La médecine du futur

La cybercriminalité et le monde médical : les hackers ont plusieurs longueurs d'avance

Coucke PA (1)

Résumé : La criminalité cybernétique s'attaque à tous les domaines d'activité humaine. Le monde hospitalier est particulièrement vulnérable. En effet, d'une part, un dossier médical personnel (DMP) volé se vend aisément plus de 1.000 dollars sur le «darknet» et, d'autre part, les structures informatiques vieillissantes de nos institutions et de nos cabinets médicaux privés sont particulièrement exposées aux attaques. Viennent s'y ajouter une réelle méconnaissance du danger par les professionnels de soins et un manque de culture de sécurité informatique, illustré par l'absence quasi totale d'une formation initiale et d'une formation continue en la matière. Il n'y a pas une seule réponse simple et définitive à ce fléau, mais différentes solutions peuvent être mises en place rapidement afin de limiter les risques encourus et les dégâts.

Mots-clés : ***Sécurité informatique - Hacking - Intelligence artificielle***

Cybersecurity in the health care sector

Summary : Cybersecurity is a real threat in almost all human activity domains. The health sector is a particular vulnerable target for cybercriminals. The first reason is obviously the financial incentive: the value of the content of a personal electronic health record, sold on the darknet, easily exceeds 1000 US dollars. The second reason is the aging Information Technology (IT) infrastructure we are dealing with, both in the hospital sector as well as in the vast majority of private medical practices. There is also an astonishing lack of environmental consciousness and an absence of a real safety culture in the medical profession. Very often there is neither an institutional basic training, nor a continuous and mandatory education in institutional cybersecurity. There is no single magic bullet to solve the problem, but various mechanisms can be put in place to mitigate the risks and limit the hazards as much as possible.

Keywords : ***Cybersecurity - Hacking - Artificial intelligence***

Les attaques informatiques contre la technologie médicale : une réelle épidémie !

La sécurité informatique préoccupe très fortement les différents secteurs d'activité humaine. Même les plus grands acteurs industriels savent qu'ils ne sont pas à l'abri d'attaques, par ailleurs de plus en plus fréquentes et de plus en plus sophistiquées. Récemment, des organisations prestigieuses et supposées très bien protégées, comme la NASA, ont été obligées d'admettre, humblement et publiquement, avoir été la cible de criminels informatiques (1, 2). La deuxième annonce de la NASA est interpellante : l'attaque a été rendue possible par la simple connexion d'un ordinateur personnel introduit dans l'entreprise, ce qui est formellement interdit. Cette connexion était donc non autorisée et, par définition, non vérifiée par le personnel dédié à la sécurité informatique de l'agence. Vingt-trois dossiers sensibles ont été volés, mais, ce qui est pire encore, c'est que l'attaque a été identifiée après seulement 8 mois.

Si des structures telles que la NASA sont sensibles à ce genre de criminalité informatique, qu'en est-il du monde des soins, et en particulier du secteur hospitalier ? De plus, si dans le monde hospitalier, il existe de multiples annonces publiques de piratage ou «hacking», ce n'est pas le cas pour des structures informatiques qui trônent dans les cabinets privés, et qui - en règle générale - sont peu ou prou sécurisées, car souvent obsolètes et, quoi qu'il en soit, dépassées par la force de frappe et l'inventivité sans limite des criminels cybernétiques.

Depuis un certain temps, les annonces d'attaques informatiques contre les hôpitaux se multiplient. Ces attaques font régulièrement la une de la presse non médicale. Il semble bien que les données sensibles dans les dossiers médicaux personnels (DMP's), soient devenues une nouvelle cible lucrative. C'est notamment le cas depuis que le Hollywood Presbyterian Medical Center, en Californie, a payé en crypto-monnaie une somme équivalente à 17.000 dollars US à un hacker qui avait fait main basse sur leur système informatique (3). L'incitatif financier pour les pirates informatiques est puissant puisque l'on estime la valeur marchande d'un DMP à 1.000 dollars sur le «darknet», la face sombre et cachée d'internet (4). Faire un listing exhaustif de telles attaques est devenu tout simplement impossible. Mais certaines d'entre elles méritent notre attention.

Quelques exemples...

