La cybersécurité des entreprises d'Alcatel-Lucent Enterprise

Brochure

Alcatel·Lucent
Enterprise

Aperçu

La cybersécurité est depuis longtemps considérée comme une priorité absolue pour les entreprises. Cependant, avec la transformation numérique en cours, les exigences en matière de cybersécurité évoluent. La transformation numérique va de pair avec une utilisation accrue des appareils connectés et mobiles au sein du réseau des entreprises, alors que les employés accèdent de plus en plus à des applications et à des données situées au-delà du périmètre du réseau.

En raison de l'accélération des changements, les anciennes méthodes de sécurité des réseaux ne suffisent plus. Ce document présente les tendances qui modifient les exigences actuelles en matière de cybersécurité des entreprises. Il recommande aussi des stratégies que les entreprises peuvent adopter ainsi que des technologies à déployer, afin d'assurer la sécurité des données et des systèmes à l'ère de la transformation numérique.

La solution de cybersécurité d'Alcatel-Lucent Enterprise répond aux exigences d'une entreprise ayant adopté le numérique. Grâce à une approche multidimensionnelle de la cybersécurité, les entreprises peuvent fournir un accès basé sur des règles, aux appareils connectés, aux données sécurisées et applications logicielles au sein de l'écosystème professionnel.

Évolution des défis

La nature des menaces de cybersécurité évolue. Les pirates informatiques utilisent l'intelligence artificielle (IA) et l'apprentissage automatique (AA) pour créer des attaques plus sophistiquées et automatisées. De nouvelles techniques d'ingénierie sociale permettent aux criminels de relier des miettes d'informations extraites sur les réseaux sociaux pour créer des profils de personnes ou de données détenues par des organisations.

La transformation numérique des entreprises impacte également les exigences en matière de cybersécurité, ce qui se traduit par une plus grande complexité, une utilisation accrue d'appareils connectés, un périmètre qui s'estompe, et tout cela à un rythme accéléré.

Plus d'appareils, plus de complexité

Les entreprises adoptent de nouvelles technologies, notamment le cloud, la téléphonie mobile, l'IoT, le Big Data et l'analyse avancée. Ces nouvelles solutions font naître une complexité différente qui exige un nouveau regard sur la sécurité. En outre, le nombre d'appareils connectés augmente, tout comme les vulnérabilités et les possibilités de violation.

Par exemple, dans de nombreux cas, la première génération d'appareils connectés n'exigeaient aucun mot de passe. Les appareils étant connectés au réseau, les pirates pouvaient s'en servir comme passerelle vers le réseau. Aujourd'hui, des fonctions de sécurité tels que les mots de passe codés en dur sont souvent imposés dans les appareils. Cependant, les failles de sécurité restent inévitables et, lorsqu'elles se produisent, les pirates peuvent toujours accéder au réseau.

La disparition du périmètre

La plupart des entreprises ont depuis longtemps clairement délimité les utilisateurs et les ressources situés à l'intérieur et à l'extérieur du réseau. Toutefois, à mesure que les entreprises accélèrent leur transformation numérique, elles s'ouvrent davantage aux échanges avec l'écosystème au sens large, y compris les autres partenaires et fournisseurs dans un environnement collaboratif intégré. Les utilisateurs ne se contentent plus d'accéder aux ressources depuis le périmètre réseau, ils peuvent le faire de n'importe où. Échanger des informations avec des contacts situés sur un autre réseau devient possible. Les ressources informatiques ne sont également plus confinées au sein du périmètre de l'entreprise. Elles peuvent se trouver sur site et dans le cloud, et être connectées à l'aide d'API. Les entreprises ont besoin de moyens modernes pour protéger les ressources lorsque le périmètre a disparu.

