ALE | Where Everything Connects

La cybersécurité sur les campus à l'ère de l'IoT et du RGPD

Alcatel·Lucent Enterprise

Table des matières

Introduction

La cybersécurité sur les campus est un sujet de réflexion permanent pour l'enseignement supérieur. Pour la seconde fois en trois ans, la sécurité de l'information est arrivée en tête de l'enquête annuelle « Higher Ed CIO Top 10 IT Issues » de l'Educause.[1]. Cela ne devrait pas surprendre, selon le dernier rapport d'enquête DBIR (Data Breach Investigations Report - Rapport d'enquêtes sur la violation de données) de Verizon[2]. Le rapport, qui montre une tendance à la hausse des activités cybercriminelles, identifie les trois secteurs les plus ciblés, à savoir les finances et les assurances, les soins de santé et l'enseignement.

La sécurité de l'information dans l'enseignement a toujours été une compétition entre facilité d'utilisation et sécurité totale ; la sécurité gagne parfois, mais le plus souvent, la facilité d'utilisation est la priorité. Ajoutez à cela la nouvelle législation européenne sur le respect de la vie privée connue sous le nom de Règlement Général sur la Protection des Données[3, 4], (RGPD), l'introduction d'une grande variété de terminaux IoT, et il n'est pas étonnant que la sécurité de l'information et la protection de la réputation de l'institution soient au premier plan des préoccupations des directeurs informatiques de l'enseignement supérieur.

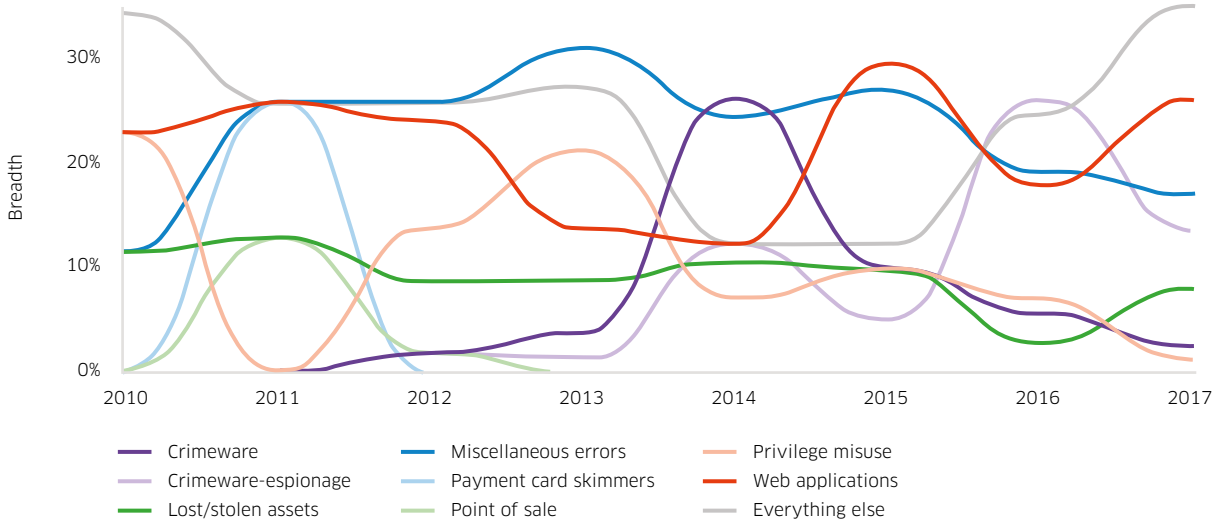
Cet accent sur la sécurité informatique est opportun. Jamais auparavant la technologie de l'information n'avait joué un rôle aussi important dans l'enseignement. Qu'il s'agisse de rechercher un sujet en classe ou de soumettre un travail en classe, la technologie de l'information est au cœur de la pédagogie et des stratégies mises en œuvre pour identifier et favoriser la réussite scolaire des étudiants.

Le rapport de l'enquête sur les violations des données de 2018 réalisé par Verizon fournit des informations très intéressantes sur les vecteurs d'attaque et les motivations de l'activité cybernétique malveillante.

