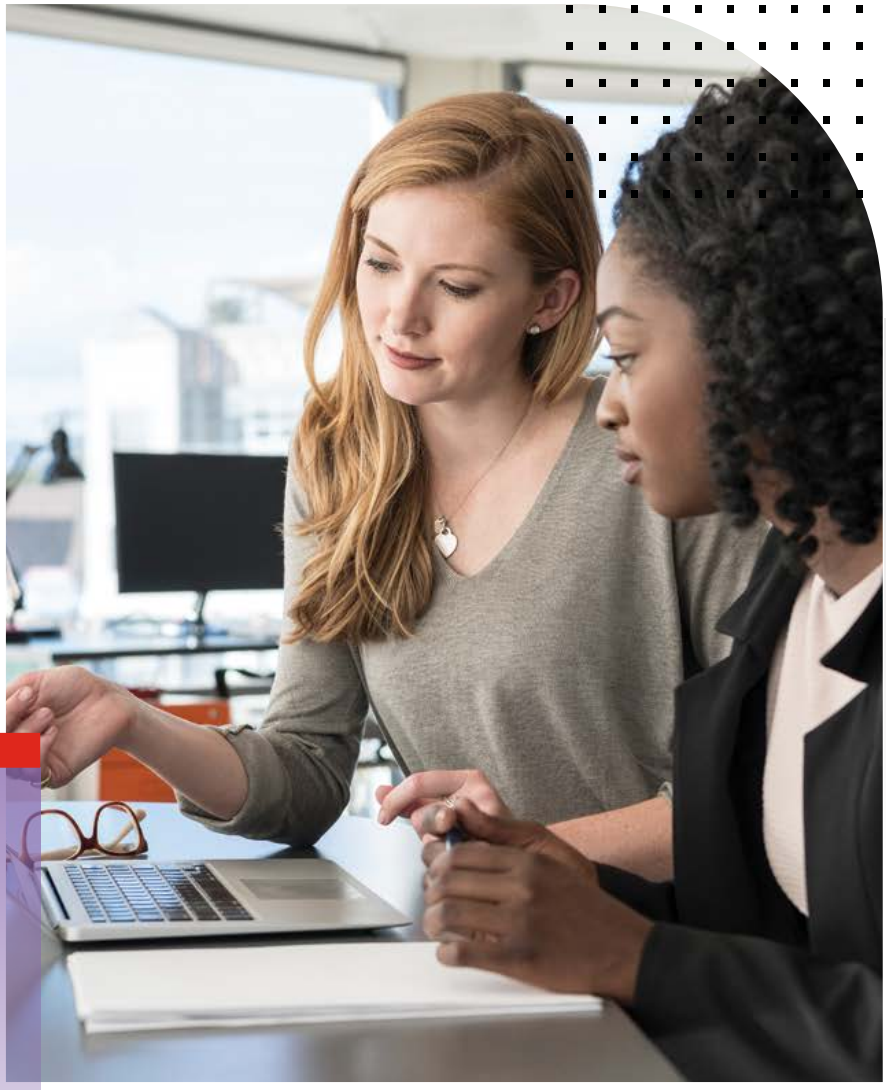
LIVRE BLANC

Sécuriser l'innovation numérique exige un accès Zero Trust

Les RSSI font face à de nouveaux risques alors que la surface d'attaque s'étend



Synthèse

Pour doper leur business et rester compétitives, les entreprises déploient des projets d'innovation numérique. Les applications et les données de l'entreprise sont désormais disséminées sur plusieurs sites, ce qui permet aux travailleurs d'accéder à davantage ressources d'entreprise à partir de multiples lieux. Pour cette raison, le périmètre réseau traditionnel s'estompe, ce qui étend la surface d'attaque, une préoccupation majeure pour les RSSI.

En réponse à ces menaces, les organisations doivent adopter une approche de méfiance en matière de sécurité : ne faire confiance à personne, ne faire confiance à aucun dispositif. Plus précisément, les RSSI doivent protéger le réseau avec une politique d'accès à vérification systématique (Zero Trust Access ou ZTA), en s'assurant que tous les utilisateurs, dispositifs et applications Web du cloud sont fiables, authentifiés et qu'ils disposent d'un niveau d'accès pertinent. Le Zero Trust est essentiel pour sécuriser l'innovation numérique, quelle que soit la nature du projet auquel il s'applique.

