utilisaient déjà de fausses applications pornographiques pour extorquer plus de 890 000 dollars au travers d'un million de téléphones Android ciblés. Et sur les ordinateurs, on peut compter plus de 300 000 logiciels malveillants pornographiques…

Are we heading towards a trade in shame?

The vulnerability of active members of these sites is all the greater because they provide personal information about themselves. In 2015, the leaking of the personal data of 32 million people registered on the adulterous dating site Ashley Madison caused a stir in the United States. And it launched the sextortion trend, a new form of cyberattack, based on shame and fear.

Matthieu Bonenfant, Chief Marketing Officer at Stormshield, confirms this underlying trend. "In the event of an attack, users feel a strong sense of guilt and will not necessarily report it. And given the high level of traffic on these sites, cybercriminals are making them a prime target."

A rush towards premium accounts

It is only a short step from dating sites to pornographic sites, and cybercriminals are not lacking in ideas when it comes to blackmailing their vulnerable users. They prefer to steal premium accounts, which are packed with information about their users. It is an effective method for blackmail and threats. At the end of last year, the hacking of eight pornographic sites led to the theft of more than one million user accounts and associated personal data.

This information can be used to blackmail the people in question, or it can be resold on the dark web to allow buyers to access these sites anonymously. You can never be too careful... In 2018, Kaspersky Lab found about 10,000 unique offers of premium access accounts to pornographic sites on the dark web, about twice the number of offers recorded the previous year (2017).

The explosion in webcam attacks

In addition to the threat hanging over these sites, a further one has become considerably more serious in recent months: webcam blackmail. "At the beginning

"Since the beginning of 2019, we have seen several thousand of webcam blackmail per week"

Adrienne Charmet
Project Manager,
Cybermalveillance.gouv

Vers un marketing de la honte ?

La vulnérabilité des membres actifs de ces sites est d'autant plus grande qu'ils y livrent des informations touchant leur intimité. En 2015, la publication sauvage de données personnelles de 32 millions de personnes inscrites sur le site de rencontres adultères Ashley Madison avait ainsi semé un vent de trouble aux États-Unis. Et lancé la mode des sextorsions, une nouvelle forme de cyberattaques, basée sur la honte et la peur.

Matthieu Bonenfant, Directeur Marketing Stormshield, confirme cette tendance de fond. « En cas d'attaques, les utilisateurs éprouvent un fort sentiment de culpabilité et ne porteront pas forcément plainte. Et compte tenu de l'importance du trafic sur ces sites, les cybercriminels en font une cible de choix ».

Une ruée sur les comptes premium

Des sites de rencontre aux sites pornographiques, il n'y a qu'un pas à franchir et les cybercriminels ne manquent pas alors d'imagination pour faire chanter leurs utilisateurs fragilisés. Ils privilégient le vol de comptes premium, riches en informations sur leurs utilisateurs. Un bon angle d'attaque pour procéder à des menaces et à du chantage. À la fin de l'année dernière, le piratage de huit sites pornographiques a ainsi entraîné le vol de plus d'un million de comptes utilisateurs et de données personnelles associées.

Des informations permettant de faire chanter leur propriétaire, ou alors revendues sur le dark web pour permettre à des acquéreurs d'accéder à ces sites de façon anonyme. On n'est jamais trop prudent… En 2018, Kaspersky y avait trouvé environ 10 000 offres uniques de comptes d'accès premium à des sites pornographiques, soit environ le double du nombre d'offres enregistrées l'année précédente, en 2017.

L'explosion des attaques à la webcam

En parallèle de celle qui plane sur les sites, une autre menace a pris une ampleur considérable ces derniers mois : le chantage à la webcam. « Début 2018, nous enregistrions 400 à

of 2018, we recorded 400 to 500 reports per week of this type of attack. Since the beginning of 2019, we have seen several thousand of them per week," says Adrienne Charmet, Project Manager at cybermalveillance.gouv.fr.

Created in 2017 with the support of private actors such as Stormshield, this public platform is actively campaigning on its website and social networks to inform the public about webcam piracy. "In most cases, it's a hoax. So don't panic, don't answer and don't pay," explains Adrienne Charmet, who has a few tips in terms of what to do. Take screenshots in order to record the messages and file a complaint in order to report the attempted extortion.

Because here is precisely how these cyberattacks work: after threatening to disclose a compromising video to your family, colleagues or bosses, cybercriminals urge you to click on a link to check that the video exists; using a variety of strategies that vary in their credibility... The link contains a harmful file that infects your device using GandCrab ransomware, whose popularity will certainly not be affected by the retirement of its creators in May 2019… ¶

500 signalements par semaine concernant ce type d'attaque. Depuis le début de l'année 2019, nous en comptons plusieurs milliers par semaine », constate Adrienne Charmet, chargée de mission chez cybermalveillance.gouv.fr.

Créée en 2017 avec le soutien d'acteurs privés tels que Stormshield, cette plateforme publique mène une campagne active sur son site et sur les réseaux sociaux pour informer le public sur le piratage à la webcam. « Dans la plupart des cas, il s'agit d'une opération de bluff. Il ne faut donc pas paniquer, ne pas répondre et surtout ne pas payer », explique Adrienne Charmet, qui partage quelques bonnes pratiques. Faites des copies d'écran, pour conserver les messages et portez plainte, pour signaler cette tentative d'extorsion.

Car il s'agit bien là du mécanisme de ces cyberattaques : après avoir menacé de divulguer une vidéo compromettante à vos proches, collègues ou patrons, les cybercriminels vous incitent à cliquer sur un lien pour vérifier l'existence de la vidéo. En utilisant différents stratagèmes plus ou moins crédibles, allant jusqu'à se faire passer pour un agent corrompu de la CIA… Derrière le lien, un fichier malveillant qui vient infecter votre terminal à l'aide du ransomware GandCrab. Un ransomware dont la popularité ne sera sûrement pas affectée par le départ à la retraite de ses auteurs en mai 2019… ¶

A future without USB sticks?

Vers un futur sans clé USB ?

By Victor Poitevin – June 26, 2019

In terms of cybersecurity, USB sticks fit the profile of the perfect offender. However, getting rid of them entirely means the only channel for exchanging documents will be through the company's IT network. This might be reassuring, but the danger just takes on another form: if everything happens online, a hacker doesn't even need to leave his home to attack. With a closed network requiring physical hardware, hackers are at least forced to move. So, what should be the policy concerning USB sticks?

The USB stick: a hotbed of computer viruses

Unfortunately, USB sticks are still one of the main sources of computer viruses, despite regular campaigns reminding users of basic protection rules. Honeywell's latest report provides an frightening overview: 40% of USB sticks contain at least one risky file and 26% of these threats could lead to operational problems.

En matière de cybersécurité, les clés USB ont le profil du coupable parfait. Mais, à vouloir s'en débarrasser entièrement, il ne restera plus qu'à échanger les documents au travers du réseau informatique. C'est confortable, mais le danger change de forme : si tout se joue en ligne, un hacker n'a même plus besoin de sortir de chez lui pour attaquer. Avec un réseau fermé nécessitant un matériel physique, les pirates informatiques doivent au moins continuer à se déplacer. Alors, quelle politique envers les clés USB ?

Les clés USB, nids à cyber-MST

Les clés USB sont en effet, malheureusement, toujours l'une des principales sources d'infection informatique malgré des campagnes de rappel des règles de protection élémentaires à intervalles réguliers. Le dernier rapport d'Honeywell dresse ainsi un panorama effrayant : 40% des clés USB contiendraient au moins un fichier présentant des risques et 26% de ces menaces sont susceptibles d'engendrer des problèmes opérationnels.

While the exchange of data in companies is crucial today, it is sometimes difficult to transfer documents. Given the singularities of every company, with their many departments scattered across different locations, and fragmented networks to which some workstations aren't always connected, as well as internal reluctance to use the cloud; USB sticks can still be useful. The other option would entail opening networks. However, even if firewalls are multiplied and defensive protocols stepped up, this would still represent a risk. In certain restricted environments, such as the military or industrial field for example, the network must remain completely isolated.

40%
of USB sticks contain at least one risky file

Faced with such a risky tool, we can finally understand why IBM made the decision – be it a controversial one – to ban the use of USB sticks. In France, the National Assembly is also taking action to raise awareness of digital hygiene with the same aim of banning the use of USB sticks given to deputies during meetings. Is such a ban viable? Useful even? Under what conditions can we continue to use USB sticks with peace of mind?

When constraint rhymes with shadow IT

A whole fleet of computers simply cannot be replaced by workstations without USB ports with a simple click of the fingers. So, should employees be searched at the entrance? Should chewing gum be stuck into USB ports? Computer towers put under lock and key? "No one can control all the USB drives in a company, not unless they block or monitor every device in its network of computers," said Marco Genovese, Product Manager at Stormshield. We can't deny man's basic way of thinking: if the alternative method becomes too restrictive, employees will soon revert back to the simplest option, whether authorised to do so or not. As a result, employees will use devices without the IT department's knowledge, thus awakening the infamous shadow IT plague. Some companies work entirely in the cloud, but this means they are completely dependent on their network connection. Is this really a solution?

Mais alors que l'échange de données est capital de nos jours au sein des entreprises, il est parfois compliqué de pouvoir transmettre des documents. Face aux particularités de chaque entreprise, avec de nombreux services, éparpillés dans des lieux différents, des réseaux fragmentés, des postes parfois non connectés ou encore des réticences en interne à l'utilisation du Cloud ; les clés USB peuvent encore rendre service. L'autre option consisterait à ouvrir les réseaux mais, même en multipliant pare-feux et protocoles défensifs, le lien réseau représente un danger. Dans certains milieux restreints, comme le domaine militaire ou industriel par exemple, le réseau doit même rester complètement isolé.

Devant un outil aussi porteur de risques, on peut finalement comprendre qu'IBM ait pris la décision – pourtant controversée – de bannir purement et simplement l'usage des clés USB. Dans les couloirs de l'Assemblée nationale française, des actions de sensibilisation à l'hygiène numérique visent également à interdire l'utilisation de clés USB offertes à des députés sur des salons. Une telle interdiction est-elle viable ? Utile ? À quelles conditions peut-on continuer de les utiliser sans crainte ?

Quand contrainte rime avec shadow IT

Impossible de remplacer toute une flotte d'ordinateurs par des postes sans ports USB d'un claquement de doigts. Va-t-on fouiller les employés à l'entrée ? Coller des chewing-gums dans les prises ? Enfermer les unités centrales dans des caisses cadenassées ? « Personne n'est capable de contrôler l'intégralité des clés USB de l'entreprise, sauf à bloquer ou monitorer tous les périphériques du parc informatique » assure Marco Genovese, Product Manager Stormshield. On ne peut donc faire l'économie d'un peu de psychologie de base : si la méthode de substitution est trop contraignante, les employés auront vite fait d'en revenir à l'option la plus simple, autorisation ou non. Résultat : les collaborateurs auront recours à des outils sous les radars de la Direction des Systèmes d'Information – réveillant le spectre du fameux shadow IT. Des entreprises 100% Cloud existent déjà, mais sont de fait entièrement dépendantes de leur connexion réseau. Est-ce vraiment une solution ?

Could we use USB keys to detect cyberattacks?

For Adrien Brochot, Endpoint Security Product Leader at Stormshield, banning USB sticks is not a good idea. In addition to missing out on a convenient way of exchanging data in companies with segmented networks, "USB sticks can also function as an alert system". When a monitoring software program detects that a drive is no longer reliable, it serves as an alert of a potential cyberattack in progress.

In addition, setting up a generalised network can also allow cyberattacks to spread faster within a company once the first line of defence is breached. It is difficult to avoid USB sticks in companies despite the related security problems, and it's too risky to switch to an all-network approach despite the appeal of ease. But what if we could find the right protection tools for both devices and networks?

Using keys to combat human error

The biggest risk comes primarily from users. If a USB stick stays inside the same network of computers, all is well. However, this is rarely the case. It might seem insignificant, but an employee who transfers photos from his home computer onto a USB stick to then show colleagues at work can be very dangerous. The danger is that the device becomes infected from an external PC with inadequate defences: in general, viruses attack computers with the least protection.

In such situations, the countermove consists in using USB sticks and having a software program scan to track the movements of a stick within a fleet of computers. The approach is the same if a user deliberately inserts an infected stick. The stick is first inserted into an antivirus terminal, completely separate from any computer, which runs full analyses. This in turn generates a notion of trust. Once the stick has been scanned by the antivirus terminal, it can be used inside the computer network and the user can check that no files have been modified externally. However, as soon as data is transferred from a computer that does not have the tracking software installed, the trust is broken and the stick must be reanalysed by the antivirus terminal. The tracking software can easily be installed on a personal computer, so the approach is not as restrictive as it may appear.

Des clés USB pour détecter des cyberattaques ?

Pour Adrien Brochot, Product Leader Endpoint Security Stormshield, bannir les clés USB n'est donc pas une bonne idée. Outre le fait de se priver d'un moyen pratique d'échange de données dans des entreprises aux réseaux segmentés, « les clés USB peuvent aussi fonctionner comme des sonnettes d'alarmes ou des points de contrôle ». Dès qu'un logiciel de surveillance détecte qu'une clé n'est plus fiable, c'est le signal d'une cyberattaque potentielle en cours.

Par ailleurs, une mise en réseau généralisée peut également permettre aux cyberattaques de se diffuser plus vite à l'intérieur d'une entreprise, une fois la première ligne de défense franchie. Difficile de se passer de clés USB en entreprise malgré les problèmes de sécurité afférents ; trop risqué de passer au tout-réseau malgré l'attrait du confort. Et si l'idéal serait de ne pas avoir à choisir, en trouvant les bons outils de protection, côté clés comme côté réseau ?

