

Comment se protéger des cyberattaques de façon simple et durable ?



Jérôme Beaufile,
Président de Sasety

L'Agence nationale de la sécurité des systèmes d'information (ANSSI) a récemment publié le bulletin CERTFR-2022-ACT-008 qui présente les dix vulnérabilités les plus critiques de 2021. Bien que les techniques de développement logiciel et les bonnes pratiques aient évolué en termes de sécurité, il reste impossible de garantir l'absence de vulnérabilités. Leur correction fait partie intégrante du cycle de vie des solutions.

En 2021, de nombreux événements de sécurité ont exploité des vulnérabilités bien connues, et certaines souvent anciennes.

Aussi, le principal enjeu en termes de cybersécurité consiste à protéger ses actifs au sein d'un réseau privé virtuel sécurisé, et à maintenir toutes les composantes du système d'information dans des conditions optimales de sécurité.

Parmi celles qui nécessitent une attention maximale, l'ANSSI met l'accent sur les passerelles VPN (Réseaux privés virtuels) qui permettent d'accéder au système d'information depuis l'Internet.

Ces solutions doivent être mises à jour très rapidement et les mécanismes d'authentification et de transport doivent être particulièrement robustes (authentification multifacteur, chiffrement, historisation). Ces opérations sont sensibles et doivent

être correctement réalisées pour limiter les risques d'impact sur la production.

Le modèle SASE Secure Access Service Edge défini par l'entreprise américaine de conseil et de recherche Gartner aide clairement les organisations dans ce travail vital, complexe et coûteux.

Le SASE, ou Secure Access Service Edge, consiste à s'appuyer sur une architecture réseau et sécurité de nouvelle génération délivrée dans le Cloud. Elle permet aux organisations de connecter de façon sécurisée n'importe quel utilisateur à n'importe quelle application, partout dans le monde. Les entreprises peuvent alors mener à bien la mutation de leurs infrastructures réseau et sécurité pour réussir leur transformation numérique. Il s'agit d'un dispositif unique qui permet aux équipes de travailler en toute sécurité en s'appuyant sur des infrastructures à hautes performances.

Par ailleurs, face à l'exposition aux cybermenaces, le réflexe de beaucoup d'organisations est d'accroître le nombre d'outils de sécurité.

Une étude récente a montré que ceux-ci ont augmenté de près de 20 % depuis 2019.

Le mieux étant souvent l'ennemi du bien, cette approche provoque l'effet contraire de celui escompté.

Car au-delà de la fuite en avant financière, l'empilement des outils augmente la complexité.

Les équipes IT ou leurs prestataires doivent réaliser des efforts d'intégration et de maintien en conditions opérationnelles très importants.

Ceci requiert une expertise et une charge très conséquente pour un résultat souvent hypothétique, car :

- comment collecter et corréler efficacement les informations provenant de sources et de formats multiples ?
- comment évaluer leur pertinence et identifier avec précision les faux positifs ?
- comment s'assurer que les outils fonctionnent correctement ensemble alors qu'ils doivent être en permanence mis à jour ?

Ces outils contribuent-ils vraiment à une posture de sécurité efficace et pérenne ?

Pour preuve, les marqueurs précurseurs d'une attaque sont présents au sein du Système d'Information des semaines voire des mois avant la concrétisation de leurs actions.

Pendant cette période, les équipes IT disposent de nombreuses possibilités de détecter, limiter, voire juguler l'attaque en identifiant les opérations en cours de réalisation :

- collecte de mots de passe ;

- exécution d'outils systèmes ;
- modification des privilèges, déplacement latéral vers des données à valeur ajoutée, ou encore mise en place de tunnels d'exfiltration.

Pourtant dans la majorité des cas, ces signaux échappent aux contrôles de sécurité en place.

Alors, plutôt que de tenter d'ajouter en permanence de nouvelles fonctions de défense, il est plus utile de se concentrer sur l'utilisation efficace de solutions simples.

Car peu importe comment les attaquants ont pénétré le Système d'Information, leur agilité leur permettra toujours de trouver le moyen d'y parvenir.

Ce qui est important, c'est de contrer ce qu'ils sont venus y faire.

Et sur ce point, les attaquants ont toujours les mêmes objectifs : hameçonnage, vol de mots de passe, analyse des vulnérabilités.

L'empilement des solutions de sécurité apporte donc plus de

complexité que d'efficacité dans la cybersécurité des organisations.

Il est plus utile de capitaliser sur des solutions simples et bien maîtrisées par les équipes IT.

Cette approche, basée sur la simplicité et l'efficacité de la sécurité, est l'un des piliers du modèle SASE.

Dans ce modèle, les fonctions de sécurité essentielles contre les intrusions et les logiciels malveillants :

- sont délivrées dans le Cloud et n'ont aucune empreinte sur le Système d'information, ce qui simplifie leur mise en œuvre ;
- couvrent tous les actifs et les modes de travail ;
- sont mises à jour automatiquement par l'éditeur sans action nécessaire des équipes IT ;
- unifient tous les événements de sécurité pour permettre une analyse directe et efficace.

Les bénéfices sont alors mesurables à différents niveaux :

- réduction de la surface d'attaque du Système d'Information ;

- protection en temps réel et 0-day contre les intrusions et les logiciels malveillants ;
- élimination de la charge et des risques associés aux mises à jour de sécurité ;
- contrôle des accès aux applications internes et Cloud réalisés par les utilisateurs sur site ou en situation de mobilité ;
- historisation de tous les échanges.

En conclusion, la réduction du risque d'exposition aux cyberattaques repose sur des solutions simples à déployer et à opérer.

Le modèle SASE constitue véritablement aujourd'hui le socle pérenne de la performance et de la sécurité IT des entreprises.

Plus tôt elles amorceront son adoption, plus vite elles pourront répondre efficacement aux enjeux digitaux de leurs métiers et aux nouveaux modes de production de leurs collaborateurs.

2022-8325