Dans le système de santé à St Louis aux USA, une analyse interne met en évidence que 33.000 dossiers ont été accessibles par internet pendant huit mois, tout simplement parce qu'un

(1) Service de Radiothérapie, CHU Liège, Belgique.

serveur avait été mal configuré (5). Des données sensibles telles que les noms des patients, dates de naissance, adresses, numéros de sécurité sociale, informations sur les traitements, étaient aisément disponibles durant ce laps de temps. Toutes ces données sont une mine d'or pour les cybercriminels qui peuvent les utiliser afin de frauder les instances qui financent les soins (facturation de prestations médicales non effectuées permettant un détournement d'argent).

En juin 2018, on a signalé dans la presse spécialisée qu'à Singapour, les criminels se sont emparés de 1.500.000 de DMP's, en ciblant tous les patients ayant consulté entre le 1er mai 2015 et le 4 juillet 2018. L'attaque était parfaitement bien structurée et organisée. Pour la majorité, ils ont essentiellement ciblé les données démographiques et les numéros d'identification. Par contre, pour 160.000 victimes, dont le premier ministre, ils se sont intéressés au type de médicaments prescrits en ambulatoire (6).

Pour des pays avec des populations importantes, le nombre de victimes peut être astronomique. C'est le cas pour l'attaque sur Banner Health en Arizona. Banner Health est un système de santé à but non lucratif, qui exploite 28 hôpitaux et plusieurs installations spécialisées dans six états américains. Il y a eu 3,5 millions de DMP's exposés. Ce qui rend l'attaque «originale», c'est que les criminels sont parvenus à pénétrer le réseau par le biais du système de paiement des boissons et des repas. De cette façon, ils ont accédé aux serveurs qui contenaient les données sensibles des patients (7).

Une histoire comparable nous vient du Oklahoma State University Center for Health Sciences. Le pirate informatique s'est introduit par le biais du serveur utilisé pour la facturation. Ce dernier contenait les données de 250.000 patients, en particulier les noms, les numéros d'identification (Medicaid), les médecins en charge, le(s) date(s) des prestations et les informations sur le type de traitement. Même si les responsables de l'institution visée ont clamé qu'il n'y a eu aucun vol de dossiers médicaux en tant que tel, il est un fait que toutes ces informations ont pu être utilisées dans un but de fraude (8).

Cette longue liste d'événements indésirables est malheureusement alimentée de façon continue (9). On pourrait naïvement croire que les hackers ciblent de préférence de grandes institutions de soins qui abritent, par définition, une quantité considérable de dossiers médicaux. L'incident récent en région liégeoise dément cette croyance. En effet, même des structures hospitalières belges, quelle que soit leur taille, semblent tout autant intéresser les criminels qui recherchent des proies faciles pour rançonner les responsables administratifs ou faire main basse sur l'information contenue dans les dossiers médicaux (10). Toutefois, un rapport récent montre qu'en nombre absolu, il y aurait l'amorce d'une diminution, si l'on compare l'année 2018 à 2017. Il n'en reste pas moins qu'on peut s'attendre, dans certains pays densément peuplés, à un «mega breach», qui pourrait impliquer des dizaines de millions de dossiers touchés par une seule attaque (11), dossiers qui trouveraient, à coup sûr, preneurs peu scrupuleux sur le «darknet».

Sécurité informatique : état des lieux et constats inquiétants

On estime que d'ici 2020, il y aura 20 milliards d'objets connectés reliés à l'Internet des Objets (IO). Chacun de ces objets connectés est un portail d'entrée potentiel pour les criminels. Par conséquent, selon l'agence Gartner (entreprise américaine de Conseil et de Recherche dans le domaine des techniques avancées), le marché de la sécurité informatique va littéralement exploser. Ce marché, plus que juteux, représente déjà, en 2018, la somme incroyable de 96 milliards de dollars (12), ce qui, sans aucun doute, offre de superbes perspectives professionnelles pour des hackers reconvertis…

Etat des lieux

Si les objets connectés sont une entrée facile, n'oublions pas pour autant les objets médicaux classiques, en particulier ceux disponibles depuis plusieurs années dans nos structures hospitalières (13). VECTRA (un des leaders mondiaux en matière de détection de la menace informatique, qui utilise la plateforme Cognito, une intelligence artificielle) signale que ces dispositifs médicaux qui prennent de l'âge, contiennent des tunnels HTTPS cachés non sécurisés (HTTPS = Hypertext Transfer Protocol Secure). Les tunnels HTTPS sont normalement censés protéger la confidentialité de l'échange de données entre un client et un serveur. Ils sont destinés à éviter l'écoute illicite et la falsification des données (14). Même si cette faiblesse particulière des HTTPS cachés est connue, il est clair aussi qu'il est inconcevable de demander aux hôpitaux de remplacer immédiatement tous les anciens systèmes par des applications plus sécurisées. C'est totalement irréaliste, car n'oublions pas que certaines de

ces machines sont amorties sur des périodes prolongées, pouvant aisément atteindre 10 ans.