81 % des dirigeants d'entreprises déclarent que les employés constituent désormais le plus grand risque pour la sécurité mobile.[1]

L'évolution de la périphérie du réseau

Pour les organisations de toute taille, les initiatives d'innovation numérique favorisent la croissance. L'un des aspects de cette croissance est la prolifération de nouveaux edges (périphéries) de réseau : infrastructures privées et publiques dans le cloud, Internet des objets (IoT), appareils mobiles et sites distants bénéficiant une infrastructure IT virtualisée. Voilà qui génère un volume important de données, d'applications et de workflows. Pour gérer l'accès des utilisateurs et interconnecter une série de dispositifs provenant de différents endroits, tant sur le réseau qu'en dehors, les organisations augmentent le nombre de dispositifs déployés en périphérie de ces réseaux.

Pour les RSSI, la complexité est au rendez-vous. Ces dernières années, les edges réseau se sont démultipliés, à tel point que le périmètre traditionnel s'estompe, créant un environnement ouvert qui est idéal pour les attaques. Les cybermenaces sont de plus en plus prolifiques et s'adaptent continuellement. Dans le passé, la sécurité du périmètre était basée sur une approche de « confiance mais avec vérification ». Mais face à l'inflation des utilisateurs, dispositifs et applications sur le réseau, il est difficile de savoir à qui faire confiance. Les détournements d'identité et les malware permettent aux acteurs malveillants d'accéder à des comptes légitimes. Une fois dans la place, ces cyberdélinquants identifient facilement des moyens pour se propager rapidement au sein d'un réseau non segmenté et bénéficient d'une confiance par défaut. Une fois qu'ils accèdent à un dispositif edge, ils peuvent lancer des attaques dont l'impact est lourd : mise à l'arrêt de systèmes, vols de données, pertes financières et réputation ternie.

Pour les responsables de la sécurité, il est impossible de suivre le nombre croissant d'attaques en se contentant d'un accès réseau traditionnel. D'où une vraie évolution dans les mentalités : les évènements sur le réseau, autrefois de confiance, attisent désormais la méfiance. Avec un modèle d'accès Zero Trust, les RSSI repensent leur approche en considérant certains edges réseau comme n'étant pas de confiance, car vulnérables : utilisateurs, appareils et ressources, sur et hors du réseau.

Savoir *qui* est connecté au réseau

Les responsables de la sécurité doivent savoir à tout moment qui se trouve sur le réseau. Cependant, les entreprises courent un risque accru avec des collaborateurs qui utilisent des mots de passe faibles pour se connecter au réseau. De nombreux comptes nécessitent désormais des identifiants et ce sont, aujourd'hui, de nombreux mots de passe qui sont trop simplistes et faciles à compromettre par des attaques de phishing notamment. Il est essentiel pour les entreprises de connaître chaque utilisateur et le rôle qu'il joue dans l'entreprise. Ce n'est qu'avec cette connaissance qu'elles peuvent accorder en toute sécurité l'accès aux ressources nécessaires pour chaque rôle ou fonction, tout en fournissant un accès supplémentaire aux autres, au cas par cas.

Alors que la tendance du BYOD est bien ancrée parmi les utilisateurs, certains RSSI en négligent les dangers. La surface d'attaque élargie permet aux menaces de pénétrer plus facilement les défenses périmétriques traditionnelles et de se déplacer latéralement à l'intérieur du réseau, ce qui est l'une des raisons pour lesquelles les incidents peuvent rester inaperçus pendant longtemps. Certaines des violations les plus préjudiciables ont été commises par des utilisateurs non autorisés qui ont accédé au réseau, ou résultent de niveaux d'accès inappropriés accordés à des utilisateurs de confiance. Le BYOD devient omniprésent dans les entreprises, et 83 % des responsables de la sécurité affirment que leurs organisations doivent faire face à des menaces mobiles.[2]

Un autre défi auquel les organisations sont confrontées est la dissémination géographique des collaborateurs. Ces derniers travaillent de différents endroits : au bureau, en déplacement, au sein des filiales ou depuis leur maison. Avec autant d'utilisateurs accédant au réseau à distance, les possibilités de développement de la surface d'attaque sont beaucoup plus nombreuses. Par exemple, les travailleurs se connectent souvent via des hotspots ou des réseaux Wi-Fi publics dans les cafés, les aéroports ou les transports. Ce type de connectivité présente des risques importants pour la sécurité. Des tiers peuvent intercepter les

informations transitant entre l'utilisateur et le réseau de l'entreprise. Les assaillants peuvent exploiter des vulnérabilités logicielles non corrigées pour injecter des logiciels malveillants dans le terminal, non seulement pour accéder à des informations locales, mais aussi pour accéder au réseau de l'entreprise via ce terminal.

