Le déchiffrement TLS/SSL, l'un des principaux piliers du modèle Zero-Trust

Risques internes : ne plus se cantonner à l'approche de type « château fort »

Les cyberattaques actuelles ne se limitent plus aux intrusions provenant de l'extérieur. Les attaques les plus sophistiquées sont souvent menées par des personnes déjà infiltrées dans l'entreprise.

À l'origine, nous pensions en termes de zones, périmètres et de segments réseau, et toutes les ressources à protéger étaient placées « à l'intérieur » de ce périmètre. Toutefois, les méthodes d'attaques évoluent sans cesse et exploitent systématiquement les points faibles du réseau, afin de trouver de nouvelles possibilités d'infiltration du périmètre de sécurité. Il est également important de réaliser que l'approche « château fort » des défenses réseau est surtout efficace contre les menaces provenant de l'extérieur.

Mais que se passe-t-il lorsque ces menaces viennent de l'intérieur ? Comment gérer les attaques modernes qui jouent sur plusieurs niveaux pour neutraliser le réseau ? Comment protéger son réseau contre les personnes qui ont un accès légitime à l'ensemble des ressources ? Comment combattre des cyberattaques qui évoluent désormais constamment et sont de plus en plus fréquentes ? A ces questions s'ajoutent des réglementations telles que le RGPD et les amendes records qui les accompagnent. Il est donc évident qu'une attaque du réseau et une violation des données font partie des pires menaces pouvant arriver à une entreprise.
Avec ces problèmes en toile de fond, nous sommes contraints de réévaluer et de repenser les modes de défense de nos réseaux, de nos utilisateurs et de nos données.

Modèle Zero-Trust : une approche moderne de la cybersécurité

Le modèle Zero-Trust permet de remédier aux problèmes et de combler les lacunes de nos stratégies de cybersécurité. Ce modèle revient essentiellement à « ne faire confiance à personne ». Il pose le principe que personne n'est totalement fiable, que l'accès doit être aussi limité que possible, et que la confiance est une vulnérabilité comme une autre qui peut mettre votre réseau en danger.

Les principaux préceptes du modèle Zero-Trust :

· Les réseaux doivent être repensés de sorte que le trafic et l'accès Est-Ouest puissent être limités.

· La détection des incidents et les contre-mesures doivent être facilitées et améliorées en utilisant

des solutions d'analyse et d'automatisation poussées, ainsi qu'en mettant en place une gestion et une vision centralisée du réseau, des données, des charges de travail, des utilisateurs et des périphériques utilisés.

· L'accès doit être aussi limité que possible, en limitant les privilèges excessifs quels que soient les utilisateurs.

· Dans les réseaux multifournisseurs, toutes les solutions doivent être intégrées et interagir de façon transparente, afin d'assurer la mise en conformité et une sécurité unifiée. Ces solutions doivent également rester simples à utiliser, afin d'éviter toute complexité superflue.

Danger des angles morts de sécurité

Le chiffrement sur Internet a connu une croissance phénoménale ces dernières années. Google indique que plus de 90 % du trafic traversant ses services est chiffré. Les autres fournisseurs font le même constat. Cette augmentation est liée à de nombreux facteurs et notamment la demande de confidentialité.

Cependant, le chiffrement crée un « angle mort » dans les défenses de nos réseaux, car la plupart des périphériques de sécurité que nous utilisons ne sont pas conçus pour déchiffrer et inspecter le trafic. Le modèle Zero-Trust n'est pas à l'abri de ce problème, car la visibilité est considérée comme l'un des éléments clés d'une implémentation réussie. En l'absence d'une visibilité totale du trafic chiffré, le modèle échoue, ce qui introduit des vulnérabilités exploitables par les hackers aussi bien de l'intérieur que de l'extérieur.

Déchiffrement TLS/SSL : un des principaux piliers du modèle Zero-Trust

Une solution de déchiffrement centralisée et dédiée doit être placée au cœur du modèle Zero-Trust et doit faire partie intégrante des composants de la stratégie de sécurité.

De nombreux fournisseurs de solutions de sécurité disent pouvoir déchiffrer leur propre trafic, indépendamment d'une solution de déchiffrement centralisée. Cependant, cette approche de « déchiffrement distribué » peut introduire de nouveaux problèmes, notamment sous la forme de pertes de performances réseau et de goulots d'étranglement, et les corriger impliquerait des mises à niveau coûteuses.
Dans une infrastructure de sécurité multifournisseurs et couvrant des périphériques très différents, le « déchiffrement distribué » force également à déployer les clés privées à plusieurs endroits, créant ainsi une surface d'attaque inutilement large et ouverte aux abus.

Les clés d'une solution de déchiffrement TLS/SSL

efficace

Il est important qu'une solution de déchiffrement dédiée et centralisée offre une visibilité complète de l'infrastructure de sécurité de l'entreprise pour le trafic TLS/SSL. Mais ce n'est pas tout, l'approche de sécurité de cette solution doit également porter sur plusieurs couches, afin de lui permettre d'être déployée au cœur d'un réseau Zero-Trust.

Voici quelques-unes des fonctionnalités à rechercher lors de l'implémentation d'une solution de chiffrement TLS/SSL :

- **Visibilité complète du trafic**
  L'ensemble de l'infrastructure de sécurité doit être en mesure d'inspecter l'intégralité du trafic en texte clair, très rapidement, afin de bloquer les attaques chiffrées et les violations de données
- **Simplicité d'intégration**
  Elle doit rester agnostique par rapport aux fournisseurs et s'intégrer avec les périphériques de sécurité déjà déployés sur le réseau. Cela permet de maîtriser les coûts et les mises à niveau.
- **Services de sécurité portant sur plusieurs couches**
  Il s'agit ici de services de sécurité supplémentaires, notamment le filtrage d'URL, la visibilité des applications et leur contrôle, le renseignement sur les menaces et des investigations poussées, afin de renforcer l'efficacité de la sécurité de l'ensemble du réseau de l'entreprise
- **Contrôle de l'accès utilisateur**
  Le produit doit être en mesure d'appliquer les politiques d'authentification et d'autorisation pour limiter les accès inutiles, tenir un registre des informations d'accès et différencier les politiques de sécurité en fonction des identifiants de l'utilisateur et des groupes.
- **Microsegmentation**
  La solution doit faciliter la microsegmentation en autorisant un contrôle granulaire du trafic, basé sur les identifiants de l'utilisateur et du groupe, et prendre en charge le mode multilocataire.
- **Sécurisation de l'accès au cloud**
  La sécurité SaaS est une fonctionnalité importante qui peut être assurée en appliquant le contrôle d'accès du locataire et la visibilité des activités de l'utilisateur.

En conclusion, en l'absence d'une solution de déchiffrement TLS/SSL centralisée et dédiée, le modèle Zero-Trust ne peut plus remplir sa fonction principale, qui est de protéger les réseaux, les utilisateurs et les données aussi bien contre les menaces venant de l'extérieur, que de l'intérieur.