Tableau 1. Résumé des violations des données du secteur de l'enseignement 2017

Fréquence	292 incidents, 101 avec confirmation de la divulgation des données
Modèles des 3 principaux problèmes	Les problèmes libellés Autres, Attaques d'application Web et Erreurs diverses représentent 76 % des violations de sécurité
Acteurs de la menace	Externe (81 %), Interne (19 %), Partenaire (2 %), Parties multiples (2 %) (violations)
Motifs de l'acteur	Financier (70 %), Espionnage (20 %), Plaisir (11 %)
Données compromises	Personnel (72 %), Confidentialité (14 %) et Médical (11 %)

Figure 1. Tendances observées dans les violations de l'enseignement



1 EDUCAUSE Center for Analysis and Research (ECAR), "Top 10 IT Issues 2018," EDUCAUSE Research Snapshot, *EDUCAUSE Review*, 29 janvier 2018.

2 Verizon Enterprise, "Verizon Data Breach Investigations Report (DBIR) 2018", Avril 2018, pages 29-30

3 https://eugdpr.org

4 https://gdpr-info.eu

Ce livre blanc explore la mise en œuvre de stratégies de sécurité basées sur les risques, telles que le concept de « défense en profondeur ». Ce concept favorise la protection d'un réseau informatique avec une série de mécanismes de défense individuels tels que, si une attaque est lancée, l'attaquant devra vaincre plusieurs couches indépendantes pour réussir.

La « triade CIA » sera évoquée tout au long de cet article. Cette construction identifie les cyber-cibles qui possèdent des informations « Confidentielles », qui ont un impact sur « l'Intégrité » des informations ou qui refusent leur « Accessibilité ». La triade CIA s'avère pour la formulation de règles de sécurité à l'échelle du campus et l'attribution de valeurs de risque. Par exemple, un ordinateur portable volé ou perdu contenant des informations d'identification personnelle (IIP) représenterait une attaque d'informations confidentielles. Un pirate informatique qui altère des notes violerait l'intégrité du système d'information sur les étudiants. Et des imprimantes BYOD dans des dortoirs d'étudiants pourraient être cooptées pour participer à une attaque par déni de service (DoS), qui serait classée comme une attaque d'accessibilité, car le but d'une attaque par DoS est d'inonder un serveur Web avec autant de demandes fictives que le serveur cessera de répondre aux requêtes légitimes.

Dans le présent document, les menaces à la sécurité de l'information sont désignées par le terme « activité cybernétique malveillante », définie par le gouvernement fédéral américain comme étant :

> « Des activités, autres que celles autorisées par ou conformément à la législation américaine, qui visent à détériorer ou à compromettre la confidentialité, l'intégrité ou l'accessibilité d'ordinateurs, de systèmes d'information ou de communication, de réseaux, d'infrastructures physiques ou virtuelles contrôlées par des ordinateurs ou de systèmes d'information, ou d'informations qui y résident. »

Les effets de la cyberactivité malveillante sont les suivants :

> « La manipulation, la perturbation, le refus d'accès, la dégradation ou la destruction d'ordinateurs, de systèmes d'information ou de communication, de réseaux, d'infrastructures physiques ou virtuelles contrôlées par des ordinateurs ou des systèmes d'information, ou d'informations qui y résident. »

Le déluge de terminaux Internet des objets (IoT) sur les campus et l'instauration d'une réglementation de la confidentialité dans le cyberespace, en particulier du Règlement général sur la protection des données de l'Union européenne, a fait de 2018 une année charnière. Le RGPD a des ramifications pour les universités du monde entier et les deux sujets seront discutés en profondeur.

Règlement général sur la protection des données

Le RGPD a été adopté le 25 mai 2018 par l'Union européenne pour redonner aux citoyens le contrôle de leurs cyber-informations. Le règlement général confère essentiellement à chaque résident de l'Union européenne le droit de savoir et de décider de la manière dont ses données personnelles sont utilisées, stockées, protégées, transférées et supprimées. Les personnes ont également le « droit à l'oubli » en demandant la suppression de l'ensemble de leurs données. Contrairement aux autres pays, qui définissent les informations personnelles identifiables, le RGPD couvre également les données de localisation, notamment les adresses IP, ce qui pourrait avoir un impact majeur sur le déploiement des services basés sur la localisation (LBS) sur le campus ou même des journaux d'équipement réseau.

En tant que législation sur la protection de la vie privée la plus progressiste au monde, outre les droits énoncés ci-dessus, le RGPD a également le pouvoir de faire respecter toute non-conformité. Les infractions au RGPD pourraient entraîner des pénalités de non-conformité équivalant à 4 % du chiffre d'affaires mondial annuel ou à 23 millions USD, le montant le plus élevé étant retenu.