L'enrôlement des clés contre l'erreur humaine

Le plus gros danger tient surtout aux utilisateurs. Tant qu'une clé demeure dans son parc, tout va bien ! Mais une promenade est si vite arrivée. Celle-ci peut paraître anodine, un employé peut simplement vouloir montrer ses photos de vacances à ses collègues après être allé les récolter chez lui. Le danger est de se faire infecter à l'extérieur du parc, en se connectant à un PC qui manque de défenses : en général, les attaques visent les ordinateurs les moins protégés.

Ici, la parade consiste à enrôler les clés, c'est-à-dire à demander à un logiciel de scanner et de suivre ensuite les déplacements d'une clé au sein d'un parc. La parade est la même si un utilisateur se connecte délibérément avec une clé vérolée, bien sûr. Une notion de confiance est créée : la clé passe d'abord par une « station blanche », poste à part équipé de plusieurs antivirus pour des analyses complètes. À chaque fois que la clé préalablement scannée par la station blanche est branchée sur un poste du parc, il est possible de vérifier qu'aucun fichier n'a été modifié à l'extérieur. En revanche, dès qu'un changement de données depuis un poste qui n'est pas équipé du logiciel de suivi des clés scannées a lieu, la confiance est rompue et une nouvelle analyse complète de la clé est nécessaire, auprès de la station blanche. La chose est moins contraignante qu'elle en a l'air : le logiciel de suivi peut tout à fait être installé sur un poste personnel.

The role of behavioural analysis

Stormshield Endpoint Security is another form of defence for user terminals. Designed to detect any attempt to take advantage of vulnerabilities and using resource control rules, it is able to block processes whose behaviour is malicious or altered by an attacker. If an infected USB stick enters the computer network, the erratic behaviour of the software that ensues is immediately identified. This protection technique, known as a Host Intrusion Prevention System, or HIPS, is able to block the attack.

However, it still needs some fine-tuning. HIPS sometimes have trouble blocking malicious activity when it consists of a succession of multiple actions that do not appear malicious individually. Endpoint Detection and Response (EDR) technology can extend and refine the detection of these cyberattacks. In the future, HIPS and EDR are likely to be used together and with enough protection of this type, there will be "no need to ban USB sticks," concludes Genovese. "IBM's idea of banning USB drives was primarily driven by concerns for their reputation, rather than cybersecurity. Can you imagine the damage that could be done if someone found a USB stick containing sensitive data from a company whose business is cybersecurity?" ¶

Le rôle des analyses comportementales

La solution Stormshield Endpoint Security est un autre outil de défense des postes utilisateurs : ses mécanismes de détection et de blocage d'exploitation de vulnérabilités, ainsi que ses règles de contrôle de ressources, permettent de détecter et bloquer des processus ayant des comportements malveillants ou altérés par un attaquant. Si une clé USB infectée entre dans le parc informatique, les comportements erratiques des logiciels qui s'ensuivent sont aussitôt identifiés. Cette technique de protection, nommée Host Intrusion Prevention System ou HIPS, est ainsi capable de bloquer l'attaque.

Mais cette dernière option reste également à perfectionner. Les HIPS ont parfois du mal à bloquer les actions malveillantes constituées d'une succession d'actions qui, dans leur unité, n'ont pas l'air malveillantes. La technologie Endpoint Detection and Response (EDR) permet ainsi d'étendre et d'affiner la visibilité face à ces cyberattaques. À l'avenir, HIPS et EDR sont voués à être complémentaires et avec suffisamment de protections de ce type, « inutile de se donner la peine de bannir les clés USB » conclut Marco Genovese. « L'idée d'IBM de bannir les clés USB est d'abord guidée par des considérations d'image, plus que de cybersécurité. Avez-vous déjà pensé aux dégâts possibles si quelqu'un trouvait une clé USB contenant des données sensibles d'une entreprise qui opère dans la cybersécurité ? » ¶

But who still uses Internet Explorer today?

Mais qui utilise encore Internet Explorer aujourd'hui ?

By Victor Poitevin – July 22, 2019

At the start of the year, Microsoft warned Internet users that using Internet Explorer posed risks: the browser is no longer updated and security flaws are accumulating. So are there still long-standing users of IE?

En début d'année, Microsoft a prévenu les internautes qu'utiliser Internet Explorer comportait des risques : le navigateur n'est plus mis à jour et cumule les failles de sécurité. Il y aurait donc des irréductibles qui utilisent encore IE ?

Abandoned around ten years ago in favour of Firefox and then Chrome, we imagined IE sacrificed on the altar of (many) waning digital stars. To the point of becoming a popular geek joke: while it weeps and asks "what is my purpose?" IE receives the response "you download Chrome". There is nothing more to say.

Délaissé depuis une dizaine d'années au profit de Firefox puis de Chrome, on pensait IE sacrifié sur l'autel des (nombreuses) stars déchues du numérique. Au point d'être devenu une blague geek populaire : alors qu'il se désole et demande « what is my purpose? », IE s'entend répondre « you download Chrome ». La messe est dite.

And yet, here we are in 2019 and many businesses are still using Internet Explorer for their internal web applications. Is this eccentricity? No. If businesses are still using IE, it is essentially due to habit, a lack of resources to migrate, or a lack of cyber awareness…

Et pourtant, nous sommes en 2019 et de nombreuses entreprises utilisent encore Internet Explorer pour leurs applications web internes. Excentricité ? Non. Si les entreprises utilisent encore IE, c'est essentiellement par habitude ou par manque de moyens de migrer. Et par manque de conscience cyber…

The rise and fall of Internet Explorer

"To understand, we need to go back to the arrival of IE 6 in 2001. Twenty years ago, IE was more or less the only browser that existed as it was provided with Windows", says Robert Wakim, Offers Manager at Stormshield. "At the same time, web development and its related technologies such as JavaScript and CSS were only just emerging. There was still no standard and Microsoft used its IE platform to enable its partners to provide third party applications to its clients." Businesses then developed internal applications that used the non-standardised mechanics internal to IE. They didn't know it yet but the battle of the browsers that would follow was going to impact their business.

Apogée et chute d'Internet Explorer

« Pour comprendre, il faut remonter à l'avènement d'IE 6, en 2001. Il y a vingt ans, IE était à peu près le seul navigateur qui existait parce qu'il était fourni avec Windows, rappelle Robert Wakim, Offers Manager Stormshield. Au même moment, le développement web et ses technologies associées, comme javascript et css, sont tout juste émergents. On n'a pas encore de standard et Microsoft se sert de sa plateforme IE pour permettre à ses partenaires de fournir des applications tierces à ses clients. » Les entreprises développent alors des applications internes qui reposent entièrement sur les mécaniques internes à IE, non standardisées. Elles ne le savent pas encore, mais la bataille des navigateurs qui va suivre va impacter leur activité.

Twenty years later, the top three web browsers are shaken up by the successive arrival of Firefox (2002) and Chrome (2008),. Today, Chrome is the leading

Vingt ans plus tard, le tiercé de tête des navigateurs web est chamboulé par l'arrivée successive de Firefox (2002) et

browser used worldwide (68% market share in March 2019), followed by Firefox (9%). Far from its past dominance, Internet Explorer plummeted to 7%. Result: businesses that have built their internal ecosystems on IE have inherited applications that cannot be operated on other browsers. "We find ourselves with two versions of web applications: the standardised version for everyone and the proprietary version for IE 6 and Microsoft. From a cybersecurity perspective, this poses real problems as it requires users of these applications to have IE 6 or the correct version of IE installed on their machine", warns Robert Wakim. However, these versions are no longer updated. Besides which Microsoft decided to bring an end to its browser.

RIP IE?

In February 2019, in an article entitled "The perils of using Internet Explorer as your default Internet browser", published on Microsoft's official blog, Chris Jackson warned that "Internet Explorer is not adapted to new Web standards, and even if many sites continue to run properly, the developers no longer test their site on there". "From a cybersecurity point of view, we are in the worst situation possible", says Robert Wakim. "That's to say that the technological building block that is used to support a company's business is no longer updated." A Zero-day vulnerability affecting IE 11 was discovered last April. A few months before, in December 2018, Microsoft had to release an emergency patch for Internet Explorer due to a critical vulnerability.

"It's an interesting situation", says Florian Bonnet, Product Management Director at Stormshield. "When you look closely, you notice that Microsoft continues to support IE from a security perspective at the time of serious flaws. They are capable of releasing patches to correct vulnerabilities. And if they do so, it's because they know very well that today there are many IE applications and they cannot afford to say that they will no longer do anything." Does Microsoft not abandon its vulnerable users due to the issue of image or because it has a real awareness of cybersecurity? The debate is under way.

"From a cybersecurity point of view, we are in the worst situation possible"

Robert Wakim
Offers Manager, Stormshield

Chrome (2008). Aujourd'hui, Chrome est le premier navigateur utilisé dans le monde (68% de parts de marché en mars 2019), suivi de Firefox (9%). Bien loin de son hégémonie passée, Internet Explorer plonge à 7%. Résultat : les entreprises qui ont bâti leur écosystème interne sur IE héritent d'applications qui ne sont pas exploitables sous d'autres navigateurs. « On se retrouve avec deux versions d'applicatifs web : la version standardisée pour tout le monde et la version propriétaire pour IE 6 et pour Microsoft. Dans une perspective de cybersécurité, cela pose de vrais problèmes puisque cela oblige les utilisateurs de ces applications à avoir IE 6 ou avoir un IE de la bonne version installé sur leur machine », prévient Robert Wakim. Or, ces versions ne sont plus mises à jour. Sans compter que Microsoft a décidé à en finir avec son navigateur.

RIP IE ?

En février 2019, dans un billet intitulé « Les périls d'utiliser Internet Explorer comme votre navigateur internet par défaut », publié sur le blog officiel de Microsoft, Chris Jackson prévenait que « Internet Explorer n'est pas adapté aux nouvelles normes du Web, et même si de nombreux sites continuent de fonctionner correctement, les développeurs n'y testent plus leur site ». « D'un point de vue cybersécuritaire, on est dans la pire situation possible, alerte Robert Wakim. C'est-à-dire que la brique technologique qui est utilisée pour supporter le business d'une entreprise n'est absolument plus mise à jour. » Une faille Zero-day touchant IE 11 a ainsi été découverte en avril dernier. Un peu plus tôt, en décembre 2018, Microsoft a dû sortir un patch en urgence pour Internet Explorer à cause d'une faille critique.

« C'est une situation intéressante, analyse Florian Bonnet, Directeur du Product Management Stormshield. Quand on regarde attentivement, on s'aperçoit que Microsoft continue de supporter IE d'un point de vue sécurité lors de failles graves. Ils sont capables de faire des patchs pour corriger des vulnérabilités. Et s'ils le font, c'est parce qu'ils savent très bien qu'aujourd'hui, il existe un parc d'applicatifs IE et ils ne peuvent pas se permettre de dire qu'ils ne font plus rien. » Ne pas laisser les utilisateurs exposés serait alors un enjeu d'image ou une réelle conscience de cybersécurité chez Microsoft ? Le débat est ouvert.

How many IE applications are there exactly? Who still uses IE? It's difficult to say. "There is no particular sector, we find IE used in administration as well as in health or industry for example", says Florian Bonnet. "It is complicated to estimate the percentage of businesses that use IE. It concerns applications used internally, so we don't have any data on this", says Robert Wakim, who states however that: "we are talking about internal software, which has very often been customised for the company: intranet, accounting software, stock management software, etc." Strategic applications for the business which, if they were compromised, could bring all or part of its activity to a standstill.

Migrate or stay with IE?

Nevertheless, the businesses concerned have an ever decreasing window of opportunity to adapt as Internet Explorer security updates are expected to end by 2025. First response: protect your user station. A solution such as Stormshield Endpoint Security is based on behavioural analysis that can quickly identify a series of malicious actions and therefore detect an attack and react.

Another possible option: put Internet Explorer in a virtual machine and ask its users to start it when they need the application. "This makes it possible to create a clean version of IE each time it is used", says Robert Wakim. "But it is a short-term solution. It is clear that in the long term, the only way of maintaining security is to migrate to other browsers, which means fully rebuilding the entire application."

