# Chapitre 7 : Fortifier le royaume

La « fortification du royaume » est un processus continu qui consiste à sécuriser l'infrastructure de réseau d'une entreprise. Elle exige de la part des acteurs une vigilance constante à l'égard des menaces qui pèsent sur celui-ci et il faut prendre des mesures pour empêcher toute atteinte à la sécurité. Ce chapitre traite des technologies, processus et procédures que les spécialistes de la cybersécurité emploient pour protéger les systèmes, les équipements et les données qui constituent l'infrastructure du réseau.

Un réseau sécurisé est aussi robuste que sa liaison la plus faible. Il est important de sécuriser les terminaux qui résident sur le réseau. Pour garantir la sécurité de ceux-ci, il convient notamment de sécuriser les périphériques réseau, ainsi que les systèmes des utilisateurs, tels que les postes de travail, les serveurs, les téléphones IP et les points d'accès.

Le renforcement des équipements est une tâche essentielle dans le cadre de la sécurisation du réseau. Cela consiste à mettre en œuvre des méthodes éprouvées de sécurisation physique des périphériques réseau, telles que sécuriser l'accès administratif, gérer des mots de passe et instaurer des communications sécurisées.

# Sécurité du système d'exploitation

Le système d'exploitation joue un rôle essentiel dans le fonctionnement d'un système informatique et est donc la cible de nombreuses attaques. Le degré de sécurité du système d'exploitation a un effet domino sur la sécurité globale d'un système informatique.

Un administrateur renforce un système d'exploitation en modifiant la configuration par défaut pour mieux le protéger face aux menaces extérieures. Ce processus implique notamment la suppression des programmes et des services inutiles. Pour renforcer les systèmes d'exploitation, il est également essentiel d'appliquer les mises à jour et les correctifs de sécurité. Les correctifs de sécurité et les mises à jour sont des solutions proposées par les entreprises dans le but de réduire la vulnérabilité de leurs produits et d'en corriger les failles.

Une entreprise doit adopter une approche méthodique relativement aux mises à jour du système :

* Mise en place de procédures de surveillance des informations relatives à la sécurité
* Évaluation de l'applicabilité des mises à jour
* Planification de l'installation des mises à jour et correctifs des applications
* Installation des mises à jour à l'aide d'un plan documenté

S'agissant de la sécurisation des systèmes d'exploitation, une autre exigence essentielle consiste à identifier les vulnérabilités potentielles. Pour ce faire, il est possible d'établir un point de référence. Cela permet à l'administrateur d'avoir un point de comparaison entre les performances attendues d'un système et ses performances réelles.

MBSA (Microsoft Baseline Security Analyzer) évalue les mises à jour de sécurité manquantes et les mauvaises configurations de la sécurité dans Microsoft Windows. MBSA vérifie les mots de passe vides, simples ou inexistants, les paramètres du pare-feu, l'état du compte invité, les informations du compte administrateur, l'audit des événements liés à la sécurité, les services inutiles, les partages réseau et les paramètres du registre. Une fois le système d'exploitation renforcé, l'administrateur crée les politiques et procédures nécessaires pour maintenir un niveau élevé de sécurité.

Protection contre les logiciels malveillants

Les programmes malveillants peuvent être des virus, des vers, des chevaux de Troie, des enregistreurs de frappe, des logiciels espions ou des logiciels publicitaires. Ils portent atteinte à la vie privée des utilisateurs, dérobent des informations, endommagent le système ou suppriment et corrompent des données.

Il est important de protéger les ordinateurs et les terminaux mobiles à l'aide d'un logiciel antimalware renommé. Voici les types de logiciels existants :

* Protection antivirus : le programme surveille en permanence les virus. Lorsque le programme détecte un virus, il en informe l'utilisateur et tente de le mettre en quarantaine ou de le supprimer, comme illustré à la Figure 1.
* Protection contre les logiciels publicitaires : ce programme recherche en continu les programmes qui affichent de la publicité sur un ordinateur.
* Protection contre l'hameçonnage : ce programme bloque les adresses IP des sites Web d'hameçonnage connus et signale les sites suspects à l'utilisateur.
* Protection contre les logiciels espions : ce programme recherche les enregistreurs de frappe et autres logiciels espions.
* Sources approuvées/non approuvées : le programme avertit l'utilisateur que des programmes dangereux tentent de s'installer ou informe les internautes de la dangerosité de sites web avant qu'ils les consultent.

Plusieurs programmes et analyses différents peuvent être nécessaires pour les supprimer complètement. Toutefois, n'exécutez qu'un seul utilitaire de protection à la fois.

Plusieurs entreprises réputées sont spécialisées dans la sécurité, comme McAfee, Symantec et Kaspersky. Elles offrent une protection complète contre les programmes malveillants pour les ordinateurs et les appareils mobiles.

Méfiez-vous des faux programmes antivirus qui peuvent s'afficher pendant la navigation sur Internet. La plupart de ces faux programmes antivirus s'affichent dans une publicité ou dans une fenêtre contextuelle qui se présente comme une vraie fenêtre d'avertissement de Windows, voir l'illustration 2. Ils indiquent généralement que des programmes malveillants infectent l'ordinateur et invitent l'utilisateur à les nettoyer. Si vous cliquez n'importe où dans cette fenêtre, vous risquez, en réalité, de télécharger et d'installer un programme malveillant.

Les logiciels non approuvés ou non conformes ne se limitent pas aux logiciels installés de façon involontaire sur l'ordinateur. Ils peuvent également provenir des utilisateurs, qui souhaitaient les installer. Même s'ils ne sont pas forcément malveillants, ils enfreignent les stratégies de sécurité. Ce type de système non conforme peut perturber le fonctionnement des logiciels de l'entreprise ou des services réseau. Les utilisateurs doivent supprimer immédiatement les logiciels non approuvés.

Gestion des correctifs

Les correctifs sont des mises à jour du code que les éditeurs fournissent afin d'empêcher un nouveau virus ou ver de contaminer un ordinateur. De temps à autre, les correctifs et les mises à jour sont combinés dans une application de mise à jour complète appelée Service Pack. De nombreuses attaques de virus particulièrement dévastatrices auraient pu être beaucoup moins graves si davantage d'utilisateurs avaient téléchargé et installé le Service Pack le plus récent.

Windows vérifie régulièrement si le site Web de Windows Update contient des mises à jour cruciales qui peuvent contribuer à la protection d'un ordinateur contre les menaces les plus récentes. On y trouve des mises à jour de sécurité, des mises à jour critiques et des Services Packs. Vous pouvez configurer Windows pour qu'il télécharge et installe automatiquement les mises à jour prioritaires dont l'ordinateur a besoin ou qu'il informe l'utilisateur de leur disponibilité.

Au sein de certaines entreprises, le test d'un correctif est une étape obligée avant de le déployer à grande échelle. L'entreprise utilise alors un service pour gérer les correctifs en local au lieu d'utiliser le service de mise à jour en ligne de l'éditeur. L'utilisation d'un service de mise à jour automatisé de correctifs présente les bénéfices suivants :

* Les administrateurs peuvent approuver ou refuser les mises à jour
* Les administrateurs peuvent forcer la mise à jour des systèmes à une date bien précise
* Les administrateurs peuvent obtenir des rapports sur la mise à niveau requise par chaque système
* Les ordinateurs ne doivent pas se connecter individuellement au service de l'éditeur pour télécharger les correctifs ; un système reçoit la mise à jour depuis un serveur local
* Les utilisateurs ne peuvent ni désactiver ni « éluder » les mises à jour

Un service automatisé d'application de correctifs garantit aux administrateurs un meilleur contrôle sur la configuration.

# WPA/WPA2

L'introduction des mécanismes WPA et WPA2 marqua une étape importante dans l'amélioration de la sécurité sans fil. WPA (Wi-Fi Protected Access) a été développé par les entreprises du secteur pour répondre aux faiblesses du standard WEP. La configuration WPA la plus répandue est WPA-PSK (Pre-shared key). Les clés utilisées par le mécanisme WPA ont une longueur de 256 bits, une augmentation considérable par rapport à la longueur des clés de 64 bits et 128 bits utilisées dans le système WEP.

Le standard WPA apporte aussi plusieurs améliorations relatives à la sécurité. Tout d'abord, WPA publiait des messages Integrity Check (MIC) capables de détecter si un hacker avait intercepté et modifié des données transmises entre le point d'accès sans fil et un client sans fil. Le protocole TKIP (Temporal Key Integrity Protocol) constitue une autre amélioration majeure sur le plan de la sécurité, en offrant la possibilité de mieux gérer, protéger et modifier les clés de cryptage. AES (Advanced Encryption Standard) a remplacé le protocole TKIP pour garantir une protection encore meilleure du chiffrement et une gestion améliorée des clés.

WPA, comme son prédécesseur WEP, comportait plusieurs vulnérabilités manifestes. C'est donc en toute logique que le standard WPA2 (Wi-Fi Protected Access II) a été lancé en 2006. L'une des améliorations les plus importantes sur le plan de la sécurité entre les mécanismes WPA et WPA2 fut l'utilisation obligatoire des algorithmes AES et l'introduction du Counter Mode avec Cipher Block Chaining Message Authentication Code Protocol (CCMP) en remplacement de TKIP.

