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.

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.

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.

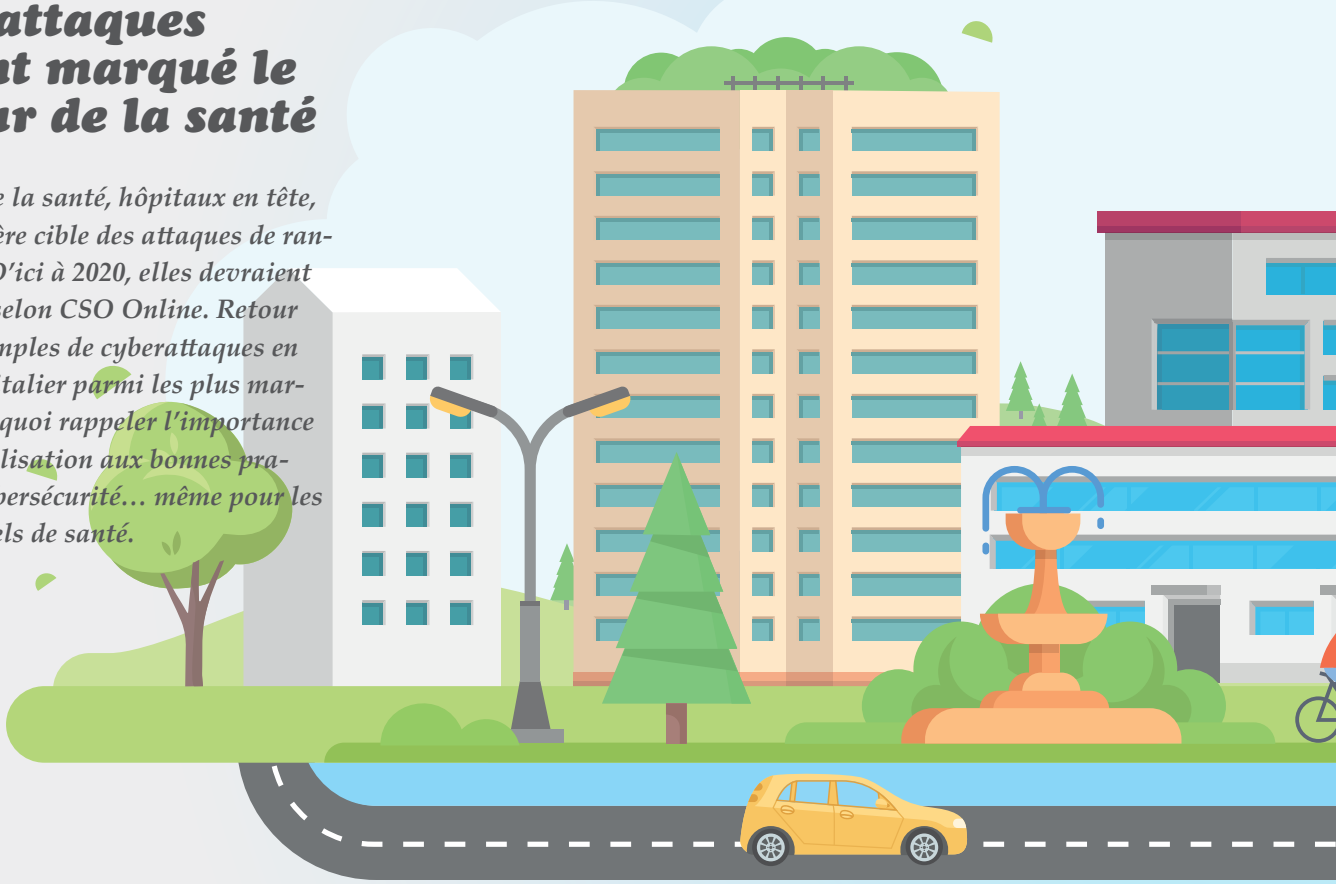
4 A PHISHING ATTACK

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.



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.