Cybersécurité en entreprise : les clés pour se prémunir

EntrepriseVie des entreprises - Publié le 25 avril 2022 à 08h00, par Affiches Parisiennes

Rançongiciel, piratage de compte, hameçonnage...

(© Adobe Stock)

Lors d'un récent webinaire, Nicolas Touchet et Angelina Kahn-Dubois, experts Technologie/digital et conformité Walter France, accompagnés d'Olivier Delmas-Leguéry, courtier et formateur, pour le Cabinet Rouge, ont fait le panorama des attaques informatiques les plus courantes que subissent les entreprises, et les bonnes pratiques qu'elles ont tout intérêt à développer pour s'en prémunir.

La digitalisation accrue des entreprises, les outils informatiques qui sont de plus en plus dans le cloud et le développement du télétravail sont des facteurs propices au développement des cyber-attaques.

Des techniques de plus en plus sophistiquées

De récentes « affaires » ont récemment fait la une de l'actualité. Pour n'en citer que quelques-unes, MMA, après une très grosse attaque en juillet 2020, n'a pu rattraper qu'à l'automne suivant son retard de gestion. En décembre 2020, le piratage Solarwinds a ciblé le gouvernement américain, des agences fédérales et de nombreuses entreprises publiques et privées. Plus récemment en France, en mars dernier, l'assurance maladie et plusieurs hôpitaux ont été piratés, entraînant le vol de données de 500 000 assurés.

Mais attention, alerte Angelina Kahn-Dubois, les hackers ne s'attaquent pas qu'aux grandes structures. *« Tout le monde est touché, y compris des PME. En 2021, l'ANSSI (Agence nationale de la sécurité des systèmes d'information) a recensé 1082 intrusions. 52 % des attaques par rançongiciels qu'elle a traitées en 2021 ont concerné des TPE, des PME et des ETI. Le coût médian pour une TPE-PME se monte à 50 000 euros, et à 500 000 euros pour une ETI. »*

La finalité des cyberattaques à l'encontre des entreprises est de récupérer des données qui ont de la valeur et qui peuvent être revendues. Mais elles peuvent aussi faire partie d'une stratégie de piratage industriel et concurrentiel. Et au niveau mondial, certains Etats mettent en place des cyber-armées qui jouent un rôle de plus en plus important lors de conflits, comme la guerre entre la Russie et l'Ukraine le démontre.

Un système mafieux plus lucratif que la drogue

Il devient de plus en plus difficile d'identifier d'où viennent les hackers, car ils copient leurs méthodes les uns sur les autres. Il existe même des solutions de cyberattaques qui se mettent sur le marché ! Il devient désormais possible d'acheter un module permettant d'exploiter un type de faille. C'est un véritable système mafieux, plus lucratif que le trafic de drogue, et moins risqué…

Des techniques de plus en plus sophistiquées

Les cyberattaques peuvent être classées en six catégories.

- **Le phishing (hameçonnage)** consiste à usurper l'identité d'une personne ou d'une organisation et d'amener la victime à exécuter une action, par exemple donner un mot de passe, effectuer un virement, etc. La technique du faux RIB rentre dans cette catégorie : un soi-disant fournisseur vous envoie son « nouveau » RIB afin que vous effectuiez un virement.

- Le ransomware (rançongiciel) : le hacker subtilise les données d'une entreprise ou bloque son système, et exige une rançon pour remettre lesdites données à disposition.

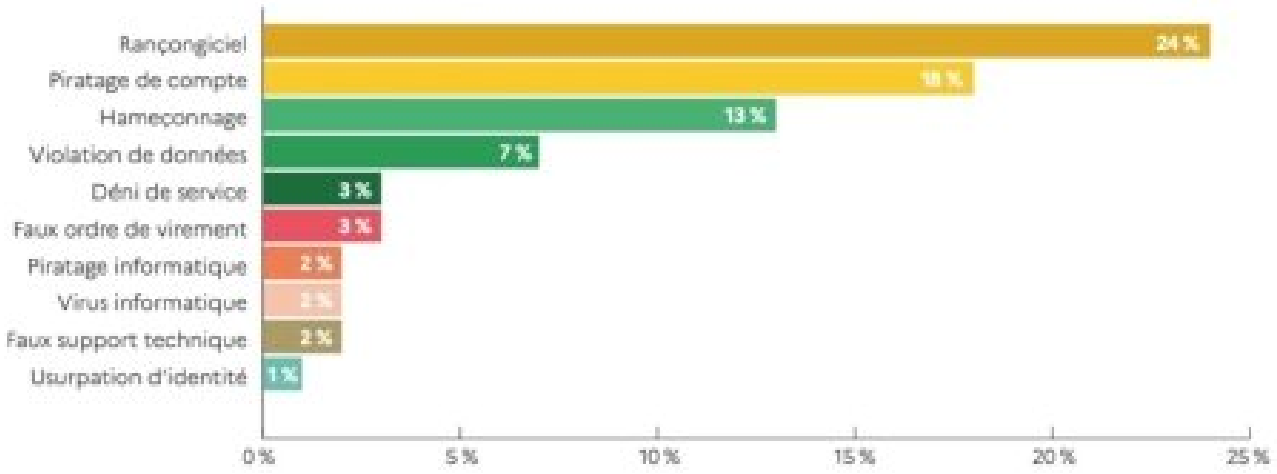
- L'attaque par supply chain (attaque de la chaîne d'approvisionnement) : le hacker va toucher un éditeur de logiciel ou un logiciel de supervision informatique, et, à travers lui, va pouvoir atteindre tous ses clients.