# WEP

Le terminal mobile constitue l'un des composants essentiels de l'informatique moderne. La majorité des appareils qui se trouvent aujourd'hui sur les réseaux sont des ordinateurs portables, des tablettes, des smartphones et d'autres terminaux sans fil. Tout appareil équipé d'une antenne compatible peut recevoir les données que les terminaux mobiles transmettent par signaux radio. C'est pourquoi les acteurs du secteur de l'informatique ont développé toute une série d'appareils, de produits et de normes de sécurité mobile et sans fil. Ces normes chiffrent les données transmises par les terminaux mobiles par le biais des ondes radio.

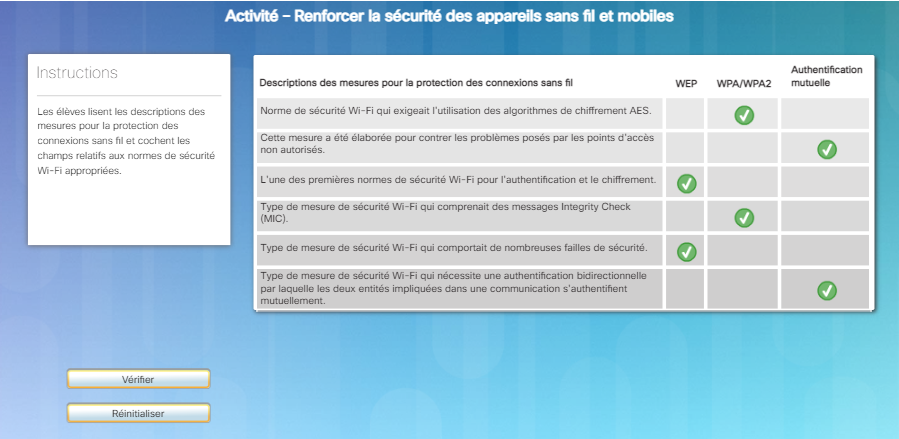
WEP (Wired Equivalent Privacy), l'un des premiers standards de sécurité Wi-Fi, a été adopté à grande échelle. Le standard WEP protège le réseau grâce à des systèmes d'authentification et de chiffrement. Les standards WEP sont aujourd'hui obsolètes, mais de nombreux appareils en assurent toujours la prise en charge à des fins de rétrocompatibilité. Le protocole WEP est devenu un standard de sécurité Wi-Fi en 1999, alors que la technologie sans fil commençait à se populariser. Malgré plusieurs révisions et une augmentation de la taille de clé, le protocole WEP comportait de nombreuses failles de sécurité. Les cybercriminels peuvent ainsi pirater des mots de passe WEP en quelques minutes en utilisant simplement un logiciel gratuit. Malgré les améliorations, le protocole WEP reste extrêmement vulnérable et les utilisateurs doivent mettre à niveau les systèmes qui reposent sur cette norme.

# Authentification mutuelle

L'utilisation de points d'accès non autorisés est l'une des principales vulnérabilités des réseaux sans fil. Les points d'accès sont les appareils qui communiquent avec les appareils sans fil et les reconnectent au réseau filaire. Tout appareil équipé d'un émetteur sans fil et d'une interface câblée vers un réseau peut être considéré comme un point d'accès non autorisé potentiel. Le point d'accès non autorisé peut imiter un point d'accès autorisé. Par conséquent, les périphériques sans fil connectés au réseau sans fil établissent une communication avec le point d'accès non autorisé au lieu du point d'accès autorisé.

L'imposteur peut alors recevoir des requêtes de connexion, copier les données qu'elles contiennent et transmettre les données au point d'accès réseau autorisé. Ce type d'attaque, dite man-in-the-middle, s'avère particulièrement difficile à détecter, et peut se traduire par le vol d'identifiants de connexion et des données transmises. Pour éviter les points d'accès non autorisés, les acteurs du secteur informatique ont développé le processus d'authentification mutuelle. L'authentification mutuelle, aussi appelée authentification bidirectionnelle, est un processus ou une technologie qui permet aux deux entités impliquées dans une communication de s'authentifier mutuellement. Dans un environnement réseau sans fil, le client s'authentifie auprès du point d'accès qui, à son tour, authentifie le client. Cette évolution a permis aux clients de détecter les points d'accès non autorisés avant de s'y connecter.

# La sécurité des appareils sans fil et mobiles



Contrôle d'accès aux fichiers

Les autorisations sont des règles configurées pour limiter l'accès à un dossier ou à un fichier pour un utilisateur ou un groupe d'utilisateurs. L'illustration ci-contre présente les autorisations possibles pour les fichiers et les dossiers.

Principe du privilège minimum

Les utilisateurs ne doivent avoir accès qu'aux ressources dont ils ont besoin, que ce soit sur un ordinateur ou sur un réseau. Par exemple, ils ne doivent pas pouvoir accéder à tous les fichiers d'un serveur s'ils n'ont besoin d'accéder qu'à un seul dossier. Il peut être plus facile d'autoriser l'accès à un lecteur complet, mais il est plus sûr de restreindre l'accès aux seules ressources nécessaires. En quoi consiste le « principe de privilège minimal » ? Limiter l'accès aux ressources permet également de bloquer l'accès des programmes malveillants, au cas où un ordinateur serait contaminé.

Restriction des autorisations attribuées aux utilisateurs

Si un administrateur refuse à un individu ou à un groupe l'autorisation d'accès à un partage réseau, cette décision est prioritaire sur tout autre paramètre d'autorisation. Par exemple, si l'administrateur refuse d'accorder une autorisation d'accès à un partage réseau, l'utilisateur ne peut pas accéder à ce partage, même s'il est l'administrateur ou membre du groupe des administrateurs. La stratégie de sécurité doit indiquer quels sont les ressources et les types d'accès applicables pour chaque utilisateur et chaque groupe.

Lorsqu'un utilisateur modifie les autorisations d'un dossier, il a la possibilité d'appliquer les mêmes autorisations à tous les sous-dossiers. C'est ce que l'on désigne sous le nom de propagation d'autorisations. Il permet d'appliquer les mêmes autorisations à plusieurs fichiers et dossiers rapidement et facilement. Une fois les autorisations définies pour un dossier, les dossiers et fichiers créés à l'intérieur de ce dossier héritent des autorisations du dossier parent.

De plus, l'emplacement des données et les opérations dont elles font l'objet déterminent la propagation des autorisations :

* Les données déplacées sur le même volume conservent les autorisations initiales
* Les données copiées sur le même volume héritent des nouvelles autorisations
* Les données déplacées sur un autre volume héritent des nouvelles autorisations
* Les données copiées sur un autre volume héritent des nouvelles autorisations

# Chiffrement de fichier

Le chiffrement est une technique utilisée pour protéger les données. Le chiffrement transforme les données à l'aide d'un algorithme complexe pour les rendre illisibles. Une clé spéciale reconvertit les données illisibles en données lisibles. Des programmes chiffrent des fichiers, des dossiers et même des disques entiers.

Le système EFS (Encrypting File System) de Windows permet de chiffrer les données. L'implémentation Windows du système EFS le relie directement à un compte utilisateur spécifique. Seul l'utilisateur qui a chiffré les données pourra accéder aux fichiers ou dossiers chiffrés.

L'utilisateur peut également choisir de chiffrer l'intégralité d'un disque dur sous Windows avec la fonctionnalité BitLocker. Pour l'utiliser, vous devez disposer d'au moins deux volumes sur un disque dur.

Avant d'utiliser BitLocker, il convient d'activer le TPM (Trusted Platform Module) dans le BIOS. Le TPM est une puce spécialisée installée sur la carte mère. Le TPM stocke des informations spécifiques au système hôte, telles que les clés de chiffrement, les certificats numériques et les mots de passe. Certaines applications comme BitLocker, qui utilisent le chiffrement, peuvent utiliser la puce TPM. Cliquez sur Gestion TPM pour afficher les détails sur la puce TPM (voir l'illustration).

BitLocker To Go chiffre les lecteurs amovibles. BitLocker To Go n'utilise pas de puce TPM, mais il propose un chiffrement des données et nécessite un mot de passe.

Sauvegardes des données et du système

Une perte de données peut se produire en cas de vol perpétré par un cybercriminel, en raison d'une défaillance matérielle ou encore à la suite d'un sinistre. Il est donc important d'effectuer régulièrement une sauvegarde des données.

Une sauvegarde des données stocke une copie des informations d'un ordinateur sur des supports de sauvegarde amovibles. L'opérateur stocke ensuite les supports de sauvegarde dans un endroit sûr. La sauvegarde des données est l'un des moyens de protection les plus efficaces contre la perte de données. En cas de panne matérielle, l'utilisateur peut restaurer les données de sauvegarde, une fois le système de nouveau opérationnel.

La politique de sécurité de l'entreprise doit inclure des sauvegardes des données. Les utilisateurs doivent effectuer des sauvegardes des données régulières. Les sauvegardes sont généralement stockées en dehors des installations, afin de protéger le support de sauvegarde en cas de sinistre dans le bâtiment principal.