For some businesses or institutions, this can be up to 40 or 50 applications, with the issue of competitiveness and maintaining the activity beyond. Better to anticipate and start now. "They have six years to secure a budget and migrate their applications", says Florian Bonnet. "2025 will soon be upon us. And the more the internal software is complicated, the more time will be needed for analysis, redesign, development, migration of old data, validation and adoption, etc. We are working on projects that will easily take 24 or 36 months", warns Robert Wakim. And what if businesses do nothing? According to Florian Bonnet, they run a real risk: "They may continue to use IE internally but they will no longer have any security patches. They will use it at their own risk." ¶

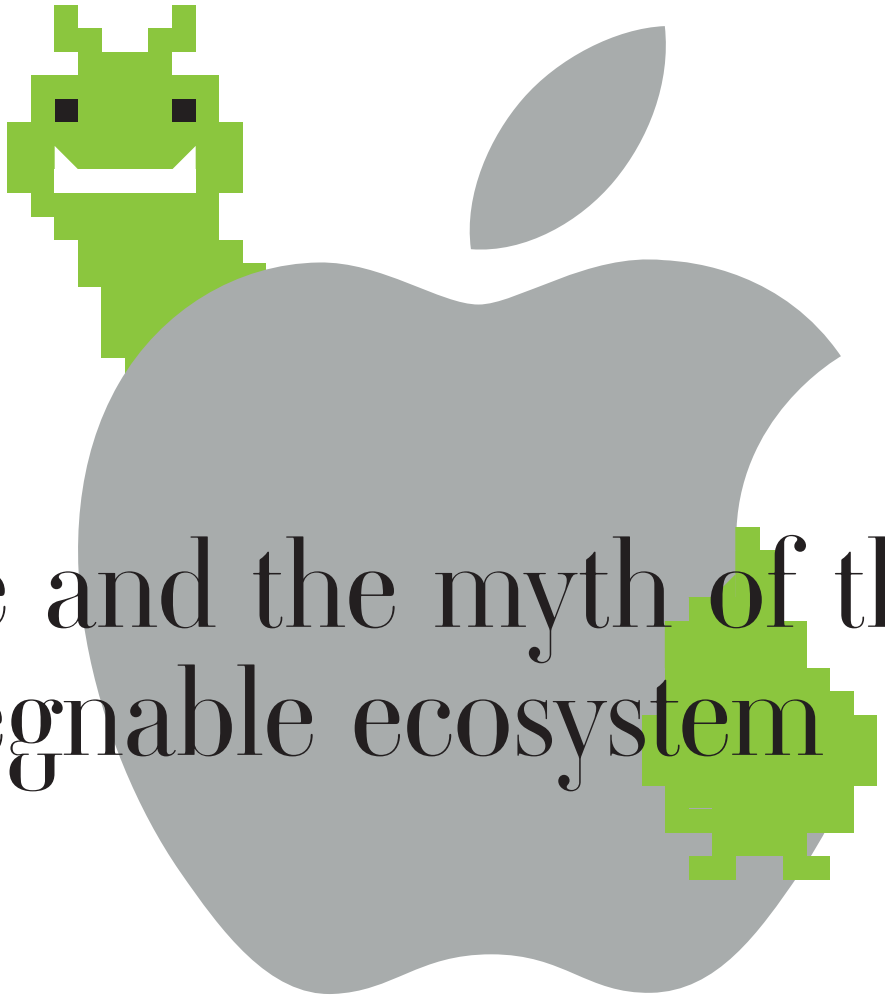
Quelle est la taille de ce parc justement ? Qui utilise encore IE ? Difficile à dire. « Il n'y a pas de secteur en particulier, on trouve aussi bien IE dans l'administration que dans la santé ou l'industrie par exemple », souligne Florian Bonnet. « La part d'entreprises qui utilisent IE est compliquée à évaluer. Il s'agit d'applications à usage interne, donc nous n'avons pas de données dessus », abonde Robert Wakim, qui précise toutefois : « on est sur des logiciels internes, qui ont très souvent été faits sur mesure pour l'entreprise : intranet, logiciel de comptabilité, de gestion de stock… » Des applicatifs stratégiques pour l'entreprise qui, s'ils étaient compromis, pourraient paralyser tout ou partie de son activité.

Migrer ou rester sous IE ?

Or, les entreprises concernées ont une fenêtre de tir de plus en plus réduite pour s'adapter puisque la fin des mises à jour de sécurité d'Internet Explorer est attendue à horizon 2025. Premier réflexe : protéger son poste utilisateur. Une solution comme Stormshield Endpoint Security repose sur une analyse comportementale qui permet d'identifier rapidement une suite d'actions malveillantes, donc de détecter une attaque et de réagir.

Autre option possible : mettre Internet Explorer dans une machine virtuelle et demander à ses utilisateurs de la lancer quand ils ont besoin de l'applicatif. « Cela permet de créer une version propre d'IE à chaque utilisation, souligne Robert Wakim. Mais c'est une solution à court-terme. Il est évident qu'à long terme, la seule façon de se maintenir en condition de sécurité est de migrer vers les autres navigateurs, ce qui implique de refaire intégralement tout l'applicatif. »

Pour certaines entreprises ou institutions, cela peut représenter jusqu'à 40 ou 50 applicatifs, avec un enjeu fort de compétitivité et de maintien de l'activité derrière. Mieux vaut anticiper et commencer dès aujourd'hui. « Il leur reste six ans pour trouver un budget et migrer leurs applications », insiste Florian Bonnet. « 2025 va arriver vite. Et plus les logiciels internes sont compliqués, plus ils vont nécessiter de temps d'analyse, de redesign, de développement, de migration des anciennes données, de validation et d'adoption... On est facilement sur des projets qui vont prendre 24 voire 36 mois », prévient Robert Wakim. Et si les entreprises ne font rien ? Pour Florian Bonnet, elles courent un vrai risque : « Elles pourront continuer à utiliser IE en interne mais elles n'auront plus de patch de sécurité. À leurs risques et périls. » ¶



Apple and the myth of the impregnable ecosystem

By Victor Poitevin – February 19, 2019

With its locked ecosystem and skilfully orchestrated communications, Apple is fine-tuning its image as the unassailable fortress. But when it comes to cybersecurity, nobody is invulnerable.

"What happens in your iPhone stays in your iPhone". People attending the CES were met with this message, in white letters, on a huge black billboard covering 13 floors. A major communications operation by Apple to publicise its ecosystem and present itself as a staunch defender of privacy. Alas, a mere three weeks later, the company was forced to admit to a major security loophole on FaceTime which meant that iPhone conversations could be listened to without the users' knowledge. This was immediately followed by the news that MacOSX was infected by CookieMiner, a malware that

Apple ou le mythe de l'écosystème inviolable

Avec son écosystème verrouillé et sa communication savamment orchestrée, Apple peaufine son image de citadelle inattaquable. Mais en matière de cybersécurité, personne n'est invulnérable.

"What happens in your iPhone stays in your iPhone". Sur un gigantesques panneau noir déployé sur 13 étages, voici le message en lettres blanches qu'ont pu lire les visiteurs du CES cette année. Une grande opération de communication d'Apple pour promouvoir son écosystème et se poser en ardent défenseur de la privacy. Las, à peine trois semaines plus tard, l'entreprise a dû reconnaître une importante faille de sécurité sur FaceTime permettant d'écouter des utilisateurs d'iPhone à leur insu. Dans la foulée, MacOSX a été infecté par le malware CookieMiner, une attaque permettant de

hacked and stole cryptocurrencies held by its victims. And after the discovery of a Zero-day vulnerability on the new version of macOS, Mojave, the start of 2019 alone confirms that, when it comes to security, nobody is invulnerable. Not even the apple brand.

The myth of Apple's inviolability

Apple, however, has long been considered to be a tamper-proof system. There are three main reasons for this myth, according to David Gueluy, Innovation Leader at Stormshield. "Historically, Apple was initially exempted from attack because it had fewer users than Microsoft and therefore was not a prime target. Next, Apple's closed ecosystem creates the illusion of control and immunity to attacks. Finally, privacy protection has become a selling point for Apple, who make a lot of references to it, thus reinforcing in people's minds an association between Apple and the concept of security."

But, for several years now, Apple has repeatedly been a target for attacks. The successes of the iPhone and MacBook have boosted the number of Apple ecosystem users and their profile – mostly upper socio-professional category and VIP – is sharpening appetites. "Cyberattacks are often financially motivated," says David Gueluy. As a result, the vulnerability discovered on Apple's products is on the rise, sometimes attracting significant media attention, such as the 2014 iCloud hack, when several Hollywood stars had their data compromised and their privacy violated. "The iCloud case is emblematic because it reminds us that security is a global issue: we tend to think mostly in terms of hardware (smartphone, tablet, computer), yet all the services and softwares we use bring additional risks," notes David Gueluy.

The App Store, a nest of spies

This is enough to make some people say the Mac user is no better protected than a Windows user. You only have to glance at the National Vulnerability Database to see that the Apple ecosystem also has its share of CVE (Common Vulnerabilities and Exposures).

> **"All the services and softwares we use bring additional risks."**
>
> **David Gueluy**
> **Innovation Leader, Stormshield**

pirater et de voler les cryptomonnaies détenues par les victimes. Et après la découverte d'une vulnérabilité Zero-day sur la nouvelle version de macOS, Mojave, le début d'année 2019 confirme à lui seul qu'en matière de sécurité, personne n'est invulnérable. Pas même la marque à la pomme.

Le mythe de l'inviolabilité d'Apple

Pourtant, Apple a longtemps été perçu comme un système inviolable. Un mythe qui s'explique par trois grandes raisons, selon David Gueluy, Innovation Leader Stormshield. « Historiquement, Apple a d'abord été épargné par les attaques parce qu'il comptait moins d'utilisateurs que Microsoft ; il n'était donc pas une cible de choix. Ensuite, l'écosystème fermé d'Apple donne une illusion de maîtrise et d'imperméabilité aux attaques. Enfin, la protection de la vie privée est devenu un argument commercial d'Apple, qui communique beaucoup dessus et renforce ainsi dans les esprits une association entre Apple et la notion de sécurité. »

Mais depuis plusieurs années, Apple est devenu une cible récurrente des attaques. Les succès de l'iPhone et du MacBook ont dopé le nombre d'utilisateurs de l'écosystème Apple, et leur profil – plutôt CSP+ et VIP – aiguise les appétits. « La motivation des cyberattaques est souvent pécuniaire », rappelle David Gueluy. Résultat : les vulnérabilités découvertes sur les produits d'Apple se multiplient, parfois avec un fort écho médiatique, comme le piratage d'iCloud en 2014, où plusieurs stars hollywoodiennes avaient vu leurs données compromises et leur intimité exposée. « Le cas d'iCloud est emblématique car il rappelle que la sécurité est un problème global : on a tendance à beaucoup penser matériel (smartphone, tablette, ordinateur), or tous les services et logiciels utilisés apportent des risques supplémentaires », note David Gueluy.

L'App Store, nid d'espions

De quoi faire dire à certains que l'utilisateur Mac n'est pas plus protégé qu'un utilisateur Windows. Un coup d'œil au National Vulnerability Database suffit pour constater que l'écosystème Apple connaît lui aussi son lot de CVE (Common Vulnerabilities and Exposures).

Currently, a third of attacks target mobiles. Android might still be the most targeted OS but iOS is just as susceptible. But before the CookieMiner malware put in an appearance in 2019, we already had, in no particular order, the XCodeGhost malware (which infected more than 4,000 App Store applications according to FireEye), Pegasus spyware, the Acedeceiver Trojan and also the KeRanger ransomware.

The Apple user, a primary vulnerability factor

"Ecosystems are becoming increasingly reliable. Nowadays the user is the most vulnerable entry point," according to one of Stormshield's security researchers. However, everyone can follow some simple good practices in order to limit risks. "Like all publishers, Apple has dedicated teams who work to resolve vulnerabilities. The most important cybersecurity habit is regular updating," he asserts.

At a minimum, you should never download suspicious attachments, you should use two-factor authentication, set a strong password and change it regularly. And, of course, don't install applications without knowing their source. "You either have to download it from the App Store or go and find it on the publisher's official website," notes the cybersecurity specialist. If you want to avoid ending up with a malicious application, always check the publisher's identity to see if it is the same as other applications in the store, have a look at the comments and, most importantly, check the price. If the application is much less expensive than expected, be wary. "It's the same as the rules for vigilance regarding phishing," says Julien Paffumi, Product Marketing Manager at Stormshield. "If it's too good to be true, it's definitely a trap!"

And this trend no longer only applies to personal use. With increased power, new features and effective marketing campaigns, Apple's various products are finding their place in businesses. Where these businesses are concerned, more advanced solutions allow protection on several levels. Like a firewall that protects network traffic by filtering data feeds in order to detect dangerous sites and content. Or like encryption solutions, that protect data on MacBook and other iPhones. ¶

Désormais, un tiers des attaques ciblent les mobiles. Si Android reste l'OS le plus visé, iOS est également vulnérable. Avant l'arrivée du malware CookieMiner en 2019, citons pêle-mêle le malware XCodeGhost (qui aurait infecté plus de 4 000 applications de l'App Store selon FireEye), le spyware Pegasus, le cheval de Troie Acedeceiver ou encore le ransomware KeRanger.

L'utilisateur Apple, premier facteur de vulnérabilité

« Les écosystèmes sont de plus en plus robustes. Aujourd'hui, le point d'entrée le plus vulnérable, c'est l'utilisateur », souligne un chercheur en sécurité chez Stormshield. Il existe pourtant des bonnes pratiques simples que chacun peut mettre en œuvre pour limiter les risques. « Comme tous les éditeurs, Apple a des équipes dédiées qui travaillent à la résolution des vulnérabilités. La pratique de cybersécurité numéro une est donc de se mettre régulièrement à jour », rappelle-t-il.

Ne pas télécharger de pièce-jointe suspecte, opter pour une authentification à deux facteurs ou encore définir un mot de passe fort et en changer régulièrement sont également des réflexes basiques à avoir. Et, bien sûr, n'installer que des applications dont on connaît la source. « Il faut soit la télécharger de l'App Store, soit aller la chercher sur le site officiel de l'éditeur », note encore ce spécialiste en cybersécurité. Pour éviter de se retrouver avec une application malveillante, on contrôle l'identité de l'éditeur, pour voir s'il s'agit bien du même que celui d'autres applications dans le store, on regarde les commentaires et surtout… son prix. Si l'application est beaucoup moins chère que le prix attendu, c'est suspect. « Il s'agit des mêmes règles de vigilance que pour le phishing, résume Julien Paffumi, Product Marketing Manager Stormshield. Si c'est trop beau pour être vrai, c'est très certainement un piège ! »

Et le phénomène ne concerne plus seulement les usages personnels. Avec une puissance accrue, de nouvelles fonctionnalités et des campagnes marketing efficaces, les différents produits Apple trouvent leur place dans les entreprises. Pour ces entreprises, des solutions plus poussées permettent de se protéger sur plusieurs niveaux. D'une part, un pare-feu protège le trafic réseau en filtrant les flux pour repérer les sites et contenus dangereux. Et d'autre part, des solutions de chiffrement pour protéger les données sur MacBook et autres iPhones. ¶

Top 6 most surprising entry points for cyberattacks

Top 6 des points d'entrée de cyberattaques les plus inattendus

By Victor Poitevin – September 02, 2019.

