LIVRE BLANC

Mettre en œuvre un modèle de sécurité « Zero Trust » dans l'environnement hostile actuel

Akamai

Présentation

Les entreprises de tous types ont à cœur de réussir leur transformation digitale, l'objectif étant d'augmenter la valeur client, d'accroître l'efficacité et l'agilité opérationnelles et de stimuler l'innovation. Mais alors qu'elles tirent profit des nouveaux flux cloud et DevOps pour développer leurs activités digitales, la sécurité n'a pas évolué en conséquence. La prolifération des applications cloud et la mobilité grandissante des collaborateurs ont profondément réduit l'efficacité du périmètre réseau. Les applications, les données, les utilisateurs et les terminaux sortent progressivement de la sphère de contrôle de l'entreprise, ce qui étend considérablement la surface d'exposition aux attaques. D'un côté, l'infrastructure devient plus perméable afin de permettre aux entreprises de mettre en œuvre de nouveaux modèles économiques ; de l'autre, les cybercriminels sont davantage incités à trouver des moyens de contourner les mesures de sécurité et font preuve d'une plus grande dextérité et subtilité en la matière. La sécurité périmétrique classique n'est tout simplement pas adaptée à la réalité actuelle.

Face à la prolifération des cyberattaques, et des violations de sécurité qui s'en suivent, comment les entreprises peuvent-elles se protéger ? Ce livre blanc présente un paradigme de sécurité pour l'environnement hostile d'aujourd'hui : le « Zero Trust ». Ce modèle repose sur un postulat simple : les utilisateurs et les terminaux ne sont jamais considérés comme fiables, et l'environnement est supposé hostile. Le « Zero Trust » met en avant le fait qu'il ne doit y avoir aucune distinction entre les réseaux internes et externes. Avec ce modèle, l'ensemble des terminaux et demandes d'accès font l'objet de vérifications systématiques avec journalisation complète et analyses des comportements. Ce livre blanc explique en outre pourquoi le secteur informatique a tout intérêt à se tourner vers les services cloud pour s'éloigner du modèle de sécurité reposant sur la notion de périmètre.

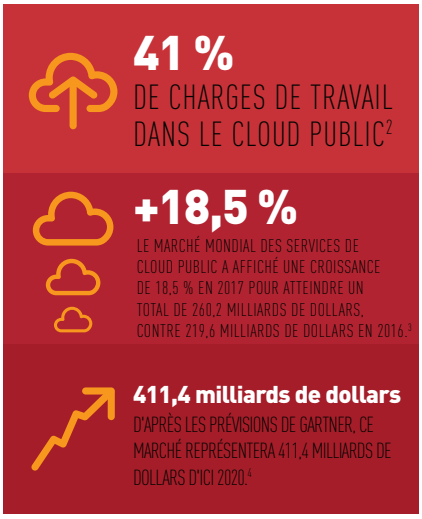
Une transformation digitale omniprésente

Une importante transformation digitale s'observe à présent partout dans la plupart des secteurs. Et la tendance s'accélère. D'après une étude IDC, l'investissement mondial dédié à la transformation digitale atteindra 2 200 milliards de dollars en 2019, soit une augmentation de près de 60 % par rapport à 2016.[1]

Les entreprises s'appuient sur des architectures cloud et réseau avancées pour dégager une nouvelle valeur client tout en progressant en matière d'efficacité opérationnelle, d'agilité et d'innovation. La transformation digitale est bénéfique pour les utilisateurs, car elle permet aux entreprises de proposer des produits digitaux, des services de meilleure qualité, des échanges personnalisés et une expérience client supérieure. Quant aux employés, ils s'appuient sur les technologies digitales pour communiquer et collaborer facilement en ligne, ce qui améliore leur productivité et leur moral.

Un périmètre de confiance qui n'existe plus

Le recours à des services digitaux présente de nombreux avantages, mais souffre d'un inconvénient : les entreprises voient leur surface d'exposition aux attaques s'étendre dans le paysage de menaces actuel, de plus en plus hostile. Elles doivent par conséquent repenser les bases de la sécurité périmétrique et la façon dont elles protègent leurs applications stratégiques, leurs données et leurs utilisateurs.



