FMH SERVICES

Comment protéger votre cabinet contre les cyberattaques?

La numérisation s'accompagne d'une augmentation des cyberattaques. Le fait qu'elles puissent toucher tout le monde, y compris les cabinets médicaux et les institutions du système de santé, est malheureusement une réalité. Si l'on a conscience du danger et que l'on s'y prépare en conséquence, on ne sera pas démuni face aux cybercriminels.

En 2023, le nombre de cyberattaques perpétuées en Suisse a une nouvelle fois augmenté. Le système de santé avec ses données sensibles est une cible privilégiée des cybercriminels. Et comme les victimes sont généralement choisies aléatoirement, ces attaques peuvent toucher n' importe qui.

Rançongiciels : lorsque les données apparaissent sur le darknet
Vous vous souvenez peut-être de « Play », un nom souvent cité dans les médias en 2023. Il s'agit d'un groupe criminel qui a lancé de nombreuses attaques par rançongiciels contre des entreprises suisses. Lors de telles attaques, les cybercriminels tentent d'accéder aux données sensibles, les cryptent et exigent ensuite le versement d'une rançon pour le décryptage. Souvent, ils menacent de publier les données si la rançon n'est pas payée.

Parmi les victimes de « Play » figuraient notamment Xplain, une entreprise qui fournit des logiciels aux autorités, et le prestataire informatique bernois Unico Data AG. Lors des deux attaques, des données des entreprises clientes ont été dérobées et en partie publiées sur le darknet. Elles provenaient de l'Office fédéral de la police (fedpol), des CFF, du canton d'Argovie, de la chaîne de cinémas Pathé et du groupe Siloah, un fournisseur de prestations dans le domaine de la gériatrie de la région de Berne. En juin 2023, les entreprises de médias NZZ et CH Media ont été attaquées, ce qui a conduit au vol de données d'adresses de membres de la FMH.

Déni de service : surcharge malveillante de sites internet
Les attaques par déni de service (DDoS, DistributedDenial of Service) poursuivent un autre but. Les hackers tentent de surcharger les serveurs en augmentant artificiellement le nombre de demandes. En conséquence, les sites internet attaqués ne sont plus joignables ou seulement de manière limitée. On citera comme exemple l'attaque contre le site internet des Chambres fédérales www.parlament.ch en juin 2023, qui avait rendu le site temporairement injoignable.

Protégez votre cabinet
Mieux vous protégez l'infrastructure informatique de votre cabinet ou institution, plus vous compliquez la tâche des cybercriminels et réduisez le risque d'être victime d'un dommage en raison de leurs agissements. Nous vous donnons ci-après quelques conseils que vous pouvez mettre en oeuvre vous-même ou avec le soutien de votre partenaire informatique.

Maintenez votre infrastructure à jour
Les systèmes d'exploitation et logiciels dépassés sont une porte d'entrée très prisée des cybercriminels. Les mises à jour permettent de combler les lacunes de sécurité. Pour protéger au mieux votre cabinet ou institution, vous devez vous assurer que votre infrastructure informatique, c'est-à-dire chaque appareil, est à jour.

- Maintenez votre système à jour. Cela comprend les systèmes d'exploitation des appareils ainsi que les navigateurs, les logiciels de messagerie, les logiciels antivirus et d'autres logiciels utilisés sur les appareils.
- Installez immédiatement les mises à jour, en particulier lorsqu'il s'agit de mises à jour de sécurité.
- Effectuez régulièrement des sauvegardes de vos systèmes.

Protégez chaque appareil
Un ordinateur ou smartphone sans protection suffisante permet aux cybercriminels d'attaquer votre institution. Il peut être utile de dresser un inventaire de tous les appareils utilisés afin de garder une vue d'ensemble des mesures de protection prises.

- Installez sur chaque appareil de votre institution une protection antivirus à jour et activez les fonctions de sécurité de votre système d'exploitation. Cela vaut pour les appareils Windows et Mac.
- Protégez tous vos appareils (ordinateur, ordinateur portable, routeur, smartphone etc.) avec des mots de passe sûrs qui comportent au moins huit à dix caractères, y compris des chiffres et des caractères spéciaux.
- Mettez en place des droits d'utilisateur limités et ne travaillez pas avec le compte administrateur.

Une vigilance permanente

La meilleure infrastructure technique ne vous sera pas d'un grand secours si vos utilisateurs ne se comportent pas correctement. Un simple clic peut, dans le pire des cas, causer d'importants dégâts. Vous devez donc en permanence avoir conscience de l' importance de la sécurité informatique. Cela vaut pour chaque collaborateur ou collaboratrice, de l'assistante médicale au médecin-chef.

- Soyez prudent lorsque vous recevez des courriels suspects, même s'ils proviennent d'expéditeurs que vous connaissez, car les données de l'expéditeur peuvent facilement être manipulées.
- Effacez immédiatement les messages suspects, sans ouvrir les éventuels fichiers joints. Supprimez le message également dans votre corbeille et dans votre logiciel de messagerie.
- Ne cliquez jamais sur des liens dans des courriels suspects et n'ouvrez jamais les fichiers joints.
- Utilisez des mots de passe sûrs pour vos comptes d'utilisateurs.
- Attention lorsque vous naviguez sur internet ! Ne téléchargez pas de logiciels inconnus. Veillez à un cryptage
- Ne transmettez des données sensibles que de manière cryptée à des destinataires clairement identifiés.

Un investissement utile

Une cyberattaque peut causer d'importants dégâts: une interruption de l'exploitation normale du cabinet de plusieurs heures ou jours, des frais pour rétablir les données, une contrainte et un stress considérables pour vous, sans oublier la perte de confiance de vos patientes et patients s'ils doivent craindre que leurs données de santé apparaissent sur le darknet. Oui, une infrastructure informatique bien entretenue, une sauvegarde appropriée et si possible la formation de tous les collaborateurs et collaboratrices demandent une planification et un travail important, mais peuvent aussi vous épargner bien des problèmes !

i Comment reconnaître les courriels malveillants

— Courriels impersonnels
— Formule de salutation erronée
— Demande directe de cliquer sur la pièce jointe ou sur le lien
— Demande prétendument urgente
— La partie connue de l'adresse électronique est utilisée plusieurs fois, mais n'est pas davantage personnalisée
— Les liens renvoient vers d'autres cibles que le prétendu expéditeur (vous reconnaissez ce-la en déplaçant avec la souris le curseur sur le lien, mais sans cliquer dessus).

À noter : les courriels malveillants sont fréquemment bien camouflés. Ils ne comprennent souvent pas tous les points susmentionnés.

A Propos

Daniel Huser, responsable du secteur gestion de projet & architecture IT
membre de la direction élargie

Health Info Net SA
Seidenstrasse 4
8304 Wallisellen
Téléphone 0848 830 740
daniel.huser@hin.ch
www.hin.ch