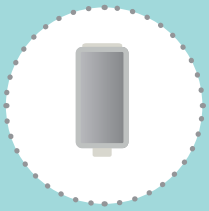
Whether at home or at work, hackers are becoming ever more ingenious when it comes to getting into IT networks. They exploit the vulnerabilities of susceptible smart devices to come up with cyberattacks which use very imaginative entry points. Synopsis of the most surprising entry points.

All the smart devices in your private and professional life represent a potential threat as long as manufacturers fail to incorporate security measures at the design stage. But, in addition to this "Security by design" approach, it is essential to maintain these devices in safe operating condition throughout their life cycle. And, therefore, users must be educated in a basic level of digital health. But that's another story.

Que ce soit au domicile ou sur le lieu de travail, les hackers redoublent d'ingéniosité pour infiltrer les réseaux informatiques. Exploitant les failles d'objets connectés souvent vulnérables, ils imaginent des cyberattaques aux points d'entrée pour le moins originaux. Tour d'horizon des plus inattendus.

Tous les objets connectés présents dans votre vie personnelle ou professionnelle représentent donc une menace potentielle tant que leurs constructeurs n'intégreront pas la sécurité dès la phase de conception. Mais en plus de cette approche « security-by-design », il est fondamental de maintenir ces objets dans des conditions opérationnelles de sécurité tout au long de leur cycle de vie. Et donc d'éduquer les utilisateurs à une certaine hygiène numérique. Mais ça, c'est une autre histoire…

AN ELECTRIC WATER HEATER

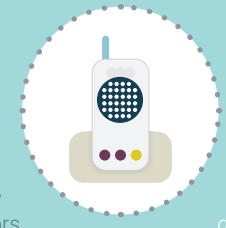


Researchers at Princeton University have simulated a scenario that could easily occur in the privacy of our own homes. In this sort of attack, hackers take control of power-hungry devices in order to disrupt the electricity network. According to this study, only 42,000 electric water heaters would be required to take down 86% of the Polish electrical grid. It's a chilling thought.

UN CHAUFFE-EAU ÉLECTRIQUE

Des chercheurs de l'Université de Princeton ont testé un scénario qui pourrait bien se dérouler dans l'intimité de nos propres maisons… Durant cette attaque, les hackers prennent le contrôle d'appareils énergivores afin de déstabiliser le réseau électrique. D'après cette étude, seuls 42 000 chauffe-eaux électriques suffiraient à couper 86% du réseau électrique polonais. De quoi en refroidir plus d'un.

A BABY MONITOR

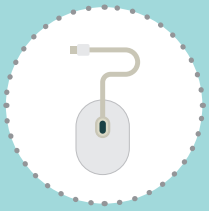


And, while on the subject of our homes, it was partly by hacking baby monitors that hackers orchestrated a distributed denial of service (DDoS) attack against Dyn in 2016. By overloading this service provider's servers, attackers managed to make some sites, including the very popular Twitter, Amazon and Airbnb, inaccessible for nearly 12 hours.

UN BABYPHONE

Toujours au cœur de nos habitations, c'est en partie en piratant des babyphones que des hackers ont dirigé une attaque par déni de service distribué (DDoS) contre la société Dyn en 2016. En saturant les serveurs de ce prestataire de service, les attaquants ont réussi à rendre certains sites inaccessibles dont les très populaires Twitter, Amazon ou encore Airbnb, et ce, pendant près de 12 heures.

A COMPUTER MOUSE

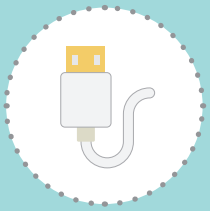


Whether it sits on your desk at work or at home, the mouse seems harmless. That's why Netragard, the IT security audit specialists, came up with the idea of hacking into one for the purpose of embedding spyware. It was sent as a promotional package to an employee and, once plugged in, it connected to a third-party server. Mission accomplished for Netragard, who were engaged by the company in question to investigate possible security vulnerabilities.

UNE SOURIS D'ORDINA-TEUR

Qu'elle trône sur votre bureau au travail ou à la maison, la souris paraît inoffensive. C'est pourquoi la société Netragard, spécialisée dans l'audit de sécurité informatique, a eu l'idée d'en pirater une pour y intégrer un logiciel espion. Envoyée sous forme de colis publicitaire à un employé, elle s'est connectée à un serveur tiers après branchement. Mission accomplie pour Netragard, missionné par l'entreprise en question pour rechercher d'éventuelles failles de sécurité…

A USB CABLE



We are often wary of USB sticks that we connect to our computer but did you know that USB cables can be compromised? So be extra careful the next time you go to use a USB device that you have received as a freebie at some event or that someone has loaned you.

UN CÂBLE USB

On se méfie souvent des clés USB que l'on connecte à son ordinateur mais saviez-vous que des câbles USB peuvent être corrompus ? Redoublez donc d'attention la prochaine fois que vous utiliserez un objet USB reçu en cadeau sur un événement ou prêté par quelqu'un.

AN AQUARIUM THERMOMETER

Hackers have used the smart thermometer from a North American casino aquarium to gain access to their data. Once again, this demonstrates that vulnerability can often be found in "gadgets" that aren't covered by the general security policy.

UN THERMOMÈTRE D'AQUARIUM

Des hackers ont utilisé le thermomètre connecté de l'aquarium d'un casino nord-américain pour accéder à ses données. La preuve encore une fois que la vulnérabilité réside souvent dans des « gadgets » non couverts par la politique de sécurité globale.

A FAX MACHINE

You thought the fax machine was obsolete? You were wrong! Nearly 17 billion faxes are still sent each year, especially in the health sector which processes a large volume of sensitive data. This information has not escaped the attention of the hackers who target these devices' vulnerabilities as a way of getting into an organisation's networks. You think you're protected because you've gone over completely to printers? Maybe you should check that your printer doesn't have a fax function!

UN TÉLÉCOPIEUR

Vous pensiez que le télécopieur était dépassé ? Détrompez-vous, près de 17 milliards de fax sont encore envoyés chaque année, notamment dans le secteur de la santé qui traite une grande quantité de données sensibles. Cette information n'a pas échappé aux hackers qui ciblent les vulnérabilités de ces appareils pour infiltrer les réseaux des entreprises. Vous vous pensez protégés car vous êtes passés au tout imprimante ? Vérifiez que votre machine n'intègre pas une fonction télécopie…

Digital transformation of companies:

2019 edition

The digital transformation of businesses: maturity and numerous questions

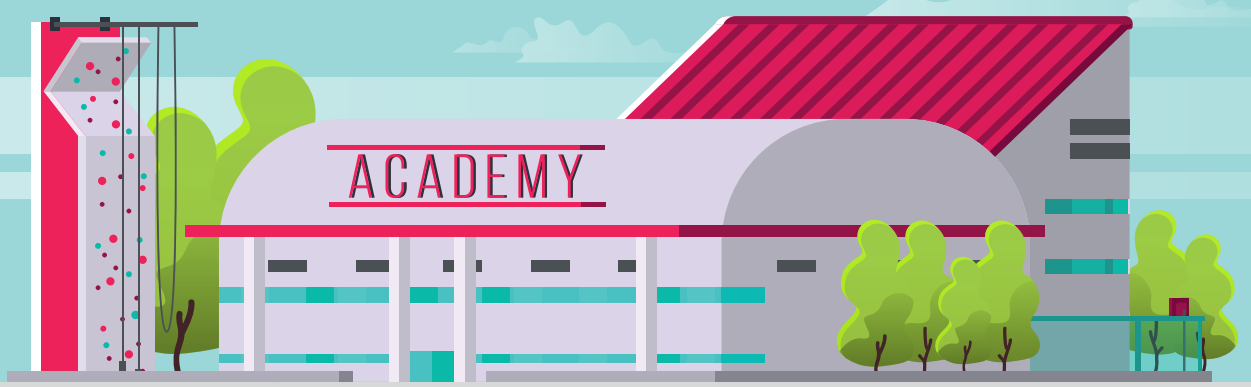
How are IT Departments, General Managers and Business Departments dealing with this transformation and the risks it entails? Which strategies, means and resources are being deployed? How can we prepare for tomorrow today? Discover our second barometer survey for some proposed answers to these questions.

Transformation numérique des entreprises : une maturité en questions

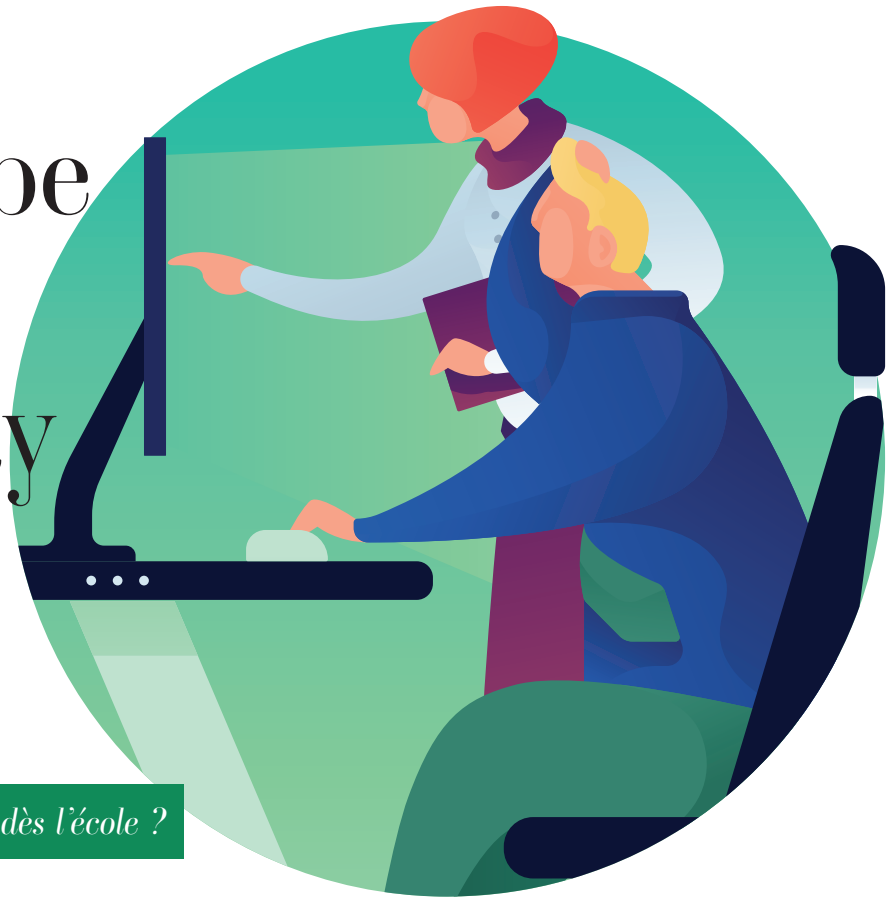
Comment les Directions Informatiques, les Directions Générales et les Directions Métiers appréhendent-elles cette transformation et les risques qu'elle engendre ? Quelles stratégies de moyens sont mises en oeuvre ? Comment préparer demain dès aujourd'hui ? Éléments de réponse à retrouver dans la deuxième édition de notre baromètre.

The topic of cybersecurity training and exchanges

La question de la formation et des échanges en cybersécurité



Should we be teaching cybersecurity in school?



Et si la cybersécurité devait s'enseigner dès l'école ?

By Victor Poitevin – September 9, 2019

It will soon be 2020, and human beings are still the weakest link in any cyberattack. Too many of us still lack digital health training, and are unwittingly exposing themselves to easily avoidable risks. But cybersecurity is an issue of national importance, so shouldn't it be taught at school?

The world is divided into two categories: those able to walk resolutely past a discarded USB stick, and those who will calmly plug it into their computer to see what will happen. Clearly, we all have different understandings and responses when it comes to cybersecurity.

However, the aforementioned USB stick is just one example. After all, some people have little awareness of the risks they are taking, and cause their company endless problems by circulating their personal data on the internet, illegally downloading files, using a plethora of smart objects... or simply replying to an email. "In terms of cybersecurity, there's a sad lack of a consistent approach across French society", says Sylvie Blondel, Human Resources Director at Stormshield. "I remem-

Nous sommes bientôt en 2020 et l'humain est toujours le maillon faible d'une cyberattaque. Trop de personnes manquent encore d'hygiène numérique et s'exposent sans le savoir à des risques facilement évitables. Puisque la cybersécurité est un enjeu national, ne devrait-on pas l'enseigner dès l'école ?

Le monde se divise en deux catégories : ceux qui continuent leur chemin face à une clé USB abandonnée, et ceux qui la ramassent avant de la brancher sur leur ordinateur sans trembler. À l'évidence, en matière de cybersécurité, nous n'avons pas tous les mêmes connaissances ni les mêmes réflexes.

Mais cette clé USB n'est qu'un exemple parmi d'autres. Certaines personnes ont en effet peu conscience des risques qu'elles prennent ou font courir à leur entreprise en semant leurs données personnelles sur Internet, en téléchargeant illégalement des fichiers, en multipliant les objets connectés ou en répondant à un simple email. « En matière de cybersécurité, il y a un vrai manque de culture globale dans toute

ber a train journey I took, where the passenger next to me had got up from their seat, leaving their computer switched on and the current session open… People aren't aware of the risks, because it's a world that we see as purely virtual. But the virtual world can have an impact on real life."

> **"There's a sad lack of a consistent approach across French society"**
>
> **Sylvie Blondel**
> **Human Resources Director, Stormshield**

And contrary to popular belief, any data is a potential target for hacking. Or blocking. "Firstly, some people think their data is of no interest or value, so no-one will take the trouble. And secondly, in some attacks, the attackers aren't even interested in your data, but simply in blocking your activities", warns Xavier Prost, Training Manager at Stormshield. "And then thirdly, you could even be collateral damage in an attack which is not aimed directly at you — but will lock you out anyway because you don't have enough protection. As they lock or steal your data, these cyberattacks will prevent you from conducting your business." Ransomware, spyware, scareware, trojans, credential stuffing... computer viruses can take many different forms as they infect your networks and devices. But would you have fallen into the trap if you had been properly informed?