La planification du RGPD serait incluse dans la section Confidentialité de la triade CIA et serait spécifiquement abordée dans la section Sécurité des applications.

IoT (Internet des objets)

L'Internet des objets est un sujet intéressant. Contrairement aux réseaux SDN (Software-Defined Networking), qui reposaient sur la cohérence de la mise en œuvre de la communauté des réseaux, les terminaux IoT sont déjà sur le campus et leur empreinte continuera à se développer. Un terminal IoT est un terminal connecté qui a la capacité d'envoyer et/ou de recevoir des informations sans

intervention humaine pour le faire fonctionner. Sur un campus, cela pourrait inclure une imprimante Wi-Fi grand public, des caméras de sécurité et des capteurs IoT, ou même des projecteurs de salle de lecture/salle de classe.

Dans des conditions normales d'utilisation, ces terminaux sont essentiellement inoffensifs. Toutefois, comme il s'agit de terminaux réseau et d'un système d'exploitation, ils sont exposés au hacking et aux programmes malveillants : les mettant en danger d'être recrutés et asservis dans une armée de bots. Vous vous souvenez peut-être de l'attaque DDoS (déni de service distribué) d'octobre 2016[5] contre Dyn, un fournisseur de services de noms de domaine basé aux États-Unis ayant des clients en Europe et en Amérique du Nord. Dyn a été attaqué trois fois au cours de la même journée. L'analyse résultante a confirmé que des terminaux IoT (caméras, moniteurs pour bébé, routeurs Wi-Fi et imprimantes) avaient été compromis avec une variante de programme malveillant basée sur le code source du virus Mirai.

La planification de l'IoT réside principalement dans la section Accessibilité de la triade CIA et sera spécifiquement traitée dans la section Sécurité d'accès réseau.

Défense en profondeur

La défense en profondeur consiste à défendre un ordinateur avec des couches de stratégies ou de terminaux de sécurité indépendants. Elle a été initialement conçue par l'agence NSA (National Security Agency) des États-Unis comme une approche globale de la protection des informations. Cette construction s'articule autour de trois axes :

1. Personnes : l'assurance des informations est l'objectif du leadership informatique et comprend l'application de services de sécurité tels que : Accessibilité, Intégrité, Authentification, Confidentialité et Non-répudiation. L'application de ces services devrait être basée sur les paradigmes Protéger, Détecter et Réagir. Sont également inclues ici la formation et les pratiques d'embauche/licenciement.
2. Technologie : comprend le matériel et les logiciels empêchant l'accès au contenu d'un système.
3. Opérations : se concentre sur toutes les activités nécessaires au maintien de la sécurité d'une organisation au quotidien et peut inclure des évaluations de la sécurité des systèmes, une récupération et une reconstitution, un contrôle des modifications et le traitement des données.

Le reste de ce livre blanc explore ces domaines d'intervention en explorant les couches suivantes : sécurité de la périphérie du réseau ; sécurité des applications ; sécurité du réseau LAN local, segmentation et gestion du réseau.

Sécurité de la périphérie du réseau

La périphérie du réseau se situe à l'endroit où le réseau interne de l'entreprise s'interface avec un autre réseau, notamment un opérateur, REN ou Internet public. Il s'agit de la première couche d'une architecture de défense en profondeur. Cette couche peut également être considérée comme protégeant les informations fournies par les « barbares à la porte » et leur activité malveillante.

La périphérie du réseau comporte à la fois du trafic entrant et sortant, ce qui signifie que nous devrons traiter chaque type de trafic.

Trafic entrant

Trafic entrant : que le trafic provienne d'un lien de réseau étendu, de l'Internet public ou d'un lien de réseau de recherche, certaines ou la totalité des technologies suivantes doivent s'appliquer :

1. Pare-feu : résidant normalement dans la zone démilitarisée (DMZ), un pare-feu peut effectuer plusieurs tâches de sécurité, notamment la traduction d'adresses de réseau (NAT), le réseau privé virtuel (VPN) et bien sûr l'application d'une logique de sécurité au trafic.
2. Système de détection d'intrusion (IDS)/Système de détection et de prévention d'intrusion (IDP) : sont importants pour protéger le réseau contre les attaques. Il existe deux types :
    1) Basé sur les signatures qui reconnaît les modèles d'attaques connus
    2) Anomalie basée qui reconnaît des écarts par rapport à l'activité du réseau « de base »

