La cybersécurité pour un enseignement et un apprentissage exceptionnels

Livre blanc

Alcatel·Lucent Enterprise

Sommaire

- Un secteur dans la tourmente
- Sortir des sentiers battus
- De la situation actuelle au Zero Trust
- Plus que la somme de ses composants
- Récolter les fruits de son travail
- Un partenaire expert pour une sécurité experte

Un secteur dans la tourmente

Ces dernières années, le nombre des cyberattaques et leur sophistication visant les établissements universitaires du monde entier ont augmenté à un rythme alarmant. Certains rapports ont déclaré que le secteur de l'éducation traversait une crise cybernétique, notant que le récent passage à l'apprentissage virtuel basé sur le cloud avait permis aux pirates d'exploiter de nouvelles opportunités de piratage.[1]

Malheureusement, ce type d'affirmations audacieuses repose sur des statistiques réelles. Entre août et septembre 2021, les établissements universitaires ont été la cible de plus de 5,8 millions d'attaques de logiciels malveillants dans le monde, soit 63 % de l'ensemble des attaques de ce type.[2] Les données publiées en 2022 confirment que les secteurs de l'éducation et de la recherche restent les plus ciblés. Le rapport identifie l'Australie/Nouvelle-Zélande comme la région la plus attaquée, suivie de l'Asie et de l'Europe, l'Amérique latine connaissant la plus forte augmentation des cyberattaques hebdomadaires.[3]

Les cyberattaques contre les établissements universitaires sont devenues si fréquentes qu'en 2022, plusieurs agences américaines, dont le FBI et la Cybersecurity and Infrastructure Security Agency (CISA ou l'Agence de cybersécurité et de sécurité des infrastructures), ont uni leurs forces pour publier un avis mettant en garde ces établissements contre les attaques avec demande de rançon (ransomware) dont ils sont la cible de manière disproportionnée.[4]

L'augmentation de la portée et de l'ampleur des cyberattaques, et en particulier les attaques par ransomware, ont de graves répercussions sur les institutions à l'échelle mondiale. Les étudiants et les professeurs perdent des informations et un temps précieux en classe, mettant ainsi en péril les objectifs éducatifs.

Considérez les points suivants :

- Une attaque par ransomware contre le Los Angeles Unified School District (LAUSD) en septembre 2022 a provoqué un arrêt sans précédent des systèmes informatiques qui a conduit à des perturbations continues du courrier électronique, des systèmes informatiques et des applications.[5]
- En 2021, une cyberattaque au Royaume-Uni a interrompu les communications par courrier électronique, téléphone et site web dans 15 écoles, provoquant l'arrêt de l'apprentissage en ligne.[6]
- Une cyberattaque à grande échelle menée en 2021 contre l'Universidad El Bosque à Bogotá, en Colombie, a compromis les plateformes institutionnelles, pédagogiques et financières pendant trois jours.[7]

Les cyberattaques portent également atteinte à la réputation et à la confiance des institutions, ce qui peut réduire le nombre d'inscriptions et entraîner une perte de revenus. En mai 2022, le Lincoln College de l'Illinois a dû fermer définitivement ses portes, 157 ans après sa création, à la suite d'une attaque avec demande de rançon qui avait créé un défi financier débilitant.[8]

1 America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, mai 2022.
2 America's Schools Face Mounting Threats from Cyberattacks. RealClear Education, mai 2022.
3 Education sector seeing highest volumes of cyber attacks. SecurityBrief New Zealand, août 2022.
4 Alert AA22-249A: #StopRansomware: Vice Society. Cybersecurity & Infrastructure Security Agency, septembre 2022.
5 Los Angeles school district warns of disruption as it battles ongoing ransomware attack. TechCrunch+, septembre 2022.
6 Cyberattack shuts down online learning at 15 UK schools. zdnet.com, mars 2021.
7 The Universidad El Bosque has regained control of its digital platforms. NewsBeezer.com, juillet 2021.
8 Ransomware attack shutters 157-year-old Lincoln College. CBS News, mai 2022.