Maths, history, geography, sports and... cybersecurity?

What if it all started in school? If we want to make sure everyone understands the essentials of cybersecurity, and change (bad) habits, shouldn't we start raising awareness as early as possible? After all, the process of preparing children for tomorrow's world includes a digital education. And just as some schools run coding and computer literacy classes, there could be good arguments for holding "digital health" classes to teach children to adopt good cybersecurity practices. "I really believe schools have a role to play in cybersecurity education; not only to teach how the internet works, but also to discover new potential areas of work", Sylvie insists. However, some objections need to be overcome first... "Parents are often reluctant because they believe their children are already overexposed to screens. But I think that rather than trying to get rid of screens, we should be providing education about them. Children

la société française, analyse Sylvie Blondel, Directrice des Ressources Humaines Stormshield. Je me souviens d'un voyage en train où le passager à côté de moi avait quitté son siège mais avait laissé son ordinateur allumé, avec sa session ouverte… Les gens ne se rendent pas comptent des risques parce que c'est un monde qui nous semble virtuel. Or, le virtuel a un impact dans la vie réelle. »

Et contrairement aux idées reçues, toute donnée est bonne à pirater. Ou à bloquer. « D'une part, certaines personnes pensent que leurs données ne sont pas intéressantes ou inutiles, donc que personne ne va les embêter. Et d'autre part, dans certaines attaques, ce ne sont même pas vos données elles-mêmes qui intéressent les assaillants, mais simplement de bloquer votre activité, prévient Xavier Prost, Responsable Formation Stormshield. Troisième possibilité, vous pouvez être même le dommage collatéral d'une attaque qui ne vous cible pas directement – mais qui va vous bloquer tout de même car vous n'êtes pas suffisamment protégé. En verrouillant ou en volant vos données, ces cyberattaques vont vous empêcher d'exercer votre activité. » Ransomware, spyware, scareware, trojan, credential stuffing… les virus informatiques peuvent prendre de nombreuses formes pour infecter vos réseaux et vos terminaux. Mais seriez-vous tombés dans le panneau si vous aviez été sensibilisés ?

Français, maths, histoire-géo, sport, anglais et… cybersécurité ?

Et si tout commençait dès l'école ? Pour s'assurer que chacun dispose des bases en matière de cybersécurité et changer les (mauvaises) habitudes, ne faudrait-il pas commencer à sensibiliser le plus tôt possible ? Après tout, préparer les enfants au monde de demain, cela signifie aussi les éduquer au numérique. Tout comme il existe déjà des cours de codage et de sensibilisation au langage informatique dans certaines écoles, on pourrait envisager des cours d'hygiène numérique, pour inculquer aux enfants les bons réflexes de cybersécurité. « Je suis intimement persuadée que l'école a un rôle à jouer dans l'éducation à la cybersécurité, à la fois pour comprendre comment fonctionne Internet mais aussi pour découvrir de nouveaux métiers », défend Sylvie Blondel. À condition de lever quelques freins… « Souvent les parents sont réticents car ils estiment que leurs enfants sont trop exposés aux écrans. Or, je pense qu'il ne faut pas chercher à

are already immersed in that world, so they might as well learn how to use it!"

A Statista study looking at the proportion of 8-14-year-olds using a mobile phone in France in 2018 emphasises the extent to which the device is ingrained in their habits. This is confirmed by Florian Bonnet, Product Management Director at Stormshield, who volunteers at primary and secondary schools to educate the youngest children in cybersecurity issues. "This work has taught me that more than 90% of children are online, and no one social environment is more exposed than any other", he notes.

Hyperconnected kids

Smartphones (their own, or their parents'), games consoles, televisions, home computers... all ways in which kids are exposed to screens every day. According to a 2018 digital survey, the percentage of smartphone-carrying French children in the 12-and-over segment has risen sharply since 2011 (+58 points), reaching 75% in 2018. They have also mastered the art of downloading new apps, playing online games and communicating on social networks that are (at least theoretically) closed to them. "Children are every bit as skilled at their parents – and possibly even more so – at creating multiple accounts and circumventing age restriction rules to create accounts on social media or accessing sites and media that are officially closed to them", Florian warns.

"When targeting children or teenagers, attackers develop ruses to encourage them to click on links."

Florian Bonnet
Product Management Director, Stormshield

And if you think parental control filters will be enough... think again! The parental controls implemented on set-top boxes and computers are often not "granular" enough. Instead, they are often too restrictive at times when students need to do online research for their homework. The result: they often end up being disabled.

And most importantly, children have their own way of seeing things. Although they might be reluctant to lend their pen or eraser to a friend, they will still willingly share their internet connection and login details with others! "When I talk to them about the risks,

supprimer les écrans, mais éduquer aux écrans. Les enfants baignent déjà dedans, autant qu'ils apprennent vraiment à s'en servir ! »

Une étude Statista sur la part des 8-14 ans qui utilisent un téléphone mobile en France en 2018 souligne à quel point ce terminal est ancré dans les habitudes. Ce que confirme Florian Bonnet, Directeur du Product Management Stormshield, qui intervient bénévolement dans des classes de primaire et au collège pour sensibiliser les plus jeunes à la cybersécurité. « Ces interventions m'ont appris que plus de 90% des enfants sont connectés, il n'y a pas de milieu social plus exposé qu'un autre », note-t-il.

Des enfants déjà hyperconnectés

Smartphone personnel ou parental, console de jeu, télévision, ordinateur du foyer… les enfants sont quotidiennement exposés aux écrans. Selon le baromètre du numérique 2018, le taux d'équipement en smartphone des Français de 12 ans et plus a très nettement progressé depuis 2011 (+58 points) pour atteindre 75% en 2018. Ils maîtrisent également l'art de télécharger de nouvelles appli, de jouer en ligne ou de communiquer sur les réseaux sociaux qui leur sont pourtant, en théorie, interdits. « Les enfants, sont aussi compétents que leurs parents, voire plus, pour se créer des comptes à gogo et transgresser les règles de déclaration de leur âge pour se créer un compte sur des réseaux sociaux ou accéder à des sites ou médias qui leur sont officiellement interdits », prévient Florian Bonnet.

Et ne pensez pas que le filtre du contrôle parental suffit ! Les contrôles parentaux mis en place sur les box ou ordinateurs ne sont souvent pas assez « fins ». À l'inverse, ils sont parfois trop restrictifs lorsque les élèves doivent faire des recherches sur Internet pour leurs devoirs. Résultat : ils finissent souvent par être désactivés.

Surtout, les enfants ont leur propre logique. Autant ils sont réticents à prêter leur stylo ou leur gomme à un camarade, autant ils partagent sans problème leur connexion internet et leurs identifiants ! « Lorsque je leur parle des risques, ils répondent souvent "mais je fais attention ! Je n'échange qu'avec

they often answer, "Yes, but I'm careful... I only share things with friends!", Florian smiles. Ah, yes... friends! My friend's friend's friend's friend... But how well do they really know their friend? At that age, the concept of friendship is flexible, and therefore very broad. To say nothing of the USB sticks picked up on the way to school and handed around, which sometimes end up connected to their parents' PCs..."

Children: a key target for cybercriminals

As you'll already have realised, when it comes to cybersecurity, awareness among children is a flexible concept, even though some campaigns seem to have paid off. "Children are aware mainly of risks associated with child pornography or cyber-bullying", notes Florian, "but they are extremely naive when it comes to cyberattacks."

Cybercriminals make use of this, and tailor their methods. "In situations where they would usually send phishing emails or simple links in the hope that the end user will click on them, when targeting children or teenagers, attackers develop ruses (free games, or free extras for their favourite games, etc.) to encourage them to click on links", warns Florian.

Having read this far, no doubt you're considering the option of simply cutting off all of your children's internet access. If so, think again. "They'd find a way around such a ban in any case. And by depriving children of access to the internet, we deprive them of an enormous wealth of information and communication options", Florian claims. "And that's where we, as cybersecurity professionals, have a role to play. And that role is to educate our young people about the risks they face."

Working with teachers to demystify cybersecurity

For his part, Xavier Prost believes that "if we want to reach all children, the initiative also needs to be implemented at government level. Companies can work

"If teaching teams are not familiar with best practices themselves, they will not be able to pass them on to their students."

Xavier Prost
Training Manager, Stormshield

des amis !", sourit Florian Bonnet. Les fameux amis ! L'ami de mon ami de mon ami de mon ami… Mais connaissent-ils vraiment cet ami ? À leur âge, la notion d'amitié est souvent une relation transitive, donc très large. Sans parler des clés USB récupérées sur le chemin de l'école ou échangées entre eux pour parfois finir connectées au PC de leurs parents… »

Les enfants, une cible privilégiée des cybercriminels

Vous l'aurez compris, en matière de cybersécurité, les enfants ont une conscience à géométrie variable, même si certaines campagnes de sensibilisation semblent avoir porté leurs fruits. « Les enfants ont plutôt conscience des risques liés à la pédopornographie ou au cyber-harcèlement, note Florian Bonnet, mais ils sont extrêmement naïfs concernant les cyberattaques. »

Les cybercriminels en jouent et adaptent leurs méthodes. « Là où d'ordinaire, ils se contentent d'envoyer des emails frauduleux ou de simples liens en espérant que l'utilisateur final cliquera dessus, pour adresser des enfants ou adolescents, les attaquants développent des subterfuges (jeux gratuits, bonus gratuits sur leurs jeux favoris…) pour inciter à cliquer sur les liens », avertit Florian Bonnet.

À ce stade de la lecture, vous envisagez sûrement de couper purement et simplement tout accès Internet à vos enfants. Et bien, vous auriez tort. « Cette interdiction serait de toute façon transgressée. Et en les privant d'accès à Internet, on priverait les enfants d'une richesse énorme d'informations et de facilités de communications, estime Florian Bonnet. C'est là que nous, professionnels du monde de la cybersécurité, avons un rôle à jouer. Celui d'éduquer nos jeunes aux risques auxquels ils sont exposés. »

Accompagner les professeurs pour démystifier la cybersécurité

De son côté, Xavier Prost estime que « si on veut toucher l'ensemble des enfants, l'initiative doit aussi se faire au niveau de l'État. Les entreprises peuvent accompagner les pouvoirs publics sur ces sujets pour identifier les messages

alongside authorities in these areas to identify key messages to be understood and then disseminated in schools. But the message must be conveyed by the State, and by public bodies."

This comes down to training teachers, who are themselves often unaware of the basic principles of digital health. "I've observed that we often ask students to do research on the web, or to watch films or documentaries, without specifying which sites they can find them on", warns Florian Bonnet. "And the children then just happily look up the first site that will give them the information. But is that site secure? And is the information correct? They have no idea...". Xavier Prost is very clear: "I think we need to start from scratch. Teachers themselves often have too little awareness about the subject. And if teaching teams are not familiar with best practices themselves, they will not be able to pass them on to their students."

Stormshield has been working for a number of years to raise teachers' awareness of cybersecurity issues via the Stormshield Academy programme, whose training courses are approved and recognised by France's agency (ANSSI). In addition to training for the teachers and free access to virtual machines, institutions may — if they so choose — become Stormshield certification centres. "Our goal is for institutions to be able to incorporate cybersecurity independently into their curriculum and strategy", explains Xavier Prost. "In recent years, we've seen a surge in interest for cybersecurity. Three years ago, we had six partners. Now we have around fifty. In particular, we've signed a national partnership to train BTS teachers how to use our products and implement a security and filtering policy to protect corporate networks." Some channels are now designing cybersecurity into their own programmes. But these are specialised higher education courses... in other words, too late to educate children.

forts à connaître et à diffuser ensuite dans les écoles. Mais le message doit être porté par l'État et les acteurs publics. »

Ce qui signifie former les professeurs, qui ignorent souvent eux-mêmes les bases de l'hygiène numérique. « J'ai pu constater que l'on demande parfois aux élèves de faire des recherches sur Internet ou de visionner des films ou des documentaires sans préciser sur quels sites les trouver, déplore Florian Bonnet. Les enfants se contentent alors de chercher le premier site qui leur donnera l'information. Mais le site est-il sécurisé ? L'information est-elle la bonne ? Ils n'en savent rien… » « Pour moi, on part de zéro, tranche Xavier Prost. Les enseignants eux-mêmes sont trop peu sensibilisés au sujet. Or, si les équipes pédagogiques ne connaissent pas elles-mêmes les bonnes pratiques, elles ne pourront pas les transmettre à leurs élèves. »

Depuis quelques années, Stormshield sensibilise les enseignants aux enjeux de cybersécurité via le programme Stormshield Academy, dont les formations sont labellisées et reconnues par l'ANSSI. En plus de la formation des professeurs et de l'accès gratuit à des machines virtuelles, les établissements peuvent, s'ils le veulent, devenir un centre de certification Stormshield. « Notre objectif est que les établissements soient autonomes pour intégrer la cybersécurité dans leur cursus et dans leur démarche », explique Xavier Prost. Ces dernières années, on constate un engouement pour la cybersécurité. « Il y a trois ans, on avait six partenaires. Aujourd'hui on en a une cinquantaine. Nous avons notamment signé un partenariat national pour former les enseignants en BTS à nos produits et à la mise en place d'une politique de sécurité et de filtrage pour protéger des réseaux d'entreprise. » Certaines filières intègrent désormais la cybersécurité dans la conception de leur programme. Mais il s'agit de cursus spécialisés post-Bac… donc trop tard pour éduquer les enfants.