5 https://en.wikipedia.org/wiki/2016_Dyn_cyberattack

3. VPN (Virtual Private Network - Réseau privé virtuel) : fournit une connexion cryptée au réseau local. Ce type de connexion est préférable pour les communications sécurisées et utilise généralement des schémas d'authentification multifactorielle (MFA).
4. Filtres anti-spam : considérés par beaucoup comme un pare-feu de serveur de messagerie. Les filtres anti-spam ont acquis une sophistication et des capacités permettant d'identifier les pièces jointes infectées par des programmes malveillants, les adresses falsifiées (phishing) et d'autres attaques. Selon le rapport sur les violations des données réalisé par Verizon, le phishing (hameçonnage) est l'un des principaux vecteurs d'attaque dans le cas de l'enseignement supérieur. La mise en œuvre d'un filtre anti-spam peut aider à réduire le nombre d'attaques.
5. Filtre de trafic Web : certains pare-feux peuvent accomplir cette tâche et, bien sûr, toutes les institutions n'implémentent pas de filtre de trafic Web. Cependant, cette technologie permet à une université d'autoriser ou de refuser l'accès à des sites Web à partir de son réseau. Ce terminal de sécurité, qui est le plus souvent utilisé dans les établissements d'enseignement primaire et secondaire, aide à garder les utilisateurs à l'écart des sites susceptibles de conduire à une infection ou à une perte de contrôle.
6. Surveillance de la sécurité du réseau : des applications telles que Bro[6] ou Splunk[7] peuvent fournir des données utiles sur le trafic réseau et les anomalies de sécurité potentielles.

Trafic sortant

En plus de demander du trafic, un réseau enverra également des informations en dehors du réseau. Bien que ce type de trafic ne soit généralement pas suspect, sa surveillance peut informer l'institution en cas d'infraction à la sécurité (par exemple, des terminaux infectés par des programmes malveillants IoT participant à une attaque DDoS).

Le trafic sortant doit traverser les défenses du trafic entrant, mais il existe une technologie utile pour la protection du trafic sortant, à savoir le cryptage.

1. Le cryptage MACSec est également connu sous la désignation IEEE 802.1AE. Cette technologie prend en charge les transmissions cryptées sur un lien. Par exemple, si vous avez un site de récupération après sinistre (DR) pour votre data center, vous pouvez alimenter ce site via un lien crypté MACSec, garantissant la confidentialité, l'intégrité et l'authentification de l'origine des données.

Sécurité des applications

La sécurité des applications est la couche suivante dans la lutte contre les menaces de cybersécurité actuelles. Cette couche englobe à la fois les terminaux informatiques des utilisateurs finaux et les applications basées sur le réseau. La sécurité des applications est un outil important dans l'arsenal de sécurité d'une université. Elle aborde les domaines confidentiel et d'intégrité de la triade CIA et il est important de la prendre en compte lors de la mise en œuvre des protections RGPD.

Les technologies et les tactiques de cette couche comprennent :

1. Chiffrement des données : les deux principaux systèmes d'exploitation d'ordinateur possèdent des fonctionnalités de cryptage des données de disque. Ceci est important car il protège les données de l'utilisateur des accès occasionnels. Le cryptage du stockage réseau gagne en popularité et améliore l'intégrité et la confidentialité des informations.
2. Authentification multifactorielle (MFA, Multifactor Authentication) : l'authentification multifactorielle est un mécanisme nécessitant le fonctionnement simultané de deux terminaux pour pouvoir accéder à une application ou à une ressource. En règle générale, le flux est la paire nom d'utilisateur/mot de passe, puis une chaîne de nombres est entrée et envoyée au smartphone de l'utilisateur. Cela fournit une autre couche de confirmation que la personne est ce qu'elle dit être. Un autre mécanisme permettant de fournir une authentification multifactorielle consiste à utiliser des jetons matériels tels que ceux de RSA et de Google au lieu du texte d'un smartphone. Cette stratégie présente l'avantage de pouvoir être exploitée dans les stratégies de réseau privé virtuel (VPN) et autres stratégies de communication sécurisées.

6 https://www.bro.org
7 https://www.splunk.com

3. Micro-segmentation : le data center est passé des serveurs physiques à des serveurs virtuels, des dizaines de serveurs virtuels occupant l'espace d'un ou deux serveurs physiques. Toutefois, avec cette densité vient le risque. Les pare-feu d'inspection à états traditionnels n'ont pas la capacité d'analyser, au niveau local, les flux de trafic d'un data center. VMWare[8], un important fournisseur d'hyperviseurs, a mis en œuvre une technologie appelée « micro-segmentation ». Cela signifie que chaque application peut désormais avoir son propre périmètre de sécurité sans s'appuyer exclusivement sur des VLAN.

