11 manières de protéger son entreprise face aux cyberattaques

Avec la généralisation du télétravail en temps de crise sanitaire, les attaques informatiques criminelles à destination des entreprises ont explosé en 2020. Voici une série de conseils pour protéger au mieux sa société de ce risque croissant.

Depuis quelques semaines, les hôpitaux – comme ceeux de Dax ou de Villefranche-sur-Saône – sont présentés comme les cibles privilégiées des cybercriminels en quête de rançon. Mais ces structures ne sont malheureusement pas les seules à pâtir d'une augmentation massive des attaques de leurs systèmes informatiques. Les entreprises ont aussi vu exploser les tentatives de piratage à leur égard. Ces dernières auraient même été multipliées par quatre, selon Guillaume Poupard, directeur général de l'Anssi, l'agence publique gardienne de la sécurité informatique en France.

Voici une série de conseils pour muscler la sécurité informatique de son entreprise.

Se prémunir d'une attaque

Faire l'inventaire des appareils connectés à son réseau

Cela peut paraître basique, mais il est primordial de savoir précisément quelles

machines sont présentes sur le système d'information de son entreprise. « *Cette vue d'ensemble permet de maitriser la surface de connexion, l'exposition, de faciliter le monitoring de la sécurité et donc de mieux se protéger* » , résume Thomas Roccia, chercheur en cybersécurité chez McAfee. « *C'est une mesure classique mais absolument indispensable* » , confirme Antoine Baranger, conseiller en gestion des risques chez RSM.

Mettre à jour ses machines et systèmes antivirus

Un inventaire des ordinateurs du réseau, c'est bien, mais quand ils sont mis à jour, c'est mieux. « *Ne pas faire les mises à jour génère des vulnérabilités qui peuvent ensuite être exploitées par des cyberattaquants*, poursuit Antoine Baranger. Et cette étape ne concerne pas que les ordinateurs, mais aussi les logiciels antivirus : « *Il ne suffit pas d'installer l'outil pour qu'il soit fonctionnel dans la durée. S'il n'est pas mis à jour, l'antivirus ne détectera pas tous les nouveaux virus qui sont nés entre temps* » , précise-t-il.

Sensibiliser les salarié·e·s

« *Le premier rempart contre un cyber-incident, c'est l'humain* » , insiste Antoine Baranger, qui défend l'importance de sensibiliser les employé·e·s. « *On pourra mettre tous les outils que l'on veut en place, si les collaborateurs ne sont pas formés à la vigilance à adopter face aux mails suspects, à sécuriser leurs mots de passe, à l'attention aux informations qu'ils exposent sur les réseaux sociaux ou à l'importance de la double identification par exemple, ça sera vain* » , martèle Thomas Roccia.

Faire des sauvegardes régulières et fonctionnelles

Quand l'entreprise est attaquée, il est malheureusement trop tard pour vérifier qu'on a bien fait toutes nos sauvegardes et que celles-ci ont bien fonctionné. D'où l'importance de vérifier régulièrement en amont toutes les procédures de réponse à une potentielle attaque. « *Faire ces vérifications a un coût et ne rapporte pas d'argent, c'est pourquoi les entreprises en font souvent l'économie, mais c'est une erreur,* explique le manager chez RSM. *Des problématiques techniques peuvent entraver les sauvegardes et il est important de tester ces dernières pour anticiper la qualité de la restauration des données en cas d'attaque* » .

« *Les ransomware – attaques de plus en plus communes qui séquestrent des données contre une rançon, seront moins graves pour une entreprise qui sait que son système de sauvegarde est fonctionnel et bien en place*, relance le chercheur en cybersécurité chez McAfee. *Être au fait sur le sujet permet d'être moins sensible au chantage et à la demande de rançon des hackers qui se sont infiltrés dans les systèmes d'informations d'une entreprise* ».

Se faire accompagner par des experts

Les entreprises doivent identifier des experts qui peuvent accompagner leur structure pour analyser leur niveau de sécurité, les potentiels incidents dont ils seraient victimes et les accompagner dans la restauration de données hackées. « *L'Anssi fournit un annuaire de toutes les entreprises qui peuvent intervenir sur ces problématiques* » , précise Antoine Baranger.

« *Mettre en place des monitorings de sécurité nécessite des technologies, mais aussi des moyens humains,* martèle Thomas Roccia*. Ces experts sont les yeux et les oreilles du système d'information, qui sont les seuls à pouvoir analyser les données, investiguer, comprendre et alerter sur les failles potentielles des entreprises*« .