Un Permis Cyber sur le modèle du Permis Piéton

« Il est nécessaire de mettre en place une cyber-éducation ! Dès les classes de primaire, les enfants passent le permis

A "Cyber Licence" along the same lines as "Pedestrian Licence"

"We need to set up a cyber-education system! Primary school children in France take a permis piéton ("pedestrian licence") to learn road safety; then, in secondary school, they take their "computing and internet" (B2I) certificate. Why not create a cyber licence?", asks Florian Bonnet. But when you're educating the youngest children, what age do you start from? Sylvie Blondel believes that this education should start as young as possible, using age-appropriate teaching and explanations. "Digital education is more than just surfing the internet; it's about giving children the keys to an understanding of how it all works, to help them discover the careers of tomorrow. I think this approach needs to start fairly early, and no later than the last year of primary school, but I believe we can also develop a play-based teaching system for even younger children, attracting their attention and laying the first foundations of digital culture for the youngest children." "The subjects to be covered at primary age will be different from those covered at secondary school. Different messages need to be identified based on age and usage (cyber-bullying, online management of identity and private life, use of social media, etc.), then this knowledge must be built upon over time" adds Xavier Prost.

Initiatives already exist for educating students in digital technologies at primary level, similar to France's Permis Internet pour les enfants (Internet Licence for Children). This kit, launched by France's Gendarmerie nationale, national police, Prefecture of Police and the AXA Prévention association, is intended for final-year primary children. It presents condensed advice and real-life stories to raise awareness about Internet risks: scams, violent images, privacy, fake news, etc. A number of countries have already incorporated cybersecurity into their programmes, such as the United Kingdom, which provides training to children from age 10, or Australia, which organises School Cyber Security Challenges in high schools.

Educating children at school... and at home!

But the process of educating children in cybersecurity issues actually begins... at home! "Children need to be educated from the moment they start accessing the internet. And because they can most easily access it at home, that's where the support needs to be provided.

piéton ; au collège ils passent ensuite le brevet informatique et internet (B2I). Pourquoi ne pas mettre en place un permis cyber ? », interroge Florian Bonnet. Mais à partir de quel âge sensibiliser les plus jeunes ? Pour Sylvie Blondel, cette éducation doit être menée tout jeune, en adaptant la pédagogie et le discours. « Éduquer au numérique, ce n'est pas simplement aller sur Internet, c'est donner les clés pour comprendre comment ça marche et découvrir des métiers de demain. Je pense qu'il faut avoir cette démarche assez tôt, au minimum en CM2, mais je pense qu'on peut aussi développer une pédagogie par le jeu avant, pour attirer l'attention et développer les premières briques de culture numérique chez les plus jeunes. » « Les sujets identifiés pour le primaire ne seront pas les mêmes au collège et au lycée. Il est nécessaire d'identifier différents messages en fonction de l'âge et des usages (cyberharcèlement, gestion de son identité en ligne et de sa vie privée, rapport aux réseaux sociaux…) puis intensifier les connaissances avec le temps », complète Xavier Prost.

Il existe déjà des initiatives pour éduquer les élèves au numérique dès le primaire, à l'image du Permis Internet pour les enfants. Ce kit lancé par la Gendarmerie nationale, la Police nationale, la Préfecture de Police et l'association AXA Prévention est destiné aux élèves de CM2. Il distille conseils et témoignages pour sensibiliser aux risques d'Internet : arnaques, images violentes, vie privée, fake news…

À l'étranger, certains pays ont déjà inscrit la cybersécurité à leurs programmes, à l'image du Royaume-Uni, qui sensibilise les enfants dès 10 ans, ou de l'Australie, qui organise des Schools Cyber Security Challenges dans les lycées.

Éduquer les enfants à l'école… et à la maison !

Mais éduquer les enfants à la cybersécurité commence en réalité… chez soi ! « Les enfants doivent être éduqués dès le moment où ils ont accès à Internet. Or, un enfant a plus facilement accès à Internet chez lui, donc c'est à la maison qu'il faut l'accompagner. Aux côtés de l'école, c'est le cadre familial qui doit également jouer ce rôle », souligne Xavier Prost. Quand on y pense, l'éducation à la cybersécurité fait partie de l'éducation à la sécurité, au sens large. « Prenons l'exemple du Permis piéton et du Code de la route, poursuit Xavier Prost. Ce sont d'abord les parents qui apprennent aux enfants à marcher sur les trottoirs ou à regarder avant de traverser… L'école vient en complément et formalise cet apprentissage. Tout comme on explique à ses enfants qu'il ne faut pas parler aux inconnus dans la rue, on doit leur

So the family environment must work in conjunction with the school in playing this role", points out Xavier Prost. After all, cybersecurity education is, in a general sense, part of security education. "Let's take the example of the Highway Code and France's Permis piéton pedestrian licence", Xavier continues. "The responsibility of teaching children to walk on the pavements or look before crossing lies initially with the parent... The school assists in this task, and formalises this learning. In the same way that we explain to our children that they shouldn't talk to strangers in the street, we should teach them not to talk to strangers on the internet. What we learn in the real world also applies to the cyber world."

"People don't realise how vulnerable we've become, and the extent to which everything we do online leaves a trail we have no control over, because our data are stored in other countries. And that can have an impact. What we need to teach in schools, and elsewhere, is that the virtual world comes with real-life consequences. Explaining that to children is important... and also to parents, who are often light-years away from facing these issues." Without succumbing to paranoia, we need to be sufficiently aware of these issues to be enlightened (and not captive) users of the cyber world.

Is cybersecurity the new sexy?

Cybersecurity is not only a security issue, it also presents us all with an opportunity. France does not have a sufficiently large pool of cybersecurity skills. "One of the ways to fix this is to start discussing digital and cybersecurity issues at primary school level. In Israel, cyber profiles are identified from age 14 onwards", stated ANSSI's Guillaume Poupard in an interview with the Usine Nouvelle publication in January.

"There are plenty of vacancies in cybersecurity", confirms Sylvie Blondel, a well-placed observer of the shortage of talent in this domain. "However, educational advisors and careers guidance staff are not necessarily familiar with such jobs, which are often recent developments and seen as highly technical. Considering that we are still at the very beginning of the digital revolution, it is critically important to inform younger children about such jobs. In addition, working in the field of cybersecurity is fairly "sexy", since it is a job whose purpose is to protect people. This may appeal to younger generations, who are looking for more meaning in their work." ¶

apprendre à ne pas parler à un inconnu sur Internet. Ce que l'on apprend dans le monde réel vaut aussi pour le monde cyber. »

« Les gens ne se rendent pas compte à quel point on est devenu fragiles, à quel point tout ce que l'on fait en ligne laisse des traces sur lesquelles nous n'avons pas de contrôle, parce que nos données sont enregistrées dans d'autres pays. Et cela peut avoir un impact. C'est ce qu'il faut enseigner dans les écoles et ailleurs : le virtuel a des conséquences réelles. Expliquer cela aux enfants est important, ainsi qu'aux parents, qui sont souvent à des années-lumière de ces enjeux. » Sans sombrer dans la paranoïa, il faut être suffisamment conscient de ces problématiques pour pouvoir être un utilisateur éclairé, et pas captif, du monde cyber.

Cybersecurity is the new sexy?

Au-delà de l'aspect sécuritaire, l'éducation cyber est aussi une opportunité pour tous. La France ne dispose pas d'un vivier de compétences en cybersécurité suffisant. « L'un des moyens d'y remédier, c'est de parler de numérique et de cybersécurité dès l'école primaire. En Israël, on identifie les profils cyber à partir de 14 ans », soulignait Guillaume Poupard de l'ANSSI, dans une interview à l'Usine Nouvelle en janvier dernier.

« Il y a de nombreux postes à pourvoir en cybersécurité, confirme Sylvie Blondel, bien placée pour mesurer la pénurie de talents dans la filière. Mais les CPE et les personnes qui orientent les enfants ne connaissent pas forcément ces métiers, souvent récents et pensés comme très techniques. Or, nous ne sommes qu'au tout début de la transformation numérique, il faut donc absolument informer les plus jeunes sur ces métiers. En plus, travailler dans le domaine de la cybersécurité est assez "sexy" car c'est un métier où on protège des personnes. Cela peut parler à des jeunes des nouvelles générations qui cherchent plus de sens dans leur travail. » ¶

A partnership to include cybersecurity training in education

Un partenariat pour sensibiliser à la cybersécurité dès la formation

By Xavier Prost – May 13, 2019

In January 2019, Stormshield and CESI signed a nationwide partnership to provide Stormshield hardware and teacher training. This represents a major new step for the Stormshield Academy and its efforts to expand access to cybersecurity training for future engineers.

On a voluntary basis, all teachers and industry specialists teaching at the CESI may now receive CSNA and CSNE training, which they may then provide to their students.

The CESI and Stormshield: a lasting partnership

Stormshield and the CESI, a group of private industrial engineering schools with 25 campuses in France and 22,000 students per year, have a shared history that goes back several years. Indeed, Stormshield facilities in Villeneuve d'Ascq have long played host to work-study students from the CESI of Arras – even as far back as the Netasq era!

Once they've graduated and found employment, some of these former students return to the campus to teach cybersecurity courses. Alejandro Castano was the first of them. Since 2015, this technical specialist has spent 10 days out of the year teaching Linux intro courses and skills development courses to work-study students. "A former colleague gave me the opportunity to teach at the CESI. And since I love sharing knowledge and helping students explore a world they've never known before, I decided to take the leap", he explains. "These courses are very well received by the students, who enjoy the hands-on experience and working closely with the teacher", adds Rayane Ayate, a Stormshield technical specialist who teaches courses on web services and Linux administration. ¶

En janvier 2019, Stormshield et le CESI ont signé un partenariat national pour mettre à disposition du matériel Stormshield et y former le corps enseignant. Une nouvelle étape majeure dans la démarche de formation Stormshield Academy, pour démocratiser la connaissance en cybersécurité dans le cursus des ingénieurs de demain.

Sur la base du volontariat, tous les enseignants et intervenants extérieurs du CESI pourront désormais passer les formations CSNA et CSNE, pour ensuite pouvoir les dispenser à leurs étudiants.

Le CESI et Stormshield, une histoire qui dure

Ce groupement d'écoles privées d'ingénieurs industriels, fort de 25 campus en France et de 22 000 apprenants par an, et Stormshield ont une histoire commune qui remonte déjà à plusieurs années en arrière. En effet, les locaux de Stormshield à Villeneuve d'Ascq ont toujours accueilli des étudiants en alternance du CESI d'Arras – et ce, depuis l'époque de Netasq !

Des anciens étudiants qui, une fois diplômés et recrutés, reviennent dans le campus pour dispenser des cours autour des notions de cybersécurité. Alejandro Castano était le premier d'entre eux. Depuis 2015, cet expert technique intervient 10 jours par an devant des alternants pour leur dispenser des cours d'initiation et de renforcement sous Linux. « Un ancien collègue m'a ouvert une opportunité au sein du CESI. Et parce que j'aime partager des connaissances et l'idée de faire découvrir aux étudiants un monde qu'ils ne connaissent pas, j'ai décidé de sauter le pas », explique-t-il. « Ces interventions sont très bien accueillis par les étudiants, qui apprécient les travaux pratiques et notre proximité », ajoute Rayane Ayate, un second expert technique Stormshield qui donne de son côté des cours de services web et d'administration Linux. ¶

Cybersecurity: Enhanced by APIs

By Victor Poitevin – October 29, 2019

In an increasingly digital world, interconnection is often presented as a cybersecurity risk. So exactly how could APIs improve its security?

In response to ever-more complex cyberattacks, cybersecurity solutions are springing up... on workstations, networks, control centers and elsewhere. Are we sure to fully exploit the potential of all these tools, which are often supplied by different producers? Given that fact, how can you deliver optimum security levels? The answer may lie in the creation of interactions via an applications programming interface (API). How interconnection can improve security.

Cybersécurité : Quand les API haussent le niveau

Dans un monde toujours plus numérique, l'interconnexion est souvent présentée comme un risque pour la cybersécurité. Alors pourquoi considérer que les API peuvent la renforcer ?

En réponse à des cyberattaques de plus en plus complexes, les solutions de cybersécurité se multiplient sur les postes de travail, le réseau, les centres de contrôle… Est-on sûr d'exploiter au maximum les capacités de tous ces outils souvent issus d'éditeurs différents ? Comment assurer le meilleur niveau de sécurité dans ces conditions ? La réponse tient sûrement à créer des interactions par le biais d'interfaces de programmation applicative ou API (Applications Programming Interface). Quand l'interconnexion peut servir la sécurité.

Getting the best out of complementary solutions

Imagine a scenario in which, following an exchange of information between a firewall and the SIEM display console, a machine affected by malicious activity is automatically quarantined without human intervention. That's the promise of the API, which – when used for cybersecurity purposes – can create a dialogue between fault detection solutions and other tools which are able to implement appropriate countermeasures.

A closer look at the Python API - Stormshield

The Python - Stormshield API enables third-party products and programs to connect directly to Stormshield Network Security (SNS) firewalls to issue commands without resorting to traditional graphical administration interfaces. "It's a real building block for future intelligent systems," explains Yvan Vanhullebus, Technical Leader at Stormshield.

Another example using Stormshield Data Security (SDS): when driven by the SDS Connector API, this program can automatically encrypt files reported as sensitive by a third-party program specialising in data loss prevention (DLP).

Automating and integrating security from the deployment stage

In addition to ensuring that alerts are handled by the most appropriate security systems, APIs can also be very useful for orchestration purposes. During the deployment of a virtual machine or new application, an orchestration tool such as Ansible can use the API to automatically install not only the basic configuration for the firewall, but also a specific configuration based on pre-defined options. Security rules are set automatically as a result.