Dans le monde des dispositifs médicaux classiques, il y a moyen de citer plusieurs autres exemples de hacking. Il y a, tout d'abord, le malware «Orangeworm» qui cible les ordinateurs nécessaires pour le fonctionnement des différentes machines utilisées en radiologie. Si le virus rencontre une information intéressante, il va se dupliquer automatiquement, et se propager dans le réseau (15). Dans un tout autre domaine, une alerte a été émise, en octobre 2018, par la Food and Drug Administration aux USA, pour un produit de MedTronic, le CareLinkTM. Ce produit est labellisé par la firme comme «un logiciel sécurisé accessible sur un site web, qui permet de télécharger les informations de la pompe d'insuline, et ainsi d'obtenir les rapports correspondants pour suivre l'évolution du diabète». Dans ce logiciel CareLinkTM, la faille majeure se trouve dans le processus de mise à jour. Medtronic a été obligé de retirer immédiatement la possibilité de mise à jour en ligne (16). On vient également de signaler une faille majeure dans le protocole de transfert de données par WiFi. Il s'agit de KRACK, un bug informatique, largement répandu dans le secteur des soins où l'on fait appel fréquemment au principe de transfert de données sans fil en utilisant le protocole WPA-2 (Wifi Protected Access 2). Ce protocole est d'ailleurs censé, en temps normal, protéger tous les réseaux modernes WiFi (17).

Les attaques pleuvent...

L'état des lieux est donc pour le moins inquiétant. Devant un tel constat, il est indispensable d'identifier les différents problèmes. Plusieurs rapports d'experts en font une liste non exhaustive. Le rapport produit par Carbon Black Inc (Société de Cyber-Sécurité basée à Waltham, Massachusetts) souligne l'importance de la multiplication et la sophistication des attaques. Pratiquement la moitié des institutions américaines disent avoir été la cible d'une attaque en 2018 (18). C'est aussi la conclusion du rapport «Data Security Incident Report» par BakerHostetler, prestigieux cabinet d'avocats aux USA qui regroupe plus de 1.000 hommes de loi (19). Ils mettent clairement en évidence une situation explosive constituée, d'une part, d'une infrastructure informatique insuffisante pour se prémunir efficacement du danger, et d'autre part, d'une accumulation d'informations hautement sensibles et particulièrement lucratives pour les hackers.

Causes multiples

Les experts de la société Aon, multinationale britannique actrice dans le domaine de la gestion des risques, évoquent les différentes causes d'une situation qu'ils taxent de chaotique : la multiplication des objets connectés, les menaces internes (mauvaise utilisation des systèmes informatiques par les professionnels de soins), les piratages de mots de passe et les manquements dans les systèmes de reconnaissance biométrique. Ils soulignent aussi l'absence trop fréquente d'un CISO (Chief Information Security Officer = responsable de la sécurité des systèmes d'information) dans les structures de soins, les rendant d'autant plus vulnérables (20). Et visiblement, les personnes qui siègent actuellement dans les conseils d'administration des différents hôpitaux ne sont pas particulièrement sensibilisées à cette problématique de sécurité informatique. En effet, une étude récente montre que 88 % des administrateurs interrogés n'ont aucune notion des risques en la matière, et 9 personnes sur dix ne savent même pas ce que représente l'intelligence artificielle (IA) et l'apprentissage machine (21). Pire encore, certains hôpitaux ne se rendent pas forcément compte qu'ils ont été victimes d'une attaque (22).