La transformation digitale influe profondément sur la manière dont les entreprises fournissent des solutions informatiques, ainsi que sur leur exposition aux menaces. Dans le modèle classique, les utilisateurs considérés comme fiables ont accès aux applications par le biais de réseaux locaux privés (LAN), de réseaux étendus (WAN) ou de réseaux privés virtuels (VPN). Les entreprises ont adopté la sécurité périmétrique, qui inclut les pare-feu, les VPN et les contrôles d'accès au réseau (NAC), pour garder les cybercriminels à l'extérieur des réseaux internes. Une fois à l'intérieur du réseau, les utilisateurs étaient de ce fait considérés comme fiables et pouvaient aller où bon leur semblait.

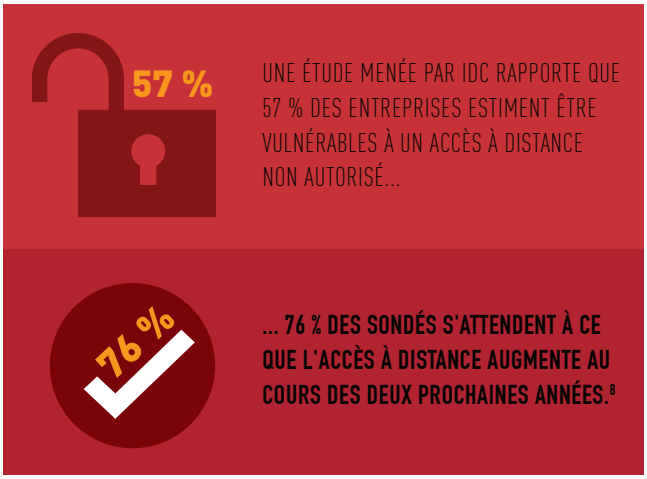
Mais maintenant que les entreprises opèrent leur transformation digitale, les notions de réseaux externes et internes n'ont plus lieu d'être. De plus en plus

d'applications sont hébergées dans le cloud, en dehors de la sphère de contrôle classique des services informatiques. Les participants à une enquête RightScale ont déclaré qu'ils exécutaient 41 % de leurs charges de travail dans le cloud public.[2] Le marché mondial des services de cloud public a augmenté de 18,5 % en 2017 pour atteindre un total de 260,2 milliards de dollars, contre 219,6 milliards de dollars en 2016.[3] D'après les prévisions de Gartner, ce marché représentera 411,4 milliards de dollars d'ici 2020.[4]

Les employés ne se connectent plus principalement entre les quatre murs d'un bureau. Beaucoup d'entre eux sont souvent en déplacement ou travaillent régulièrement à distance, sont dispersés aux quatre coins du monde et se connectent via des réseaux non sécurisés. L'enquête de PGI sur le télétravail à l'échelle mondiale (Global Telework Survey) révèle que 79 % des travailleurs de la connaissance dans le monde sont des télétravailleurs.[5]

Par ailleurs, l'idée qu'une entreprise digitale emploie uniquement des travailleurs à temps plein est obsolète. La plupart des entreprises dépendent de fournisseurs, distributeurs, sous-traitants et partenaires qui ont besoin d'avoir accès à des applications internes spécifiques pour accroître leur productivité. Sans surprise, tout accès tiers augmente le risque que des informations professionnelles critiques tombent entre de mauvaises mains. Sans compter que la prolifération des politiques Bring Your Own Device (BYOD) signifie que les services informatiques ont plus de difficultés à contrôler les terminaux que les utilisateurs accèdent aux applications et données de l'entreprise.