Macro et micro-segmentation dans un monde de confiance zéro

Il existe deux types de segmentation : la macro et la micro. Dans la macro-segmentation, le réseau physique est divisé en différents segments logiques. Toutes les entreprises utilisent la segmentation, mais pas toujours pour des raisons de sécurité. La macro-segmentation est souvent utilisée pour des raisons administratives, structurelles ou d'évolutivité. Ces segments peuvent être un VLAN, une combinaison de VLAN + VRF (Virtual Routing and Forwarding) ainsi qu'un VPN lorsqu'on parle de Shortest Path Bridging, de MPLS, ou même de tunnels VXLAN ou GRE. Le trafic entre les utilisateurs ou les appareils sur différents segments est contrôlé par un pare-feu physique. Si deux appareils sont affectés à des VLAN différents et qu'ils peuvent communiquer sans passer par un pare-feu, ils se trouvent sur le même macro-segment. Par exemple, les caméras et les serrures de porte peuvent être contrôlées par le groupe de sécurité d'accès, alors que les thermostats peuvent être contrôlés par le groupe de maintenance des bâtiments.

La micro-segmentation va encore plus loin. Les utilisateurs ne sont pas tous identiques et ils n'ont pas tous un besoin légitime d'accéder à l'ensemble des ressources. Le même profil qui associe les utilisateurs à un segment comprend également un ensemble de règles qui ajoutent un contrôle granulaire sur les privilèges des utilisateurs/appareils différents pour des rôles distincts tels que les RH ou la finance. C'est ce que l'on appelle l'« accès basé sur les rôles », qui est directement lié au « principe du moindre privilège ». Ainsi, même si les caméras et les serrures de porte se trouvent sur le même segment, elles n'ont pas besoin d'utiliser les mêmes ressources. La caméra doit communiquer avec l'enregistreur vidéo et la serrure de porte avec son serveur. Tout comme une caméra n'a pas à communiquer avec une serrure de porte, deux serrures de porte n'ont pas besoin de communiquer entre elles. Ces autorisations granulaires sont mises en œuvre par le biais de règles qui font partie du profil et sont appliquées dynamiquement à l'appareil après authentification.

La question est de savoir si nous avons vraiment besoin des deux. Le problème avec une approche par macro-segmentation uniquement est que le pare-feu devient un goulot d'étranglement car tous les VLAN doivent être terminés au niveau du pare-feu, générant alors des problèmes de performance. Une autre solution consiste à déployer davantage de pare-feu au niveau de la couche de distribution. Toutefois, cette solution pourrait se révéler assez coûteuse et pas toujours satisfaisante en matière de performance. En outre, un plus grand nombre de pare-feu signifie qu'il y a plusieurs points d'application des règles, ces dernières devant alors être mises à jour à plusieurs endroits.

La micro-segmentation seule peut également être problématique. Si l'application des règles se fait par le biais de politiques de contrôle d'accès au réseau (NAC), les listes de politiques deviennent longues et complexes, et peuvent épuiser les limites de capacité de l'appareil. Trouver le juste équilibre entre ces deux types de segmentation permet au pare-feu de contrôler le trafic entre les différents segments (verticaux), et aux politiques NAC de contrôler le trafic au sein d'un segment donné (latéral). La combinaison de la macro et de la micro-segmentation permettrait d'agir sur les menaces de sécurité qui débordent d'un segment de sécurité à un autre, ainsi que sur celles qui se déplacent latéralement à travers le même segment.

Quant à l'approche de la sécurité des réseaux fondée sur la confiance zéro, le principe directeur est le suivant : « agir comme si les attaquants étaient déjà présents ». Cela signifie que toutes les connexions doivent être authentifiées. Aucun actif et aucun utilisateur n'est entièrement fiable. Qu'ils se trouvent sur site ou hors site, ils subissent les mêmes contrôles. On ne peut faire confiance aux utilisateurs internes. Chaque accès est authentifié.

Dans l'approche traditionnelle de la sécurité, le réseau est considéré comme une forteresse construite autour de l'entreprise. La forteresse représente le pare-feu, si bien que tout ce qui se trouve à l'extérieur n'est pas fiable et est minutieusement contrôlé, tandis que tout ce qui se trouve à l'intérieur est implicitement digne de confiance et autorisé. Cependant, la micro-segmentation, et plus précisément la micro-segmentation définie par logiciel, va encore plus loin. Outre la forteresse et la sécurité autour du bâtiment, des protections de sécurité demandent également une authentification. Cette frontière de confiance est floue, distribuée et mobile. Elle n'est pas liée à un emplacement, un port de commutation ou un VLAN particulier. Elle dépend de l'identité, de l'appareil, de la situation et du moment de la journée. Elle est définie par logiciel et s'adapte à tout moment. L'élément clé de cette approche est que les composants sont gérés et qu'ils doivent pouvoir réagir et se reconfigurer si nécessaire afin de répondre aux menaces ou aux changements dans le flux de travail.

