Cybercriminalité : ransomware, ingénierie sociale… comment y faire face ?

Si les outils et solutions de défense contre la cybercriminalité, internes comme externes sont nombreux, la problématique de la protection et / ou de la récupération des données demeure.

Ransomware : la question prioritaire des données

Dès la détection d'un ransomware, l'un des premiers réflexes est de chercher à isoler son matériel informatique en se déconnectant du réseau le plus rapidement, pour éviter naturellement toute propagation du programme malveillant aux autres postes du réseau (connexions filaires et WiFi).

Dans ce cas, la récupération des données devient le sujet d'inquiétude principal. Selon la nature du ransomware, il est possible de faire appel à des sociétés de sécurité informatique. Certaines disposent d'outils permettant de récupérer les données cryptées et rendues inaccessibles. Mais reconnaissons que le résultat de ce type d'outil demeure approximatif.

Les cas de récupération impossible étant encore nombreux, la meilleure attitude à adopter est l'anticipation du risque, ceci en mettant en place, en amont, une sauvegarde de l'intégralité des données sensibles. C'est dans un lieu sécurisé, distant du site primaire où se trouvent les données, que cette sauvegarde se réalise.

En répliquant sur un site distant l'ensemble de ses données, mais également les configurations propres aux équipements les hébergeant, une entreprise peut se protéger totalement d'un risque de cyberattaque de type ransomware. Elle sera ainsi en capacité de recouvrer l'intégralité de ses données, dans un laps de temps relativement court, après bascule de l'infrastructure infectée vers la nouvelle, dans le cadre d'un plan de reprise d'activité.

Ingénierie sociale : hacker, sans en avoir l'air

L'ingénierie sociale vise à entrer en relation avec un individu de manière discrète, mais suffisamment poussée pour pouvoir utiliser, à des fins frauduleuses, des informations utiles qui pourraient lui être soutirées. Les hackers adoptant ces pratiques mettent ainsi sur pied des techniques « d'hameçonnage » (phishing) lesquelles, par le biais d'interactions, de questions posées et d'une relation de confiance qui se noue, vont permettre de récupérer une quantité suffisante de renseignements personnels.

En apparence non stratégiques, ces informations une fois cumulées et recoupées entre elles

deviennent un levier puissant de détournement, permettant aux hackers d'accéder à l'argent (comptes bancaires…), aux données privées (bulletins de salaires, données de santé…) et aux secrets de leurs victimes (mots de passe, code d'accès…).

Les escroqueries qui mobilisent des techniques d'ingénierie sociale se divisent généralement en deux grandes catégories. D'un côté, les fraudes massives ciblent un grand nombre de personnes et utilisent des techniques rudimentaires (l'envoi de spam touchant plusieurs millions de destinataires). De l'autre, les fraudes ciblées plus sophistiquées visent des individus ou des entreprises spécifiques (ainsi, la tristement célèbre fraude au président).

Les quatre phases caractéristiques d'une arnaque à l'ingénierie sociale sont la collecte d'informations, l'établissement de la relation avec l'individu ciblé, l'exploitation de vulnérabilités identifiées et son exécution.

En cas de fraude par ingénierie sociale, le premier réflexe, concernant une organisation professionnelle, doit être de prévenir les administrateurs réseaux afin qu'ils redoublent de vigilance dans la détection de toute activité suspecte. Si la fraude concerne des comptes bancaires, il faut contacter au plus vite l'établissement financier pour clôturer les comptes, repérer d'éventuels frais inexpliqués et réinitialiser ses mots de passe.

Un autre bon réflexe est aussi de signaler toute attaque aux autorités. Un portail est mis à disposition des internautes pour transmettre des signalements de contenus ou de comportements illicites : internet-signalement.gouv.fr.

Sensibiliser les utilisateurs avant tout : la clé en matière de cybersécurité

Dans une grande majorité des cas, l'action de l'utilisateur final, faite de mauvaises pratiques, apparait comme le point d'origine d'une faille de sécurité informatique. La consultation de pages web douteuses, l'ouverture de fichiers joints ou de liens malveillants portant en eux le germe d'une attaque ou encore l'utilisation directe de logiciels corrompus, sont autant d'occasions d'infecter un ordinateur et le réseau informatique auquel il appartient.

L'étude « The Global State of Information Security » menée par PwC indiquait déjà en 2017 que près d'une entreprise sur trois estimait que ses collaborateurs étaient involontairement à l'origine de certaines attaques. Sensibiliser régulièrement ses équipes et évaluer leurs connaissances en matière de règles de sécurité informatique n'est désormais plus une option.

A ce titre, il existe de nombreuses formations et supports pour former son personnel à la sécurité et aux risques auxquels s'expose une société informatisée : charte informatique, sessions d'e-learning, formations de groupe afin de favoriser le partage d'expérience, dispositifs ludiques et participatifs de type quiz, tests d'intrusion en social engineering et autres serious games, jusqu'à la mise en conditions réelles avec des sessions de live-hacking.

Au même titre que la connaissance des gestes de premiers secours peut sauver une vie, la maîtrise

des bonnes pratiques de sécurité informatique peut enrayer une cyberattaque même élaborée.

Dans tous les cas, l'une des meilleures alternatives pour protéger et prévenir son système d'information face à toute menace cybercriminelle reste encore l'audit informatique de son SI. L'expert réalisera un point complet sur l'état de la sécurité du système, déterminera les priorités et préconisera les actions utiles afin d'optimiser le niveau de sécurité et sensibiliser les collaborateurs aux principales menaces évaluées