Sortir des sentiers battus

Malheureusement, les cyberattaques visant les établissements universitaires se produisent même lorsque les approches traditionnelles de la cybersécurité sont en place. En 2019, le Centre national de cybersécurité du Royaume-Uni a constaté que 83 % des 432 écoles analysées avaient été touchées par au moins un événement de cybersécurité, bien que 98 % d'entre elles aient installé des solutions antivirus et 99 % disposaient d'un pare-feu.

Pour prévenir plus efficacement les cyberattaques, les établissements universitaires doivent se détourner des approches traditionnelles de la cybersécurité. Si des approches telles que la sécurité approfondie du modèle du « château entouré de douves » étaient efficaces à une époque plus simple, aujourd'hui elles n'offrent plus une protection adéquate. À une époque où Internet et les appareils portables dominent, la limite du réseau - et le potentiel d'accès non autorisé au réseau - peut désormais s'étendre bien au-delà du périmètre physique du campus.

Aucun utilisateur, aucun appareil ou aucune application ne doit faire l'objet d'une confiance implicite.

La seule stratégie de cybersécurité réseau capable de contrer efficacement les menaces actuelles est celle qui ne fait confiance à aucun utilisateur, appareil ou application, quelle que soit sa localisation - sur le campus, dans le cloud ou à l'extérieur du campus. Cette stratégie, connue sous le nom de Accès réseau Zero Trust (Zero Trust Network Access - ZTNA), repose sur cinq affirmations clés :

- Le réseau est hostile
- Les menaces externes et internes sont omniprésentes
- La localisation ne suffit pas à déterminer la confiance
- Chaque appareil, chaque utilisateur et chaque flux de réseau doit être authentifié et autorisé
- Les politiques doivent être dynamiques et utiliser autant de sources de données que possible

En adoptant la bonne approche pour mettre en œuvre la sécurité ZTNA, les institutions peuvent continuer à se concentrer sur l'enseignement et l'apprentissage, plutôt que sur les technologies et les menaces.

De la situation actuelle au Zero Trust

Alors que les institutions développent leur stratégie de cybersécurité ZTNA, il est important de se rappeler que l'évolution vers le Zero Trust est un parcours. Celui-ci ne s'effectue pas du jour au lendemain. Il n'existe pas de solution ou d'ensemble de solutions de confiance zéro qu'il suffit d'acheter et de mettre en œuvre. La mise en place d'un environnement Zero Trust pour toutes les technologies prend du temps.

Il est également essentiel que les établissements universitaires développent et maintiennent une approche équilibrée de la cybersécurité. Si les mécanismes de sécurité mis en œuvre sont trop rigides ou trop restrictifs, les personnes chercheront à contourner les procédures mêmes qui sont censées protéger leurs appareils, données et applications. Les utilisateurs seront tentés d'ajouter leurs propres points d'accès, appareils et applications non autorisés afin d'éviter les longs contrôles de cybersécurité et les mises à jour logicielles et ce, afin d'accomplir leurs tâches plus rapidement. Il s'agit d'une tactique connue sous le nom de « shadow IT » (IT fantôme), qui présente de nombreux risques en matière de cybersécurité.

En outre, chaque institution devra identifier et examiner les réglementations en matière de protection de la vie privée qui doivent être respectées pour les données qui circulent sur le réseau, ainsi que les listes de contrôle d'accès (ACL) et les politiques de pare-feu pour les données stockées dans le cloud.

Lors de l'examen des exigences réglementaires, il est important de tenir compte des réglementations nationales et internationales en matière de protection de la vie privée. Par exemple, aux États-Unis, les établissements universitaires doivent se conformer à la Health Insurance Portability and Accountability Act (FERPA) (loi relative à la santé et l'assurance maladie) et au Health Insurance Portability and Accountability Act (HIPAA). Mais ils doivent aussi se rappeler que le règlement général sur la protection des données (RGPD) de l'Union européenne (UE) s'applique à tous les établissements qui accueillent des étudiants de l'UE, quel que soit leur localisation.