Une solution pour l'entreprise en constante évolution

Alcatel-Lucent Enterprise fournit une approche multidimensionnelle de la cybersécurité des entreprises qui permet de sécuriser en profondeur les appareils connectés et les applications grâce à de multiples couches de sécurité.

Connectivité flexible

Notre stratégie commence par un réseau autonome flexible qui permet de configurer rapidement et aisément les politiques en matière de réseau et de cybersécurité pour le nombre important d'utilisateurs, d'appareils connectés et d'applications qui alimentent la transformation numérique.

Dans le passé, l'informatique consistait à réparer ce qui ne fonctionnait pas. Le service informatique installait les nouveaux équipements, les mettait en œuvre et gérait le réseau à l'aide de processus manuels fastidieux. La solution Digital Age Network d'Alcatel-Lucent Enterprise offre un réseau intelligent et automatisé qui facilite la connexion sécurisée des utilisateurs et des appareils à leurs applications spécifiques. Construit à l'aide de la technologie Intelligent Fabric (iFab) d'ALE, Digital Age Networking combine iFab avec la norme industrielle Shortest Path Bridging (SPB). Ensemble, ces technologies permettent de simplifier la création et la configuration des réseaux tout en permettant le routage rapide à trajets multiples et l'agrégation de liens afin de combiner plusieurs connexions réseau en parallèle pour accroître le débit et assurer la redondance.

Avec la stratégie d'ALE, le service IT définit les services, l'architecture, les politiques d'accès et les conteneurs du réseau, permettant ainsi au réseau de se construire automatiquement. Une fois l'architecture du réseau établie, en cas de déplacement, de modification ou d'ajout d'un élément, le réseau procède automatiquement aux ajustements nécessaires et ce, de manière indétectable. Par exemple, si un commutateur est mis hors service, le réseau est automatiquement redirigé autour de ce commutateur.

En utilisant un réseau autonome, les entreprises bénéficient d'une automatisation qui permet de réduire les erreurs de configuration manuelle et de les aider à suivre l'accélération du rythme des changements au sein de leur organisations. En raison de la suppression du travail manuel par l'automatisation, le service IT devient le moteur d'une entreprise.

Contrôle des accès à l'aide de politiques intelligentes et automatisées

Les entreprises peuvent s'appuyer sur le Digital Age Networking pour définir les règles et les politiques d'accès des utilisateurs qui régissent les applications qu'il peuvent utiliser et les appareils auxquels ils peuvent accéder – et ainsi suivre l'ensemble des déplacements des utilisateurs. Par exemple, elles peuvent mettre en place des politiques leur permettant d'accéder à des :

- Systèmes spécifiques
- Services Internet
- Autres partenaires sur une politique basée sur les entrepreneurs

ALE offre également des services de localisation, tels que le guidage et la géonotification au sein des bâtiments, le suivi des équipements et des personnes, destinés à aider les entreprises à mettre en place des politiques qui tiennent compte de la localisation des utilisateurs.

Chaque fois qu'un utilisateur se connecte, le gestionnaire UPAM (Unified Policy Access Management) applique automatiquement les politiques adaptées, afin de garantir qu'il ne dispose que des privilèges d'accès autorisés. Après s'être connecté au réseau à l'aide d'un dispositif et une fois ses identifiants validés, l'utilisateur n'a plus besoin de s'authentifier à nouveau. Il reste connecté si l'appareil est allumé, et le système applique alors automatiquement la politique pour cet utilisateur.

Les politiques permettent de garantir que tous les utilisateurs, situés tant à l'intérieur qu'à l'extérieur de l'organisation, n'ont accès qu'aux zones autorisées et que les contrôles d'accès sont appliqués de manière cohérente. Elles simplifient également les flux de travail des entreprises tout en veillant à l'application de la cybersécurité. Les utilisateurs peuvent accéder rapidement aux systèmes et aux informations dont ils ont besoin, sans avoir à suivre de lourdes procédures de connexion de sécurité.

