La quête du Saint Graal de la sécurité des données passe par la visibilité

Selon une étude de BT et KPMG, 97 % des personnes interrogées déclarent avoir subi une cyberattaque, et 44 % s'inquiètent de devoir solliciter des tiers pour certains aspects de leur politique de protection. Pourtant, face à l'ampleur croissante de la cybercriminalité au cours des dernières années, l'intervention d'expertises tierces est un atout pour sécuriser les données.

En effet, l'humain, bien que considéré comme un maillon faible de la sécurité, reste indispensable pour la gestion des outils de détection des anomalies, le machine learning, ou les outils d'analyse du comportement. Ceux-ci visent avant tout à analyser le trafic réseau et à alerter toute action inhabituelle ou anormale. Or, la clé est de savoir distinguer une bonne d'une mauvaise activité, ce qui n'est pas possible sans une stratégie de sécurité définie et des expertises spécifiques telles que la gestion des réseaux par exemple. Une connaissance qui constitue le Saint Graal de la sécurité de l'information. «

À vaincre sans péril on triomphe sans gloire » : verrouiller son CID

Sans lien avec l'oeuvre de Corneille, l'acronyme CID correspond ici à « Confidentialité, Intégrité et Disponibilité », trio simple mais indispensable à une sécurité de l'information sans couture pour une organisation. Ainsi, sans un CID irréprochable, il est quasiment impossible de faire la distinction entre les bonnes et les mauvaises activités.

- Pour comprendre la confidentialité, prenons l'exemple du PDG d'une organisation ayant une heure devant lui avant un comité de direction. Celui-ci doit extraire, d'un fichier situé sur l'un des serveurs, des données financières top secrètes afin de fournir un rapport sur les résultats trimestriels sans craindre que des personnes malveillantes ou hors-CODIR puissent voir ces données sur le réseau au même moment. Partant du constat que Ponemon a évalué à 440 milliards de dollars le montant des pertes attribuées aux fuites de données, si le PDG - ou tout autre utilisateur dans une situation similaire - considère qu'il bénéficie d'une confidentialité totale, il ne consultera pas ces informations de la même manière que s'il pense être potentiellement épié.
- L'intégrité consiste quant à elle à déterminer la fiabilité et la pertinence des données issues du serveur, ou si quelqu'un aurait pu les altérer.
- Enfin, la disponibilité est essentielle, que ce soit l'accès permanent aux informations, une bande-passante adaptée ou un nombre suffisant de serveurs. Il est également important de savoir si ces derniers sont toujours connectés, s'ils subissent des pannes et enfin avoir la garantie que ces systèmes envoient les bonnes données aux bonnes personnes.

Si un seul des éléments du CID est brisé, il devient alors compliqué d'évaluer si un événement est positif ou négatif. Ainsi en cas de panne, il sera difficile de déterminer si celle-ci résulte d'une cyberattaque ou de l'échec de l'un de ces trois éléments. En revanche, si le CID fonctionne, l'organisation possède des fondations de cybersécurité solides et peut commencer à analyser les activités.

Une histoire classique du bien contre le mal : connaître son réseau

Il était une fois, à son arrivée au bureau, un employé qui reçoit une notification lui indiquant la nécessité de changer son mot de passe de connexion réseau. Trop occupé, il oublie rapidement de le faire. La semaine s'écoule, et le vendredi après-midi, il reçoit une ultime notification l'invitant à changer son mot de passe avant la fin de la journée. Sur le point de quitter le bureau, il prend tout de même le temps de le faire mais à son retour, le lundi suivant, il s'aperçoit qu'il a déjà oublié son nouveau mot de passe. Après plusieurs vaines tentatives de connexion, le support technique prend contact avec lui afin de qualifier son problème et lui venir en aide. En réalité, même si l'employé ne s'était pas trouvé à son poste au moment de cet appel, le service IT ayant identifié la tentative de connexion à son compte comme une potentielle tentative d'intrusion malveillante sur le réseau, il aurait pu ainsi transmettre l'information aux équipes de sécurité informatique. Les choses ne sont malheureusement pas toujours aussi simples, chaque réseau étant intrinsèquement différent. Par exemple, dans certains cas, il peut être risqué de mettre ses données bancaires à disposition sur un réseau, mais si celui-ci est certifié PCI, cela peut s'avérer nécessaire ; tout dépend du contexte et de la visibilité du trafic du réseau.

Le bon, la brute et le truand inconnu : on ne peut pas protéger l'invisible

Conçus pour créer une norme « bon vs mauvais », les outils de détection des anomalies et d'analyse du comportement d'un réseau peuvent, au bout de quelques mois, identifier et déterminer des comportements types. Ils sont ainsi en mesure de repérer toute activité déviante telle qu'une tentative de vol de données, d'intrusion dans les réseaux ou d'installation de malware, et donc de donner l'alerte. Toutefois, chacun de ces outils possède une catégorie « inconnue » dans laquelle sont envoyés les conversations ou trafic qu'ils ne voient que partiellement, ce qui les empêche d'identifier la nature du trafic ; cela les rend inutiles. Afin de prendre d'évaluer la nature d'une activité, il est nécessaire de connaître le contexte, c'est-à-dire d'avoir 100 % de visibilité dans le trafic réseau. Cela s'applique quelle que soit la situation, qu'une solution anti-malwares tente de déterminer si un fichier exécutable est bon ou mauvais, ou qu'un outil de sécurité décide si un document peut être autorisé à quitter un serveur.

Par conséquent, le credo de toute entreprise devrait être le suivant : « Si je ne peux pas obtenir pour mon outil le trafic dont il a besoin pour fonctionner efficacement, pourquoi acheter l'outil ? Il est temps de trouver une autre solution. » Au final, tout réside dans le choix judicieux et réfléchi d'outils adaptés au réseau, à son contexte et à un écosystème d'experts qui collaborent pour lutter contre les cybermenaces et l'homme invisible caché dans les réseaux.