FOCUS

Le défi de la cybersécurité dans les soins de santé

Décembre 2020

Introduction

Comme chaque année en octobre, l'Union européenne organise son mois de la cybersécurité. Il s'agit d'une campagne de promotion de la cybersécurité à destination des citoyens et des entreprises. Elle est constituée d'un travail de sensibilisation et d'un rappel des bonnes pratiques. Cette campagne est coordonnée par l'ENISA, l'agence de l'Union européenne pour la cybersécurité. A cette occasion, nous vous proposons de (re)découvrir les bases de la cybersécurité au travers de ce Focus.

Les bases de la sécurité informatique

La sécurité informatique se décline en trois pôles : la confidentialité, l'intégrité et la disponibilité.

La confidentialité empêche la divulgation non autorisée des données. En d'autres mots, seules les personnes habilitées ont accès aux informations. ***Je dépose 1000€ à la banque, je désire que personne à part mon banquier et moi ne soyons au courant de la transaction***. La confidentialité peut être assurée par le cryptage ou par le contrôle d'accès.

Dans le domaine médical, les très nombreuses données traitées sont souvent sensibles, à l'image des données médicales et du numéro de registre national, par exemple. Une perte de confidentialité telle qu'une fuite de données médicales suite à un piratage serait, outre une violation du RGPD, fort dommageable pour le ou les patients concerné(s), mais également pour la réputation de l'institution.

L'intégrité assure que les données n'ont pas été modifiées, trafiquées ou corrompues. Seules les personnes habilitées ont le droit de modifier les données. Les modifications non-autorisées seront alors le fait de personnes non habilitées, de logiciels malicieux (malwares) ou d'erreurs informatiques ou humaines. ***Je dépose 1000€ à la banque, j'y retourne deux mois plus tard et le solde affiché n'est plus que de 100€***. Une technique utilisée pour prévenir une perte d'intégrité est le hachage qui appose une signature numérique servant à valider la donnée initiale.

Dans le domaine médical, une perte d'intégrité pourrait mener à des erreurs de diagnostic ou de traitement si certaines données du Dossier Patient Informatisé (DPI) telles que les antécédents, le groupe sanguin ou encore les traitements en cours venaient à être modifiés.

santhea

La disponibilité assure que les données et les services sont disponibles quand cela est nécessaire. Pour certaines organisations, cela peut être du lundi au vendredi de 8h à 17h, pour d'autres, comme pour les établissements de soins, cela sera 7 jours sur 7, 24h sur 24. ***Je dépose 1000€ à la banque, j'y retourne 2 mois plus tard pour les retirer mais une panne informatique empêche l'accès aux comptes et toute autre opération telle que le retrait***. La disponibilité peut être assurée par la redondance des données, des systèmes, des sites ou des alimentations électriques ou encore par les sauvegardes, entre autres.

Dans le domaine médical, une perte de disponibilité pourrait entraîner, par exemple, une perte d'accès au DPI ou au stock de la pharmacie, mais aussi une panne totale de la téléphonie interne et externe, et ainsi obliger l'institution à déclencher le Plan d'Urgence Hospitalier (PUH).

La situation actuelle

Longtemps épargnés par les attaques informatiques, les établissements de soins n'en sont aujourd'hui plus à l'abri. Il y a un an, le CHU de Rouen a été la cible d'une cyberattaque par ransomware qui a complètement neutralisé ses systèmes informatiques durant plusieurs jours, obligeant le personnel à revenir « *à la bonne vieille méthode du papier et du crayon* », sans accès à l'historique des patients.

L'attaque par ransomware va provoquer le cryptage des données, empêchant leur accès par l'utilisateur et l'entreprise. L'attaquant exigera le payement d'une rançon en échange du rétablissement de l'accès. C'est un des types d'attaques les plus courants aujourd'hui. Les principaux vecteurs de ransomwares sont les mails contenant des liens ou des pièces jointes frauduleux et les fichiers illégaux téléchargés.

En septembre de cette année, une cyberattaque a viré au drame, une patiente d'un hôpital de Düsseldorf n'ayant pu être opérée à temps suite à l'indisponibilité des systèmes informatiques conséquente à une attaque informatique. Il s'agit du premier décès avéré d'un patient à la suite d'une telle attaque en Europe.

Plus récemment, fin septembre, l'Universal Health Services (UHS), une chaîne d'hôpitaux américains regroupant 400 établissements de soins, a été la cible d'une cyberattaque en pleine pandémie, allongeant l'attente aux urgences et empêchant les soignants de savoir précisément qui de leurs patients étaient infectés par la COVID-19.

Les mesures à prendre

Les cyberattaques représentent donc un danger grandissant pour les hôpitaux et la santé de leurs patients.

L'ENISA a publié en début d'année une liste de recommandations à destination des directions générales et des responsables informatiques des établissements de soins.

Parmi celles-ci citons :

- L'implication du département informatique dans la passation de marché, afin que la cybersécurité soit prise en compte dès la passation de marché ;
- La mise en œuvre d'un processus d'identification et de gestion des vulnérabilités, afin de garder sous contrôle les problèmes de sécurité potentiels ;
- Le développement d'une politique de mise à jour matérielle et logicielle. Plusieurs attaques récentes n'auraient pas été couronnées de succès si les systèmes avaient été mis à jour ;
- Le renforcement de la sécurité des communications sans fil, afin d'éviter tout dispositif indésirable et tout accès non-autorisé ;
- L'établissement de politiques de test rigoureuses pour tout nouveau système connecté au réseau informatique (y compris les équipements biomédicaux) ;
- La mise en place d'un plan de continuité d'activité (Business Continuity Plan – BCP) afin de rétablir rapidement les fonctions de base de l'hôpital en cas de désastre ;
- La journalisation des évènements afin de retracer plus facilement l'historique d'une attaque et d'évaluer quelles données ont été compromises.