Les pratiques mises en œuvre dans cette couche doivent comprendre :

4. Formation de sensibilisation à la sécurité des utilisateurs finaux : cette activité a généralement lieu pendant le mois de sensibilisation à la sécurité (octobre). Cependant, des rappels périodiques sur le phishing (hameçonnage), le spear phishing et les exploits d'ingénierie sociale (divulgation des informations d'identité) doivent être diffusés tout au long de l'année pour aider à réduire la surface de ce vecteur d'attaque.
5. Correctifs de sécurité : il est important de tester les correctifs de sécurité et les mises à jour des applications avant de les appliquer. Cependant, les versions du fabricant sont importantes et devraient être une priorité. Selon le rapport sur les violations des données réalisé par Verizon, 6 % des attaques réussies ont exploité des failles de sécurité qu'un correctif aurait pu couvrir. En fait, certaines des attaques les plus nuisibles ont été causées par l'application de correctifs différée.

Sécurité d'accès au réseau

Les réseaux locaux (LAN) et les réseaux locaux sans fil (WLAN) sont des points d'entrée pour les utilisateurs des ordinateurs du campus. Une connexion LAN désigne généralement la connexion physique d'un cordon de raccordement Ethernet du terminal réseau à un port mural RJ-45. Une connexion WLAN ne nécessite pas de connectivité physique et utilise à la place la puce Wi-Fi intégrée au terminal pour voir le réseau et se connecter à ce dernier.

Les universités ont toujours dû concilier facilité d'utilisation et sécurité totale. Il est important de ne pas alourdir l'accès sécurisé, faute de quoi les étudiants et d'autres personnes trouveront un moyen de contourner ou augmenteront le nombre de terminaux « Shadow IT ». Par exemple, sur certains campus, un invité aura besoin d'un sponsor pour pouvoir s'authentifier sur le réseau ; dans d'autres cas, il sera possible d'envoyer l'invité sur un portail en libre-service où il entre des informations personnelles sur lui-même, accepte une langue d'utilisation acceptable et peut ensuite se connecter. Ces deux systèmes fournissent la même protection au réseau, mais l'un est un peu plus onéreux que l'autre.

Dans une architecture de défense en profondeur, la sécurité d'accès réseau constitue l'un des investissements les plus importants à réaliser. Cette couche concerne les 4 A : Authenticate (Authentification), Authorize (Autorisation), Audit (Audit) et Administer (Administration). Une authentification réussie entraîne l'autorisation des ressources réseau autorisées pour un rôle spécifique. L'audit concerne la surveillance du trafic et du comportement du réseau et, le cas échéant, l'authentification administre des règles de quarantaine ou de trafic du réseau.

Les technologies de sécurité d'accès réseau prenant en charge les 4 A comprennent :

1. 802.1X : un mécanisme de contrôle d'accès au réseau basé sur les ports standard IEEE, fournissant un mécanisme d'authentification pour les terminaux LAN et WLAN. La norme 802.1X nécessite un demandeur (ordinateur ou terminal demandant l'accès) ; un authentificateur (généralement le commutateur Ethernet ou un point d'accès AP (WLAN) ou un contrôleur) ; et un serveur d'authentification (généralement un serveur RADIUS ou EAP). Le demandeur fournit les informations d'identification au serveur d'authentification. S'il est correct, l'authentificateur accorde l'accès au réseau.
2. Biométrie : une nouvelle méthode d'authentification de sécurité potentiellement plus simple consiste à utiliser la biométrie, ou quelque chose d'unique pour l'utilisateur, comme une empreinte digitale, un scan de l'iris ou une empreinte vocale. Bien que cela n'aide en rien les terminaux IoT, elle fournit un moyen simple d'accorder un accès humain au réseau en toute sécurité.