Connaître les cyber-risques et les exigences réglementaires

Avant de commencer à élaborer une stratégie ZTNA, il convient de procéder à une évaluation approfondie des risques auxquels l'institution est confrontée aujourd'hui et d'en évaluer la gravité. Lors de la préparation de l'évaluation des risques, veillez à éviter les pièges les plus courants suivants :

- Les appareils IoT qui ne sont pas gérés par les services informatiques. Souvent, ces appareils pirates ne respectent pas les politiques de sécurité, utilisent des microprogrammes obsolètes et ne disposent pas de protection antivirus, augmentant ainsi les possibilités d'utilisation par un acteur malveillant en tant que point d'entrée pour une attaque.
- Les équipements et les appareils personnels non autorisés qui accèdent au réseau. Ces dispositifs informatiques fantômes pourraient utiliser n'importe quel logiciel et être déjà infectés par des virus et des logiciels malveillants prêts à attaquer le réseau.
- Les politiques de sécurité incohérentes. Ces incohérences introduisent des faiblesses dans la protection du réseau qui peut être ciblé par des parties non fiables.
- Les réseaux avec une segmentation statique de la sécurité et confiance implicite. Ces approches traditionnelles de la cybersécurité permettent aux utilisateurs, appareils et applications initialement fiables d'attaquer le réseau sans qu'aucune autre vérification ne soit effectuée pour s'assurer qu'ils sont toujours fiables. Elles supposent également que les cyberattaques ne peuvent provenir de l'intérieur, ce qui n'est pas le cas.

Une méthodologie en cinq étapes pour la cybersécurité ZTNA

Les cinq étapes suivantes sont essentielles à l'élaboration d'une stratégie de cybersécurité ZTNA. Elles permettent de garantir que le réseau dispose d'un ensemble complet de mécanismes de protection afin d'empêcher les utilisateurs, les appareils et les applications non autorisés d'accéder au réseau.

- **Étape 1 : surveiller.** Surveillez le réseau en direct afin de dresser un inventaire de tous les dispositifs et applications - autorisés ou non - qui demandent ou fournissent des informations sur le réseau, ainsi que les protocoles qu'ils utilisent pour y parvenir. Il existe de nombreux outils qui permettent de collecter ces informations sur le réseau et de créer un rapport d'inventaire classant les appareils par type, fabricant, modèle, système d'exploitation et autres facteurs. Il existe également des outils de surveillance des flux qui identifient les différents flux de trafic des applications sur le réseau.
- **Étape 2 : évaluer et valider votre inventaire.** Commencez par évaluer les appareils et les applications en fonction de leur type et de leur rôle. Par exemple, l'appareil ou l'application est-il utilisé à des fins éducatives ou IoT ? Est-il lié à des objectifs professionnels, sociaux, pédagogiques ou de recherche ? Contribue-t-il à améliorer l'efficacité, la sûreté, la sécurité ou la protection de la vie privée ? Doit-il répondre à des exigences réglementaires ? Ce processus permet d'identifier les dispositifs informatiques fantômes pouvant être éliminés afin de réduire immédiatement la surface d'attaque.
- **Étape 3 : planifier votre approche de l'authentification, de l'audit des autorisations et de l'administration.** Pour obtenir les meilleurs résultats, élaborez un plan multidimensionnel comprenant une macro-segmentation et une micro-segmentation. La macro-segmentation utilise des réseaux locaux virtuels (VLAN), le routage et le transfert virtuels (VRF), les réseaux privés virtuels (VPN) et d'autres approches pour séparer les utilisateurs, les appareils et les applications sur le réseau. La micro-segmentation définit la manière dont ces utilisateurs, appareils et applications sont associés à leur segment de réseau et à leurs politiques de sécurité.
- **Étape 4 :** testez et validez l'approche développée à l'étape 3, puis utilisez les informations obtenues pour affiner les politiques de sécurité et vous assurer qu'elles couvrent tous les scénarios. Au cours de cette phase, il est important de tester tous les aspects de l'approche. Par exemple, assurez-vous que les simulations incluent l'émission de certificats, la configuration de politique et de scénarios de quarantaine, la simulation de flux de journaux et les tests d'intégrations de pare-feu.
- **Étape 5 : appliquer.** Une fois que les politiques de sécurité sont complètes et affinées, elles peuvent être appliquées à la périphérie du réseau, là où les utilisateurs, les appareils et les applications tentent d'y accéder. Lorsque des politiques de sécurité testées et validées sont appliquées, les appareils non autorisés ne peuvent plus accéder au réseau et les flux inattendus sont éliminés. En outre, les appareils peuvent être mis en quarantaine et les équipes informatiques alertées de la situation. Ces mécanismes fonctionnent comme une série de points de contrôle qui empêchent les conducteurs dangereux de s'engager sur une autoroute.

