Gestion des menaces persistantes (APT) : connaissance, prévention et protection

Partout dans le monde, des entreprises se sont retrouvées prises pour cible par des APT (Advanced Persistent Threat). Cette forme de cyberattaque a la particularité de perdurer longtemps dans les réseaux avant d'être détectée, lui permettant ainsi d'extraire un maximum de données et d'informations.

Si bon nombre de ces attaques visent des organismes étatiques et de grandes structures, notamment SolarWinds et Microsoft Exchange, ce risque concerne en réalité toutes les entreprises.

Selon un rapport publié par Research Dive, le marché mondial de la protection contre les APT devrait générer un revenu de plus de 20 milliards de dollars et croître au rythme soutenu de 20,9 % au cours de la période 2020-2027.

Compte tenu de la persistance de ce type de cyberattaque, le taux d'incidence des APT n'a pas vraiment augmenté pour les grandes entreprises. À l'inverse, les petites organisations en sont de plus en plus victimes.

Toutefois, il existe des mesures proactives qu'elles peuvent appliquer pour se protéger et protéger leurs réseaux.

Comprendre les APT et leur évolution

Les attaques APT se caractérisent généralement par une technicité élevée et une simplicité remarquable. Elles font généralement appel à de nouvelles techniques ou à des failles pas encore connues (Attaque zero day) afin d'accéder à un système ou à un ensemble de systèmes. Elles s'installent ensuite, de manière très habile, aux endroits où l'on est le moins susceptible d'y prêter attention.

La meilleure comparaison qui puisse être faite est celle de la souris domestique. Lorsque l'on en capture une, on comprend rapidement qu'elle n'est pas seule mais s'accompagne de nombreux autres individus. Et comme pour cette analogie, le seul moyen d'éliminer une APT de ses systèmes est de procéder à une recherche minutieuse, partout où l'on ne s'attend pas à trouver de problème.

Les APT se dissimulent dans les endroits dont on oublie qu'ils disposent d'une connexion réseau, notamment dans les imprimantes, les claviers et les dispositifs IoT des réseaux.

Nous vivons dans un monde où il est possible d'acquérir un processeur 32 bits avec WiFi pour une somme ridiculement faible. Cela explique que l'on puisse dissimuler un code malveillant n'importe où. On dit souvent que la façon la plus simple de supprimer une APT consiste à tout détruire avant de repartir à zéro. Ce n'est pas pratique, mais cela fait allusion au fait que l'on va devoir tout à coup mieux connaître ses systèmes que ce ne fut le cas par le passé.

La prévention comme un atout pour les entreprises

Alors que la meilleure défense contre les APT consiste à adopter une stratégie préventive, le secteur de la sécurité privilégie plutôt les approches défensives (installer le meilleur piège à souris pour reprendre l'analogie précédente). Mais elle est fondamentalement erronée.

Autrement dit, il ne s'agit pas de trouver un moyen de résoudre le problème, mais plutôt de n'y être jamais confronté. Cela signifie qu'il vaut mieux renforcer les bonnes pratiques opérationnelles et l'hygiène de ses systèmes, plutôt que d'investir dans des solutions destinées à résoudre les problèmes.

La sécurité n'est pas quelque chose de particulier mais seulement un ensemble d'opérations menées correctement. Cela signifie qu'il faut recruter du personnel compétent qui adopte une attitude proactive et ne se place pas dans une logique d'économies ou de compression des coûts.

Les informations internes et la capacité de les traiter constituent le principal atout d'une entreprise. Elles ne figurent probablement pas dans le bilan, mais il serait difficile de justifier l'existence d'une organisation sans elles. Leur protection contre les APT est par conséquent de toute première importance.

Une entreprise qui traiterait l'un de ses biens majeurs (usine, flotte de véhicule…) avec le même manque de considération et l'approche de réduction des coûts que l'on observe dans le secteur IT, devrait sûrement rendre des comptes au conseil d'administration. En prenant soin de leurs systèmes d'information et des personnes qui les exploitent, les organisations deviennent des cibles moins attrayantes.

La défense contre les APT peut s'avérer délicate, mais efficace

Au milieu des années 2000, le terme de « Cyber Black Start » est apparu dans le monde de la cybersécurité des infrastructures critiques. Ce concept s'inspire de ce qui se fait pour les réseaux électriques qui parfois, pour être rétablis, doivent être complètement éteints puis remis en route. Ce fût le cas lors de la panne survenue en 2003 dans le nord-est des États-Unis et du Canada. La démonstration qui suit est l'équivalent pour les technologies de l'information.

En cas d'attaque APT, il est nécessaire d'agir rapidement. Il faut tout arrêter et rétablir les systèmes par ordre de priorité, en s'assurant que chacun est opérationnel avant de le réintégrer dans le réseau. Il s'agit d'une mesure coûteuse et délicate, mais elle est bénéfique car une tentative d'identification et de neutralisation au cas par cas sera plus coûteuse et plus douloureuse à long terme.

En effectuant ce travail de « Cyber Black Start », on découvre des éléments qui ne sont pas

réellement nécessaires aux opérations de base et que l'on peut ne jamais redémarrer. En diminuant la complexité des systèmes, l'acteur malveillant aura alors moins d'endroits pour se dissimuler. Il est également important de faire appel à l'expertise d'une entreprise spécialisée dans la cybersécurité, puis de mettre en place tout ce qui est indispensable pour que cela ne se reproduise plus.

Au regard de la prévalence actuelle des APT, dont plusieurs violations ont été très médiatisées rien qu'en 2021, il est compréhensible que les entreprises se préoccupent de leurs propres vulnérabilités.

Pour prévenir les attaques APT, les entreprises doivent simplement appliquer les principes fondamentaux de l'hygiène numérique. Il s'agit notamment de ne pas cliquer sur des liens externes, de mettre en place une protection des systèmes informatiques avec des configurations à jour, de contrôler les éventuels dysfonctionnements des réseaux, de maintenir le cloisonnement des réseaux et de prêter attention aux retours des collaborateurs sur d'éventuels incidents inquiétants.

Ces bonnes pratiques fonctionnent mais la plupart des organisations ne les suivent pas. C'est pourtant tout ce qu'elles ont à faire. Ainsi, les souris choisiront la maison du voisin qui n'aura pas pris le soin de calfeutrer ses portes !