Pour les PME et ETI, qui n'ont pas forcément ni le budget ni le besoin d'avoir un expert à plein temps, plusieurs solutions existent. « *Soit l'entreprise décide de faire monter en compétences son responsable informatique sur les questions de cybersécurité, soit elle fait ponctuellement appel à des experts extérieurs, tous les 6 mois par exemple, pour faire des revues et audits, mais aussi des campagnes de sensibilisation* » , détaille Antoine Baranger.

Redoubler de vigilance dans un contexte de télétravail

Le télétravail augmente la surface d'attaque de l'entreprise et génère des opportunités pour les cybercriminels. « *Dans ce contexte, il est primordial de sensibiliser les collaborateurs aux risques,* avertit Antoine Baranger. *Certaines bonnes pratiques permettent de limiter le risque : il faut par exemple interdire aux salariés de faire un usage personnel de leur ordinateur professionnel. Cela passe notamment par l'utilisation de leur adresse mail personnelle ou des différents réseaux sociaux qu'ils utilisent*« .

En cas d'attaque

Débrancher les machines

« *Si, par exemple, un collaborateur ouvre une pièce jointe dans un mail avec un cryptolocker* (logiciel malveillant type Cheval de Troie, dans le but de prendre en otage des données personnelles, NDLR) *il faut débrancher l'ordinateur du réseau dans l'immédiat* » , explique Antoine Baranger. « *C'est la seule solution pour éviter l'hémorragie et la propagation du virus, qui peut être dévastateur pour l'entreprise touchée* » , poursuit Thomas Roccia.

Garder son calme et communiquer

Si un·e salarié·e est victime, et donc la porte d'entrée d'un logiciel malveillant

dans le réseau de son entreprise, il ne faut surtout pas paniquer, tenter de masquer ou de gérer seul·e le problème car le temps est un facteur clé dans la gestion de ces attaques. « *Il faut immédiatement prévenir les équipes IT de son entreprise pour qu'ils puissent prendre la main à distance et réagir rapidement* » , insiste le chercheur chez McAfee. « *Ensuite, il ne faut pas oublier de prévenir à la fois ses clients -notamment de l'impact de cette cyberattaque sur de potentiels retards ou failles de sécurité, mais aussi de faire une déclaration d'incident de sécurité aux instances réglementaires comme la CNIL, pour mise en danger des données personnelles* » , ajoute Antoine Baranger.

Ne pas payer de rançon

C'est facile à dire mais les deux experts en cybersécurité l'affirment : payer la rançon n'est pas la solution. D'une part, « *ça alimente le cybercrime* » , prévient Thomas Roccia, mais en plus payer ne veut pas dire être sorti d'affaire. « *Payer la rançon n'assure pas que le crypto locker (l*ogiciel malveillant, NDLR*) soit réellement retiré par les hackers, qui sont parfois sans foi ni loi »* , précise Antoine Baranger.

Pour tenter de convaincre les entreprises de ne pas succomber au chantage et lutter contre les ransomware, le projet « No More Ransom », développé par McAfee en partenariat avec Europol et différents pays européens, met à disposition de tous les internautes, gratuitement, un site qui permet aux victimes d'attaques informatiques de les déchiffrer. Menée par un groupe de chercheurs en cybersécurité, dont Thomas Roccia fait partie, l'initiative publie toutes les solutions trouvées par ces experts pour casser le chiffrement des différentes attaques qu'ils ont trouvées. S'ils n'ont pas toutes les solutions, certaines intrusions peuvent être contournées grâce à cet outil.

Repasser à un fonctionnement à l'ancienne

Rien de plus fiable d'un papier et un stylo. « *Lors d'une cyberattaque, toute l'activité d'une entreprise est mise à l'arrêt d'un coup, empêchant toutes les équipes d'utiliser leurs outils informatiques et leur messagerie,* explique Antoine Baranger. *Pas de recette miracle contre cela, le mieux étant d'anticiper ce risque, de penser en amont comment on pourrait gérer un fonctionnement très dégradé et minimal de la société en revenant au papier et aux échanges téléphoniques uniquement, sans tout arrêter pour autant, le temps de la résolution de l'incident* » .

Changer tous les mots de passe

Une fois l'attaque passée, l'entreprise reste tout de même plus vulnérable. Il faut donc être très vigilant à restaurer tout le système d'information pour assurer sa sécurité. « *Toutes les machines précédemment hackées doivent*

être restaurées par des experts et tous les mots de passe nécessitent d'être modifiés par chacun des collaborateurs de l'entreprise » , conclut Antoine Baranger. *Si cela n'est pas fait, le cybercriminel qui a fait irruption dans le réseau de l'entreprise avec les identifiants et mots de passe d'un des salariés peut à tout moment revenir et recommencer le même schéma, puisqu'il a toujours la clé pour entrer*« . Une personne avertie en vaut deux.

S'inscrire

Article écrit par HELOÏSE PONS