A ce constat, viennent s'ajouter deux mauvaises nouvelles. La première, c'est que les hackers ont accès, au minimum, au même niveau de technologie que celui mis en place par les hôpitaux pour se défendre. Le rapport «The malicious use of artificial intelligence: forecasting, prevention and mitigation», publié par the «Future of Humanity Institute», stipule qu'en ce qui concerne l'IA, on peut établir un parallélisme avec les drones autonomes : un drone capable de livrer un médicament est fondamentalement doté de la même technologie que celle qui est destinée à larguer une bombe (23, 24). La deuxième mauvaise nouvelle, c'est que ces pirates informatiques sont particulièrement doués et rapides. Ils seraient capables – selon une enquête menée par la société Nuix – de trouver des données dans un dossier patient en moins d'une heure (25), de rentrer dans le cœur même d'un système informatique hospitalier en moins de 15 heures, et, pour 23 % d'entre eux, en moins de 5 heures (26).

Dans une enquête menée par HIMSS (Health Care Information and Management Systems Society) de décembre 2017 à janvier 2018, auprès de 239 leaders du monde hospitalier, les auteurs du rapport clament que, dans 96 % des cas, l'acteur de la menace est identifiable.

Il s'agit du «phishing» (hameçonnage : on fait croire au destinataire qu'il se trouve sur un site officiel et on essaie de lui retirer des informations sensibles comme, par exemple, son mot de passe), de «hacking» (exploitation des failles du système de défense) ou de négligence interne. Dans 61 % des cas, le point d'entrée est un courriel malveillant (27).

Force est de constater que le maillon le plus faible en matière de sécurité informatique est bien le facteur humain. Les responsables de Verizon – entreprise de télécommunication américaine - constatent que le secteur des soins de santé est le plus exposé car les risques internes sont supérieurs aux risques externes (28). Plus de la moitié des attaques (56 %) proviennent de l'intérieur, 24 % sont des abus et 35 % sont des erreurs d'utilisation. Cette situation ne serait-elle pas fondamentalement liée au fait que ce secteur prépare particulièrement mal ses ressources humaines pour faire face à la criminalité cybernétique (29) ? C'est du moins l'avis émis par le «Institute for Critical Infrastructure Technology» (30).

Une prise de conscience environnementale s'impose

Il ne suffit plus simplement de dire que la structure informatique hospitalière répond aux critères établis dans le HIPAA (Health Insurance Portability and Accountability Act = loi votée par le congrès américain) ou dans le RGPD (Réglementation Générale de la Protection des Données = directive européenne). La plupart de nos institutions de soins sont, d'ailleurs, bien incapables de répondre réellement à toutes les exigences émises par l'Europe ! Il faut aller beaucoup plus loin. La sécurité informatique doit être placée tout en haut dans les priorités institutionnelles, car il est primordial de restaurer la confiance. Le problème aujourd'hui reste le sous-investissement en informatique hospitalière qui dure depuis plus de 10 ans, ce qui laisse le champ libre aux cybercriminels qui utilisent des techniques toujours plus évoluées (31). Ce qui est encore beaucoup plus inquiétant, c'est la confiance inébranlable qu'ont 70 % des leaders des institutions de soins dans leur propre système de sécurité informatique. Ils ne font que répliquer le trop répandu sacro-saint concept du «cela n'arrive qu'aux autres» (32). Toutefois, la plupart de nos institutions ne possèdent pas, tout simplement, les outils adéquats pour mesurer et surveiller le flux, la quantité et la variété des données personnelles qui entrent et sortent de l'institution.

Solutions potentielles (mais pas uniques ni «miracles»)

Il existe de multiples actions qui peuvent être mises en place afin de sécuriser le système. Le premier des éléments de solution est d'être conscient du danger, et de considérer que tout un chacun dans l'entreprise est concerné (33). La sécurité informatique institutionnelle est un réel sport d'équipe, car n'oublions pas qu'en face de nos institutions se trouvent de vrais teams constitués d'athlètes de très haut niveau en criminalité, parfois soutenus par certains gouvernements peu scrupuleux. Il faut donc une «défense collective contre une attaque collective». La collaboration et l'échange d'informations en matière de cybersécurité doivent dépasser les limites propres des institutions et s'étendre au secteur tout entier (33).