8 https://www.vmware.com

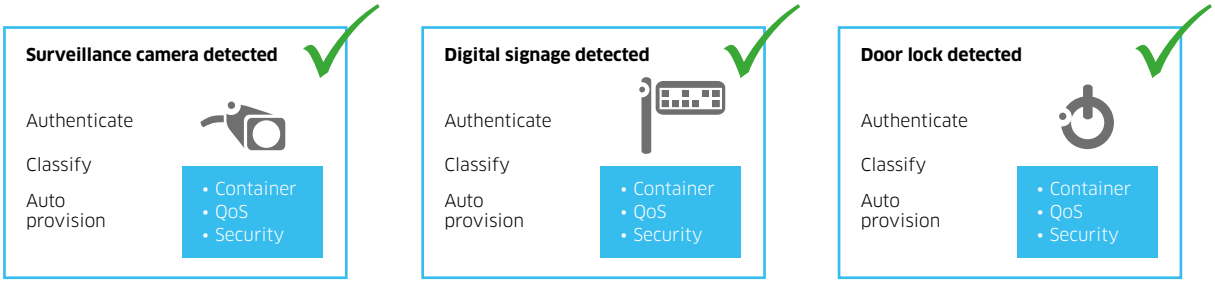
3. Cryptage : alors qu'il était auparavant référencé comme mécanisme de sécurité pour les données au repos et en transit d'un data center à un autre, le cryptage MACSec est de plus en plus répandu dans le réseau local (LAN), du cœur à la périphérie. En outre, les normes IEEE WLAN ont adressé le cryptage avec la norme 802.11i, qui protège les transmissions Wi-Fi d'un point d'accès à un utilisateur contre les attaques de type Man-in-the-Middle (une des principales raisons de ne pas utiliser de réseau Wi-Fi public, non crypté). En outre, l'alliance Wi-Fi a récemment annoncé le protocole WPA3 (Wi-Fi Protected Access 3). Le protocole WPA3 ajoute de nouvelles fonctionnalités pour simplifier la sécurité Wi-Fi, permettre une authentification plus robuste, renforcer la capacité cryptographique des marchés de données extrêmement sensibles, tout en maintenant la résilience des réseaux stratégiques.
4. Système d'exploitation renforcé : de nombreux terminaux réseau sont achetés avec des profils d'authentification d'administrateur par défaut. Malheureusement, et le plus souvent dans le cas des terminaux IoT, ces paramètres par défaut ne sont jamais modifiés, ce qui en fait une cible facile pour l'insertion de programmes malveillants ou même le changement de code. Un système d'exploitation de terminal renforcé est un système d'exploitation qui brouille le code et l'emplacement de la mémoire, de sorte qu'une violation réussie d'un terminal ne sera pas répétée avec succès de manière automatique. En plus de protéger l'intégrité du terminal, un système d'exploitation renforcé peut également posséder les caractéristiques suivantes :
    1) Sensibilisation aux attaques DoS et atténuation : certains terminaux d'infrastructure de réseau peuvent reconnaître qu'une attaque DoS est en cours et contrecarrer immédiatement l'attaque en supprimant le trafic incriminé.
    2) Connaissance des attaques basées sur IP : certains terminaux d'infrastructure de réseau peuvent s'intégrer à SNORT ou à d'autres produits IDS/IDP, réagir à une signature d'attaque IP positive et mettre en quarantaine le trafic incriminé.
5. Stratégies d'accès au réseau unifié : après une authentification réussie, cette structure autorise l'accès au réseau en fonction de paramètres tels que l'adresse MAC, l'heure de la journée, le rôle de l'utilisateur, le département (étudiant, invité, faculté, personnel, fournisseur, administration, salle de sports, etc.) ou même l'emplacement à partir duquel ils s'authentifient. Cette structure prend en charge les accès LAN et WLAN. Elle élimine les erreurs de concordance et de duplication des profils de sécurité et fournit un accès réseau cohérent et sécurisé.
6. Terminaux IoT : les stratégies d'accès au réseau unifié sont une fonctionnalité essentielle pour l'activation de terminaux IoT. En outre, l'empreinte digitale des terminaux DHCP permet d'identifier rapidement les terminaux IoT de plusieurs fabricants. Cette fonctionnalité exploite les options DHCP qui fournissent des informations spécifiques au fournisseur sur le système d'exploitation ou le matériel du terminal. L'échange se fait à l'aide des options DHCP définies par la documentation RFC 2132.[9] L'utilisation des options DHCP fournit des informations sur le fournisseur, le terminal et le système d'exploitation, qui constituent « l'empreinte digitale » du terminal. Par exemple, une récente demande de propositions en matière de vidéosurveillance a été attribuée à un seul fabricant. Ces nouveaux produits coexisteront avec les anciennes caméras de vidéosurveillance. Avec la mise en œuvre de l'UNAP, l'équipe de sécurité dispose de deux moyens pour identifier et appliquer les règles de sécurité du réseau. : empreinte digitale DHCP ou masquage d'adresse MAC. Le masquage d'adresse MAC utilise les 24 premiers bits de l'adresse MAC, qui contient l'identificateur unique d'organisation (OUI)[10]. Tirer parti de l'UNAP avec une stratégie d'adresse MAC masquée permettrait à l'institution de déployer rapidement et en toute sécurité ses nouvelles caméras de surveillance. L'empreinte digitale DHCP permettrait au campus d'identifier toutes les caméras de vidéosurveillance et d'appliquer des politiques de sécurité cohérentes.