Ces défis sont d'autant plus importants que le télétravail a le vent en poupe depuis la pandémie de COVID-19, en 2020. La plupart des organisations qui avaient peut-être prévu que moins de 15 % de leurs effectifs seraient basés à distance ont soudain dû s'assurer qu'elles disposaient de l'infrastructure et des contrôles de sécurité adéquats pour 90 % ou plus de leurs équipes.

Ces besoins expliquent en partie pourquoi un accès Zero Trust est si important. Étant donné que les dispositifs se connectent au réseau et s'en déconnectent régulièrement, les responsables de la sécurité doivent connaître à tout moment les utilisateurs présents sur le réseau et s'assurer qu'ils disposent d'un niveau d'accès adéquat. Lorsqu'un collaborateur change de rôle, en passant des ventes à l'opérationnel par exemple, il n'a peut-être pas besoin d'accéder aux mêmes zones du réseau que dans son rôle précédent, et les équipes de sécurité doivent pouvoir effectuer une transition en douceur.

Un grand nombre des attaques les plus dommageables subies par les organisations ces dernières années a ciblé des dispositifs présents sur les edges du réseau.[3]

Savoir *ce qui* est connecté au réseau

En plus de savoir qui se trouve sur le réseau, les responsables de la sécurité doivent identifier à tout moment quels sont les appareils présents sur le réseau. Toutefois, la prolifération des appareils mobiles et des objets connectés a fragmenté le périmètre réseau traditionnel en de multiples micro-périmètres, étendant ainsi la surface d'attaque de l'entreprise. Comme chaque micro-périmètre est associé à un appareil d'utilisateur, les endpoints deviennent des cibles privilégiées pour les malware et exploits sophistiqués.

En raison de cette prolifération des endpoints et de l'élargissement de la surface d'attaque, de nombreuses organisations perdent le contrôle du réseau en ce sens qu'elles ne savent plus quels sont les appareils qui s'y connectent. En fait, il n'existe pratiquement aucune configuration normalisée pour les dispositifs personnels (BYOD) ou les objets connectés. En ce qui concerne le BYOD, les appareils mobiles font courir des risques majeurs aux réseaux. Il peut s'agir de fuites de données, de Wi-Fi non sécurisé, de spoofing sur le réseau, de phishing, de logiciels espions, de chiffrement ou d'une gestion inappropriée des sessions. Cependant, ce qui est le plus préoccupant sur la surface d'attaque des endpoint est l'explosion des objets connectés.

Les cyberattaques contre ces objets connectés sont en plein essor, car les entreprises connectent de plus en plus de ces dispositifs « intelligents ». Les acteurs malveillants exploitent ces appareils pour mener des attaques par déni de service distribué (DDoS), ainsi que de nombreuses autres actions malveillantes.

Afin de sécuriser totalement les dispositifs BYOD et IoT, les entreprises doivent connaître la localisation de chacun d'entre eux, son activité et la façon dont il se connecte aux autres appareils présents sur le réseau. Le manque de visibilité rend l'organisation vulnérable à des risques invisibles. Les responsables de la sécurité doivent être en mesure de suivre les appareils en périphérie du réseau. Pourtant, près de la moitié des professionnels de la cybersécurité déclarent ne pas avoir de plan en place pour faire face aux attaques contre les appareils IoT, même si neuf sur dix expriment des inquiétudes quant aux menaces futures.[4]

La segmentation traditionnelle des réseaux est utilisée par certaines organisations, mais il est difficile de définir des segments de réseau sécurisés qui puissent être simultanément accessibles à tous les utilisateurs et applications légitimes et totalement inaccessibles à tous les autres. Même la segmentation la plus poussée laisse des lacunes dans les défenses du réseau (des scénarios d'accès que les architectes de réseau n'ont pas envisagés) que des acteurs malveillants peuvent exploiter.

En outre, les entreprises subissent des attaques si les dispositifs contrôlés bénéficient d'une confiance par défaut. De nombreuses organisations ont été surprises par des attaques provenant de collaborateurs et de sous-traitants qui avaient auparavant leur confiance. Un appareil perdu ou volé peut révéler des mots de passe qui permettent de futures attaques sur le réseau. C'est pourquoi une approche de vérification systématique par accès Zero Trust est si importante. Alors que les cybercriminels s'efforcent de compromettre le large panel des dispositifs sur le réseau, les responsables de la sécurité ont besoin d'améliorer la visibilité et la détection de chaque appareil se connectant au réseau.