Voici quelques considérations sur les sauvegardes de données :

* Fréquence : une sauvegarde peut nécessiter beaucoup de temps. Il est parfois plus facile d'effectuer une sauvegarde complète tous les mois ou toutes les semaines, puis de configurer des sauvegardes partielles et fréquentes des données qui ont été modifiées depuis la dernière sauvegarde complète. Toutefois, si vous devez restaurer les données, le fait de disposer d'un grand nombre de sauvegardes partielles augmentera la durée nécessaire à la restauration.
* Stockage : pour plus de sécurité, les sauvegardes doivent être stockées sur un site dédié et agréé. Le transfert des sauvegardes doit être effectué une fois par jour, par semaine ou par mois, conformément à la politique de sécurité.
* Sécurité : protégez les sauvegardes à l'aide de mots de passe. L'opérateur doit alors saisir un mot de passe avant de restaurer les données stockées sur les supports de sauvegarde.
* Validation : les sauvegardes doivent impérativement être vérifiées afin de garantir l'intégrité des données.

Le contrôle et le blocage du contenu

Un logiciel de contrôle du contenu limite le contenu auquel un utilisateur peut accéder sur Internet à l'aide d'un navigateur web. Le logiciel de contrôle du contenu peut bloquer les sites composés de certains types de contenus, comme la pornographie et des informations politiques ou religieuses controversées. Un parent peut activer un logiciel de contrôle du contenu sur l'ordinateur utilisé par un enfant. Les bibliothèques et les écoles peuvent également implémenter ce type de logiciel pour empêcher tout accès à du contenu considéré comme répréhensible.

Un administrateur peut implémenter les types de filtres suivants :

* Filtres basés sur le navigateur à l'aide d'une extension de navigateur tierce
* Filtres de messagerie via un filtre client ou serveur
* Filtres côté client installés sur un ordinateur spécifique
* Filtres de contenu basés sur le routeur qui bloquent tout trafic entrant sur le réseau
* Filtrage du contenu basé sur l'appliance, semblable au filtrage basé sur le routeur
* Filtrage du contenu basé dans le cloud

Les moteurs de recherche tels que Google offrent la possibilité d'activer un filtre de sécurité afin d'exclure les liens inappropriés des résultats de la recherche.

Cliquez [ici](https://en.wikipedia.org/wiki/Comparison_of_content-control_software_and_providers) pour comparer les différents éditeurs de logiciels de contrôle du contenu.

Le clonage des disques et Deep Freeze

De nombreuses applications tierces capables de restaurer un système sont disponibles. Cela permet à l'administrateur de protéger le système d'exploitation et les fichiers de configuration d'un système.

Le clonage des disques copie le contenu du disque dur d'un ordinateur dans un fichier image. Un administrateur peut, par exemple, créer les partitions requises sur un système, formater une partition, puis installer le système d'exploitation. Puis il installe le logiciel requis et configure tout le matériel. Ensuite, il utilise le logiciel de clonage de disque pour créer le fichier image. Il peut utiliser l'image clonée comme suit :

* Pour nettoyer automatiquement un système et restaurer une image principale « propre »
* Pour déployer de nouveaux ordinateurs au sein de l'entreprise
* Pour fournir une sauvegarde complète du système

Cliquez [ici](https://en.wikipedia.org/wiki/Comparison_of_disk_cloning_software) pour comparer les différents logiciels de clonage de disque.

Deep Freeze « gèle » la partition du disque dur. Lorsqu'un utilisateur redémarre le système, ce dernier rétablit sa configuration gelée. Le système n'enregistre pas les modifications apportées par l'utilisateur, toutes les applications installées ou tous les fichiers sauvegardés sont donc perdus au redémarrage du système.

S'il s'avère nécessaire de modifier la configuration du système, l'administrateur doit d'abord « libérer » la partition protégée en désactivant Deep Freeze. Une fois les modifications effectuées, il doit réactiver le programme. L'administrateur peut configurer Deep Freeze de sorte qu'il redémarre après la déconnexion d'un utilisateur, qu'il s'arrête après une période d'inactivité ou encore qu'il s'arrête à une heure planifiée.

Ces produits n'offrent pas de protection en temps réel. Un système reste vulnérable jusqu'à ce qu'un utilisateur ou un événement planifié le redémarre. Cependant, dans le cas d'un système infecté par du code malveillant, le système redémarrera sain la prochaine fois.

Câbles de sécurité et verrous

Il existe plusieurs méthodes de protection physique des ordinateurs :

* Utilisez des câbles antivol sur l'équipement (voir Figure 1).
* Gardez les salles de télécommunications fermées à clé.
* Installez des cages de sécurité autour des équipements.

De nombreux appareils portables et moniteurs d'ordinateur coûteux sont pourvus d'une encoche de sécurité en acier utilisable avec des câbles antivol.

Le verrou à clé est le type de dispositif de verrouillage de porte le plus courant. Il ne se verrouille pas automatiquement lorsque la porte se ferme. De plus, il suffit de glisser une fine carte plastique, comme une carte de crédit, entre le verrou et l'encadrement de porte pour forcer l'ouverture. Les serrures des portes des bâtiments commerciaux sont différentes de celles utilisées pour les immeubles résidentiels. Un pêne dormant est ainsi utilisé pour garantir une sécurité accrue. L'utilisation de serrures à clé présente toutefois un problème de sécurité en cas de perte, de vol ou de duplication des clés.

Dans le cas d'une serrure à code (voir la Figure 2), l'utilisateur doit appuyer sur des boutons dans un ordre bien précis pour ouvrir la porte. Ce type de serrure peut être programmé. Cela signifie que le code d'un utilisateur peut ne fonctionner que certains jours ou à certaines heures. Il se peut, par exemple, qu'une serrure à code autorise Bob à accéder à la salle des serveurs seulement entre 7h00 et 18h00 du lundi au vendredi. Les serrures à code peuvent également conserver un historique des ouvertures de la porte, ainsi que du code utilisé pour l'ouvrir.

# Délais avant déconnexion

Un employé se lève et quitte son poste de travail pour faire une pause. Si ce collaborateur ne prend pas de mesures pour protéger son poste de travail, toutes les informations qu'il contient sont vulnérables et peuvent tomber entre les mains d'un intrus. Une entreprise peut prendre les mesures suivantes pour prévenir les accès non autorisés :

Délai d'inactivité et verrouillage de l'écran

Les employés peuvent choisir de se déconnecter ou non de leur ordinateur lorsqu'ils quittent leur poste de travail. Par conséquent, il est recommandé, pour des raisons de sécurité, de configurer un minuteur d'inactivité qui déconnecte automatiquement l'utilisateur et bloque l'écran après une période donnée. L'utilisateur doit se reconnecter pour déverrouiller l'écran.

Horaires de connexion

Dans certains cas, une entreprise peut imposer des plages de connexion pour ses employés ; entre 7h00 et 18h00, par exemple. Ce faisant, le système bloquera toute tentative de connexion en dehors de ces heures.

# Suivi GPS

Le système de localisation GPS utilise des satellites et des ordinateurs pour déterminer la position d'un appareil. La technologie GPS est une fonctionnalité standard sur les smartphones pour fournir un suivi de position en temps réel. Le GPS peut localiser un emplacement à 100 mètres près. Cette technologie est disponible pour le suivi des enfants, des personnes âges, des animaux familiers et des véhicules. Cependant, utiliser le GPS pour localiser un téléphone portable sans l'autorisation de l'utilisateur est considéré comme une atteinte à la vie privée et, de ce fait, est une pratique illégale.

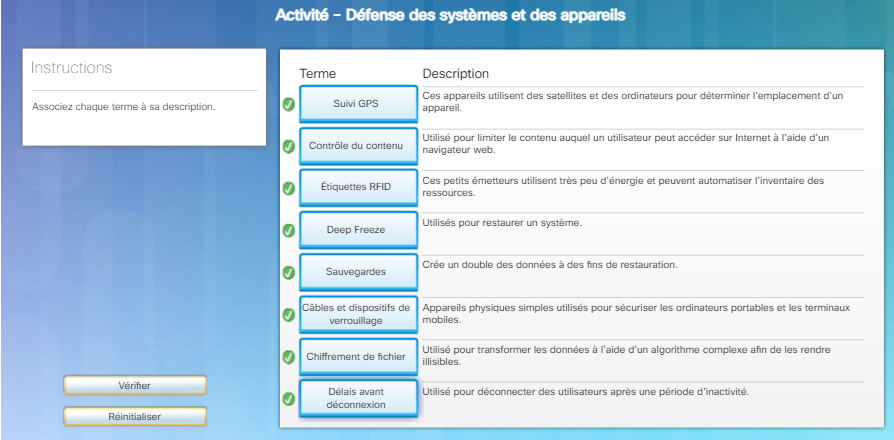
De nombreuses applications de téléphone portable utilisent le suivi par GPS pour repérer la position d'un appareil. Facebook, par exemple, permet aux utilisateurs de signaler leur présence à un endroit ; cette information est alors visible par tous les membres de leurs réseaux.