Si l'on veut obtenir une défense collective, il faut, bien entendu, que les employés soient rôdés à ce «sport». Tout sport de haut niveau nécessite des séances d'entraînement répétées. Et même si certains pensent qu'en passant par la mise en place de technologies informatiques sur le cloud (avec une sécurité assurée par de l'IA) (34), on peut faire l'économie d'un tel effort, il suffit de leur rappeler qu'un des facteurs de risque le plus important reste le facteur «interne», c'est-à-dire le facteur humain (35). Pour la formation des professionnels de soins, certains CISO (Chief Information Security Officer) se sont montrés particulièrement innovants. C'est le cas, par exemple, de Scott Larsen, au Beaumont Health System à Dearborn (Michigan, USA). Ayant fait le constat que la formation classique basée sur une présentation de type «powerpoint» était devenue totalement stérile et inintéressante pour les agents, il a fait appel à une société spécialisée en jeux interactifs (Security Mentor). Cette dernière a alors développé une douzaine de modules interactifs sous forme de jeux, ce qui a permis d'augmenter l'intérêt et l'adhésion des agents à la formation continue (36).

A la conférence HIMMS & Health 2.0 qui s'est tenue à Helsinki en 2019, plusieurs pistes de solutions ont été évoquées comme le concept «cybersecurity by design» (37). Cela recouvre, par exemple, le remplacement du trop classique «mot de passe» par des paramètres biométriques (l'empreinte digitale, l'empreinte de la paume de la main, la reconnaissance faciale, la reconnaissance de l'iris ou de la rétine) et, surtout, la multiplication des paramètres d'identification (20). Les experts réunis à Helsinki estiment qu'il faut mettre en place «un audit et une

certification raisonnable» (37). Ils insistent également sur la nécessité de la prévention, et cela passe forcément par des formations obligatoires pour les employés.

Il n'y aura jamais de solution miracle parfaitement étanche à toute velléité d'attaque. Mais il faut sensibiliser le monde professionnel au principe de la responsabilité partagée (33, 37). Il faut se préparer à une éventuelle attaque en rédigeant un plan de bataille comparable à ceux qu'ont les institutions hospitalières en cas de catastrophe naturelle. Ce plan doit, d'ailleurs, faire intégralement partie du plan catastrophe institutionnel. Une étude de IBM Security et du Ponemon Institute démontre que posséder un tel plan, et l'avoir testé, réduit le coût total d'une attaque en moyenne de 1,23 millions de dollars (38). Il faut aussi insister sur la responsabilisation des différents départements et services afin qu'ils définissent l'impact que peut avoir une attaque informatique à leur niveau en particulier (37).

Selon le rapport Carbon Black, il faut bien entendu effectuer des sauvegardes, mais il faut aussi envisager la conduite d'essais automatiques de compliance et de vulnérabilité (18). On évoque d'ailleurs, de plus en plus, la possibilité de faire appel à un «hacker éthique certifié» afin de tester les défenses du système avec les mêmes armes que celles utilisées par les pirates informatiques. Signalons qu'il existe déjà une agréation de «hacker éthique certifié» mise en place par le Conseil européen (39).

Conclusion

Le consensus est unanime : il y a un gouffre entre les capacités des hackers et les défenses établies dans nos institutions de soins. Nos structures semblent bien démunies, en particulier face à ce nouveau monde hyper-connecté. Un effort intense et rapide est indispensable si nous voulons maintenir la confiance de l'utilisateur.

Selon les experts du WEF (World Economic Forum), l'intelligence artificielle (seule capable de détecter efficacement les attaques et de les gérer en temps réel) et l'identification par facteurs biométriques vont largement modifier le paysage de la sécurité informatique dans les dix prochaines années. Ce même rapport souligne toutefois l'énorme danger que représentera l'avènement de la 5G, avec une meilleure latence, une meilleure densité et un débit beaucoup plus important. En effet, la vitesse d'échange d'informations par internet va s'accroître d'un facteur 1.000 d'ici 2025 (40). Il nous reste peu de temps pour réfléchir à la mise en place de nouvelles architectures informatiques, mieux à même de résister aux multiples attaques. En effet, la 5G est déjà présente dans certains pays (comme la Finlande, par exemple). Il faut aussi radicalement changer la culture des organisations de soins, car la coopération au-delà des simples frontières institutionnelles est, et sera, indispensable pour juguler l'énorme potentiel de cybercriminalité à l'ère de la 5G (40).

Bibliographie

Les références web citées dans cet article sont consultables via le lien suivant :

https://www.rmlg.ulg.ac.be/ANNEXES/A20200212.pdf

Les demandes de tirés à part doivent être adressées au Pr P.A. Coucke, Service de Radiothérapie, CHU Liège, Belgique.

Email : pcoucke@chuliege.be