Le volume d'attaques par rançongiciel (ransomware) a augmenté considérablement durant la pandémie, autant auprès des entreprises québécoises que sur le plan international. Une augmentation de près de 148 % a été enregistrée au cours de l'année 2020 par le fournisseur d'antivirus Carbon Black. Ce type de cyberattaque vise à infiltrer les réseaux corporatifs pour se propager au plus grand nombre d'appareils possibles afin de les chiffrer et d'exiger une rançon.

Une infection par rançongiciel peut avoir de lourdes conséquences pour les victimes ne possédant pas de mesures adéquates pour récupérer. Dans certains cas, les organisations ciblées sont contraintes d'interrompre l'ensemble de leurs opérations pour quelques jours, voire quelques semaines. Pour cette raison, il est primordial d'être préparé à toute attaque potentielle en instaurant quelques mesures permettant de prévenir l'impact d'une attaque par rançongiciel.

« Il est essentiel d'anticiper tous les scénarios possibles pour la reprise de vos opérations à la suite d'une attaque. »

1. Sensibilisez vos employés

L'approche principalement utilisée par les attaquants pour infecter une entreprise est sans aucun doute les courriels d'hameçonnage, également connus sous le nom de « phishing ». En effet, une étude a révélé que 93 % des courriels d'hameçonnage dissimulent un rançongiciel. Ces courriels sont généralement distribués de manière aléatoire à tous les employés d'une entreprise, mais ils peuvent également être très ciblés et s'adresser à un individu en particulier.

Autrement dit, les pirates élaborent des scénarios convaincants pour inciter les utilisateurs à télécharger une pièce jointe contenant le logiciel malveillant. Par exemple, dans les premiers mois de la pandémie, des pirates ont distribué des courriels à grande échelle invitant les destinataires à s'inscrire à l'essai clinique d'un vaccin en remplissant un formulaire fourni en pièce jointe. De cette façon, les attaquants ont été en mesure d'introduire un rançongiciel sur l'appareil des utilisateurs qui l'ont téléchargé, pour ensuite le propager à l'ensemble des appareils disponibles sur le réseau.

La sensibilisation à la cybersécurité constitue un des éléments clés pour prévenir les attaques par « ransomware », puisqu'elle outille les employés pour mieux identifier les tentatives d'hameçonnage et par le fait même, réduit les risques qu'un rançongiciel se retrouve sur l'un de vos appareils. Cependant, ces formations ne sont pas infaillibles et ne protègent pas votre entreprise intégralement. Des mesures additionnelles devraient également être instaurées pour protéger votre organisation advenant qu'un logiciel malveillant se retrouve dans vos systèmes.

2. Tenez vos systèmes et logiciels à jour

Malgré l'efficacité des formations de cybersécurité pour prévenir l'hameçonnage, il est possible qu'un logiciel s'infiltre tout de même dans l'un de vos postes de travail. En l'occurrence, les rançongiciels tenteront d'exploiter toute vulnérabilité technique présente dans votre réseau ou dans vos appareils de manière à se propager dans votre organisation.

Cela a été le cas pour le NHS (National Health Service) au Royaume-Uni qui a subi l'une des plus importantes attaques par rançongiciel de l'histoire. Celle-ci s'est produite alors qu'un logiciel malveillant a exploité une vulnérabilité présente dans une version obsolète du système d'exploitation Windows 7, lui permettant d'infecter des centaines de centres médicaux en quelques heures seulement.

L'équipe informatique a omis de tenir un grand nombre de postes de travail à jour, ce qui a laissé le système de la santé vulnérable à l'exploitation de la vulnérabilité bien connue par les pirates dans cette version du système d'exploitation. Par la mise à jour rigoureuse de tous ses appareils et logiciels, toute organisation atténuera grandement l'impact potentiel d'un rançongiciel en limitant la possibilité pour l'attaque de se propager dans son réseau. Cela dit, vous devriez toutefois être préparé à une reprise de vos opérations dans l'éventualité qu'une attaque affecte un ou plusieurs de vos postes de travail.

3. Effectuez des copies de sauvegarde

Enfin, il est essentiel d'anticiper tous les scénarios possibles pour la reprise de vos opérations à la suite d'une attaque, que ce soit sur l'ensemble de vos systèmes ou un seul appareil. En effectuant des copies de sauvegarde de tous vos ordinateurs et de votre infrastructure sur une base régulière, vous serez en mesure de restaurer vos postes de travail chiffrés et limiterez ainsi l'impact sur vos opérations. Cependant, il est tout aussi important de considérer la sécurité des copies de sauvegarde, soit en utilisant un service externe d'hébergement des sauvegardes ou en isolant celles-ci du reste de votre réseau corporatif. De cette façon, elles seront à l'abri du chiffrement par un rançongiciel.

En somme, il existe un grand nombre de précautions permettant de prévenir une infection par rançongiciel. Les trois mesures traitées dans cet article devraient être privilégiées pour éviter une cyberattaque potentiellement coûteuse, mais il est également fortement recommandé de faire appel à un professionnel en cybersécurité qui, par le biais d'un test d'intrusion, identifiera les vulnérabilités pouvant être exploitées par les pirates et fournira des recommandations pour les corriger. Ainsi, vous protégerez votre entreprise des attaques par rançongiciel, mais aussi de tout autre type d'attaque.