# Inventaire et étiquettes RFID

La technologie d'identification par radiofréquence (RFID) utilise des ondes radio pour l'identification et le suivi des objets. Les systèmes d'inventaire RFID consistent à installer des balises sur tous les éléments que l'entreprise souhaite suivre. Les étiquettes contiennent un circuit intégré qui se connecte à une antenne. De par leur petite taille, les étiquettes utilisent très peu d'énergie. Elles n'ont donc pas besoin de batterie pour stocker les informations à échanger avec un lecteur. La technologie RFID peut automatiser le suivi de ressources ou permettre le verrouillage, le déverrouillage ou la configuration sans fil d'appareils électroniques.

Les systèmes RFID fonctionnent sous différentes fréquences. Les systèmes à basse fréquence ont une portée en lecture et des débits de lecture de données plus faibles, mais ils sont moins sensibles aux interférences radioélectriques causées par les liquides et les métaux que les systèmes à haute fréquence.

# Défenses des systèmes et des appareils



# Gestion des accès à distance

Le concept d'accès à distance fait référence à une combinaison de composants matériels et logiciels permettant d'accéder, à distance, à un réseau interne local.

Avec le système d'exploitation Windows, les techniciens peuvent utiliser les fonctionnalités Bureau à distance et Assistance à distance pour réparer et mettre à niveau des ordinateurs. Le Bureau à distance (voir l'illustration) permet aux techniciens de voir et de contrôler un ordinateur à distance. L'assistance à distance permet aux techniciens d'aider les clients qui rencontrent des problèmes. L'assistance à distance permet également au client de visualiser la réparation ou la mise à niveau en temps réel sur son écran.

La procédure d'installation de Windows n'active pas le Bureau à distance par défaut. L'activation de cette fonctionnalité ouvre le port 3389 (RDP Remote Desktop Protocol) et peut entraîner une vulnérabilité si un utilisateur n'a pas besoin de ce service.

# Telnet, SSH et SCP

Secure Shell (SSH) est un protocole qui permet d'établir une connexion sécurisée (chiffrée) pour la gestion des périphériques distants. SSH doit remplacer Telnet pour les connexions de gestion. Telnet est un protocole plus ancien qui utilise un mode de transmission en texte clair non sécurisé des informations d'identification (nom d'utilisateur et mot de passe) et des données entre les périphériques. SSH permet de sécuriser les connexions distantes grâce à une méthode de chiffrement fort lors de l'authentification d'un appareil (nom d'utilisateur et mot de passe), mais aussi pour la transmission des données entre les appareils qui communiquent. SSH utilise le port TCP 22. Telnet utilise le port TCP 23.

Dans la Figure 1, les cybercriminels utilisent Wireshark pour surveiller les paquets. Dans la Figure 2, les cybercriminels peuvent visualiser le nom d'utilisateur et le mot de passe de l'administrateur à partir de la session Telnet.

La Figure 3 présente une session SSH vue depuis Wireshark. Les cybercriminels effectuent le suivi de la session à l'aide de l'adresse IP de l'appareil de l'administrateur mais, dans la Figure 4, la capture montre que le nom d'utilisateur et le mot de passe sont chiffrés.

Le protocole SCP (Secure copy) transfère les fichiers informatiques en toute sécurité entre deux systèmes distants. SCP utilise SSH pour le transfert de données (notamment l'élément d'authentification), ce qui lui permet d'assurer l'authenticité et la confidentialité des données en transit.

# Sécurisation des ports et des services

Les cybercriminels exploitent les services qui s'exécutent sur un système, car ils savent que la plupart des appareils exécutent plus de services ou de programmes que nécessaire. Un administrateur doit analyser chaque service pour vérifier qu'il est bien nécessaire et évaluer ses risques. Il est obligatoire de désactiver tous les services inutiles.

Une méthode simple à laquelle nombre d'administrateurs ont recours pour mieux protéger le réseau contre tout accès non autorisé est de désactiver tous les ports qui ne sont pas exploités sur un commutateur. Par exemple, si un commutateur Cisco est doté de 24 ports et si trois connexions Fast Ethernet sont utilisées, il est conseillé de désactiver les 21 ports inutilisés.

Le processus d'activation et de désactivation des ports peut être long, mais il renforce la sécurité sur le réseau et en vaut vraiment la peine.

Comptes avec privilèges

Les cybercriminels exploitent les comptes avec privilèges, car il s'agit des comptes les plus puissants au sein de l'entreprise. Les comptes disposant de privilèges ont les informations d'identification permettant d'accéder aux systèmes et offrent un accès élevé et non limité. Les administrateurs utilisent ces comptes pour déployer et gérer des systèmes d'exploitation, des applications et des appareils réseau. Cette illustration présente une synthèse des types de comptes avec privilèges.

L'entreprise doit adopter les bonnes pratiques suivantes pour sécuriser les comptes avec privilèges :

* Identifier les comptes avec privilèges et réduire leur nombre
* Appliquer le principe de « privilège minimal »
* Mettre en place un processus de révocation des droits lorsque des employés quittent l'entreprise ou changent de poste
* Éliminer les comptes partagés associés à des mots de passe sans date d'expiration
* Sécuriser le stockage des mots de passe
* Éliminer les informations d'identification partagées pour plusieurs administrateurs
* Modifier automatiquement les mots de passe des comptes avec privilèges tous les 30 ou 60 jours
* Enregistrer les sessions avec privilèges
* Mettre en place un processus de modification des mots de passe intégrés pour les scripts et les comptes de service
* Consigner toutes les activités des utilisateurs
* Générer des alertes en cas de comportement inhabituel
* Désactiver les comptes avec privilèges inactifs
* Utiliser une authentification multifacteur pour tous les accès administratifs
* Mettre en place une passerelle entre l'utilisateur final et les ressources sensibles afin de limiter l'exposition du réseau aux malwares

Il est essentiel de verrouiller les comptes avec privilèges pour assurer la sécurité de l'entreprise. Il doit s'agir d'un processus continu. L'entreprise doit évaluer ce processus en vue d'effectuer les éventuels ajustements nécessaires pour améliorer la sécurité.

# Politiques de groupe

Dans la plupart des réseaux composés d'ordinateurs Windows, l'administrateur configure Active Directory avec des domaines sur Windows Server. Les ordinateurs Windows sont membres d'un domaine. L'administrateur configure une stratégie de sécurité du domaine qui s'applique à tous les ordinateurs qui le rejoignent. Les stratégies de compte sont automatiquement définies dès que l'utilisateur ouvre une session Windows.

Si un ordinateur ne fait pas partie d'un domaine Active Directory, l'utilisateur configure les politiques à l'aide de l'outil Stratégie de sécurité locale de Windows. Dans toutes les versions de Windows, à l'exception de l'édition familiale, dans la zone Exécuter saisissez secpol.msc pour ouvrir l'outil Stratégie de sécurité locale.

L'administrateur configure les stratégies de comptes d'utilisateurs, telles que celles relatives au mot de passe et au verrouillage, en sélectionnant Stratégies de comptes > Stratégie de mot de passe. Lorsque les paramètres illustrés à la Figure 1 sont actifs, les utilisateurs doivent modifier leur mot de passe tous les 90 jours et utiliser le nouveau mot de passe pendant au moins un (1) jour. Les mots de passe doivent comporter huit (8) caractères et répondre aux critères de complexité suivants : lettres majuscules, lettres minuscules, chiffres et symboles. Enfin, le nombre de mots de passe mémorisés est de 24, donc un utilisateur pourra employer le même mot de passe la 25ème fois.

Une politique de verrouillage du compte bloque un ordinateur pendant une période configurée si le nombre de tentatives de connexion ayant échoué est trop élevé. Par exemple, la stratégie illustrée à la Figure 2 autorise l'utilisateur à entrer cinq fois un mauvais nom d'utilisateur ou mot de passe. Après cinq tentatives, le compte utilisateur sera verrouillé pendant 30 minutes. Au bout de ces 30 minutes, le nombre de tentatives est remis à zéro et l'utilisateur peut à nouveau essayer d'ouvrir une session.

D'autres paramètres de sécurité sont disponibles en ouvrant le dossier Stratégies locales. Une politique d'audit crée un fichier journal de sécurité utilisé dans le cadre du suivi des événements (voir Figure 3).

Activer les journaux et les alertes

Un administrat enregistre tous les événements à mesure qu'ils se produisent. Un fichier journal se compose d'entrées qui contiennent toutes les informations relatives à un événement spécifique. Les journaux qui traitent de la sécurité informatique ont pris de plus en plus d'importance.

Par exemple, un journal d'audit consigne les tentatives d'authentification des utilisateurs, tandis qu'un journal d'accès fournit toutes les informations relatives à des demandes de fichiers spécifiques sur un système. La surveillance des journaux système permet de déterminer comment une attaque s'est produite, ainsi que l'efficacité des moyens de protection mis en œuvre.

Face à l'augmentation du nombre de fichiers journaux générés dans le cadre de la sécurité informatique, l'entreprise doit envisager la mise en place d'un processus de gestion des évènements. Ce type de gestion détermine le processus à appliquer pour la génération, la transmission, le stockage, l'analyse et l'élimination des données de journal de sécurité informatique.