Réduire la vulnérabilité des appareils

Les entreprises se connectent à de nombreux appareils IoT. La solution Digital Age Networking d'Alcatel-Lucent Enterprise permet aux organisations de placer chaque appareil dans un conteneur, créant ainsi un segment de réseau virtuel pour celui-ci afin d'empêcher qu'un appareil ne devienne un point d'attaque. La conteneurisation au sein du Digital Age Networking permet de simplifier la création par le service informatique de plusieurs réseaux virtuels à partir d'un seul réseau physique, lequel est géré par un système de gestion unique. Cette solution détecte automatiquement chaque appareil existant sur le réseau. Lorsqu'un appareil est connecté au réseau, Alcatel-Lucent OmniVista® Network Management System, accessible sur site ou dans le cloud, tente de l'identifier. S'il ne figure pas dans la base de données du système de gestion, ce dernier consultera une base de données située dans le cloud qui contient plus de 29 millions d'appareils.

Une fois l'appareil identifié, le système le classera, par exemple, comme une caméra de sécurité. S'il figure sur la liste des fournisseurs agréés de caméras de sécurité, il sera connecté au réseau. Sinon, sa connexion ne sera pas autorisée. La solution est ensuite installée dans un conteneur virtuel pour l'appareil, le segmentant du reste du réseau. Si quelqu'un pirate un appareil en réseau, il ne pourra pas s'en servir pour accéder au reste du réseau.

L'intelligence artificielle pour un environnement de confiance

Une fois que les appareils sont connectés, ils doivent être surveillés en permanence afin d'identifier toute menace et de maintenir la confiance. L'analyse d'ALE et la visibilité des applications permettent aux administrateurs réseau de voir ce qui se passe au sein du réseau, appareil par appareil. L'analyse identifie les modèles de comportement normal et attendu du réseau, ainsi que toute tendance inhabituelle lorsqu'elle se produit. Le comportement des applications en périphérie du réseau peut être surveillé afin de décider si l'on peut s'y connecter ou non, ainsi que le comportement inhabituel des applications autorisées, comme une caméra vidéo qui produit un plus grand nombre de données qu'elle ne le devrait.

Cette analyse permettra de signaler une anomalie ou un comportement inhabituel sur l'appareil au responsable de la sécurité du réseau afin qu'il puisse intervenir. Aujourd'hui, la recherche doit être effectuée manuellement, mais ALE œuvre à automatiser la réponse à l'aide de l'IA et de l'AA.

Sécuriser le réseau

Si les organisations sont aujourd'hui conscientes de la nécessité de sécuriser les objets connectés sur le réseau, elles peuvent omettre de prendre en compte ceux qui constituent la base du réseau, tels que les commutateurs et les points d'accès. Alcatel-Lucent Enterprise a recours à de nombreuses technologies destinées à réduire la menace de ces appareils. Solutions d'Alcatel-Lucent Enterprise :

- Renforcer le logiciel du système d'exploitation afin de fournir un code sécurisé et diversifié
- Envoyer le logiciel du système d'exploitation pour vérification et validation par un tiers afin de s'assurer qu'il ne comporte pas de points d'entrée faciles ou de portes dérobées
- Vérifier qu'à chaque mise en service d'un commutateur, la mémoire est compilée et affichée d'une manière différente. Bien que les commutateurs fonctionnent de manière identique, il n'existe pas deux configurations de mémoire semblables en interne. Si une personne réussissait à pénétrer dans un commutateur ALE, elle ne pourrait accéder à aucun autre commutateur en procédant de la même manière
- Fournir une protection intégrée contre le déni de service (DoS). Le processeur peut détecter toute augmentation inhabituelle du trafic réseau et s'arrêter automatiquement si nécessaire
- Plusieurs certifications de sécurité telles que JDIC et FIPS
- Effectuer des mises à niveau logicielles en continu

Sécuriser les connexions pour le trafic entrant et sortant

Pour le trafic entrant, nos capacités VPN fournissent une connexion chiffrée au réseau local, alors que le trafic de bout en bout est protégé par le chiffrement MACsec (également connu sous le nom d'IEEE 802.1AE) afin de protéger les informations lorsqu'elles traversent le réseau. En outre, le rechargement des services tels que TLS et HTTPS n'exigeant aucun redémarrage, le réseau n'est pas interrompu.