- Le DDOS (déni de service) : ces attaques entraînent le blocage d'un site internet par exemple, pour le mettre hors service, par l'envoi massif de requêtes saturant sa capacité.

- L'ingénierie sociale. C'est une technique de manipulation par tromperie. Un bon exemple est la fraude aux présidents : un hacker se fait passer pour un supérieur hiérarchique et vous incite à exécuter un virement ou autre.

- Le spyware (logiciel espion). L'entreprise peut ne pas s'en rendre compte, car c'est un logiciel qui enregistre des informations et l'activité des équipes. C'est une pratique de hacking de plus en plus courante.

Principales recherches d'assistance Cybermalveillance.gouv.fr pour les entreprises et associations en 2021



Des coûts indirects tout aussi préjudiciables que les coûts directs

Plusieurs types de coûts sont visibles :

- les coûts liés à l'analyse de l'incident : les investigations internes et externes, les mesures réactives qui doivent être mises en place ;
- les coûts liés au ralentissement ou à l'arrêt de la production, que ce soit des biens ou des services ;
- les coûts de correction et d'amélioration du système d'information ;
- les coûts liés à la reprise de l'activité normale ;
- les coûts de communication pour prévenir les clients et les partenaires touchés, ainsi que les coûts de communication publique ;
- les coûts juridiques tels que des amendes de non-conformité, des pénalités liés aux contrats clients n'ayant pas pu être respectés, des frais d'avocat, etc.
- Les « coûts boomerang », ou coûts indirects, sont quant à eux plus difficilement quantifiables mais sont souvent extrêmement élevés. Il peut s'agir des coûts opérationnels liés aux données perdues, aux franchises d'assurance, aux pertes de contrats, aux vols de brevets, en termes d'image…

Un exemple révélateur est celui d'une entreprise qui devait être rachetée et qui a été l'objet d'une cyber-attaque. Angelina Kahn-Dubois explique qu'au final, elle a été vendue à 25 % de la valeur initialement prévue.

Les bonnes pratiques techniques à déployer

Face à ces menaces en constante augmentation, les entreprises n'ont pas d'autre choix que de se prémunir le plus efficacement possible, d'abord au niveau technique :

- renforcer les accès avec une identification à deux facteurs ;
- superviser les évènements de sécurité en exploitant la journalisation des évènements/incidents sur les points d'entrée les plus critiques du système d'information ;
- sauvegarder régulièrement les données et les applications vitales hors ligne ;
- prioriser les services numériques devant absolument être protégés ;
- établir un dispositif de gestion de crise qui permettra de remettre en état les fonctions les plus

critiques de l'entreprise.

Les défaillances humaines profitent au crime…

Toutefois, ces précautions techniques ne suffiront pas car ce sont les défaillances humaines qui sont le plus exploitées lors des cyberattaques. Attention donc au partage des données dans le cloud, attention à interdire toute installation de logiciels non autorisés par le service informatique, à l'usage croisé des outils personnels pour le professionnel et des outils professionnels pour le personnel, et bien évidemment attention aux modalités du télétravail.

Le top 3 des enjeux pour les prochaines années

Les entreprises doivent placer la gouvernance de la cybersécurité au bon niveau pour que celle-ci soit efficace et mieux former et sensibiliser les équipes à ces questions. Nicolas Touchet recommande de lancer de fausses campagnes d'hameçonnage pour tester la « résistance » des managers et des collaborateurs, et bien évidemment, ensuite, de former et de diffuser les bons réflexes.

Enfin, il est important que les entreprises se dotent des moyens financiers nécessaires. Il existe encore des entreprises qui consacrent moins de 5 % de leur budget IT à la cybersécurité.

A noter qu'il existe un certain nombre d'organismes tels que l'ANSSI, une agence gouvernementale, qui peuvent accompagner les entreprises dans leur démarche.

Avant de s'assurer, percevoir, prévenir et réduire les risques

Comme pour toute gestion de risque, le risque de cyberattaque doit faire l'objet d'une étude au sein des entreprises afin d'identifier le type d'attaques qui mettrait en danger la survie de l'entreprise, de prévoir les actions de prévention et de protection à mettre en œuvre.

Pour Olivier Delmas-Leguéry : *« C'est seulement une fois ce travail accompli que l'entreprise pourra solliciter une assurance, qui peut intervenir à trois niveaux : la gestion de l'attaque en faisant restaurer les données par des experts informatiques ; l'indemnisation des dommages subis par l'entreprise – perte d'exploitation, cyber-rançon, frais d'enquête, atteinte à la réputation… – ; et la prise en charge des dommages causés (responsabilité civile) aux clients, partenaires ou autres. »*

Nicolas Touchet conclut : *« Toutes les entreprises connaissent la dangerosité des cyber-attaques, mais les sous-évaluent encore trop souvent. Elles doivent mettre en adéquation leur plan d'action et leur budget avec la réalité de ces risques »,*