Journaux du système d'exploitation

Les journaux du système d'exploitation enregistrent les événements qui sont générés par les opérations effectuées par le système d'exploitation. Les événements système sont les suivants :

* Requêtes de clients et réponses du serveur, comme les authentifications des utilisateurs ayant réussi
* Informations sur l'utilisation contenant le nombre et la taille des transactions sur une période donnée

Journaux de sécurité des applications

Les entreprises utilisent des logiciels de sécurité basés sur le réseau ou sur le système pour détecter les activités malveillantes. Ces logiciels génèrent un journal de sécurité pour fournir des données de sécurité informatique. Ces journaux sont utiles pour effectuer des analyses d'audit et pour identifier les tendances et les problèmes à long terme. Ils permettent également à l'entreprise de fournir une documentation attestant du respect des exigences réglementaires et lois en vigueur.

Alimentation

Les questions liées à l'alimentation et aux systèmes d'alimentation électrique sont cruciales dans le cadre de la protection des systèmes d'information. Une alimentation électrique constante est indispensable sur les sites regroupant d'imposants serveurs et systèmes de stockage des données. Voici quelques règles à suivre pour déployer des systèmes d'alimentation électrique efficaces :

* Les data centers doivent être raccordés à une alimentation différente de celle du bâtiment
* Sources d'alimentation redondantes : plusieurs flux provenant de plusieurs sous-stations
* Gestion de l'alimentation
* L'utilisation de systèmes d'alimentation de secours est généralement nécessaire
* Une unité d'alimentation permanente (UPS) doit être disponible pour permettre un arrêt normal des systèmes en cas de coupure électrique

Lors de la conception de systèmes d'alimentation électrique, l'entreprise doit se prémunir contre divers problèmes auxquels elle pourrait faire face.

Surplus de puissance

* Pointe : haute tension de courte durée
* Surtension : haute tension sur une période prolongée

Perte de puissance

* Défaut : perte de puissance momentanée
* Panne de courant : perte totale d'alimentation

Diminution de la puissance

* Microcoupure/creux : baisse de tension de courte durée
* Baisse de tension : baisse de tension prolongée
* Courant d'appel : saut de puissance à l'initialisation du système

# Chauffage, ventilation et climatisation (CVC)

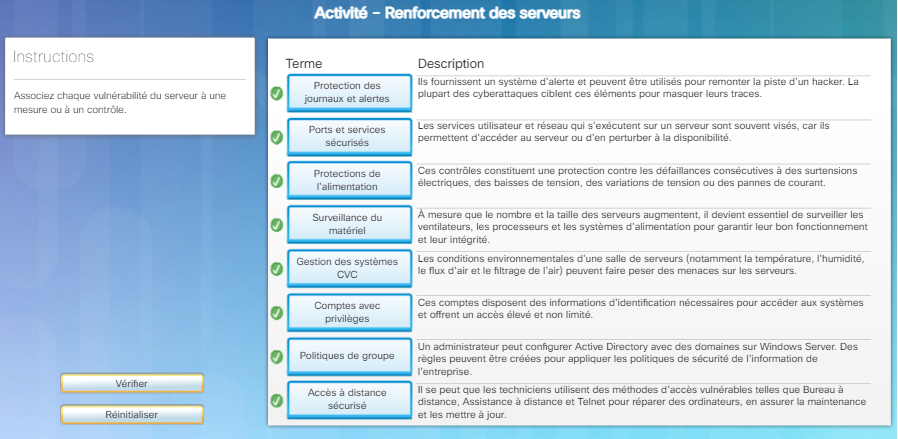
Les systèmes de chauffage, de ventilation et de climatisation (CVC) sont essentiels pour garantir la sécurité des personnes et des systèmes d'information au sein des installations de l'entreprise. Lorsque vous concevez des sites IT modernes, ces systèmes jouent un rôle primordial dans la sécurité globale. Les systèmes d'air conditionné contrôlent l'environnement ambiant (température, humidité, flux d'air et filtrage de l'air) et doivent être prévus pour fonctionner avec les autres composants du data center, comme le matériel informatique, le câblage, les systèmes de stockage des données, de protection incendie, de sécurité physique et d'électricité. Pratiquement tous les équipements informatiques ont des d'exigences concernant les plages d'humidité et les températures acceptables, celles-ci sont formulées dans un document reprenant les caractéristiques du produit ou dans un guide d'installation. Il est essentiel de respecter ces exigences pour éviter les défaillances systèmes et prolonger leur durée de vie. Les systèmes CVC en vente dans le commerce et les autres systèmes de gestion des immeubles se connectent désormais à Internet pour permettre un contrôle et une surveillance à distance. Les événements récents ont montré que ces systèmes (désignés souvent sous le nom de « systèmes intelligents ») avaient également d'importantes implications sur le plan de la sécurité.

L'un des risques associés aux systèmes intelligents est que les personnes qui accèdent au système et en assurent la gestion travaillent pour le compte d'un sous-traitant ou d'un tiers. Les techniciens CVC doivent être en mesure d'accéder rapidement aux informations. C'est pourquoi les données vitales sont généralement stockées dans plusieurs emplacements, ce qui les rend accessibles à un nombre encore plus important de personnes. De ce fait, un vaste réseau de personnes, y compris les associés des sous-traitants, peut avoir accès aux informations d'un système CVC. L'interruption de ces systèmes peut présenter des risques non négligeables pour la sécurité des informations de l'entreprise.

# Surveillance du matériel

La surveillance du matériel est une pratique courante au sein des data centers. Un data center (ferme ou batterie de serveurs) est un site qui héberge des centaines ou des milliers de serveurs pour différentes entreprises. Google gère de nombreuses batteries de serveurs réparties aux quatre coins du globe pour fournir un service optimal. Même les petites entreprises commencent à construire des batteries de serveurs locales pour héberger le nombre croissant de serveurs dont elles ont besoin dans le cadre de leurs activités. Les systèmes de surveillance du matériel sont conçus pour contrôler l'intégrité du matériel et ainsi limiter les interruptions des applications et des serveurs. Les systèmes de surveillance du matériel modernes utilisent des ports réseau et USB pour transmettre des informations telles que la température du processeur, l'état de l'alimentation, la température et la vitesse du ventilateur, l'état de la mémoire, l'espace disque ou encore l'état de la carte réseau. Grâce à ces solutions, un technicien peut surveiller des centaines, voire des milliers de systèmes à partir d'un seul terminal. Parallèlement à l'augmentation du nombre de batteries de serveurs, les systèmes de surveillance du matériel se sont imposés comme une mesure de sécurité essentielle.

# Renforcement des serveurs



# Centres d'opération

Un centre d'exploitation du réseau (NOC) se compose d'un ou de plusieurs sites regroupant les outils qui offrent aux administrateurs un état détaillé du réseau de l'entreprise. Le centre d'exploitation du réseau représente l'épicentre de nombreuses opérations : dépannage du réseau, surveillance de la performance, distribution et mise à jour des logiciels, et gestion des communications et des appareils.

Le centre d'opérations de sécurité (SOC) est un site dédié qui surveille, évalue et protège les systèmes informatiques de l'entreprise, tels que les sites web, les applications, les bases de données, les data centers, les réseaux, les serveurs et les systèmes des utilisateurs. Un SOC se compose d'une équipe d'analystes de la sécurité chargés de détecter les incidents de cybersécurité, de les analyser, d'y répondre, de dresser des rapports à leur sujet et de les prévenir.

Ces deux entités utilisent une structure hiérarchique pour traiter les événements. Le personnel du premier niveau traite tous les événements et transmet au niveau supérieur ceux qui ne peuvent pas être résolus. Le personnel du niveau 2 examine l'événement en profondeur pour tenter de remédier au problème. Si aucune solution ne peut être trouvée, l'événement est transmis aux experts du niveau 3.

Pour mesurer l'efficacité globale d'un centre d'opérations, l'entreprise organise des exercices réalistes. Un exercice structuré de simulation sur une maquette est un entraînement réalisé par l'équipe pour simuler un événement et évaluer l'efficacité du centre. Une autre action possible, plus efficace consiste à simuler une véritable intrusion sans avertir les équipes. Pour cela, on a recours aux services d'une Red Team (un groupe indépendant de personnes qui testent les processus d'une entreprise) pour évaluer l'efficacité du service. La Red Team doit, par exemple, cibler un système critique en incluant la reconnaissance et l'attaque, l'élévation des privilèges et l'accès à distance.

# Commutateurs, routeurs et appliances réseau

Les appareils réseau sont soit livrés sans aucun mot de passe, soit avec un mot de passe défini par défaut. Avant de connecter un quelconque appareil au réseau, vous devez modifier le mot de passe par défaut. Prenez note des modifications apportées aux appareils réseau et consignez-les dans un fichier journal. Pour terminer, examinez tous les journaux de configuration.

Dans les sections suivantes, il est question des mesures qu'un administrateur peut prendre pour protéger les périphériques réseau.

