01

SE PROTÉGER AVANT UNE ATTAQUE

SAUVEGARDER LES DONNÉES... ET PROTÉGER LES SAUVEGARDES

« À elle seule cette précaution ne suffit pas, car c'est la première chose que le ransomware va chercher à détruire, avant même le chiffrement. Il faut avoir recours à des sauvegardes sur bande déconnectés et bien travailler la fréquence de ces sauvegardes. Il est également nécéssaire de tester les restaurations pour s'assurer que les sauvegardes soient utilisables. »

MAINTENIR À JOUR LES LOGICIELS ET LES SYSTÈMES

« Les mises à jour doivent être faites en continu et inclure les PC Windows mais également les sytèmes Linux et Mac qui peuvent aussi être des points d'entrée. Tout le parc bureautique est concerné, de Microsoft Exchange à l'Active Directory en passant par l'ensemble des serveurs exposés, même petits. »

CLOISONNER LE SYSTÈME D'INFORMATION

« Il est recommandé pour cela d'appliquer des règles strictes de flux autorisés entre différentes zones en fonction de leur criticité. »

LIMITER LES DROITS DES UTILISATEURS ET LES AUTORISATIONS DES APPLICATIONS

« Sur ce point, c'est la gestion de temps qui est déterminante : pour arriver à maintenir la sécurité, il faut prévoir des revues régulières.»

SENSIBILISER LES COLLABORATEURS

« Avec l'ingénieurie sociale, la principale porte d'entrée dans un système d'information d'une entreprise reste ses collaborateurs. Il est donc important de parler des sujets de cybersécurité même si la sensibilisation a ses limites. »

PENSER SA STRATÉGIE DE COMMUNICATION

« Là encore, il est utile d'avoir travaillé ses messages et ses contacts en amont pour communiquer de façon adaptée auprès des différents publics. Des communications qui servent à prévenir d'un arrêt inopiné de lla production, par exemple ou encore de fuites de données personnelles comme prévu par le RGPD »

METTRE EN OEUVRE UNE SUPERVISION DES JOURNAUX

« Ce plan est crucial, car iil permet de réagir vite en contactant par exemple au plus tôt les sociétés de CERT préalablement identifiées. Il comporte bien évidemment un volet technique avec la mise en place de solution de protection comme Stormshield Endpoint Security Evolution et Stormshield Network Security. »

METTRE EN OEUVRE UN PLAN DE RÉPONSE AUX CYBERATTAQUES

ÉVALUER L'INTÉRÊT DE SOUSCRIRE À UNE ASSURANCE CYBER

« Certaines assurances cyber intègrent des clauses de déploiement de solutions de cybersécurité; elles sont intéressantes en ce sens, car elles imposent du coup une certaine protection. Pour autant, il ne faut pas voir l'assurance cyber comme une mesure de survie qui suffit seule, et encore moins comme mesure qui protège. En d'autres termes, une assurance contre les ransomwares ne sera jamais une stratégie de cybersécurité. »

Ransomware, quelles mesures à prendre pour faire face à la menace ?

Les ransomwares sont devenus la bête noire des services informatiques, et des entreprises en général. Sont-ils pour autant une fatalité ? Série de mesures à prendre pour faire face avec Sébastien Viou, Directeur Cybersécurité Produit et Cyber-Évangéliste Stormshield.

STORMSHIELD

03
SE RELEVER APRÈS UNE ATTAQUE

RESTAURER LES SYSTÈMES DEPUIS DES SOURCES SAINES

ENQUÊTER SUR LE CHEMIN D'ATTAQUE EMPRUNTÉ

« Pour comprendre le déroulé de l'attaque et les faiblesses de son propore système, il faut analyser ce qui s'est passé. Ainsi, on se donne toutes les chances d'éviter que cela ne se reproduise. »

ÉLABORER UN PLAN DE CORRECTION

« Selon le cas, peut-être faut-il mettre en place une authentification multifacteur ou améliorer les solutions de désurité présentes sur les postes ? »

ÉTABLIR UN PLAN DE PRODUCTION POUR RATTRAPER LE RETARD ACCUMULÉ

ENGAGER DES POURSUITES SI CELA N'A PAS DÉJÀ ÉTÉ ENCLENCHÉ

GÉRER L'IMPACT PSYCHOLOGIQUE SUR LES COLLABORATEURS

« Chômage technique, culpabilité, surcharge de travail des équipes IT, les ransomwares ont aussi des conséquences sur les ressources humaines, il faut les prendre en compte. »

DÉPLOYER LE PLAN DE COMMUNICATION AUPRÈS DES CLIENTS IMPACTÉS, DE VOS INVESTISSEURS ETC.

PRÉSENTER LE DOSSIER À L'ASSURANCE

DÉPOSER PLAINTE

COMMUNIQUER AU JUSTE NIVEAU

02
LIMITER LES DÉGÂTS PENDANT UNE ATTAQUE

PILOTER LA GESTION DE LA CRISE CYBER DEPUIS LE COMITÉ EXÉCUTIF

ADOPTER LES BONS RÉFLEXES

« Il faut être capable de repérer rapidement que quelque chose ne va pas, et ne pas hésiter à aller jusqu'à tout débrancher pour mitiger le risque et contenir la propagation au maximum. Au niveau individuel aussi, il faut apprendre à réagir, à dire « j'ai cliqué au mauvais endroit» car chaque minute compte. »