Protéger les ressources sur et hors du réseau

Un autre problème important pour les responsables de la sécurité est l'utilisation croissante d'appareils mobiles hors réseau ou sur d'autres réseaux, et qui représentent une menace lorsqu'ils se reconnectent sur le réseau corporate (malware, botnets, etc.). Par exemple, de nombreux collaborateurs utilisent leurs appareils BYOD à la fois pour leurs besoins personnels et professionnels.

Ils naviguent sur Internet, interagissent avec d'autres personnes sur les médias sociaux et reçoivent même des e-mails personnels lorsqu'ils ne sont pas connectés au réseau. Mais lorsqu'ils rejoignent le réseau après avoir été en ligne, les employés peuvent, par inadvertance, exposer leurs appareils, et les ressources de l'entreprise, à toute une série de menaces telles que les virus, les logiciels malveillants et autres exploits.

Cette utilisation à la fois personnelle et professionnelle des endpoints survient également à un moment où la plupart des organisations sont incapables de suivre le nombre d'endpoints qui entrent et sortent du réseau. Dans un récent rapport du Ponemon Institute, 63 % des entreprises ont déclaré ne pas pouvoir surveiller les endpoints hors réseau, et plus de la moitié ne peuvent pas déterminer le statut de conformité des endpoints.[5] La multiplicité des appareils connectés au réseau masque la visibilité sur l'ensemble d'entre eux. En conséquence, les RSSI et les équipes de sécurité ont du mal à gérer les nombreux risques qui en découlent.

63 % des organisations ne sont pas en mesure de surveiller les terminaux lorsqu'ils quittent le réseau de l'entreprise, et 53 % révèlent que le nombre de terminaux infectés par des logiciels malveillants a augmenté au cours des 12 derniers mois.[6]

En adoptant un framework ZTA qui identifie, segmente et surveille en permanence tous les appareils, les organisations peuvent remplacer leurs réseaux plats à haut risque pour garantir que les ressources internes restent sécurisées et que les données, les applications et les éléments de propriété intellectuelle restent protégés. Cette stratégie permet de réduire les risques résultant d'une sécurité fondée sur le périmètre réseau, renforce la visibilité et le contrôle des appareils hors réseau, et simplifie la gestion globale du réseau et de la sécurité.

Conclusion : un modèle Zero Trust s'impose

Les projets d'innovation numérique présentent de vrais avantages business. Ils mettent également à rude épreuve les RSSI, leurs équipes et leurs ressources compte tenu de l'expansion de la surface d'attaque qui en résulte, avec de nouveaux vecteurs d'attaque exploitables par les cybermenaces. Les acteurs malveillants deviennent plus sophistiqués et l'approche traditionnelle d'une sécurité qui protège la périphérie de réseau n'est plus suffisante. Selon la nature et la sophistication de la menace, il n'existe pas de point unique dans l'infrastructure de sécurité d'une organisation pour voir tous les aspects de la menace. Avec un accès ZTA, les RSSI peuvent se concentrer sur les utilisateurs et les appareils qui se connectent au réseau, en confirmant leur identité et en s'assurant qu'ils disposent du niveau d'accès et de confiance adéquat.

La surface d'attaque progresse compte tenu de la prolifération des objets connectés et des appareils intelligents qui arrivent sur le réseau. Les responsables de la sécurité n'ont souvent pas une visibilité totale sur le flot d'appareils qui accèdent au réseau, et les RSSI le savent : ce qu'ils ne peuvent pas voir pourrait bien leur nuire. Pour sécuriser totalement tous ces endpoints, les entreprises ont besoin d'une politique d'accès de type Zero Trust sur l'ensemble du réseau, qui permet de savoir où se trouve chaque endpoints, ce qu'il fait et comment il se connecte à d'autres endpoints sur le réseau, ainsi qu'une surveillance continue pour détecter toute anomalie de comportement qui pourrait indiquer une menace.

[1] "Mobile Security Index 2019," Verizon, 2019.

[2] Idem.

[3] Neil Jenkins and Natasha Cohen, "Living on the Edge," Cyber Threat Alliance, 30 avril 2019.

[4] "Only 47% of cybersecurity pros are prepared to deal with attacks on their IoT devices," Help Net Security, 8 novembre 2019.

[5] "The Cost of Insecure Endpoints," Ponemon Institute, 2020.

[6] Idem.

France
TOUR ATLANTIQUE
24ème étage, 1 place de la Pyramide
92911 Paris La Défense Cedex
France
Ventes: +33 (0) 1 80 42 05 40

www.fortinet.com/fr

août 24, 2021 12:11 PM
wp-securing-digital-innovation-A4
696181-A-0-FR