Commutateurs

Les commutateurs sont au cœur des réseaux de données modernes. Les principales menaces qui pèsent sur les commutateurs réseau sont le vol, le piratage et l'accès à distance, les attaques contre des protocoles réseaux comme ARP/STP ou des attaques contre la performance et la disponibilité (DOS Déni de Service). Plusieurs contre-mesures et contrôles peuvent protéger les commutateurs réseau. Il s'agit notamment d'une sécurité physique accrue, d'une configuration avancée ou encore de l'implémentation de correctifs et de mises à jour du système suivant les besoins. La mise en œuvre de la sécurité des ports constitue un autre contrôle efficace. Un administrateur doit sécuriser tous les ports (interfaces) du commutateur avant de déployer ce dernier à des fins de production. L'une des méthodes de sécurisation des ports consiste à implémenter une fonctionnalité appelée sécurité des ports, celle-ci restreint le nombre d'adresses MAC autorisées sur un port. Le commutateur accordera l'accès à tous les appareils qui possèdent une adresse MAC autorisée, tout en refusant les autres.

VLAN

Les VLAN permettent de regrouper des appareils au sein d'un LAN et sur des commutateurs individuels. Les VLAN utilisent des connexions logiques au lieu de connexions physiques. Certains ports d'un commutateur peuvent être attribués à un VLAN spécifique. D'autres ports peuvent être utilisés pour interconnecter physiquement des commutateurs et autoriser le trafic de plusieurs VLAN entre ces commutateurs. Ces ports sont désignés sous le nom de « trunks ».

Supposons que le service des ressources humaines (RH) doive protéger des données sensibles. Les VLAN permettent à un administrateur de segmenter les réseaux selon des facteurs tels que la fonction, l'équipe de projet ou l'application, quel que soit l'emplacement physique de l'utilisateur ou de l'appareil (voir Figure 1). Les appareils d'un VLAN se comportent comme s'ils se trouvaient chacun sur leur propre réseau indépendant, même s'ils partagent une infrastructure commune avec d'autres VLAN. Un VLAN peut isoler des groupes qui comportent des données sensibles du reste du réseau, réduisant ainsi les risques de compromission des informations confidentielles. Les trunks permettent aux utilisateurs du VLAN RH d'être connectés physiquement à plusieurs commutateurs.

Il existe une multitude de types d'attaques et de vulnérabilités du VLAN, dont les attaques ciblant le protocole VTP (VLAN Trunking Protocol). La description de ce type d'attaque n'entre pas dans le cadre de ce cours. Les hackers peuvent également cibler la disponibilité et les performances du VLAN. Les contre-mesures courantes consistent à surveiller les performances et les modifications du VLAN, à opter pour des configurations avancées ou encore à appliquer des correctifs système et des mises à jour régulières à IOS.

Pare-feu

Les pare-feu sont des solutions logicielles ou matérielles permettant de mettre en œuvre des stratégies de sécurité du réseau. Un pare-feu filtre le trafic non autorisé ou potentiellement dangereux, l'empêchant ainsi d'accéder au réseau (Figure 2). Un pare-feu de base fournit des fonctionnalités basiques de filtrage du trafic à l'aide de listes de contrôle d'accès (ACL). Les administrateurs utilisent des listes de contrôle d'accès pour bloquer le trafic ou n'autoriser qu'un trafic spécifique sur leurs réseaux. Une liste de contrôle d'accès est un ensemble séquentiel d'instructions d'autorisation ou de refus qui s'appliquent à des adresses ou des protocoles. Les listes de contrôle d'accès représentent un outil puissant pour contrôler le trafic entrant ou sortant d'un réseau. Les pare-feu protègent un réseau privé des attaques venant de l'extérieur. Ils sont fréquemment la cible des hackers qui tentent de mettre en échec leurs protections. Les principales menaces qui pèsent sur les pare-feu sont le vol, le piratage et l'accès à distance, les attaques visant les listes de contrôle d'accès (ACL) ou encore les attaques contre la performance et la disponibilité. Plusieurs contre-mesures et contrôles peuvent protéger les pare-feu. Il s'agit notamment d'une sécurité physique accrue, d'une configuration avancée, d'une authentification et d'un accès à distance sécurisés ou encore de l'implémentation de correctifs et de mises à jour du système suivant les besoins.

Routeurs

Les routeurs forment l'ossature d'Internet et des communications établies entre les différents réseaux. Les routeurs communiquent les uns avec les autres pour identifier le meilleur chemin pour acheminer le trafic entre les différents réseaux. Les routeurs utilisent des protocoles de routage pour prendre ce genre de décisions. Les routeurs peuvent également intégrer d'autres services, tels que des fonctionnalités de commutation et de pare-feu, ce qui en fait une cible privilégiée des hackers. Les principales menaces qui pèsent sur les routeurs réseau sont le vol, le piratage et l'accès à distance, les attaques contre des protocoles de routage comme RIP/OSPF ou encore les attaques contre la performance et la disponibilité. Plusieurs contre-mesures et contrôles peuvent protéger les routeurs réseau. Il s'agit notamment d'une sécurité physique accrue, de paramètres de configuration avancés, de l'utilisation de protocoles de routage sécurisés avec authentification ou encore de l'implémentation de correctifs et de mises à jour du système suivant les besoins.

Périphériques sans fil et mobiles

Les terminaux mobiles et sans fil se sont généralisés au sein de la plupart des réseaux modernes. Ils favorisent la mobilité et se révèlent bien pratiques, mais ils sont extrêmement vulnérables. Ils sont notamment sujets au vol, au piratage et aux accès à distance non autorisés, aux interceptions, aux attaques de l'homme du milieu et aux attaques contre la performance et la disponibilité. Le meilleur moyen de sécuriser un réseau sans fil consiste à utiliser des systèmes d'authentification et de chiffrement. Le standard sans fil initial, 801.11, comportait deux types d'authentification, comme illustré sur cette figure :

* Authentification Open system - N'importe quel appareil sans fil peut se connecter au réseau sans fil. Utilisez cette méthode lorsque la sécurité ne constitue pas une préoccupation.
* Authentification Shared key - Fournit des mécanismes pour authentifier et chiffrer les données entre un client sans fil et un point d'accès ou un routeur sans fil.

Les trois techniques d'authentification par clé partagée (Shared key) pour les réseaux locaux sans fil sont les suivantes :

* Wired Equivalent Privacy (WEP) - Premier protocole de sécurité 802.11 pour les réseaux locaux sans fil. Toutefois, la clé de chiffrement ne change jamais lors de l'échange des paquets, ce qui la rend facile à pirater.
* WPA (Wi-Fi Protected Access) - Norme utilisant la technologie WEP, mais qui sécurise les données à l'aide d'un algorithme de chiffrement TKIP (Temporal Key Integrity Protocol) bien plus robuste. Le protocole TKIP modifie la clé pour chaque paquet, rendant très difficile son piratage.
* IEEE 802.11i/WPA2 - IEEE 802.11i est la norme industrielle de sécurisation des réseaux sans fil. 802.11i et WPA2 utilisent tous deux la norme AES (Advanced Encryption Standard) pour le chiffrement ; il s'agit, à l'heure actuelle, du protocole de chiffrement le plus puissant.

Depuis 2006, tout périphérique portant le logo de certification Wi-Fi est également certifié WPA2. Les réseaux sans fil modernes doivent toujours utiliser la norme 802.11i/WPA2. Les autres contre-mesures possibles incluent l'amélioration de la sécurité physique, mais aussi l'installation régulière des mises à jour et correctifs système.

# Services réseau et de routage

Les cybercriminels ciblent les services réseau vulnérables pour attaquer un appareil ou l'utiliser dans le cadre de l'attaque. Pour vérifier l'existence de services réseau non sécurisés, recherchez les ports ouverts d'un appareil à l'aide d'un scanner de ports. Il s'agit d'une application qui sonde un appareil à la recherche de ports ouverts en envoyant un message à chaque port et en attendant une réponse. Cette réponse indique la manière dont le port est utilisé. Les cybercriminels utilisent des scanners de ports dans le même but. En protégeant les services réseau, vous êtes certain que seuls les ports nécessaires sont exposés et disponibles.

Protocole DHCP (Dynamic Host Configuration Protocol)

Le protocole DHCP utilise un serveur pour attribuer automatiquement une adresse IP et d'autres informations de configuration aux périphériques réseau. En réalité, l'appareil reçoit du serveur DHCP la permission d'utiliser le réseau. Les hackers peuvent cibler les serveurs DHCP afin de refuser l'accès au réseau de tous les périphériques. La Figure 1 présente une liste des contrôles de sécurité à appliquer pour le protocole DHCP

Système DNS (Domain Name System)

Ce service traduit en adresse IP du site une URL (Uniform Resource Locator) ou adresse de site web (http://www.cisco.com). Lorsqu'un utilisateur saisit une adresse web dans la barre d'adresse, il s'en remet aux serveurs DNS pour résoudre l'adresse IP réelle de cette destination. Les hackers peuvent cibler les serveurs DNS afin de refuser l'accès aux ressources réseau ou de rediriger le trafic vers des sites web non autorisés. Cliquez sur la Figure 2 pour afficher une liste des contrôles de sécurité pour le service DNS. Utilisez une authentification et un service sécurisés entre les serveurs DNS pour les protéger contre ces attaques.

