DOC
LE RENDEZ-VOUS
DES MÉDECINS
VAUDOIS

Ce qu'en pense

La sécurité informatique, la santé et le truand

L'informatique a pris une place prépondérante dans les services publics, les industries, les entreprises, ainsi que dans la vie quotidienne de manière générale. Cette transition vers le « tout informatique » s'est imposée rapidement, avec peu de considération pour la formation des utilisateurs et utilisatrices. Et avec une problématique de la sécurité informatique qui n'est venue que bien trop tard.

Ces dernières années, le nombre de cyberattaques a très nettement augmenté. Et les établissements de santé n'ont pas été épargnés. Si, de prime abord, il semble n'y avoir qu'un intérêt limité à pirater des structures de santé, les attaquant-es y trouvent aujourd'hui un intérêt financier (revente de données personnelles de particuliers ou de célébrités, chantage, paralysie du réseau avec demande de rançon…), et pourraient également y trouver un intérêt stratégique dans le cas d'un contexte géopolitique tendu, par exemple.

De telles attaques peuvent avoir un impact énorme, comme l'a démontré l'attaque informatique du Centre hospitalier de Dax en France voisine en février 2021. Le bilan à un an : 2'356'000 euros de coût de gestion de l'incident, 2'344'000 euros de recettes en manque par la fermeture de plusieurs activités, sans compter que l'établissement n'a pas été en mesure de remettre en place l'intégralité de ses services.

De fait, l'objectif majeur est de limiter au maximum le nombre d'attaques réussies et leur impact, le plus rapidement possible. Pour atteindre cet objectif, les premières mesures à mettre en place seraient :

- Une politique de sensibilisation pour tout le personnel
- Une détection des tentatives d'intrusions, réussies ou non
- L'isolation du réseau pour qu'une compromission s'étende le moins possible
- La capacité à sauvegarder et restaurer le plus rapidement possible des services compromis
- L'organisation d'audits de sécurité par des entreprises spécialisées, et éventuellement l'organisation de programmes pour permettre à des chercheurs en sécurité de tester la sécurité des services en tout temps de façon éthique (« bug bounty »)

Il est aujourd'hui plus important que jamais que les structures de santé et les spécialistes en sécurité informatique marchent main dans la main pour que notre système de santé reste lui-même en bonne santé.

Daniel Le Gall
Chercheur en sécurité informatique