"In a system that uses APIs, the risk of configuration errors, a frequent source of vulnerabilities in digital infrastructures, is considerably reduced. These APIs

> **"The risk of configuration errors, a frequent source of vulnerabilities in digital infrastructures, is considerably reduced"**
>
> **Julien Paffumi, Product Manager, Stormshield**

Tirer le meilleur parti de solutions complémentaires

Imaginez, au terme d'une remontée d'information d'un firewall vers la console de visualisation SIEM, une machine faisant l'objet de comportements malveillants est mise automatiquement en quarantaine sans intervention humaine. C'est la promesse de l'API appliquée à la cybersécurité, faire dialoguer des solutions capables de détecter une faille avec d'autres outils en capacité de mettre en place une contre-mesure adaptée.

Zoom sur l'API Python - Stormshield

L'API Python - Stormshield permet à des programmes et produits tiers de se connecter directement aux pare-feux Stormshield Network Security (SNS) pour passer des commandes sans recourir à l'interface graphique d'administration classique. « C'est une véritable brique de base pour de futurs systèmes intelligents », explique Yvan Vanhullebus, Technical Leader Stormshield.

Autre exemple avec Stormshield Data Security (SDS) : piloté grâce à son API SDS Connector, ce programme peut par exemple chiffrer automatiquement les fichiers signalés comme sensibles par un logiciel tiers spécialisé en prévention de fuites de données (Data Loss Prevention – DLP).

Automatiser et intégrer l'aspect sécurité dès le déploiement

En plus de supporter des fonctions d'orchestration des réactions aux alertes au niveau d'un système hétérogène (System Detection & Response), les API sont également très intéressantes du point de vue de la maîtrise des configurations des systèmes déployés. Lors du déploiement d'une machine virtuelle ou d'une nouvelle application, un orchestrateur comme Ansible peut, via l'API, installer en automatique la configuration de base du pare-feu, mais également une configuration spécifique en fonction d'options préalablement déterminées. Les règles de sécurité sont ainsi paramétrées automatiquement.

automatically integrate security into the Infrastructure-as-a-Software model", says Julien Paffumi, Product Manager at Stormshield. "That also allows teams to concentrate on the value they add to the processes, rather than constantly repeating similar admin tasks".

What are the downsides of an API?

Despite the promises offered by APIs, the investment inherent in such a deployment must not be underestimated. "This sort of interconnection project can be complex, costly and time-consuming to implement, as it may require considerable levels of service provision and technical support", warns Jocelyn Krystlik, Data Security Business Unit Manager at Stormshield. "Not to mention staff training time, for example for developers." Substantial upstream preparation is thus required in order to make best use of human resources in this area. At the same time, Yvan Vanhullebus points out that for publishers, "we need to bear in mind the fact that developers and products from different cultures must be able to interface successfully with one another. No one excels at everything, so we need to think in terms of standardisation and documentation, and have a real understanding of this ecosystem."

In addition, the cybersecurity-by-design aspect is critically important here. Since this issue has a direct bearing on how security solutions operate, there is a need to ensure the confidentiality and integrity of the data they exchange. This makes the security of the APIs themselves a major issue.

If security rules are adhered to during the design phase, APIs will then be able to improve the overall efficiency of cybersecurity solutions. By means of privileged information sharing, APIs facilitate the deployment of security solutions, improve security system performance and minimise everyday human errors. And the benefits of such open, automated solutions can be fully appreciated when emergencies arise. ¶

« Dans un système exploitant les API, le risque d'erreurs de configuration, source fréquente de failles dans les infrastructures numériques, est considérablement réduit. Ces API permettent d'intégrer automatiquement la sécurité dans le modèle d'Infrastructure-as-a-Software », confirme Julien Paffumi, Product Manager Stormshield. « Cela permet aussi aux équipes de se concentrer sur la valeur qu'ils apportent aux processus, plutôt que sur de la répétition des tâches d'administration toujours similaires ».

Quels inconvénients derrière une API ?

En dépit des promesses des API, il ne faut pas sous-estimer l'investissement que représente un tel déploiement. « Ces projets d'interconnexion peuvent être complexes, coûteux et longs à mettre en œuvre car ils peuvent nécessiter un volume de prestation de service et d'assistance technique important », prévient Jocelyn Krystlik, Data Security Business Unit Manager Stormshield. « Sans oublier le temps de formation du personnel, par exemple des développeurs. » Une réelle préparation en amont est donc requise, pour optimiser au mieux les ressources humaines sur le sujet. En parallèle, Yvan Vanhullebus complète pour les éditeurs : « il est impératif de prendre en compte le fait que des développeurs et des produits aux cultures différentes vont devoir réussir à s'interfacer entre eux. Puisqu'on ne maîtrise pas tout, il faut donc penser standardisation, documentation et avoir une réelle connaissance de cet écosystème. »

En complément, la dimension du cybersecurity-by-design est fondamentale ici. Puisqu'on touche directement au fonctionnement des solutions de sécurité, il faut assurer la confidentialité et l'intégrité des données qu'elles s'échangent. La sécurité des API elles-mêmes est donc un enjeu majeur.

Si les règles de sécurité sont respectées dans la phase de conception, les API permettent donc d'améliorer l'efficacité globale des solutions de cybersécurité. Au travers d'un partage d'informations privilégié et de capacités de contrôle, les API augmentent la performance globale des systèmes de sécurité, facilitent leur déploiement et limitent les risques d'erreurs humaines. Un travail d'ouverture et d'automatisation qui prend toute sa dimension en situation d'urgence. ¶

The matter of cybersecurity staffing

La question du recrutement en cybersécurité

Is cybersecurity a male-only environment?

By Victor Poitevin – January 17, 2019

Despite being dynamic and well-paid, the cybersecurity sector is faced with a talent shortfall – particularly in terms of female talent. According to a study by the (ISC)² consortium, women account for just 11% of cybersecurity employees. Could a better gender balance help to eliminate this skills shortage?

A lack of female role models

According to data revealed by Syntec Numérique (the leading digital ecosystem syndicate in France), women account for just 27% of employees in the digital sector, compared to 50% in South-East Asia and the Middle East. "The figures speak volumes, and the situation in France is particularly concerning when compared to South-East Asia and the Middle East," notes Syntec Numérique. "The stereotypical image of a computer scientist doesn't appeal to girls! It's a cultural and social problem."

And stereotypes are hard to overcome. "Just look at magazines: women are confined to beauty and fashion. Girls and women grow up in a stereotyped society, and many are apprehensive of studying computer science, thinking that it's just not for them," Ilijana Vavan, Managing Director of Kaspersky Lab, told Les Echos in June 2018. A third of women think that cybersecurity professionals are geeks. It's an image that TV and cinema – where women rarely take on these roles – does nothing to dispel.

The result is that the cybersecurity sector – and the digital sector in general – still lacks leading female figures. Mention Facebook and everyone's heard of Mark Zuckerberg, but who could tell you what Sheryl Sandberg does? "People have forgotten that women played an essential role in the development of computer science in the 1970s. Nowadays, who knows who Grace Murray Hopper is, for example? We have to fight these ste-

La cybersécurité serait-elle un milieu réservé aux hommes ?

Dynamique et porteur, le secteur de la cybersécurité fait pourtant face à une pénurie de talents, notamment féminins. Selon une étude du consortium (ISC)², les femmes ne représentent que 11% des effectifs. Et si une meilleure répartition femmes-hommes permettait de résorber la pénurie de compétences ?

Un manque de modèles féminins

Selon les données dévoilées par le Syntec numérique (premier syndicat de l'écosystème numérique hexagonal), les femmes ne représentent que 27% des employées du numérique, contre 50% en Asie du Sud-Est et au Moyen-Orient. « Les chiffres sont éloquents et la situation en France est particulièrement alarmante si on la compare à celle de l'Asie du Sud-Est et du Moyen-Orient, note le Syntec numérique. L'image stéréotypée de l'informaticien n'attire pas les filles ! Le blocage est culturel et sociétal ».

Et les stéréotypes sont tenaces. « Il n'y a qu'à regarder les magazines : les femmes sont cantonnées au rayon beauté et mode. Elles grandissent dans une société stéréotypée et beaucoup appréhendent de s'engager dans des études d'informatique, pensant que ce n'est pas fait pour elles », dénonçait déjà Ilijana Vavan, directrice générale de Kaspersky Lab, aux Echos en juin 2018. Un tiers des femmes pensent ainsi que les professionnels de la cybersécurité sont des geeks. Une image véhiculée par les séries et le cinéma, où les femmes endossent rarement ce rôle.

Conséquence : le secteur de la cybersécurité – et du numérique en général – manque encore de figures féminines. Si vous évoquez Facebook, tout le monde connaît Mark Zuckerberg, mais qui peut expliquer le rôle de Sheryl Sandberg ? « On a oublié que les femmes avaient joué un rôle très important à l'origine de l'informatique, dans les années 1970. Qui

reotypes and showcase women working in the sector. You can't ignore 50% of talent!" says Sylvie Blondel, Human Resources Director at Stormshield.

The feminisation of the digital world starts in school

And the key lessons start in school. "Cybersecurity needs to convey an image of an industry that's much more inclusive, diverse and egalitarian. The earlier you start, the easier it is to break down stereotypes," says Charlotte Graire, Head of Strategy & Business Development at Airbus CyberSecurity. "Boosting girls' awareness before they choose their options in secondary school is essential." "Women are under-represented in scientific and technical sectors. We have to fight prejudices at the earliest possible stage," adds Maryse Levavasseur, a software development engineer at Stormshield.

With the Femmes Ingénieurs group, they visit schools to show that their fields aren't just for men. Giving talks to students aged 14-16, the organisation aims to inform and motivate girls just before they make the crucial choice of what direction their studies will take in secondary school. The Femmes@Numérique foundation is also heavily involved in improving women's representation in the sector, and works with students in the final two years of primary school, as well as throughout secondary school.

It's an excellent way of offering female role models and addressing the lack of information about these expert roles: according to a study by Kaspersky Lab, just 20% of those surveyed knew exactly what a cybersecurity expert does, with this figure falling to 16% among women. "The cybersecurity sector is poorly understood and associated with technical computer attacks, while in fact, it's a much broader sector," says Charlotte Graire. Working in development requires a significant amount of creativity, and awareness of this aspect remains low.

"Cybersecurity needs to convey an image of an industry that's much more inclusive, diverse and egalitarian."

Charlotte Graire
Head of Business Development & Alliances, Airbus CyberSecurity

aujourd'hui sait qui est Grace Murray Hopper par exemple ? Il faut lutter contre ces stéréotypes et mettre les femmes du secteur en avant. On ne peut pas se priver de 50% des talents ! », plaide Sylvie Blondel, Directrice des Ressources Humaines Stormshield.

La féminisation du numérique commence dès l'école

Et la pédagogie commence dès l'école. « La cybersécurité doit renvoyer l'image d'une industrie beaucoup plus inclusive, mixte et égalitaire. Plus on intervient jeune, plus il sera facile de déjouer les stéréotypes, souligne Charlotte Graire, Head of Strategy & Business Development de Airbus CyberSecurity. La sensibilisation des jeunes filles avant l'orientation dans les sections au lycée est essentielle. » « Les femmes sont sous-représentées dans les filières scientifiques et techniques. Il faut combattre les préjugés le plus tôt possible », abonde Maryse Levavasseur, ingénieure en développement logiciel chez Stormshield.

Avec l'association Femmes ingénieurs, elles interviennent dans les établissements scolaires pour montrer que ces secteurs ne sont pas réservés qu'aux hommes. En s'adressant aux élèves de 3e et de 2nde, l'association espère informer et motiver les jeunes filles juste avant le choix crucial de l'orientation au lycée. La fondation Femmes@Numérique est également fortement engagée pour une meilleure représentativité des femmes dans le secteur et va s'adresser aux élèves dès l'école primaire (CM1 et CM2), le collège et le lycée.

Une bonne façon de leur proposer des modèles féminins et de combler un manque d'information sur ces métiers experts : selon une étude menée par Kaspersky Lab, seuls 20% des personnes interrogées savent exactement en quoi consiste le métier d'expert en cybersécurité, un chiffre qui tombe 16% chez les femmes. « Le secteur de la cybersécurité est mal connu et associé à des attaques techniques alors que c'est un secteur bien plus vaste », rappelle Charlotte Graire. Les métiers du développement exigent ainsi une bonne part de créativité, or cet aspect est peu connu.

Showing that women can

But getting degrees isn't enough by itself. Once they've entered the world of work, female engineers often have to fit in in a man's world. The only woman in her department, Maryse Levavasseur has a strong argument should anyone try to call her skills into question. "At Stormshield, the technical tests are extremely demanding. At my interview, I took the test and I passed it. It's an objective way of assessing someone's skills, whether they're a man or a woman."

Despite their skills, women who make it into the industry can still be seen as inferior. "Being taken seriously is a real problem. I remember one event where the people I was speaking to only addressed my male colleague, whereas I was the one responsible for buying my department's cybersecurity software!" says Florence Lecroq, a doctor in electrical engineering and industrial computing at the University of Le Havre. "Despite my CV, I still need to prove my worth — I have to try 50% harder than a man does."

The figures show that the digital sector is no stranger to gender inequality: women hold fewer key posts and are paid less than men, despite the fact that they are better qualified (51% have a master's-level qualification or higher, compared to 45% of men).

Organisations such as the CErcle des Femmes de la CYberSécurité (CEFCYS), founded by Nacira Salvan, are helping to increase the number of women in the sector and change people's mindsets. But do we need to take things further and implement a quota policy? "I don't believe in introducing a legal obligation — it doesn't work and many companies prefer to pay fines rather than comply with requirements," says Sylvie Blondel. "I think that rather than imposing quotas, the best approach is to demonstrate by example and to show that women can work in IT, that they have the knowledge and that they have a place in the sector. Providing information and fighting stereotypes requires better visibility for women working in the sector."