Reporting

Les rapports d'ALE permettent à différents profils d'accéder aux informations sur l'état, l'intégrité et les performances du réseau, le fonctionnement des applications et la satisfaction des utilisateurs. Par exemple, le service IT peut consulter les données sur les performances et le fonctionnement du réseau.

Les unités opérationnelles peuvent faire en sorte que les équipements tels que les capteurs ou les systèmes de télémétrie transmettent les données aux serveurs et aux tablettes de façon transparente. Le service informatique peut déterminer si le réseau fournit des services permettant aux employés de consacrer plus de temps à leur travail et s'ils bénéficient du réseau dont ils ont besoin.

La cybersécurité dans les secteurs

Secteur de l'éducation

À mesure que les établissements d'enseignement adopteront des stratégies de campus intelligents, davantage d'appareils connectés et mobiles seront ajoutés à leurs réseaux, et les objets connectés accéderont de plus en plus aux applications et aux données depuis l'extérieur du périmètre du réseau.

Lorsque la connectivité et l'innovation sont mises en œuvre dans les grandes infrastructures de campus, celles-ci deviennent immédiatement vulnérables aux cyber-menaces. La solution Digital Age Networking pour les campus intelligents d'Alcatel-Lucent Enterprise permet de sécuriser les équipements informatiques et les données à l'ère de la transformation numérique d'aujourd'hui. Grâce à cette solution, les établissements peuvent gérer étroitement l'accès des utilisateurs, réduire les vulnérabilités créées par les appareils IoT, mobiles et réseau, empêcher l'inévitable brèche de fournir un point d'attaque, tout en proposant les services et applications dont vos étudiants et votre personnel ont besoin.

Secteur des transports

Les progrès des systèmes de transport résultant des innovations technologiques nécessiteront la transformation de la base existante sur laquelle ils sont construits. L'intégration des appareils et des systèmes qui permettent à tout écosystème de transport de fonctionner exige des connexions rapides, fiables et sécurisées. Les réseaux de données de transport doivent être compatibles avec les objets connectés pour connecter ensemble les capteurs, les caméras, les systèmes de signalisation et de contrôle du trafic, et ce de manière transparente. La sécurité du réseau est également d'une importance capitale pour protéger les données et l'intégrité du réseau.

ALE utilise un code diversifié et sécurisé pour améliorer l'intégrité du réseau et fournir une sécurité supplémentaire contre les cyber-attaques du réseau. Le code sécurisé et diversifié protège les réseaux de toute vulnérabilité intrinsèque, des exploitations de code, des programmes malveillants et des éventuelles portes dérobées pouvant compromettre les opérations critiques pour l'entreprise. ALE propose également l'identification des empreintes digitales pour les objets connectés afin d'identifier chaque appareil, notamment les véhicules, les capteurs et les caméras, pour s'assurer qu'ils ne constituent pas une menace pour la sécurité du réseau. La stratégie de sécurité approfondie d'ALE a reçu les plus hauts niveaux de certification de la part d'organismes gouvernementaux, y compris les critères communs (EAL2 et NDcPP), le JITC, FIPS 140-2 et le NIST.

Secteur de la santé

La santé constitue depuis longtemps l'un des secteurs les plus ciblés par les pirates informatiques, et ce problème ne cesse de s'aggraver. Ainsi, en 2018, le secteur de la santé a vu 15 millions de dossiers de patients compromis en lien avec 503 failles de sécurité, soit trois fois plus qu'en 2017, selon le baromètre Protenus Breach.[1]

Les violations se produisent en raison du caractère extrêmement précieux des données de santé. Les dossiers médicaux des patients contiennent toutes leurs données personnelles, notamment leurs noms, leurs adresses actuelle et antérieures, leurs antécédents professionnels, le nom et l'âge de leurs proches, ainsi que des informations financières telles que leurs numéros de cartes de crédit et coordonnées bancaires.[2]

La solution Digital Age Networking d'ALE fournit une approche multidimensionnelle de la cybersécurité qui permet de maintenir la confiance par le biais d'un accès sécurisé basé sur des politiques aux dispositifs médicaux connectés, aux données des patients et aux applications logicielles dans tout l'écosystème de santé.