Si ce processus en cinq étapes aide les institutions à évoluer vers la cybersécurité ZTNA, il n'est pas suffisant à lui seul. Pour réussir, toute stratégie de cybersécurité ZTNA doit s'accompagner d'une approche globale de la formation, de la gestion des correctifs et d'une gestion rigoureuse de l'informatique fantôme.

Plus que la somme de ses composants

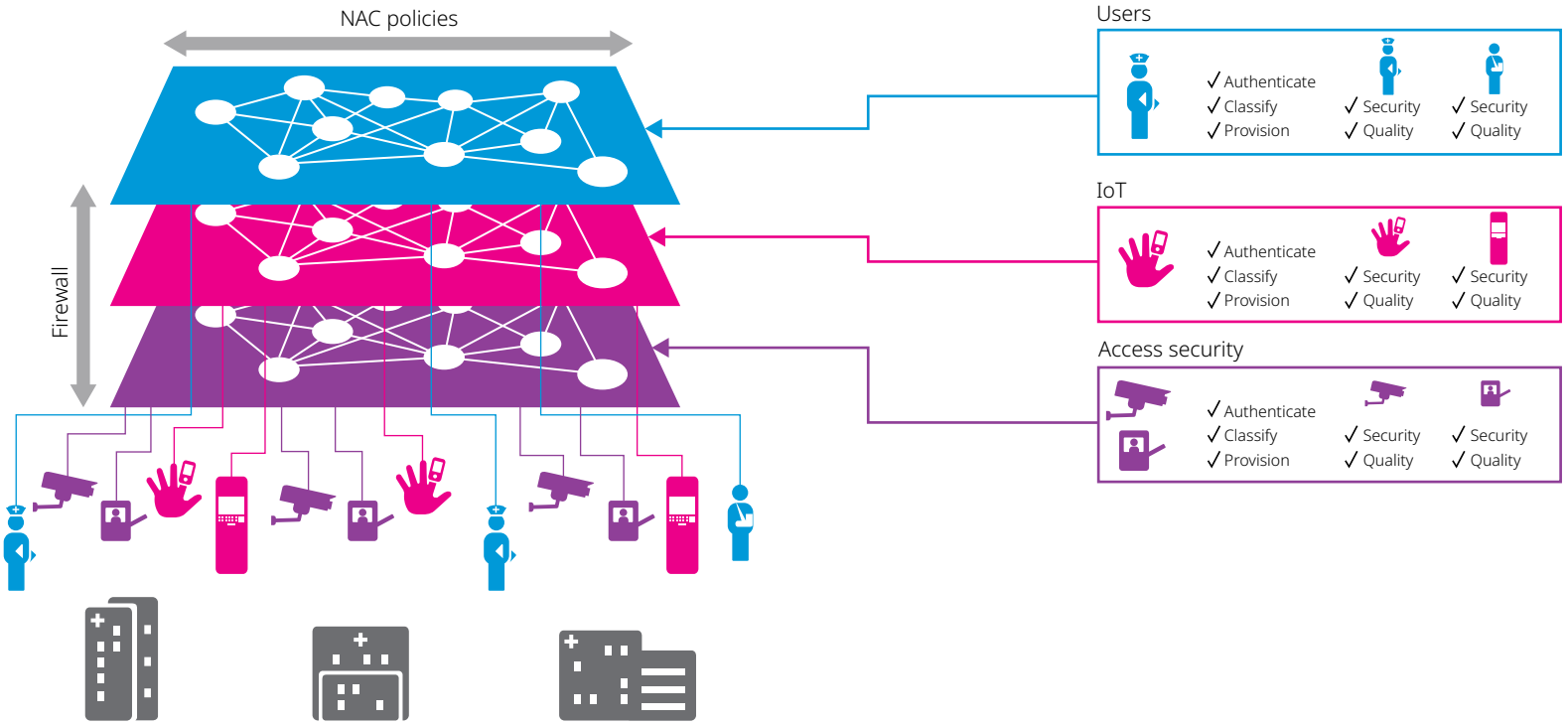
La mise en place d'une approche progressive de la cybersécurité ZTNA permet aux établissements universitaires d'obtenir des avantages importants dans tous les aspects de leurs activités. Si les avantages les plus évidents sont liés à la prévention et à la détection des accès non autorisés au réseau, il existe également de nombreux avantages éducatifs et commerciaux.

