

Zero trust : êtes-vous bien certain que tout est sécurisé ?

Vous pouvez renforcer la sécurité de votre domicile en ajoutant aux verrous de votre porte un système d'alarme et de vidéosurveillance. Cela n'empêchera pas les cambrioleurs de briser les fenêtres pour voler tout ce qui est à portée de main, d'essayer de désactiver le système d'alarme à distance, ou de vous espionner les habitants pour recueillir des informations sensibles.

De la même façon, les ZTNA (Architectures Réseau Zero-Trust) représentent une première mesure de protection importante pour améliorer la sécurité des entreprises, mais des mesures complémentaires sont nécessaires pour mettre en place une stratégie zero-trust complète.

Une ZTNA fonctionne comme un verrou qui protège des attaques réseau qui pourraient menacer les processus métier. Elle protège les chemins d'accès aux ressources stratégiques de l'entreprise sur site ou dans le cloud à l'aide de l'authentification multifactorielle, de l'analyse basée sur le [machine learning](#) et de la surveillance continue. Pourtant dans de nombreuses entreprises, le maillon faible n'est pas le réseau. En effet la majorité des vulnérabilités signalées se trouvent dans les applications. Certaines de ces failles sont bien connues et existent depuis des années, d'autres ont émergé avec les nouvelles approches de travail et de consommation.

Par conséquent, les entreprises ne doivent pas se concentrer exclusivement sur leur ZTNA : elles doivent également tenir compte de la sécurité des applications. Pour commencer, il serait judicieux de résoudre les problèmes applicatifs connus

les plus critiques. À l'heure où nous délaissions progressivement les applications héritées au profit des architectures de microservices cloud, il est logique de se concentrer non seulement sur les applications internes, mais aussi sur ces nouveaux microservices hébergés dans des clouds publics ou hybrides.

Dans le domaine de la sécurité des applications et des microservices, l'intelligence artificielle et le machine learning s'imposent comme des outils efficaces, capables de détecter des attaques sophistiquées bien plus rapidement que les humains ne le feraient. Le pare-feu d'application Web (WAF) représente un autre pilier critique de la sécurité applicative. À l'ère du cloud hybride, le WAF doit être aussi facile à déployer sur site que dans le cloud et doit offrir une faible latence et des performances élevées afin de garantir une expérience utilisateur fluide malgré les activités de sécurité qui s'exécutent à l'arrière-plan en permanence.

Les API s'imposent elles aussi comme un angle d'attaque de plus en plus critique. Elles sont universellement utilisées pour permettre aux applications de communiquer entre elles et pour automatiser des workflows inter applications. Par conséquent, les API permettent d'accéder à une multitude de données d'entreprise. Sans protection, ces données critiques sont vulnérables, augmentant ainsi l'exposition aux risques de l'entreprise. L'exfiltration des données peut même passer inaperçue si l'organisation ne dispose pas d'un système de surveillance des API. En plus du vol de données, les API peuvent également faire l'objet de surcharge pouvant interrompre totalement l'activité de l'entreprise.

Pour bien protéger les API, mieux vaut commencer par faire un inventaire complet afin d'identifier les API inconnues (ou « dans l'ombre ») et y appliquer un contrôle d'accès dans l'ensemble de l'entreprise, à l'aide de mécanismes d'authentification normalisés. Les API peuvent ensuite être

protégées contre les abus grâce à la définition de seuils d'appels. La surveillance continue permet également de collecter des informations importantes sur l'utilisation des API, leurs performances, les erreurs ou encore les échecs d'authentification.

Encore une fois, le machine learning s'imposera comme une excellente solution pour obtenir des données, protéger les API et appliquer l'état souhaité. En protégeant les API, les autorités peuvent par exemple définir des règles pour rejeter toute demande provenant d'un autre pays, limitant ainsi le risque d'abus. De leur côté, les entreprises et les fournisseurs de services dans divers secteurs peuvent empêcher le ralentissement voire l'interruption de leurs applications en raison d'un trafic API excessif.

Une fois les applications et les API protégées des attaques, il convient également d'éradiquer les bots malveillants. Néanmoins, tous les bots ne sont pas à bannir : beaucoup d'entreprises utilisent par exemple des chatbots et des bots vocaux pour traiter les messages et les appels de leurs clients. En revanche, les cybercriminels exploitent aussi ces technologies : en l'espace de quelques minutes après sa mise en ligne, un nouveau site d'entreprise sera analysé par des bots malveillants recherchant des vulnérabilités et des informations à collecter.

En 2020, le trafic web des mauvais bots représentait plus d'un quart de toutes les requêtes. En d'autres termes, les applications d'entreprise consacrent plus d'un quart de leur temps à ces bots, au détriment des clients. A titre d'exemple, entre septembre 2020 et février 2021, le trafic de bots malveillants sur les sites de santé a augmenté de 372%, un phénomène directement lié à la crise sanitaire et qui a lourdement affecté le fonctionnement des sites de prise de rendez-vous pour une vaccination.

Pour éviter cela, il faut commencer par séparer les bots

malveillants des bots inoffensifs, en filtrant les mauvais bots en fonction de leur score de réputation, de la géolocalisation, ou de ce que l'on appelle l'empreinte digitale des bots : plusieurs paramètres permettant de les distinguer des humains et de vérifier si leur comportement est anormal. Les technologies modernes de gestion de la mise à disposition des applications (Application Delivery Management, ADM) peuvent y contribuer, car elles sont capables d'identifier des bots sophistiqués.

La technologie d'atténuation des bots s'impose donc comme une composante essentielle de la cybersécurité. Elle permet par exemple aux e-commerçants de recevoir des alertes lorsque leurs concurrents tentent de collecter automatiquement les informations tarifaires de leur site, d'améliorer l'expérience client et de réduire les coûts en minimisant le trafic indésirable généré par les bots.

Si le zero-trust est à la pointe de la cybersécurité, un environnement zero-trust ne peut être obtenu simplement en déployant une ZTNA. Si ce type d'architecture permet bien de renforcer les verrous qui protègent le réseau de l'entreprise, la sécurité des API et des applications ainsi que l'atténuation des bots permettront de barricader les fenêtres par lesquelles les acteurs malveillants pourraient entrer. Le niveau de sécurité se mesure au maillon le plus faible de la chaîne : pour protéger leur activité des risques, les entreprises ont donc tout intérêt à mettre en place une stratégie zero-trust complète.