Dans le même temps, les cybercriminels parviennent de plus en plus souvent à franchir le pare-feu. Certains y parviennent en utilisant les identifiants d'un utilisateur de confiance ; d'autres, par le biais de pièces jointes ou de liens malveillants. Une étude Symantec révèle que le taux de programmes malveillants dans les e-mails a augmenté de manière significative : en 2015, un e-mail sur 220 envoyés contenait un programme malveillant, contre un e-mail sur 131 en 2016.[6] Et une fois que les cybercriminels se sont introduits sur un réseau, il faut, en moyenne dans le monde, 146 jours pour détecter leur présence.[7] Une étude IDC rapporte que 57 % des entreprises estiment être vulnérables à un accès à distance non autorisé, et 76 % des sondés s'attendent à ce que les accès à distance augmentent au cours des deux prochaines années.[8] Les pertes engendrées par les accès à distance non autorisés sont lourdes. En moyenne, les entreprises s'attendent à concéder 6,5 millions de dollars à cet égard.[9]



Une sécurité périmétrique classique inappropriée

Les applications, les données, les terminaux et les utilisateurs de l'entreprise sortent du périmètre de sécurité, tandis que les cybermenaces l'infiltrent ; la sécurité périmétrique traditionnelle n'est donc plus suffisante.

Les entreprises protègent depuis longtemps leurs réseaux professionnels à l'aide de piles de périmètre, ou DMZ (zones démilitarisées). Ces zones de cloisonnement incluent les dispositifs de contrôle d'accès (dispositifs VPN, fournisseurs d'identité, authentification unique/à plusieurs facteurs, client-serveur), les dispositifs de sécurité (Web Application Firewalls, prévention contre la perte de données, pare-feu nouvelle génération, passerelles Web sécurisées), ainsi que les dispositifs de diffusion d'applications et de gestion des performances (équilibrage de la charge et optimisation). Mais ces architectures basées sur des périmètres n'ont en aucun cas été conçues pour optimiser l'expérience des utilisateurs qui accèdent aux applications depuis différents sites. Elles n'ont pas non plus été conçues pour le modèle de logiciel en tant que service (SaaS) ou pour les applications hébergées dans le cloud. Pour remédier à cette situation, les services informatiques doivent souvent reproduire autant que nécessaire ces piles de périmètre, pour des questions de redondance et de haute disponibilité, afin de couvrir l'ensemble des régions et des centres de données, entraînant des augmentations de coût et une complexité croissante.

Les applications étant déplacées vers le cloud, les entreprises n'ont plus le même contrôle : la sécurité réseau traditionnelle basée sur les paquets, les ports et les protocoles ne fonctionne plus lorsque les entreprises ne gèrent pas l'ensemble du réseau et de l'environnement applicatif.

Les entreprises continueront d'exécuter à la fois des applications dans le cloud et sur site dans un futur prévisible. Elles devront conserver un ensemble disparate de solutions de contrôle d'accès et de sécurité susceptibles de ne pas bien fonctionner ensemble, et n'auront pas d'endroit central pour gérer et contrôler ces technologies. Or, des systèmes fragmentés conduisent à un risque accru et à une visibilité moindre.

Sans compter que la notion sous-jacente de sécurité périmétrique sur site, délimitée par des murs, est devenue obsolète. Les cybercriminels parviennent souvent à infiltrer les réseaux des entreprises en utilisant des noms d'utilisateur et

mots de passe légitimes ou en installant des programmes malveillants qui décèlent les faiblesses dans les solutions de sécurité existantes. Un rapport a récemment révélé que 91 % des cyberattaques commencent par une technique d'hameçonnage conçue pour voler les identifiants d'un utilisateur autorisé.[10] Les solutions périmétriques sont inefficaces pour protéger les données et applications professionnelles des attaques initiées à l'intérieur du périmètre.

La nouvelle ère du « Zero Trust »

Alors que la sécurité périmétrique traditionnelle connaît ses dernières heures, comment les entreprises doivent-elles protéger leurs applications, leurs données et leurs effectifs contre des menaces de cybersécurité de premier plan toujours plus nombreuses ? La réponse réside dans la mise en œuvre d'un modèle de sécurité « Zero Trust », autrement dit prônant le principe de « zéro confiance ». Le credo n'est plus de « faire confiance tout en vérifiant », mais de « ne jamais faire confiance et toujours vérifier ».