Protection étendue

D'un point de vue technologique, les listes complètes de contrôle d'accès au réseau et le contrôle d'accès basé sur les rôles permettent d'authentifier chaque connexion et d'attribuer des autorisations à chaque utilisateur et à chaque appareil accédant au réseau. Les institutions bénéficient ainsi d'un niveau de protection granulaire qui rend l'accès aux ressources et aux données du réseau beaucoup plus difficile pour les utilisateurs et les appareils malveillants.

La possibilité d'utiliser la micro-segmentation pour segmenter davantage le trafic des utilisateurs au sein d'un macro-segment permet également un contrôle plus granulaire de l'accès des utilisateurs et des appareils afin de réduire le risque de prorogation des attaques au sein du réseau. Avec la micro-segmentation, le trafic des utilisateurs au sein d'un macro-segment, tel qu'un VLAN, peut être séparé en fonction de facteurs tels que l'heure de la journée, le lieu d'accès, le fait que l'utilisateur soit un étudiant, un professeur ou un membre du personnel administratif, ainsi que d'autres contrôles d'accès (figure 1). La même politique de sécurité suit la personne, où qu'elle se trouve, ce qui permet à l'institution de mettre en œuvre une approche plus unifiée de la cybersécurité.

Figure 1. La combinaison de la macro-segmentation et de la micro-segmentation renforce les contrôles d'accès au réseau



Récolter les fruits de son travail

Les établissements universitaires qui se font connaître pour leur dévouement et leur diligence à protéger scrupuleusement la sécurité et la confidentialité des informations sur leurs réseaux peuvent améliorer leur réputation, leur marque éducative et leur image publique. Leur capacité à se protéger contre les cyberattaques et à éviter la publicité négative qui accompagne inévitablement de tels événements permet d'attirer et de retenir les étudiants et de favoriser la réussite à long terme. Elle permet également à ces établissements d'être considérés comme des exemples de bonnes pratiques en matière de cybersécurité pouvant en inspirer d'autres, ce qui permet de renforcer les défenses contre les cyberattaques visant les réseaux éducatifs dans le monde entier.

Une stratégie de cybersécurité ZTNA contribue également à de meilleurs résultats scolaires. Grâce à un réseau plus sûr, les enseignants et les étudiants peuvent profiter en toute confiance des technologies numériques innovantes qui améliorent les possibilités d'apprentissage et la réussite des étudiants. Voici quelques exemples :

- Les enseignants peuvent élaborer et dispenser des cours plus créatifs, plus attrayants et plus interactifs qui inspirent les étudiants, les exposent à des innovations de pointe et les encouragent à participer activement aux discussions et aux activités de la classe, en présentiel ou en distanciel.
- Les étudiants peuvent expérimenter les nouvelles technologies, collaborer ouvertement entre eux et avec les enseignants, en tout lieu, et intégrer les dernières innovations numériques dans leurs travaux afin de montrer leur potentiel.

Le réseau de confiance permet à chaque institution de se concentrer sur l'enseignement et l'apprentissage.

Les équipes informatiques du secteur de l'éducation bénéficient également d'une stratégie de cybersécurité ZTNA. Grâce à une meilleure connaissance de la situation de l'établissement universitaire en matière de cybersécurité, les équipes informatiques peuvent prendre des décisions plus éclairées sur les nouvelles stratégies technologiques, telles que l'adoption d'une approche orientée cloud ou la prise en charge du BYOD. Dans le même temps, elles peuvent mieux protéger et contrôler l'infrastructure numérique du campus et garantir l'utilisation appropriée des précieuses ressources du réseau et de la bande passante.

Enfin et surtout, la limitation de la surface d'attaque de l'institution présente des avantages financiers potentiels, car elle réduit le risque de devoir mettre en place des mesures d'atténuation coûteuses en réponse à des cyberattaques.

