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.

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.

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°1

« 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

« 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.

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.