Protocole ICMP (Internet Control Messaging Protocol)

Les appareils réseau utilisent le protocole ICMP pour envoyer des messages d'erreur tels que l'indisponibilité d'un service demandé ou l'impossibilité pour l'hôte d'accéder au routeur. La commande Ping est un utilitaire réseau qui utilise le protocole ICMP pour tester l'accessibilité d'un hôte sur un réseau. Elle envoie des messages ICMP à l'hôte et attend une réponse. Les cybercriminels peuvent utiliser le protocole ICMP dans le but de nuire (voir la Figure 3). Les attaques par déni de service utilisent le protocole ICMP. De nombreux réseaux filtrent donc certaines requêtes ICMP pour empêcher ce type d'attaque.

Protocole RIP (Routing Information Protocol)

Le protocole RIP limite le nombre de sauts autorisés entre la source et la destination sur le réseau. Le nombre maximum de sauts autorisés est de 15. RIP est un protocole utilisé pour échanger des informations de routage sur les réseaux que chaque routeur peut atteindre, ainsi que sur la distance qui sépare ces réseaux. Le protocole RIP calcule le meilleur itinéraire en fonction du nombre de sauts. La Figure 4 répertorie les vulnérabilités du protocole RIP et les techniques de protection contre les attaques par protocole RIP. Les hackers peuvent cibler les routeurs et le protocole RIP. Les attaques visant les services de routage peuvent nuire aux performances et à la disponibilité. Certaines attaques peuvent même entraîner une redirection du trafic. Utilisez des services sécurisés avec authentification, et appliquez des mises à jour et des correctifs système pour protéger les services de routage tels que le protocole RIP.

Protocole NTP (Network Time Protocol)

L'utilisation d'une heure correcte sur un réseau est particulièrement importante. Des horodatages exacts permettent de suivre avec précision les événements réseau tels que les violations de sécurité. Par ailleurs, la synchronisation des horloges est critique pour la bonne interprétation des événements au sein des fichiers de données Syslog, ainsi que pour les certificats numériques.

Le protocole NTP synchronise les horloges des systèmes informatiques sur des réseaux de données. Le protocole NTP permet aux périphériques réseau de synchroniser leurs paramètres de temps avec un serveur NTP. La Figure 5 présente les diverses méthodes utilisées pour garantir une synchronisation sécurisée pour le réseau. Les cybercriminels attaquent les serveurs de temps pour perturber les communications sécurisées qui dépendent de certificats numériques et pour masquer les informations d'horodatage sur les attaques.

Matériel VoIP

Le VoIP utilise des réseaux tels qu'Internet pour passer et recevoir des appels téléphoniques. Pour bénéficier du VoIP, vous devrez vous équiper d'une connexion Internet et d'un téléphone. Plusieurs options sont disponibles en ce qui concerne le combiné téléphonique :

* Téléphone traditionnel avec adaptateur (l'adaptateur fait office d'interface matérielle entre un téléphone analogique classique et une ligne VoIP numérique)
* Téléphone compatible VoIP
* Logiciel VoIP installé sur un ordinateur

Avec la plupart des services VoIP grand public, Internet est utilisé pour les appels téléphoniques. Cependant, de nombreuses entreprises utilisent leurs réseaux privés, car ils offrent une sécurité renforcée et une meilleure qualité de service. Le niveau de sécurité du VoIP est déterminé par celui du réseau sous-jacent. Les cybercriminels ciblent ces systèmes afin de bénéficier de services téléphoniques gratuits, de pratiquer des écoutes clandestines ou encore de nuire aux performances et à la disponibilité.

Vous pouvez appliquer les contre-mesures suivantes pour sécuriser le VoIP :

* Chiffrer les paquets de messages vocaux pour vous protéger contre les écoutes clandestines.
* Utiliser le protocole SSH pour protéger les passerelles et les commutateurs.
* Modifier tous les mots de passe par défaut.
* Utiliser un système de détection d'intrusions pour détecter des attaques telles que l'ARP poisoning.
* Utiliser une authentification renforcée pour réduire les risques de mystification d'enregistrement (les cybercriminels redirigent vers eux tous les appels entrants destinés à leur victime), d'usurpation d'identité du proxy (technique qui consiste à amener, par la ruse, la victime à communiquer avec un proxy non autorisé configuré par les cybercriminels) et de détournement d'appel (l'appel est intercepté et redirigé vers un autre chemin avant d'arriver à destination).
* Implémenter des pare-feu qui identifient le trafic VoIP pour surveiller les flux et filtrer les signaux anormaux.

Nota : lorsque le réseau cesse de fonctionner, les communications voix s'arrêtent également.

# Caméras

Une caméra Internet envoie et reçoit des données sur un LAN et/ou sur Internet. Un utilisateur peut regarder une vidéo en direct à distance via un navigateur sur une vaste gamme d'appareils, par exemple des systèmes informatiques, des ordinateurs portables, des tablettes et des smartphones.

Les caméras peuvent prendre diverses formes, notamment la caméra de sécurité classique. Il peut également s'agir de caméras Internet dissimulées dans des radios-réveils, des livres ou des lecteurs de DVD.

Les caméras Internet transmettent la vidéo numérique sur une connexion de données. La caméra se connecte directement au réseau et dispose de tous les éléments nécessaires pour transférer les images sur le réseau. Cette figure répertorie les bonnes pratiques en matière de systèmes de caméra.

# Équipement de vidéoconférence

La vidéoconférence permet d'établir une communication simultanée entre plusieurs sites à l'aide des technologies de télécommunication. Ces technologies tirent parti des nouveaux standards de la vidéo en haute définition. Des solutions telles que Cisco TelePresence permettent à un groupe de personnes situé à un endroit de communiquer, en temps réel, avec des personnes qui se trouvent sur d'autres sites. La vidéoconférence fait désormais partie du quotidien dans de nombreux secteurs, comme le domaine médical. Les médecins peuvent examiner les symptômes des patients et consulter des experts pour prescrire un traitement adapté.

De nombreuses pharmacies emploient des auxiliaires médicaux qui peuvent organiser des vidéoconférences avec des médecins pour planifier des visites ou des interventions d'urgence. De nombreuses entreprises de fabrication ont recours à la téléconférence pour aider les ingénieurs et les techniciens à effectuer des opérations ou des tâches de maintenance complexes. L'équipement de vidéoconférence peut être extrêmement coûteux. Il s'agit donc d'une cible de choix pour les voleurs et autres cybercriminels. Cliquez [ici](https://youtu.be/WlDkiwzzv3M) pour regarder une vidéo traitant de la puissance des systèmes de vidéoconférence. Les cybercriminels ciblent ces systèmes dans le but d'intercepter des appels vidéos à l'insu des utilisateurs ou de nuire aux performances et à la disponibilité.

# Capteurs IoT et réseau

Les capteurs et appareils intelligents connaissent actuellement un énorme engouement de la part des utilisateurs. Le secteur informatique désigne cette tendance sous le nom d'Internet des objets (IoT). Les entreprises et les clients utilisent des appareils connectés à l'IoT pour automatiser des processus, surveiller leur environnement et prévenir l'utilisateur en cas de problèmes. La plupart des appareils connectés à l'IoT se connectent à un réseau via la technologie sans fil. Ils se présentent sous la forme de caméras, de serrures de porte, de capteurs de proximité, de lampes et d'autres types de capteurs utilisés pour collecter des informations sur un environnement ou sur l'état d'un appareil. Plusieurs fabricants d'électroménagers utilisent d'ores et déjà l'Internet des objets pour informer les utilisateurs du remplacement de certaines pièces, de la panne de certains composants ou encore de l'épuisement de certains consommables.

Des entreprises utilisent ces appareils pour effectuer le suivi des stocks, des véhicules et du personnel. Les appareils IoT sont pourvus de capteurs géospatiaux. Un utilisateur peut ainsi repérer un appareil sur la surface du globe, et surveiller et contrôler à distance des variables environnementales telles que la température, l'humidité et l'éclairage. L'Internet des objets représente un réel défi pour les professionnels de la sécurité de l'information, car de nombreux appareils IoT capturent et transmettent des données sensibles. Les cybercriminels ciblent ces systèmes dans le but d'intercepter des données ou de nuire aux performances et à la disponibilité.

# Renforcement des réseaux



Clôtures et barricades

Lorsque l'on parle de sécurité physique, la barrière physique est la première chose qui vient à l'esprit. Il s'agit de la dernière couche de sécurité et ces solutions sont les plus visibles. Un système de sécurité du périmètre comprend généralement les composants suivants :

* Clôture périphérique
* Barrière de sécurité
* Bornes (il s'agit de poteaux de petite taille destinés à empêcher les intrusions de véhicules ; voir la Figure 2)
* Barrières d'accès de véhicules
* Guérites

Une clôture est une barrière qui entoure une zone sécurisée et marque les limites de la propriété. Toutes les barrières doivent répondre à des exigences spécifiques en termes de conception et à des caractéristiques structurelles. Les zones de haute sécurité nécessitent généralement une « bordure défensive » comme du fil barbelé (concertina). Lors de la conception du périmètre de sécurité, il convient de tenir compte des règles suivantes pour les clôtures :

* Une clôture de 1 mètre dissuadera uniquement les intrus occasionnels
* Une clôture de 2 mètres est trop haute à escalader pour les intrus occasionnels
* Une clôture de 2,50 mètres ralentira un intrus déterminé
* Les bordures défensives constituent un moyen de dissuasion supplémentaire et ralentiront les intrus en leur infligeant de sérieuses coupures ; ils peuvent toutefois utiliser une couverture ou un matelas pour réduire les risques de blessure

Les réglementations locales en vigueur peuvent limiter le type de clôture qu'une entreprise peut utiliser.