Les empreintes digitales des terminaux DHCP sont généralement prises en charge par les systèmes WLAN. Cependant, elles sont plus puissantes lorsque des terminaux LAN sont également inclus, car tous les terminaux IoT ne se connectent pas au réseau via Wi-Fi.

9 http://www.ietf.org/rfc/ rfc2132.txt

10 http://standards-oui.ieee.org/oui/oui.txt

Figure 2. Classification et reconnaissance automatique

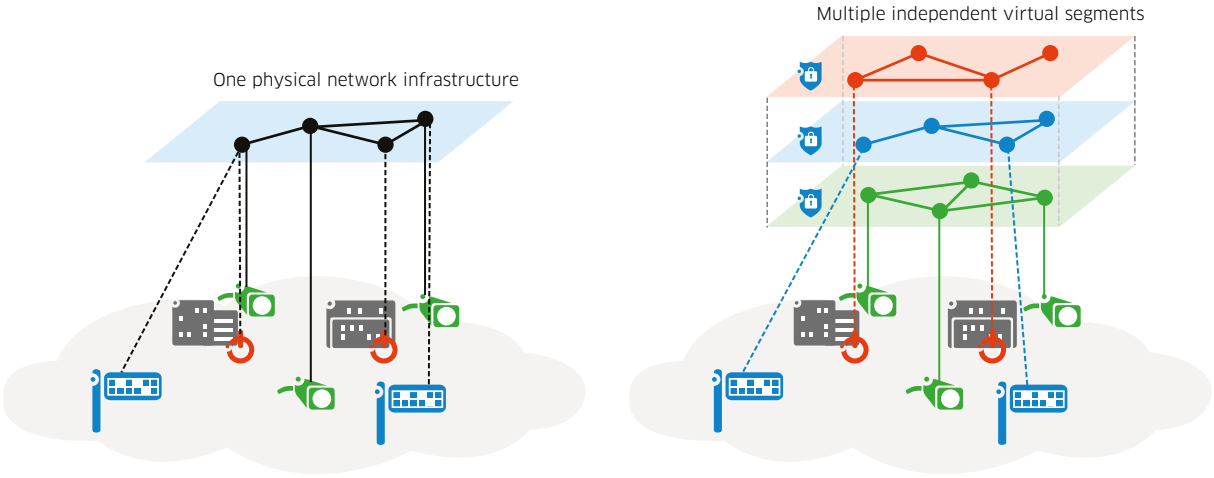


Segmentation du réseau

Avec l'introduction de la commutation LAN, la segmentation physique a été étendue pour inclure les réseaux locaux virtuels (VLAN). Cela permet de limiter les services réseau aux utilisateurs membres du VLAN, essentiellement en sécurisant les applications et les services. La plupart des équipements de réseau prennent en charge jusqu'à 4 096 VLAN, ce qui devrait être plus que suffisant, mais peut en réalité être un défi et doit être correctement architecturé.

Le sujet de l'épuisement des réseaux VLAN est réel et a été abordé dans plusieurs technologies utilisées par les campus. MPLS (Multiprotocol Label Switching)[11] et son dérivé, Shortest Path Bridging (SPB – IEEE 802.1aq)[12], utilisent tous deux le concept d'interfaces de services pour segmenter l'activité réseau.

Figure 3. SPBM - Segmentation du réseau, pas de Spanning Tree



Gestion de réseau

La gestion de réseau est une application souvent négligée par les fournisseurs d'équipements d'infrastructure. Il existe de nombreuses raisons à cela. Le plus important d'entre eux est la prévalence d'applications tierces gérant des environnements multi-constructeurs. Cependant, l'utilisation d'un système de gestion de réseau (NMS - Network Management System) tiers constitue un compromis. De nombreuses plates-formes NMS proposées par des fournisseurs peuvent intégrer des droits de support, et même suggérer des versions de maintenance qui traitent des bogues potentiels du déploiement. En outre, le système NMS OEM peut fournir une mine de statistiques, d'analyses et de tendances permettant une gestion de réseau proactive.

