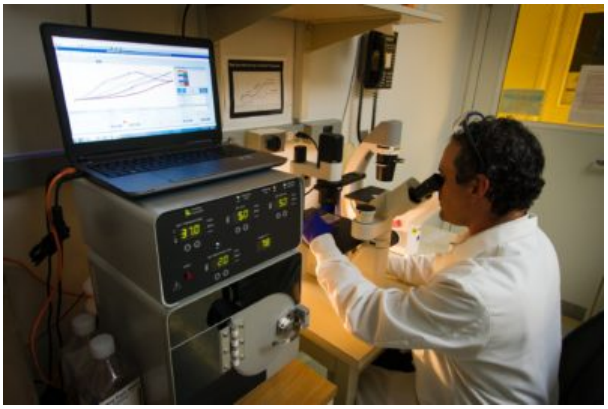

Rapport d'ICIT sur la recherche en cybersécurité pour le domaine du médical

L'*Institute for Critical Infrastructure Technology* (ICIT), premier think-tank en cybersécurité du pays, a récemment publié un rapport [1] concernant la recherche en cybersécurité liée au domaine de la santé.

Le rapport souligne notamment l'importance pour les recherches de santé d'être associées à une réflexion sur la thématique de la cybersécurité. En effet, la R&D santé représente chaque année plusieurs milliards de dollars et confère aux Etats-Unis un avantage compétitif stratégique. Pourtant, la plupart des chercheurs dans ce domaine sont trop peu conscients des risques et menaces qui existent et ne sécurisent pas suffisamment leurs données et résultats de recherche. Dans beaucoup d'organismes de recherche, les systèmes d'informations sont dépassés et non mis à jour ce qui en font des cibles très lucratives pour les attaquants et des pertes énormes pour les victimes.

Au-delà du coût financier pour les entreprises qui investissent des sommes importantes et à qui on empêche de générer des revenus grâce à leurs innovations, d'autres dégâts considérables sont à envisager. L'altération des données de recherche, par exemple, peut avoir des conséquences désastreuses et même mettre en danger la santé des patients notamment dans le cadre d'essais cliniques. Les

centres de recherche dont les données auront été corrompues pourraient voir leur réputation être mise en péril avec des effets en cascade (moins de financements reçus, difficulté à recruter des talents etc.).

La Chine encore pointée du doigt

Parmi les acteurs qui menacent particulièrement la recherche médicale américaine, la Chine est particulièrement prise pour cible. Selon le rapport, un nombre important de vols liés à la recherche serait le fait de hackers chinois et s'explique par une inquiétude grandissante quant aux cas de cancers qui augmentent, le marché pharmaceutique intérieur très lucratif mais également la volonté de développer un système de santé publique à moindre coût. Le plan « Made in China 2025 » est également mentionné comme un élément qui pourrait pousser différents acteurs à vouloir se procurer de la propriété intellectuelle de manière illégale à l'étranger pour développer eux-mêmes de nouvelles technologies. Des groupes venant de Russie et du Vietnam sont également mentionnés comme de potentiels acteurs malveillants.

Outre les acteurs étatiques, le rapport évoque également le cas d'organisations criminelles à la recherche de gains financiers rapides et qui opèrent principalement par le biais de *ransomware* (déblocage de systèmes informatiques ou menace de diffusion d'informations volées en échange d'une rançon). Le rapport inclut également les menaces posées par des acteurs autres tels que *hacktivists* qui chercheraient à faire passer un message politique ou bien divers autres collectifs et individus isolés en recherche de renommée.

Différentes sources de vulnérabilité

D'après le rapport, la recherche médicale est un domaine particulièrement vulnérable pour plusieurs raisons :

(1) Les appareils médicaux ont traditionnellement été conçus pour fonctionner de manière isolée. Leur mise en réseau progressive ou leur accès par le biais d'Internet créent des opportunités d'accès aux données et autres vulnérabilités (type prise de contrôle).

(2) Les appareils connectés non-médicaux peuvent également être utilisés comme vecteurs d'attaque cyber au sein de l'environnement de recherche. Un ordinateur portable infecté ou autre appareil peut compromettre l'intégrité du réseau de recherche auquel il se connecte. De manière générale, l'automatisation croissante et la prolifération d'appareils de contrôle (pour la climatisation, compteurs d'eau, appareils de gestion électrique etc.) sont autant de portes d'entrée supplémentaires.

(3) Les risques de menace interne continuent de peser malgré les alertes répétées formulées par les autorités et organismes du renseignement et du contre-espionnage. La menace interne peut être accidentelle et due par exemple à la négligence des personnels ou bien intentionnelle dans le cas d'employés mécontents, d'employés recrutés a posteriori ou placés par une entité extérieure.

La nécessité d'une stratégie cyber pour les organismes de recherche

Face à ces nombreux défis, une véritable stratégie en cybersécurité est nécessaire. Celle-ci conduit notamment au recrutement de personnel qualifié et dédié à la cybersécurité au sein des organismes de recherche permettant d'effectuer des contrôles réguliers des infrastructures, de former le reste du personnel aux bonnes pratiques d'hygiène cyber, de développer et mettre à jour un ensemble de mesures et standards de cybersécurité. Entre autres mesures, le rapport préconise également des relations plus étroites entre fabricants d'appareils, spécialistes de la sécurité et utilisateurs finaux que sont les chercheurs et ce, notamment, afin de concevoir des technologies adaptées aux usages mais qui répondent au principe de *sécurité de conception* (*security-by-design)*.

[1]
https://secureservercdn.net/166.62.108.22/5kb.d9b.myftpupload.com/wp-content/uploads/2020/05/ICIT-Research-The-Healthcare-Research-Security-Pandemic.pdf

Rédacteur :

Kevin KOK HEANG, Attaché adjoint pour la Science et la Technologie, deputy-ntics@ambascience-usa.org