Les clôtures doivent faire l'objet d'un entretien régulier. Des animaux peuvent creuser leur terrier sous la clôture de sécurité ; l'érosion des sols peut également rendre la clôture instable et, de ce fait, offrir un accès facile pour les intrus. Inspectez les clôtures régulièrement. Ne garez aucun véhicule à proximité d'une clôture. Un intrus pourrait, en effet, utiliser ce véhicule pour escalader la clôture ou l'endommager. Cliquez [ici](http://www.chainlinkinfo.org/security-fencing-guidelines/) pour consulter d'autres recommandations concernant les clôtures.

# Biométrie

La biométrie décrit les méthodes automatisées d'identification d'un individu sur la base d'une caractéristique physiologique ou comportementale. Les systèmes d'authentification biométrique intègrent les mesures du visage, les empreintes digitales, la géométrie de la main, l'iris, la rétine, la signature et la voix. Les technologies biométriques permettent de créer des solutions de vérification personnelle et d'identification hautement sécurisées. L'actuel engouement pour les systèmes biométriques fait suite à l'augmentation des failles de sécurité et des fraudes sur les transactions. La biométrie assure la confidentialité des données personnelles et des transactions financières. Apple, par exemple, utilise la technologie de reconnaissance d'empreintes digitales sur ses smartphones. L'empreinte digitale de l'utilisateur déverrouille l'appareil et permet d'accéder à diverses applications : pour les paiements et les transactions bancaires en ligne, par exemple.

Face à des systèmes biométriques semblables, certains facteurs clés sont à privilégier : la précision, la vitesse ou le débit, l'acceptabilité de la part des utilisateurs, l'unicité de la mesure biométriques, la résistance aux contrefaçons, la fiabilité, les exigences en termes de stockage des données, le temps d'apprentissage et le caractère intrusif de la lecture. Le facteur le plus important est la précision. La précision est exprimée en types et en taux d'erreurs.

Le premier taux d'erreurs équivaut aux erreurs de Type I ou refus erronés. Une erreur de Type I rejette un utilisateur autorisé qui s'enregistre. Dans le cadre du contrôle d'accès, si le critère essentiel est de refuser l'entrée aux hackers, un refus erroné constitue une erreur importante. Toutefois, dans de nombreuses applications biométriques, les refus erronés peuvent avoir un impact très négatif sur les activités de l'entreprise. Supposons qu'une banque ou un magasin doive authentifier l'identité d'un client pour connaître le solde de son compte. Dans ce cas, un refus erroné signifie l'abandon de la transaction ou une vente perdue, sans parler du mécontentement du client. La plupart des banquiers et des commerçants sont disposés à autoriser quelques acceptations erronées, pour autant que le nombre de refus erronés soit minime.

Le taux d'acceptation est exprimé sous la forme d'un pourcentage. Il s'agit de la fréquence à laquelle un système accepte des personnes non enregistrées ou des imposteurs en tant qu'utilisateurs authentiques. Les fausses acceptations constituent une erreur de Type II. Les erreurs de Type II autorisent les hackers à pénétrer dans le système. En règle générale, elles sont donc considérées comme les erreurs les plus importantes pour un système de contrôle d'accès biométrique.

La méthode la plus utilisée pour évaluer la précision de l'authentification biométrique est le « crossover error rate » (CER). Le CER est le seuil auquel le taux de rejets erronés est égal au taux d'acceptations erronées (comme le montre l'illustration).

# Badges et ports d'accès

Un badge d'accès permet à une personne d'accéder à une zone équipée de points d'accès automatisés. Un point d'entrée peut être une porte, un tourniquet, un portail ou toute autre barrière. Les badges d'accès emploient diverses technologies, telles que les bandes magnétiques, les codes-barres ou la biométrie.

Un lecteur de carte lit un numéro contenu sur le badge d'accès. Le système envoie le numéro à un ordinateur qui prend des décisions de contrôle d'accès sur la base des justificatifs d'identité fournis. Le système enregistre la transaction en vue de la récupérer ultérieurement. Les rapports indiquent qui est passé par un point d'entrée et à quel moment.

# Gardes et personnels d'escorte

Dans tous les systèmes de contrôle d'accès physique, y compris les systèmes de dissuasion et de détection, l'intervention d'une personne habilitée est toujours nécessaire pour mettre un terme à l'attaque ou à l'intrusion. Dans les installations de systèmes d'information haute sécurité, des gardes contrôlent l'accès aux zones sensibles de l'entreprise. Le bénéfice des gardes par rapport aux systèmes automatisés est indéniablement leur faculté d'adaptation. Cela leur permet d'identifier la situation à laquelle ils sont confrontés et de prendre rapidement des décisions appropriées. Les agents de sécurité constituent donc la solution de contrôle d'accès idéale lorsque la situation requiert une réponse adaptée et instantanée. Mais cela n'est pas toujours le cas… L'utilisation d'agents de sécurité s'accompagne de nombreux inconvénients, parmi lesquels le coût et l'impossibilité de surveiller et d'enregistrer un volume de trafic élevé. Il convient également de tenir compte d'un autre facteur : le risque d'erreur d'humaine.

# Surveillance vidéo et électronique

Les techniques de surveillance vidéo et électronique complètent ou, dans certains cas, remplacent les agents de sécurité. L'intérêt de la surveillance vidéo et électronique réside dans la capacité de surveiller des zones même lorsqu'aucun garde ou membre du personnel n'est présent, la possibilité d'enregistrer et de consigner les vidéos et les données de surveillance pendant des périodes prolongées et la capacité d'intégrer la détection de mouvement et la notification.

La surveillance vidéo et électronique permet également une capture plus précise des événements, même après qu'ils se soient produits. Un autre avantage majeur de cette technique de surveillance est de proposer des points de vue qu'il est difficile d'obtenir en ayant simplement recours à des agents de sécurité. L'utilisation de caméras peut également se révéler beaucoup plus économique pour surveiller tout le périmètre d'un site. Dans un environnement hautement sécurisé, une entreprise doit placer un équipement de surveillance vidéo et électronique à chaque entrée, sortie, baie de chargement, cage d'escalier et zone d'enlèvement des ordures. Dans la plupart des cas, ce mode de surveillance vient en complément des agents de sécurité.

# RFID et surveillance sans fil

Pour la plupart des entreprises, la gestion et la localisation des ressources d'information importantes constituent un enjeu crucial. L'augmentation du nombre de terminaux mobiles et d'appareils connectés à l'IoT a rendu cette tâche encore plus complexe. Le temps passé à rechercher du matériel critique peut se traduire par des retards ou des interruptions particulièrement coûteuses. L'utilisation d'étiquettes RFID (identification par la radiofréquence) peut avoir une valeur inestimable pour le personnel de sécurité. Une entreprise peut installer des lecteurs RFID dans les encadrements de porte des zones sécurisées afin qu'ils soient invisibles pour les utilisateurs.

Le bénéfice des étiquettes de ressource RFID est de permettre le suivi de toute ressource qui quitte physiquement une zone sécurisée. Les nouveaux systèmes d'étiquettes de ressource RFID peuvent lire plusieurs étiquettes simultanément. Les systèmes RFID ne nécessitent pas de visibilité directe pour lire les étiquettes. Un autre avantage de la technologie RFID est la possibilité de les lire en utilisant des balises qui ne sont pas visibles. Contrairement aux codes-barres et aux étiquettes lisibles par un utilisateur, les étiquettes RFID ne doivent pas nécessairement être visibles pour être lues. Prenons comme exemple l'étiquetage d'un ordinateur placé sous un bureau. En cas d'utilisation d'un code-barres ou d'un procédé manuel, la personne en charge de cette opération serait obligée de ramper sous le bureau pour localiser et voir l'étiquette. Avec la technologie RFID, la lecture peut s'effectuer sans même voir l'étiquette.

Conclusion

Ce chapitre a traité des technologies, processus et procédures que les magiciens de la cybersécurité emploient pour protéger les systèmes, les équipements et les données qui constituent l'infrastructure du réseau.

* Le renforcement de l'hôte comprend plusieurs procédures, dont la sécurisation du système d'exploitation, la mise en œuvre d'une solution antivirus et l'utilisation de solutions basées sur l'hôte, telles que des pare-feu et des systèmes de détection d'intrusions.
* La sécurisation du serveur comprend la gestion de l'accès à distance, la sécurisation des comptes privilégiés et la surveillance des services.
* La protection des données comprend le contrôle d'accès aux fichiers et la mise en œuvre de mesures de sécurité pour garantir la confidentialité, l'intégrité et la disponibilité des données.

Le renforcement des équipements implique également la mise en œuvre de méthodes éprouvées de sécurisation physique des équipements réseau. Fortifier le royaume est un processus permanent qui vise à sécuriser l'infrastructure de réseau de l'entreprise et qui nécessite une vigilance constante contre les menaces.