But time is of the essence. According to an assessment by the European Commission, Europe will be short of 756,000 digital professionals in 2020. Could tomorrow's solutions rely — at least in part — on training today's schoolgirls? ¶

Montrer que les femmes savent faire

Mais décrocher les diplômes ne fait pas tout. Une fois passée la porte des entreprises, les femmes ingénieures doivent s'intégrer dans un monde d'hommes. Seule femme de son service, Maryse Levavasseur dispose d'un solide argument pour ne pas se laisser attaquer sur ses compétences. « Chez Stormshield, les tests techniques sont très pointus. Lors de mon embauche, j'ai passé et réussi le test qui m'était demandé. C'est une façon objective d'évaluer des compétences, qu'on soit une femme ou un homme. »

Malgré leurs compétences, les femmes qui percent peuvent encore être perçues comme subalternes. « Être prise au sérieux est un vrai problème. Je me souviens d'un salon où mes interlocuteurs ne s'adressaient qu'à mon collègue, alors que c'était moi la responsable chargée d'acheter le programme de cybersécurité pour mon département ! pointe Florence Lecroq, docteur en génie électrique et informatique industrielle à l'université du Havre. Malgré mon cursus, j'ai encore besoin de prouver ma valeur, je dois déployer 50% d'énergie en plus qu'un homme. »

Les chiffres le montrent, le secteur du numérique n'échappe pas aux inégalités de genre : les femmes occupent moins de postes-clés et sont moins payées que les hommes, bien qu'elles soient plus diplômées (51% des femmes ont un master ou plus, contre 45% des hommes).

Des associations comme le CErcle des Femmes de la CYberSécurité (CEFCYS), fondé par Nacira Salvan, contribuent à féminiser le secteur et à faire évoluer les mentalités. Mais faut-il aller plus loin et passer par une politique de quotas ? « Je ne crois pas à l'obligation légale, cela ne fonctionne pas et plusieurs entreprises préfèrent payer des taxes plutôt que de se mettre en conformité, tempère Sylvie Blondel. Je pense qu'au lieu d'imposer des choix, il faut faire la preuve par l'exemple et montrer qu'on peut faire de l'IT avec des femmes, qu'elles savent faire et qu'elles ont leur place. L'information et la lutte contre les stéréotypes passent par une meilleure visibilité des femmes en poste. »

Force est de constater que le temps presse. Selon une évaluation de la Commission européenne, il manquera 756 000 professionnel.les du numérique en Europe en 2020. Et si les solutions de demain reposaient en partie sur la formation des collégiennes dès aujourd'hui ? ¶

Recruiting in cybersecurity: An ambitious and motivating challenge for the years to come

Recruter en cybersécurité :

Un challenge ambitieux et motivant pour les années à venir

By Sylvie Blondel – April 17, 2019

Faced with a skills shortage, the market is beginning to react and organise accordingly. However, the initiatives are still largely one-off and have proved difficult to implement on a large scale. How can we identify and attract the right applicants? A very important question which requires multiple and cross-cutting solutions.

Specialised, little-known activities which are changing at an ever-faster pace

We are seeing a certain lack of awareness of digital occupations: this is true of students but also their parents, some teachers and careers advisers. The "geek" image is firmly rooted in our society and is hard to shake off. Despite this, it's important not to generalise, as initia-

Face à la pénurie de compétences, le marché commence à réagir et à s'organiser. Cependant, les initiatives restent ponctuelles et compliquées à déployer à grand échelle. Comment identifier et attirer les bons profils ? Cette question est aujourd'hui plus que légitime et appelle des réponses multiples et transverses.

Des métiers pointus, peu connus, en évolution de plus en plus rapide et permanente

Nous pouvons noter une certaine méconnaissance des métiers liés au numérique : ce point est vrai pour les étudiants mais également pour leurs parents, certains enseignants ou conseillers d'orientation. L'image du « geek » est ancrée dans les esprits de notre société et peine à évoluer. Pour autant, il

tives are afoot to make people more aware of careers in the digital sector and to present a completely different image of these.

Raising the profile of these rewarding careers requiring a variety of different skills

On this particular point, it has to be admitted that the necessary awareness-building doesn't seem to be happening. With this in mind, it's vital to get them better known to avoid people focusing on only the purely technical aspects. Indeed, a career in the world of cybersecurity should not be something reserved for only a small, restricted community of people. On the contrary, it's important to be able to draw upon numerous complementary employee profiles, able to play a decisive role in the development, creation and marketing of innovations making it possible to create a safe and trusted cyberspace.

Working with schools, universities and training bodies

In addition to developing and marketing their products and solutions, the various stakeholders in the cybersecurity world also need to prepare for the future by forging partnerships with teaching professionals in order to be able to propose training courses which make it possible to train future potential applicants on a large scale. Working with schools, universities and training bodies is vital in order to change the current situation and to ensure that subjects related to IT security are given a central place within their syllabuses.

The feminisation of the digital industry

Over and above the issue of training, for several years now we have been witnessing the reappearance of women in the digital industry. Although this is still only a modest trend, it has enabled the profession to benefit from an influx of enthusiastic female staff members at every organisational level. By bringing a fresh set of eyes and a new approach to the world of cybersecurity, women undoubtably have a strategic role to play in this industry. To make this a reality, we must continue to look beyond stereotypes, to raise awareness among young women when they receive careers guidance and naturally to convey the image of a diverse, welcoming

ne faut pas tirer de généralité puisque des initiatives mettent en avant la prise de conscience d'amener une autre image des métiers du numérique.

Valoriser des métiers enrichissants et nécessitant des compétences multiples

Sur ce point, force est de constater que la valorisation des diverses compétences ne semble pas au rendez-vous. En ce sens, il serait fondamental de mieux les faire connaître afin de ne pas se focaliser uniquement sur les aspects purement techniques. En effet, travailler dans le monde de la cybersécurité ne doit pas être réservé à une communauté restreinte. Bien au contraire, il nécessite de faire appel à de nombreux profils complémentaires qui joueront un rôle déterminant dans le développement, la création et la mise sur le marché d'innovations permettant de créer un cyber espace de confiance.

Se rapprocher des écoles, des universités et des organismes de formation

Au-delà de développer et de commercialiser leurs produits et solutions, les acteurs du monde de la cybersécurité se doivent aussi de préparer l'avenir en tissant des partenariats avec les professionnels de l'enseignement pour proposer des cursus de formation qui permettront de former à grande échelle de futurs potentiels motivés. Ces collaborations avec les écoles, les universités et les organismes de formation sont incontournables pour faire bouger les lignes et positionner les sujets de la sécurité informatique au centre des programmes.

Quand l'industrie du digital se féminise

Au-delà de la formation, on assiste depuis quelques années à une réapparition des femmes dans le monde du numérique. Même si cette évolution reste encore modeste, elle a permis à la profession d'intégrer des collaboratrices passionnées à tous les niveaux des organisations. En apportant un autre regard sur le monde de la cybersécurité, les femmes ont indiscutablement un rôle stratégique à jouer dans cette industrie. Pour cela, il faut continuer à déjouer les stéréotypes, sensibiliser les jeunes femmes dans leurs orientations et bien entendu, renvoyer l'image d'une industrie mixte, accueillante et sans préjugés. Les femmes réussissent et s'épanouissent dans le numérique : il faut le faire savoir.

Les sujets du recrutement et de la formation de collaborateurs dans le numérique sont donc au centre des enjeux de

industry, free of prejudices. Women can succeed and achieve self-fulfilment in the digital industry: need to make people aware of this.

The recruitment and training of staff in the IT sector is therefore a key challenge facing today's society, one which is set to accentuate over the coming years. At a time when the digital transformation is well and truly underway, companies in all sectors are more than ever before trying to recruit the talents they need to support their changes. This transformation is accelerating and is increasing the attack surface of organisations and infrastructure every day. It can only be achieved by introducing trusted tools and solutions.

It is also why guaranteeing the cybersecurity of public and private organisations is a key point requiring the involvement of numerous experts if it is to be successfully carried through. We must be careful not to simply opt for the status quo, because the conditions for our future success are being built now, today. The scale of this recruitment problem affects the whole ecosystem and it would be a mistake to limit this to a purely educational approach. It needs to be approached as a whole, from a 360° angle, or we won't succeed. ¶

notre société dès aujourd'hui et le seront encore plus lors des prochaines années. En pleine transformation numérique, les entreprises de tous les secteurs sont plus que jamais à la recherche de talents qui pourront les accompagner dans leurs changements. Cette transformation s'accélère et augmente chaque jour la surface de vulnérabilité des organisations et des infrastructures. Elle ne pourra donc se faire qu'en mettant en place des outils de confiance.

C'est aussi pourquoi la cybersécurité des organisations publiques et privées est un point-clé qui nécessite de mobiliser de nombreux experts pour être menée à bien. Attention donc à ne pas jouer la carte du statu quo puisque c'est bien aujourd'hui que nous construisons les conditions de notre réussite de demain. La dimension de cette problématique de recrutement se joue dans tout l'écosystème, ce serait une erreur de la cantonner à une approche purement scolaire. Elle doit être appréhendée dans sa globalité faute de quoi nous n'y arriverons pas. ¶

Thank you

So here's a retrospective of 2019. This year has been studded with confirmations of existing trends and the emergence of new ones, informing all of the different work we do.

Over the coming year, we will maintain our focus on creating new content. Using a variety of formats and presenters, we will ensure that this content will have a viral appeal. And you will have a vital role to play in ensuring this new material has a high profile: as you share content of interest with those around you, you will be helping us to reach a wider audience... and raising awareness of digital hygiene and cyber risks.

By the time you read these words, our teams will already have produced further content, which you will – I hope – have enjoyed reading and sharing. Regularly updated new content can be found on our stormshield.com website, and also appears on Stormshield's various social networks.

Pierre-Yves Hentzen

CEO of Stormshield

Merci

Voici donc une rétrospective de cette année 2019. Confirmations de tendances et émergences de nouvelles pistes auront ainsi jalonné le parcours et rythmé nos différentes actions.

Pour l'année à venir, nous allons maintenir nos efforts de création de contenus. En variant les formats et les intervenants, nous insisterons sur la viralité de ces contenus. Concernant la visibilité de ceux-ci, vous aurez un rôle essentiel à jouer : en partageant les contenus qui vous intéressent autour de vous, vous nous aiderez à toucher une plus grande audience. Et ainsi faire progresser la sensibilisation à l'hygiène numérique et aux risques cyber.

À l'heure où vous lirez ces lignes, nos équipes auront produit d'autres contenus, que vous aurez eu – je l'espère – plaisir à lire et partager. Retrouvez-les régulièrement publiés sur notre site internet stormshield.com, et diffusés via les différents réseaux sociaux de Stormshield.

Florian Bonnet
Director of Product Management

As someone who spent many years in the field on the front line playing rugby, Florian also promotes that same #TeamSpirit among Stormshield's Product Managers.

Khobeib Benboubaker
Industry Business Line Manager

Heading the dedicated Business Line, Khobeib implements the company's strategic ambitions in the #IndustrialCybersecurity field.

Jocelyn Krystlik
Data Security Business Unit Manager

Big or small, smart or normal, #data holds no secrets for Jocelyn. But he prefers it when it's encrypted.

Julien Paffumi
Product Management Leader

Always on the go, Julien works to bring about continuous improvements in the #ProductManagement at Stormshield.

Marco Genovese
Product Manager

Drawing upon his background as a Pre-Sales Engineer in his native Italy, #network security holds no secrets for Marco.

Matthieu Bonenfant
Chief Marketing Officer

With proven support skills in products and #marketing, Matthieu has been working for several years to promote digital hygiene.

The authors of Stormshield's papers

Raphaël Granger
Public Sector Account Manager

As a business manager with technical skills, Raphael is the company's Mr #PublicSector.

Robert Wakim
Offers Manager

With more than 10 years' #experience behind him, Robert is a big name in his sector.

Stéphane Prévost
Product Marketing Manager

As the team's globetrotter, Stéphane has made a great job of forging solid operational links between the product and marketing #departments.

Sylvie Blondel
Human Resources Director

Operating in a key post, Sylvie is the foremost defender of the company's #values of commitment, trust and collaboration.

Victor Poitevin
Digital Manager

As the band leader for the #editorial activity, he can always count on a team of superbly talented musicians.

Xavier Prost
Training & Documentation Manager

Because awareness-building and #training go hand-in-hand, Xavier spreads the cybersecurity inception to a large number of schools and universities.

STORMSHIELD

Stormshield, the European leader in cybersecurity and a wholly-owned subsidiary of Airbus CyberSecurity, offers communicative, intelligent solutions for anticipating attacks and protecting digital infrastructure. Its mission is to ensure cybersecurity and protect the data of organisations and of their employees and customers.
Stormshield's expertise is spread over three complementary product ranges for utmost security:

- Protection of IT and industrial networks (Stormshield Network Security);
- Protection of workstations and servers (Stormshield Endpoint Security);
- Protection of data (Stormshield Data Security).

These cutting-edge and reliable solutions are certified at the highest European levels (EU Restricted, NATO Restricted, ANSSI EAL3+/EAL4+).

Leader européen de la cybersécurité et filiale à 100% d'Airbus CyberSecurity, Stormshield propose des solutions communicantes et intelligentes pour anticiper les attaques et protéger les infrastructures numériques. Sa mission : assurer la cybersécurité et la protection des données des organisations, de leurs collaborateurs et de leurs clients.
Son expertise se décline en trois gammes de produits complémentaires pour une sécurité sans failles :

- *Protection des réseaux informatiques et industriels (Stormshield Network Security).*
- *Protection des postes et serveurs (Stormshield Endpoint Security).*
- *Protection des données (Stormshield Data Security).*

Ces solutions de pointe et de confiance sont certifiées au plus haut niveau européen (Restreint UE, Restreint OTAN, ANSSI EAL3+/EAL4+).

www.stormshield.com