STUDERUS
network technologies

La menace des ransomwares

Dans cet entretien, le responsable IT de Studerus SA, Hugo Bosshard, répond à des questions sur les ransomwares et vous donne des conseils et des informations utiles.

Comment jugez-vous la menace actuelle des ransomwares ?
Le danger est très important, croissant et difficile à évaluer. Un point fait toutefois consensus : la solution absolue qui résoudrait tous les problèmes relatifs aux ransomwares n'existe malheureusement pas encore. Le secteur de l'informatique en est conscient et nous laisse espérer des solutions. Mais en attendant nous devons accepter la situation actuelle et nous protéger au maximum avec les solutions disponibles actuellement.

Peut-on sensibiliser davantage les utilisateurs face aux ransomwares ?
Pour sensibiliser nos collaborateurs nous leur avons proposé un cas concret. Une fausse candidature a été transmise par email à trois personnes différentes. Une de ces personnes a finalement ouvert cette candidature, qui était contaminée par un ransomware, et ce malgré une alerte macro de Word. Heureusement, l'antivirus installé sur l'ordinateur du collaborateur a permis d'éviter le pire. Suite à cette mise en situation, nous avons réalisé une formation de sécurité informatique pour tous les collaborateurs, au cours de laquelle nous avons échangé sur le cas concret et tiré des conclusions. Je suis convaincu que cette formation a sensibilisé nos collaborateurs qui traiteront désormais correctement les informations provenant de sources externes (email, navigateur, etc.). A l'avenir nous continuerons d'effectuer ce type de formations.

« La solution absolue qui résoudrait tous les problèmes n'existe malheureusement pas encore. »

Comment un ransomware peut-il être bloqué dans des emails entrants ?
Pour commencer, il est bien sûr nécessaire d'avoir une solution antispam avec un antivirus intégré. Toutefois les attaques ransomware sont de plus en plus sophistiquées et ne sont malheureusement pas toujours détectées par ces solutions, même avec la toute nouvelle technologie « sandbox ». Chez Studerus SA, tous les emails avec pièces jointes suspectes sont donc bloqués et mis en quarantaine. Un collaborateur de l'équipe IT doit alors traiter manuellement la quarantaine en vérifiant la fiabilité de l'email et puis en le transmettant au destinataire. Ce procédé est très chronophage, mais très efficace dans la situation actuelle. Pour des comptes email publics qui traitent beaucoup d'emails généraux et potentiellement dangereux, nous avons également installé des espaces de travail dédiés et étanches. Sur ces comptes, les utilisateurs travaillent sur un serveur de fichiers avec une autorisation limitée. En cas d'attaque ransomware, le dommage serait limité et sous contrôle.

« Chez Studerus SA, tous les emails avec pièces jointes suspectes sont bloqués et mis en quarantaine. »

Comment peut-on immuniser les systèmes contre les ransomwares ?
Il est indispensable d'installer les patchs sur les systèmes et les applicatifs dès qu'ils sont disponibles. Dès que les fabricants publient de nouveaux patchs, nous les installons le plus vite possible. Ces opérations ne sont pas réalisées qu'en weekend, mais également au cours de la journée en semaine. Nous sommes convaincus que ceci est indispensable et travaillons actuellement sur un rapport qui listera tous les clients disposant du dernier patch.

« Le grand nombre d'incidents ont montré que le maillon faible était souvent humain, et que l'homme aurait pu éviter le pire. »

A quoi faut-il faire attention lors de la sauvegarde de données sur des backups ?
Il est désormais prouvé que, lors d'attaques ransomware réussies, seules des sauvegardes régulières permettant de garantir la récupération des données nécessaires. Il faut bien sûr s'assurer que, après une sauvegarde réalisée, les données sont sécurisées et séparées du réseau d'entreprise.

Quelles sont les autres mesures mises en place par Studerus ?
- Installation du FW4.20 sur notre pare-feu Zyxel USG1900 (désormais avec les fonctionnalités GeoIP et SafeSearch)
- Désinstallation de plusieurs logiciels sur les ordinateurs (seuls les logiciels nécessaires doivent être installés)
- Mise à jour de la Charte Informatique interne
- Mise à jour des droits d'accès sur le serveur de fichiers

Avez-vous d'autres conseils pour les responsables IT ?
L'entretien et le contrôle régulier des systèmes et du réseau par les départements IT sont indispensables. Cependant, un grand nombre d'incidents ont montré que le maillon faible était souvent humain, et que l'homme aurait pu éviter le pire. Il est donc recommandé de sensibiliser régulièrement le personnel et de les informer de manière ciblée. ■

Hugo Bosshard
Responsable IT