Secteur public

Le rôle accru du numérique tant au niveau du gouvernement central que des villes a brouillé la barrière protégeant les actifs numériques qui prennent en charge le transport, la maintenance des infrastructures et la surveillance de l'environnement. Les politiques gouvernementales en matière de cybersécurité pour la sécurité des données, la vulnérabilité et la gestion de la confiance doivent être révisées.

L'approche d'ALE de la cybersécurité fournit une approche de la sécurité de bout en bout, centrée sur les services, afin de protéger toutes les couches du service, du réseau au logiciel. En ce qui concerne les appareils, les administrations publiques peuvent utiliser la conteneurisation pour créer un segment de réseau virtuel afin d'éviter que les dispositifs ne deviennent un point d'attaque.

Secteur de l'hôtellerie

La croissance des objets connectés dans l'industrie hôtelière entraîne une explosion des menaces de cybersécurité, car la prolifération des capteurs et des appareils connectés élargit considérablement la surface d'attaque du réseau. L'IoT est particulièrement vulnérable car de nombreux appareils IoT sont fabriqués sans prendre en compte la sécurité, ou construits par des entreprises qui ne comprennent pas les exigences actuelles en matière de sécurité. Par conséquent, les systèmes des objets connectés constituent de plus en plus le maillon faible de la sécurité des réseaux des entreprises dans l'hôtellerie.

La protection du trafic et des appareils IoT nécessite une approche stratégique qui tire parti de multiples garanties de sécurité. Afin d'aider les hôtels, les casinos, les stations balnéaires et les autres entreprises du secteur de l'hôtellerie à profiter des avantages et à atténuer les risques liés au déploiement de l'IoT, ALE propose une stratégie de sécurité à plusieurs niveaux qui assure une protection à chaque couche de l'infrastructure, de l'utilisateur et de l'appareil individuel à la couche réseau. Elle fournit également une stratégie de conteneurisation des objets connectés destinée à simplifier et à sécuriser l'intégration des appareils et à fournir les bonnes ressources réseau pour faire fonctionner le système correctement et efficacement, le tout dans un environnement sécurisé de façon à protéger les entreprises du secteur de l'hôtellerie contre les cyberattaques.

1 https://healthitsecurity.com/news/the-10-biggesthealthcare-data-breaches-of-2019-so-far

2 https://www.forbes.com/sites/mariyayao/2017/04/14/your-electronic-medical-records-can-be-worth-1000-tohackers/#2bb1f96b50cf

Résumé

La transformation numérique a profondément modifié les exigences de cybersécurité des entreprises en raison de l'augmentation du nombre d'appareils connectés, la disparition du périmètre réseau et l'accélération continue des changements. La solution Digital Age Networking d'Alcatel-Lucent Enterprise permet de sécuriser vos équipements informatiques et données à l'ère de la transformation numérique d'aujourd'hui. Grâce à cette solution, vous pouvez gérer étroitement l'accès des utilisateurs, réduire les vulnérabilités créées par les appareils IoT, mobiles et réseau, empêcher l'inévitable brèche de fournir un point d'attaque et fournir un écosystème professionnel de confiance.

www.al-enterprise.com/fr-fr Le nom et le logo d'Alcatel-Lucent sont des marques commerciales de Nokia utilisées sous licence par ALE. Pour en savoir plus sur les marques utilisées par les sociétés affiliées de la Holding ALE, veuillez consulter le site www.al-enterprise.com/fr-fr/legal/trademarks-copyright. Toutes les autres marques déposées appartiennent à leurs propriétaires respectifs. Les informations présentées peuvent faire l'objet de modifications sans préavis. ALE Holding et ses sociétés affiliées ne sauraient être tenues responsables d'inexactitudes éventuelles dans les informations contenues dans le présent document. © Copyright 2021 ALE International, ALE USA Inc. Tous droits réservés dans tous les pays.
DID21071901FR (Septembre 2021)