

Cybersécurité

Protéger votre réseau, c'est protéger votre réputation !

Par Yann Samama, Senior Sales Engineer chez Gigamon

« *On ne peut pas arrêter le progrès* » - À mesure que nous avançons dans l'ère de l'information, ce vieux dicton devient de plus en plus pertinent. Les innovations technologiques ouvrent la voie à d'autres avancées, créant une augmentation exponentielle de notre capacité à créer, partager et stocker les informations numériques. Malheureusement, le progrès ne se limite pas au respect de la loi et au respect des informations de chacun. Les cybercriminels évoluent tout aussi rapidement, créant un paysage de cybermenaces toujours plus étendu.

Selon *Cybersecurity Ventures*, les dommages causés par la cybercriminalité pourraient représenter un coût mondial annuel total de 6 000 milliards de dollars d'ici fin 2021, dépassant le coût annuel des dommages attribués aux catastrophes naturelles. Du côté des entreprises, ces dommages peuvent être tout aussi catastrophiques. Le coût moyen d'une cyberattaque est actuellement de 1,67 million de dollars, engendrant pour principales conséquences, d'importantes pertes opérationnelles et de productivité, ainsi qu'une dégradation non négligeable de l'expérience client.

La cybermenace, ennemi n°1 des données des entreprises

Les données sont l'élément vital des entreprises. Elles soutiennent la croissance, transportent des ressources indispensables au développement des entreprises et les aident à rester en bonne santé. Et si les données sont considérées comme le sang du système, alors le réseau est le cœur qui les pompe à travers ce dernier. Néanmoins, les cybermenaces auxquelles nous sommes aujourd'hui confrontées sont de véritables fléaux, qui mettent tout en œuvre pour ébranler le bon fonctionnement du système et ainsi s'emparer de ces données vitales.

Dans le domaine de la sécurité des réseaux, trois éléments clés doivent servir de base à toute stratégie de sécurité des réseaux : la protection, la détection et la réponse.

La protection englobe tous les outils ou politiques conçus pour prévenir les intrusions dans le réseau. La détection fait référence aux ressources qui permettent d'analyser le trafic réseau et d'identifier rapidement les problèmes avant qu'ils ne puissent nuire. Enfin, la réponse est la capacité à réagir aux menaces de sécurité réseau identifiées et à les résoudre aussi rapidement que possible.

Des entreprises suicidaires ou simplement mal équipées ?

Malheureusement, la plupart des entreprises ne savent tout simplement pas comment mettre en place correctement leur stratégie de sécurité réseau. Une enquête menée par *Hiscox* auprès de professionnels clés aux États-Unis et en Europe a révélé que près de trois entreprises sur quatre appliquent une stratégie de cybersécurité qualifiée de novice. Cette fragile stratégie représente bel et bien une menace croissante, équivalente aux

cybermenaces. En effet, lorsque des brèches dans le réseau se produisent et que des menaces malveillantes se manifestent, l'enjeu dépasse les données elles-mêmes.

Fort heureusement, des outils et dispositifs de sécurité réseau existent pour aider les entreprises à protéger non seulement leurs informations sensibles, mais aussi leurs performances globales, leur réputation et même leur capacité à rester en activité. Une capacité opérationnelle continue et une réputation solide sont deux avantages clés d'une sécurité réseau efficace.

Les outils de sécurité réseau au secours de la réputation des entreprises

L'effet néfaste qu'une violation de réseau peut avoir sur la réputation de l'entreprise est tout aussi, voire encore plus dommageable. En effet, compte tenu de la vague croissante d'usurpation d'identité et d'autres dangers liés au vol d'informations personnelles, de nombreux clients hésitent de plus en plus à partager leurs données avec les entreprises. Si une cyberattaque envers une entreprise est avérée, bon nombre de ses clients peut faire le choix de se retirer en faveur d'alternatives plus sûres.

Avec la perte ou l'altération de données précieuses, ainsi que la perturbation importante des services à la clientèle et des processus internes, il n'est pas difficile de comprendre l'enjeu de la sécurité des réseaux. Sans oublier que l'atteinte à la réputation d'une entreprise peut avoir des effets bien plus durables que les autres dommages. Bien que l'effondrement de la réputation de petites ou moyennes entreprises peut être irrémédiable, il en est de même avec les grands groupes qui pourraient perdre définitivement leur crédit de confiance.

Contrôle limitant l'accès et les ressources des utilisateurs aux seules parties du réseau ; moteur de détection d'anomalie qui analyse en continu le réseau et alerte ainsi rapidement les équipes InfoSec en cas de violation ; segmentation du réseau permettant d'accorder le bon accès au bon trafic, tout en limitant le trafic provenant de sources suspectes... Tant d'outils fiables en matière de logiciels et de matériel de sécurité réseau, qui, associés à des stratégies appropriées, sont la clé pour garantir un impact minimal en cas de cyberattaques et ainsi préserver la sécurité des données des entreprises et de leurs clients.