Cybercriminalité: dangers réels et mesures efficaces

Avec la numérisation, de nouveaux risques et menaces apparaissent également dans le secteur de la santé. Les utilisateurs partagent par conséquent la responsabilité de la sécurité de leurs systèmes et de leurs données. La protection systématique des terminaux et un comportement sûr contribuent à protéger les systèmes contre les attaques et à conserver les données sensibles en toute sécurité. Cet article donne un aperçu des méthodes d'attaque et des mesures de protection.

LUCAS SCHULT
Directeur général (CEO) et responsable informatique (CIO), Health Info Net AG, Seidenstr. 4, CH-8304 Wallisellen, lucas.schult@hin.ch, Tél.: +41 (0)52 235 02 70, www.hin.ch/fr

Cyberattaques contre le secteur de la santé Dans le monde entier, les cyberattaques visent de plus en plus souvent le secteur de la santé. Les institutions et les acteurs du système de santé ne sont souvent toujours pas encore suffisamment protégés et offrent donc une cible relativement facile. Comme les données en cas d'attaques contre les hôpitaux et les institutions comparables (à l'aide de rançongiciels, par exemple) sont sensibles et que ces attaques peuvent éventuellement mettre des vies en péril, de nombreuses personnes concernées sont rapidement prêtes à payer des rançons afin d'avoir à nouveau accès à leurs données et de pouvoir reprendre rapidement le travail.[1]

«Wanna Cry» a, par exemple, montré en 2017 les conséquences graves que peut entraîner une cyberattaque contre le secteur de la santé. Ce logiciel malveillant, combinant rançongiciel et ver, exploite une faille des serveurs Windows pour s'infiltrer dans les appareils et s'y multiplier. Outre les grandes entreprises comme FedEx ou Renault, le National Health Service (NHS) britannique avec plusieurs hôpitaux ont été victimes de ces attaques. Suite à celles-ci, les services de sauvetage n'ont pu travailler que de manière limitée, des opérations ont dû être reportées et les données des patients n'étaient que partiellement accessibles. Les hôpitaux s'en sont néanmoins tirés à bon compte. L'attaque n'a pas coûté de vie.[2]

Étant donné que les cyberattaques sont toujours plus sophistiquées, il ne suffit plus de protéger la communication électronique et les données sensibles en les cryptant. La protection des terminaux et en particulier le comportement à la fois conscient des risques et soucieux de la sécurité – «awareness» ou prise de conscience des utilisateurs – jouent un rôle déterminant.

Appareils différents – risques différents Du réfrigérateur à l'ampoule intelligente en passant par le bracelet fitness: il n'existe quasiment plus de catégorie d'appareils électroniques qui ne puissent être connectées à un réseau. Les «appareils de l'Internet des objets» (appareils IoT) communiquent entre eux via Internet et se mettent mutuellement des informations à disposition. Sous de nombreux aspects, les appareils IoT offrent souvent une valeur ajoutée à leurs utilisateurs, mais ils créent également de

nouveaux risques et angles d'attaque.

Il existe aujourd'hui déjà plus d'appareils IoT que d'êtres humains et leurs nombre ne cesse de croître. Les risques de sécurité naissent parce que ce type d'appareils ne sont qu'insuffisamment ou pas du tout protégés. Les failles de sécurité des appareils IoT sont souvent exploitées pour attaquer, à travers elles, des infrastructures critiques. Mais même les données récoltées par les appareils IoT et qui sont en parties analysées peuvent être susceptibles d'intéresser financièrement. Les bracelets fitness, smartwatches et appareils similaires en sont un bon exemple. Ces soi-disant «Wearables» ou appareils technologiques portables ne collectent pas uniquement des données sur la fréquence du pouls et les activités sportives, mais les croisent également avec les données temporelles et géographiques.

Dans le secteur médical aussi, le nombre d'appareils connectés à Internet grandit continûment. Lorsqu'à cause de cyberattaques, des appareils ne fonctionnent pas ou affichent des dysfonctionnements en salle opératoire et au service des soins intensifs, cela peut mettre en danger la santé ou la vie des patients.[3]

Méthodes d'attaque fréquentes

De nombreuses méthodes sont utilisées pour accéder illégalement à des appareils et données. Ci-après, nous vous présentons un éventail des modes d'obtentions illégales fréquents des données.

Logiciel malveillant

Les pirates accèdent aux données à l'aide de logiciels malveillants (malware en anglais) introduits dans le système informatique.
En cas d'utilisation d'un rançongiciel ou ransomware, par exemple, (de «ransom», rançon, en anglais), les données de l'ordinateur de travail sont cryptées et le/la propriétaire de ce dernier n'a plus accès à ses propres données. Dans ce cas, on demande généralement aux personnes concernées de payer une rançon afin de décrypter leurs données. Les logiciels espions ou spyware (de l'anglais espionner) s'installent généralement sur l'ordinateur à l'insu de son utilisateur. Ce type de logiciel malveillant a pour but d'accéder aux mots de passe, aux coordonnées bancaires et autres données sensibles.

Phishing

L'objectif du phishing est d'accéder aux informations personnelles moyennant des courriels, sites Internet ou messages SMS falsifiés et de les utiliser dans le cadre d'une usurpation d'identité. Selon le type d'information obtenue, les conséquences du phishing peuvent, par exemple, être un compte pillé ou l'utilisation abusive d'une carte de crédit.