Défendu en premier lieu par Forrester Research, le modèle de sécurité « Zero Trust » suppose qu'il n'existe pas de notion d'« interne » et que chaque personne et chaque terminal est considéré de la même manière comme non fiable. Toutes les applications sont traitées comme si elles se trouvaient sur Internet et le réseau tout entier est considéré comme compromis et hostile. Principaux aspects du « Zero Trust » :

- Garantir que toutes les ressources font l'objet d'un accès sécurisé, quel que soit leur emplacement ou le modèle d'hébergement employé
- Adopter une stratégie du « moindre privilège » et appliquer rigoureusement les contrôles d'accès pour limiter les risques associés aux privilèges utilisateurs excessifs
- Inspecter et enregistrer l'ensemble du trafic à la recherche de toute activité suspecte afin d'améliorer la détection et l'intervention de sécurité

Longue vie au cloud

Alors que les terminaux, les données, les applications et les comportements des utilisateurs continuent d'évoluer, la mise en œuvre d'une approche « Zero Trust » doit pouvoir se faire dans le cloud en utilisant Internet comme réseau principal. Plutôt que d'utiliser des pare-feu bloquant les IP ou les ports, la sécurité basée dans le cloud se concentre sur la couche applicative et les protocoles de niveau supérieur. Le recours à des contrôles de sécurité basés dans le cloud doit permettre aux entreprises de fermer leurs pare-feu et de conserver leurs applications internes à l'abri d'Internet. Les services d'authentification et d'autorisation contrôlent alors l'accès à chaque application à partir de terminaux gérés et non gérés, qu'il s'agisse d'applications sur site, d'applications SaaS ou d'applications faisant appel à une infrastructure en tant que service (IaaS) comme Amazon Web Services.

Les contrôles de sécurité basés dans le cloud doivent inclure la vérification de toutes les requêtes DNS sortantes provenant des terminaux de l'entreprise, y compris des ordinateurs portables et des terminaux utilisant l'Internet des objets (IoT, Internet of Things), afin de garantir qu'elles ne s'exposent pas à des sites malveillants ou inappropriés. La solution de sécurité doit également surveiller et analyser le trafic à la recherche de signes d'activité suspecte, comme une communication avec un serveur de commande et de contrôle (CnC) ou une exfiltration de données, et signaler immédiatement tout problème au service informatique.

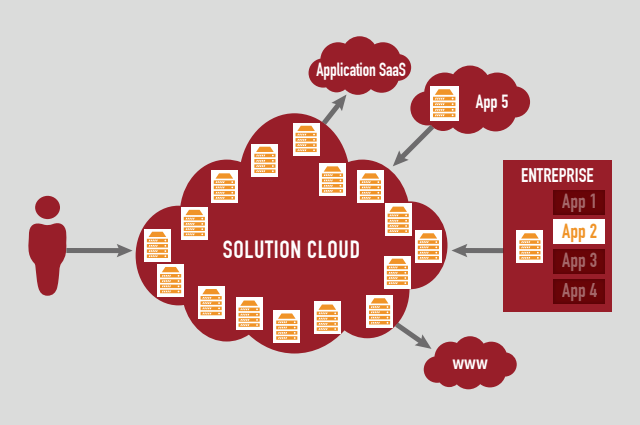
Mettre en œuvre le « Zero Trust » via le cloud résout la majorité des difficultés liées à une sécurité réseau périmétrique obsolète. Ce nouveau modèle garantit que les utilisateurs authentifiés bénéficient d'un accès autorisé uniquement pour les applications autorisées. Il empêche également les points de terminaison infectés d'accéder à des sites malveillants ou inappropriés, ou de se connecter à une infrastructure CnC malveillante capable de prendre le contrôle des machines des utilisateurs et d'en exfiltrer des données. Qui plus est, il peut empêcher les programmes malveillants de se déplacer latéralement sur le réseau.

Mise en œuvre du « Zero Trust » dans un environnement cloud

Les entreprises peuvent réduire leur surface d'exposition aux attaques en faisant le choix d'un service cloud pour mettre en œuvre un modèle de sécurité « Zero Trust », tout en profitant de l'agilité, de l'échelle et des avantages économiques d'Internet.