Un partenaire expert pour une sécurité experte

Les établissements universitaires qui mettent en œuvre une stratégie de cybersécurité ZTNA devront travailler avec un partenaire expérimenté, capable de fournir des avis et des conseils d'experts ainsi que des solutions de mise en réseau ZTNA éprouvées.

Alcatel-Lucent Enterprise jouit d'une vaste expérience pour aider les établissements universitaires à progresser vers la cybersécurité ZTNA. Nous comprenons les étapes que doivent franchir ces institutions pour mettre en œuvre une stratégie ZTNA, et nous travaillons avec vous pour fournir les solutions de réseaux sécurisés qui correspondent à votre stratégie. Votre institution peut ainsi mettre en œuvre une approche stratifiée de la sécurité du réseau, afin de tirer le meilleur parti des mécanismes clés de la cybersécurité, tels que la micro-segmentation et le contrôle d'accès basé sur les rôles.

Une sécurité totale

Les solutions de mise en réseau d'ALE sont certifiées conformes aux normes de sécurité les plus importantes, notamment :

- Les lignes directrices et spécifications internationales des Critères communs pour la sécurité informatique
- Les tests de conformité de la JITC (Joint Interoperability Test Command) américaine
- La norme fédérale américaine de traitement de l'information (FIPS) 140-2

L'intégration étroite entre les pare-feu et l'infrastructure de réseau permet aux institutions de localiser avec précision la source des activités non autorisées et malveillantes et de mettre en quarantaine les appareils incriminés. Nos solutions élargissent les investissements de nos clients en s'intégrant aux pare-feu de Palo Alto Networks et de Fortinet.

Une solide expérience

Nous sommes le partenaire de confiance des institutions universitaires du monde entier qui cherchent à améliorer leur position en matière de cybersécurité :

- À l'Université d'État de Californie aux États-Unis, nos solutions de réseau et de gestion de réseau ont permis de créer un réseau fiable et flexible qui offre une sécurité renforcée, le Wi-Fi partout et des services cloud ouverts et partagés afin d'améliorer l'expérience globale sur le campus. Le réseau extrêmement fiable supporte en toute sécurité plus de 500 000 utilisateurs sur les quelque 20 campus de l'université et a permis d'économiser plus de 100 millions de dollars en coûts d'infrastructure.
- Sur le site Centro Paula Souza au Brésil, nos solutions de mise en réseau intelligentes et sécurisées fournissent les vitesses et les performances élevées dont les utilisateurs ont besoin pour travailler mieux et plus vite. L'authentification unifiée offre une expérience de sécurité conviviale aux employés et aux visiteurs. La technologie de confinement de l'IoT permet aux appareils de se connecter au réseau de manière sécurisée et contrôlée. Le personnel informatique dispose d'une visibilité totale sur les opérations du réseau et sur les politiques d'utilisation du réseau unifié.
- Sur le site Linköping University en Suède, nos solutions de mise en réseau assurent la résilience et la sécurisation de l'accès au réseau pour les étudiants et les professeurs, ainsi que pour les invités, les partenaires externes, les locataires des bâtiments universitaires et les fournisseurs de services. Les architectures de réseau physique et logique étant complètement distinctes, les étudiants et les professeurs peuvent se connecter automatiquement et en toute sécurité au segment de réseau qui leur a été attribué, depuis n'importe quel endroit et avec n'importe quel appareil.

En savoir plus

Pour découvrir comment nous pouvons aider votre établissement universitaire à évoluer vers une stratégie de cybersécurité « Zero Trust Network Access », consultez notre site web ou contactez-nous dès aujourd'hui pour discuter de vos besoins spécifiques.

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: www.al-enterprise.com/fr-fr/documentation-juridique/marques-copyright. Toutes les autres marques sont la propriété de leurs titulaires respectifs. Ni la Holding ALE ni ses sociétés affiliées ne peuvent être tenues responsables de l'éventuelle inexactitude des informations contenues dans ce document, qui sont sujettes à modification sans préavis. © 2023 ALE International. Tous les droits sont réservés. DID23011101FR (Juin 2023)

Alcatel·Lucent
Enterprise