DDoS (Distributed Denial of Service ou attaque par déni de service)

L'attaque DDoS est une attaque ciblée et décentralisée contre l'infrastructure et les réseaux d'entreprises, sites Internet et organisation étatiques. Son objectif est de créer une surcharge des sites Internet ou services à travers une inondation de demandes et d'attaques, qui empêchent les usagers de les utiliser. Le pirate a la disponibilité du système en ligne de mire.

Attaque 0day

L'attaque dite «0day» (zero day en anglais soit «jour zéro») exploite la faille de sécurité des logiciels ou du matériel informatique avant que des mises à jour de sécurité ou des mesures de sécurité soient disponibles. En règle générale, ce genre d'attaques a lieu le jour précis où ces failles de sécurité sont découvertes.[4]

Auteurs – qui se cache derrière une attaque?

Des groupes criminels
Un danger substantiel part des organisations criminelles.[5] Ces dernières visent la plupart du temps des entreprises ou organisations, mais également des particuliers, que ce soit pour accéder à leurs moyens financiers ou données, et dans ce dernier cas de figure, les données obtenues sont généralement utilisées à des fins financières. Ces attaques sont généralement à classifier sous attaques de phishing, de logiciel malveillant ou DDoS.

Insider
Insider können für Regierungen, Firmen oder Organisationen eine Bedrohung darstellen. Motive können Whistleblowing, Geld (z. B. beabsichtigter Weiterverkauf von Daten), aber auch persönliche Rache sein. Angriffe können z. B. durch Missbrauch eigener Berechtigungen, Malware oder Social Engineering erfolgen.[6]

Hacktivistes
Les groupes de protestation font également usage des cyberattaques afin d'imposer leurs objectifs. Leurs cibles sont, en règle générale, des gouvernements ou des organisations politiques. Tout comme les organisations criminelles, les hacktivistes se servent également du phishing, des logiciels malveillants ou de DDoS et, par conséquent, les frontières avec la criminalité organisée s'estompent.

Script Kiddies
Les script kiddies (ou «skiddies») forment une catégorie à part. Il s'agit de hackers néophytes qui ne possèdent pas de connaissances approfondies et qui ont seulement pour but de s'amuser ou de vouloir impressionner autrui en attaquant des systèmes non protégés à l'aide d'outils librement accessibles sur Internet. En plus des entreprises ou des organisations, les particuliers peuvent également en devenir les victimes.

Mesures de protection

De nombreuses mesures peuvent être mises en œuvre sans grand effort et améliorent considérablement la protection des équipements. On peut classer les mesures principales en trois catégories: les mesures techniques, organisationnelles et de comportement.

Mesures techniques
Parmi les mesures techniques, on compte entre autres la protection des équipements à l'aide d'un pare-feu et d'un logiciel antivirus. En particulier, les utilisateurs d'appareils Apple se croient ici faussement en sécurité.[7] Il est par ailleurs recommandé d'installer toujours immédiatement les mises à jour des systèmes d'exploitation, des navigateurs Web et des programmes de protection anti-virus afin de combler immédiatement les failles de sécurité.

Mesures organisationnelles
La sécurité informatique incombe aux dirigeants et implique des instructions, directives (par exemple concernant la gestion des données) et processus (par exemple les sauvegardes régulières). La prise de conscience et un comportement correspondant des collaborateurs et collaboratrices sont de première priorité, pour cette raison, des formations sont indispensables.

Si, par exemple, un logiciel anti-virus échoue lors du contrôle d'une pièce jointe à un courriel, les collaborateurs formés en conséquence peuvent éviter d'importants dommages s'ils n'ouvrent pas le courriel de manière irréfléchie.

Règles de conduite
Afin d'éviter que des tiers aient accès à vos données, il est essentiel d'utiliser des mots de passe sécurisés. Il est également important de ne pas utiliser plusieurs fois le même mot de passe.

Il faut être particulièrement prudent avec les courriels provenant d'expéditeurs inconnus. La majorité des virus circulent sous formes de pièces jointes à des courriels. Les pièces jointes d'expéditeurs inconnus devraient être ouvertes avec prudence ou, en cas de doute, pas du tout. Pour la transmission de données sensibles, le cryptage des données et l'identification sûre du destinataire sont des conditions sine qua non.

Notes finales

1 Cf. Article sur Global Healthcare du 8 novembre 2018: www.tinyurl.com/y6k4sxh6, Accès 2.04.2019.

2 Cf. Article sur la NZZ on-line du 18 mai 2017: www.tinyurl.com/knw8oh3, Accès 2.04.2019.

3 Cf. Article sur ZDNet du 15 mars 2018: www.tinyurl.com/y2gcrghn, Accès 2.04.2019.

4 Cf. article du blog «Schneider on Security» du 17 janvier 2019: www.tinyurl. com/y7tspa9l, accès 02.04.2019.

5 Cf. à l'étude «Internet organised crime threat assessment 2018» d'Europol: www.tinyurl.com/y2p6m9po, accès 02.04.2019.

6 Indications de la Centrale d'enregistrement et d'analyse MELANI concernant le Social Engineering: www.tinyurl. com/y25qojjz, accès 02.04.2019.

7 Cf. article sur heise online du 26. juillet 2017: www.tinyurl.com/y2g8ktsa, accès 02.04.2019.