FMH SERVICES

Savoir réagir en cas de cyberattaque dans le système de santé

Dans cet article, vous apprendrez comment protéger votre cabinet ou votre institution des cyberattaques et comment vous comporter correctement en cas d'urgence.

Les outils numériques facilitent l'administration des cabinets médicaux pour les professionnels de la santé et permettent d'améliorer l'efficacité des processus dans le travail quotidien. Mais malheureusement, la numérisation s'accompagne aussi de nouveaux risques et de nouvelles menaces, car le système de santé est lui aussi de plus en plus souvent pris pour cible par les cybercriminels.

Avec la numérisation, les cyberattaques sont de plus en plus fréquentes. Le fait qu'elles puissent toucher tout un chacun – y compris les cabinets médicaux, les hôpitaux ou d'autres institutions du système de santé –, est malheureusement une réalité : d'une part, le système de santé est une cible attrayante pour les cybercriminels en raison de ses données sensibles et, d'autre part, les victimes de ces attaques sont souvent choisies au hasard plutôt que spécifiquement.

La défense doit précéder l'attaque

Les personnes et les institutions qui manipulent des données sensibles portent la coresponsabilité de la sécurité de leurs systèmes et de leurs données. C'est pourquoi il est essentiel de prendre des mesures préventives pour maintenir le plus haut niveau de sécurité des systèmes informatiques et par conséquent des données. N'oubliez pas : plus il est difficile pour les cybercriminels de s' attaquer à une institution, moins celle-ci devient une cible attrayante pour une cyberattaque.

Les principales mesures de protection peuvent être classées en trois catégories :

1. 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. Par ailleurs, il est important de toujours installer immédiatement les mises à jour des systèmes d'exploitation, des navigateurs Web et des programmes antivirus afin de combler immédiatement les possibles lacunes de sécurité. La FMH a publié un document [1] à ce sujet, qui donne aux médecins de cabinet un bon point de repère pour l'informatique de leur cabinet. Il comprend des exigences qui garantissent un niveau minimum de sécurité pour les données, les informations et l'infrastructure informatique

2. Mesures organisationnelles
Par dispositions organisationnelles, on entend la mise en place de processus et de directives par le propriétaire du cabinet. Il peut s'agir par exemple de l'exécution de sauve-gardes régulières ou de directives aux collaborateurs concernant la manipulation des données et des systèmes.

3. Mesures comportementales
Même une infrastructure informatique sécurisée ne peut pas garantir une protection à 100% contre les cyberattaques. Et si un e-mail de phishing parvient à contourner le logiciel antivirus et atterrit dans la boîte de réception du cabinet médical, c'est alors la personne devant l'ordinateur qui fait la différence: en s'abstenant d'ouvrir la pièce jointe du message infectée par le virus et en contactant à la place le responsable informatique, elle peut éviter de gros dégâts. C'est pourquoi il est indispensable d'organiser régulièrement des formations et de sensibiliser les collaborateurs au thème de la sécurité informatique.

Comportement correct en cas de cyberattaque
Une infrastructure informatique sécurisée et des collaborateurs bien formés compliquent la tâche des cybercriminels et réduisent la probabilité d'une cyberattaque réussie contre l'institution en question. Néanmoins, il est essentiel que tous les collaborateurs sachent également comment se comporter en cas d'attaque, car dans une telle situation, il est essentiel d'agir de manière rapide

et efficace. Nous vous recommandons de mettre à la disposition de vos collaborateurs une fiche d'information contenant les principales mesures d'urgence. Celle-ci devrait également contenir les coordonnées de la personne ou du service à contacter en cas d'urgence.

Pour vous aider, HIN a élaboré une liste de contrôle des mesures immédiates. Voici quelques points importants de cette dernière :

- Agir rapidement : en cas de suspicion d'attaque, n'attendez pas et agissez immédiatement.
- Déconnecter les appareils infectés du réseau : éteignez les adaptateurs WLAN et, pour les appareils reliés par un câble réseau, débranchez ce câble. Si les appareils infectés ne peuvent pas être clairement identifiés, déconnectez l'ensemble du réseau d'Internet.
- Supprimer le message : supprimez le message avec la pièce jointe malveillante de tous les comptes de messagerie, y compris de la corbeille.
- Informer : informez toutes les personnes travaillant sur les postes de travail. Vous éviterez ainsi que le message contenant la pièce jointe malveillante ne soit ouvert sur un autre appareil.
- Consulter le partenaire informatique : impliquez votre partenaire ou support informatique. Celui-ci peut évaluer l'ampleur des dégâts et vous aider dans la suite de la procédure.
- Signaler l'incident : nous vous recommandons de signaler la cyberattaque au Centre national pour la cybersécurité (NCSC).

Vous trouverez la liste de contrôle complète ici : www.hin.ch/cyberattaque

Faut-il payer la rançon en cas d'attaque?
Une méthode d'attaque fréquente est le rançongiciel, également appelé «ransomware». Lors d'une attaque par ransomware, les données de votre outil de travail sont cryptées et vous ne pouvez plus y accéder. Dans ce cas, on vous demande généralement de payer une rançon pour pouvoir accéder à nouveau aux données. Ceci est toutefois peu recommandé, car le paiement ne garantit pas la récupération de vos données. En outre, votre argent aide les auteurs à développer leurs méthodes d'attaque et les incite à en commettre d'autres. Dans le cas des ransomwares également : la prévention est la meilleure défense. Investissez dans une solution de sauvegarde complète pour votre cabinet ou votre institution afin de ne pas avoir à craindre pour vos données en cas d'urgence. Le mieux est de discuter du processus de sauvegarde avec votre partenaire ou support informatique.

Sources
[1] «Exigences minimales de la FMH pour la sécurité informatique des cabinets médicaux», disponible sur https://www.fmh.ch/fr/prestations/ehealth/securiteinformatique.cfm

Articles intéressants
1. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infosunternehmen/aktuelle-themen/cyberangriffe-gegen-firmen.html
2. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infosunternehmen/aktuelle-themen/schuetzen-sie-ihr-kmu.html
3. https://www.ncsc.admin.ch/ncsc/fr/home/infos-fuer/infosunternehmen/vorfall-was-nun/ransomware.html

A Propos
Uwe Gempp, Architecte CSO & IT

Health Info Net AG
Seidenstrasse 4
8304 Wallisellen
Téléphone 0848 830 740
uwe.gempp@hin.ch
www.hin.ch