11 https://en.wikipedia.org/wiki/Multiprotocol_Label_Switching
12 https://en.wikipedia.org/wiki/IEEE_802.1aq

Les professionnels de l'informatique dans l'enseignement commencent également à se pencher sur les fonctionnalités d'inspection approfondie des paquets (DPI) pour l'infrastructure LAN. La possibilité de savoir quelles applications consomment le plus de bande passante peut informer l'ensemble du service informatique des domaines dans lesquels des investissements doivent être réalisés. Par exemple, si le trafic en provenance et à destination de l'application LMS est le plus gros consommateur de bande passante, il serait probablement utile d'examiner les ressources affectées à la machine virtuelle LMS ou, si elles sont basées sur le cloud, d'examiner l'expérience utilisateur et de déterminer si des investissements supplémentaires sont nécessaires pour augmenter la bande passante, la mémoire, le traitement ou le stockage.

En ce qui concerne la cybersécurité sur le campus, le système NMS est la plate-forme où tout commence. De l'activation de l'accès SSL/CLI crypté à l'équipement d'infrastructure, en passant par la mise en place de stratégies d'accès au réseau unifié, la surveillance du trafic pour détecter les anomalies, la mise en quarantaine des terminaux/utilisateurs défectueux, le système NMS est la plate-forme capable d'accomplir tout cela, et bien plus encore.

En plus d'un solide système NMS, certains programmes tiers doivent être pris en compte :

1. perfSONAR[13] : bien que cet outil soit utilisé par de nombreux instituts de recherche, il possède des fonctionnalités qui peuvent vous aider à comprendre les performances de votre réseau. Voici un extrait de ce qu'il est censé faire :

   « Il est essentiel de veiller à ce que les choses fonctionnent bien, de bout en bout. La surveillance dans un seul domaine est une pratique commune et acceptée ; la surveillance de la performance inter-domaines est difficile à réaliser avec des outils traditionnels. perfSONAR est une infrastructure de test et de mesure largement déployée et utilisée par des réseaux et des installations scientifiques du monde entier pour surveiller et garantir les performances du réseau. »
2. Les outils de perfSONAR qui fournissent un dépannage supplémentaire :
   1) pScheduler : tests de débit sur des sites distants
   2) OWAMP : contrôles continus de la latence et de la perte de paquets

Récapitulatif

Les établissements d'enseignement sont la troisième industrie la plus ciblée au monde. La cybersécurité dans l'enseignement est plus qu'un accessoire. Il s'agit d'une dimension critique de l'architecture de l'entreprise et peut contribuer à la reconnaissance positive de la marque par une université.

La mise en œuvre d'un plan de sécurité basé sur les risques permet à l'université d'allouer son budget en fonction des besoins ou des risques. Suivre l'architecture de défense en profondeur garantit qu'un attaquant doit vaincre différentes technologies tout au long de l'exploit pour réussir.

L'utilisation de la triade CIA des classifications de confidentialité, d'intégrité et d'accessibilité dans vos actifs informatiques permet de déterminer le risque pour l'institution et son poids pour le sujet.

La mise en œuvre des 4 A (Authentification, Autorisation, Audit et Administration) fournit une structure unifiée pour l'accès au réseau et le comportement sur les réseaux LAN et WLAN.

La segmentation du réseau avec MPLS ou SPB permet un contrôle granulaire des services et des terminaux/utilisateurs accédant à ces services.

Enfin, la formation : la technologie de sécurité et l'architecture vous aideront à protéger vos actifs. Cependant, comme cela a été constaté dans de nombreuses études, le phishing et les erreurs d'utilisateurs sont les méthodes de hacking les plus courantes. Former vos étudiants, votre corps professoral, votre personnel et vos fournisseurs à la cybersécurité peut vous aider à réduire votre facteur de risque numéro un.

13 https://www.perfsonar.net/about/what-is-perfsonar/

Références et ressources

National Institute of Standards and Technology : ce lien vous mène à la page de destination du cadre de cybersécurité du NIST : https://www.nist.gov/cyberframework

EDUCAUSE : une association à but non lucratif qui aide l'enseignement supérieur à augmenter l'impact de l'informatique. Les résultats de l'enquête annuelle « Top 10 IT Issues » de 2018 et des liens vers d'autres ressources sont disponibles ici : https://er.educause.edu/articles/2018/1/top-10-it-issues-2018-the-remaking-of-higher-education

Alcatel·Lucent Enterprise