La sensibilisation des utilisateurs aux risques informatiques est également un composant essentiel de la sécurité des établissements de soins.

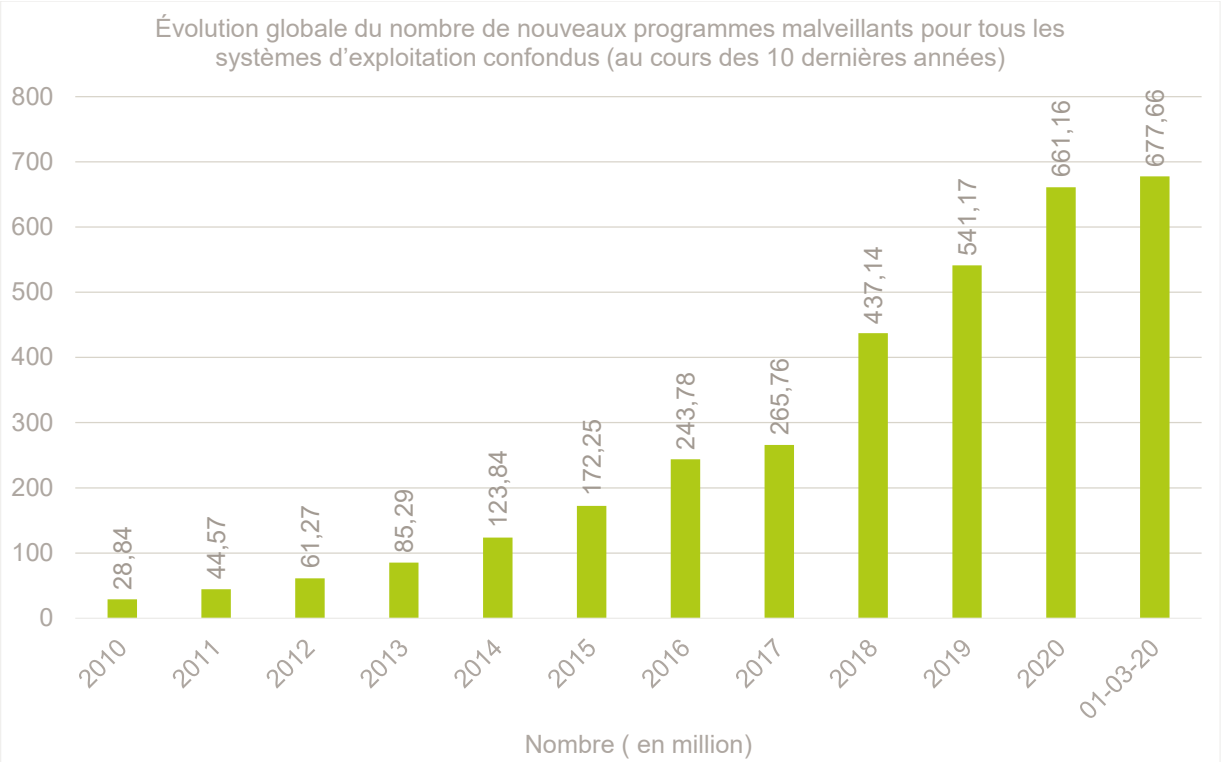
Celle-ci peut notamment couvrir :

- L'identification de pièces jointes suspectes dans les e-mails ;
- L'identification des hyperliens frauduleux dans les e-mails ;
- L'identification d'attaques par ingénierie sociale.

L'ingénierie sociale (social engineering) est une technique utilisée par les cybercriminels pour inciter les gens à partager des informations confidentielles.

Elle mise sur l'instinct de confiance de l'être humain pour voler des informations qui pourront ensuite être mises à profit lors d'une cyberattaque.

Elle peut consister en un simple coup de téléphone émanant prétendument du service informatique demandant à vérifier un mot de passe ou en un mail semblant provenir d'un collègue et renvoyant vers un formulaire dans lequel il est demandé de remplir des informations confidentielles.



Source : AV-Test (Institut de recherche indépendant allemand pour la sécurité informatique) - 2020

La crise de la COVID-19 a été l'occasion pour les cybercriminels de surfer sur l'actualité. De nombreux faux messages ont circulé à propos :

- *De collectes de fonds pour les victimes du virus ;*
- *De vente de masques de protection ;*
- *D'offres de vaccins ;*
- *De sites contenant de fausses informations sur la crise.*

Ces messages avaient pour but d'inciter les utilisateurs à cliquer sur un lien afin :

- *D'installer un logiciel malveillant ;*
- *D'obtenir des informations financières afin de soutirer de l'argent.*

Les actions de santhea

Santhea publie régulièrement des notes d'alerte ou de sensibilisation aux risques informatiques, et réuni plusieurs fois par an un groupe de travail "Informatique et sécurité" réunissant les directeurs informatiques et les responsables de la sécurité des systèmes informatiques (RSSI). Les sujets qui y sont traités sont présentés par des membres de santhea ayant déployé des techniques ou solutions novatrices et désireux de partager leurs expériences avec les autres institutions. Parmi les sujets abordés jusqu'à présent citons :

- La mise en conformité ISO 27001;
- L'authentification des patients au moyen d'itsme;
- La micro-segmentation des réseaux informatiques hospitaliers;
- La gestion des comptes à privilèges.

Editeur Responsable : Y. Smeets, Directeur général

deq@santhea.be