Accès protégé

Les entreprises en pleine transformation digitale ont besoin de fournir à leurs employés, fournisseurs, consultants et autres partenaires un accès rapide, aisé et sûr aux applications situées derrière le pare-feu, depuis n'importe quel terminal, partout dans le monde. Les technologies d'accès classiques utilisent différents dispositifs matériels et logiciels pour fournir un accès réseau à tout utilisateur disposant des bons identifiants. Toutefois, des études révèlent que la plupart des violations de sécurité résultent du vol ou d'une utilisation malveillante d'identifiants utilisateur valides. Un modèle de sécurité « Zero Trust » suppose que tous les utilisateurs présentent un risque et ne sont donc pas fiables.



L'utilisation du cloud comme extension de votre infrastructure permet un accès « Zero Trust » : un point d'entrée existe uniquement pour les applications dont les utilisateurs ont besoin, et non pour l'ensemble du réseau. Ce principe du moindre privilège s'étend à tous les terminaux et toutes les applications partout dans le monde.

Avec une sécurité basée dans le cloud, l'accès direct aux applications est refusé puisque toutes les applications sont dissimulées à l'abri d'Internet et de l'exposition publique. Le cloud repose non seulement sur le chemin d'authentification et d'autorisation, mais aussi directement sur le chemin de données de l'utilisateur. Il constitue le seul point d'entrée des utilisateurs pour avoir accès aux ressources critiques de l'entreprise. Le service cloud fournit une connexion TLS sécurisée basée sur l'authentification mutuelle à partir du réseau ou de l'IaaS de votre entreprise et distribue l'application à l'utilisateur. Des serveurs proxy sécurisés appliquent des mesures d'authentification et contrôles de sécurité stricts. Ces fonctions isolent les réseaux internes et les applications IaaS à l'abri d'Internet et déplacent la surface d'exposition aux attaques en périphérie.

Authentification

Pour fournir aux utilisateurs un accès sécurisé aux applications et aux données de grande valeur, la sécurité basée dans le cloud doit s'intégrer aux services d'authentification existants (par exemple, Okta ou Microsoft Active Directory), ou fournir ses propres solutions d'authentification, incluant des fonctions de sécurité avancées telles que l'authentification à deux facteurs ou plus. Exiger une authentification à la fois pour le terminal et pour l'utilisateur renforce la sécurité. Le cybercriminel devra en effet voler au moins deux identités pour accéder aux ressources. C'est là une amélioration majeure par rapport aux approches classiques.

Le cloud doit renforcer encore la sécurité en authentifiant les utilisateurs à l'extérieur de l'infrastructure de l'utilisateur sans nécessiter de matériel ou logiciel supplémentaire.

Autorisation

En adoptant une stratégie d'accès basée sur le principe du moindre privilège et en appliquant rigoureusement les contrôles d'accès, les entreprises réduisent les voies que les cybercriminels et les programmes malveillants peuvent emprunter pour obtenir un accès non autorisé. Une solution cloud présente alors l'avantage de fournir explicitement un accès propre à chaque application au lieu d'appliquer des privilèges généraux. Les entreprises peuvent définir des politiques de sécurité pour l'ensemble des utilisateurs, terminaux, applications et données.

Protection multicouche

Alors qu'un réseau « Zero Trust » contrôle strictement l'accès à toutes les ressources du réseau, les applications restent vulnérables aux attaques par déni de service distribué (DDoS), aux attaques par injection SQL (SQLi) ou encore aux attaques de la couche applicative, pour ne citer qu'elles. La sécurité basée dans le cloud doit inclure d'autres couches de protection pour lutter contre ces attaques. La protection contre les attaques DDoS est un rempart contre les attaques qui inondent de requêtes inutiles les applications ou sites visés afin de surcharger les systèmes et compromettre l'accès des utilisateurs légitimes à l'application. La protection de la couche applicative permet de lutter contre les attaques qui manipulent, corrompent ou suppriment des données, comme les attaques par injection SQL. Ces solutions offrent également une protection contre une méthode fréquemment utilisée qui consiste à lancer une attaque par DDoS pour faire diversion : les cybercriminels lancent simultanément une attaque par DDoS et une attaque de la couche applicative, par exemple une attaque par injection SQL ou une attaque Cross-Site Scripting (XSS).

Inspection de tout le trafic par proxy

Alors que les contrôles d'accès sécurisent les applications connues, beaucoup d'employés et partenaires utilisent des applications basées sur Internet, comme Google ou Trello. Ces applications peuvent être un véritable atout pour la productivité des employés, mais les sites Web peuvent également héberger des programmes malveillants dangereux ou des contenus inappropriés relevant de l'incitation à la haine ou de la pornographie. En outre, les attaques par hameçonnage, qui exploitent les liens vers des domaines malveillants, sont en augmentation et représentent une source d'attaques malveillantes. Alors qu'une grande partie des entreprises ont mis en place plusieurs couches de protection, l'exfiltration de données basée sur le DNS reste une importante lacune de sécurité pour la plupart des entreprises.

Au lieu de résoudre toutes les requêtes DNS à l'aveugle, les entreprises doivent avoir recours à des contrôles de sécurité dans le cloud pour exploiter efficacement les informations obtenues en temps réel et assurer une protection proactive contre les menaces en évolution constante. Les services de sécurité dans le cloud doivent être capables de fonctionner comme un serveur DNS récursif, de vérifier les noms de domaine à l'aide d'une liste des domaines malveillants connus étoffée et régulièrement mise à jour, d'exploiter les informations collectées et d'administrer des règles empêchant des requêtes d'atteindre des domaines malveillants ou dont le contenu est inapproprié. Cette validation a lieu avant que la connexion IP soit établie, les menaces peuvent donc être contrées plus tôt dans la chaîne d'attaque.

L'importance du « Zero Trust » augmente de manière exponentielle à mesure que les entreprises utilisent de plus en plus de terminaux IoT. Par exemple, le service informatique peut ne pas savoir qu'un téléviseur connecté dans une salle de conférence émet des requêtes vers des domaines malveillants sur Internet, signe d'une éventuelle compromission.

Informations en temps réel sur les menaces

« Toujours vérifier » implique une surveillance et un contrôle continus du trafic pour analyser l'activité. Le « Zero Trust » suppose que même le trafic provenant d'un LAN est suspect et doit par conséquent être analysé et enregistré comme s'il provenait d'Internet. Les analyses de comportements permettent d'identifier les modèles de trafic suspects, tels que ceux indiquant une communication avec un serveur CnC ou une exfiltration de données.

Conclusion

La mise en œuvre d'un modèle de sécurité « Zero Trust » dans une architecture basée dans le cloud permet aux entreprises d'adapter leur cybersécurité aux nouvelles réalités du secteur informatique. Que les applications et données se trouvent dans le centre de données ou le cloud, les entreprises peuvent fournir aux utilisateurs un accès sécurisé, simple et performant, où qu'ils soient et quel que soit le terminal qu'ils utilisent. Elles peuvent empêcher les utilisateurs d'accéder à des applications externes contenant des programmes malveillants susceptibles de compromettre le réseau ou contenant des ressources inappropriées. Et elles peuvent surveiller en continu le trafic afin de repérer tout comportement suspect. Rassurées de savoir que leurs données et applications de grande valeur sont sécurisées, elles peuvent tirer pleinement profit des technologies de pointe pour réussir leur transformation digitale.

Sources

1. https://www.idc.com/getdoc.jsp?containerId=prUS41888916
2. www.rightscale.com/blog/cloud-industry-insights/cloud-computing-trends-2017-state-cloud-survey
3. https://www.gartner.com/newsroom/id/3815165
4. https://www.gartner.com/newsroom/id/3815165
5. https://www.ondeck.com/blog/your-complete-guide-to-the-remote-workforce-in-2017
6. https://digitalhubshare.symantec.com/content/dam/Atlantis/campaigns-and-launches/FY17/Threat%20Protection/ISTR22_Main-FINAL-JUN8.pdf?aid=elq_
7. https://www.fireeye.com/company/press-releases/2016/fireeye-releases-first-mandiant-mtrends-emea-report.html
8. https://www.akamai.com/us/en/multimedia/documents/report/remote-access-security-challenges-and-opportunities.pdf
9. https://www.computerworld.com/article/3222829/security/state-of-remote-access-security.html
10. https://www.darkreading.com/endpoint/91--of-cyber attacks-start-with-a-phishing-email/d/d-id/1327704?