ESTIAM / PARIS

Rapport de cours
Jour 4

Victoria SAUTEREAU

Cybersécurité

E S T I A M

École d'informatique et du numérique

2ème année
2022/2023

Sommaire

Partie 1 Protéger les systèmes et les appareils

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.

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.

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.

Protection contre les logiciels malveillants

Il est important de protéger les ordinateurs et les terminaux mobiles à l'aide d'un logiciel antimalware renommé. En effet, 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. 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.

- 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.

Les 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.

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.

Systèmes de détection d'intrusions et pare-feu basés sur l'hôte

Une solution basée sur l'hôte est une application logicielle qui s'exécute sur un ordinateur hôte local afin de le protéger. Le logiciel fonctionne avec un système d'exploitation pour empêcher les attaques.

Pare-feu basés sur l'hôte

Un pare-feu logiciel est un programme qui s'exécute sur un ordinateur en vue d'autoriser ou de refuser du trafic entre un ordinateur et les autres ordinateurs connectés. Le pare-feu logiciel applique un ensemble de règles aux transmissions de données grâce à l'inspection et au filtrage des paquets de données. Le Pare-feu Windows est un pare-feu logiciel. Le système d'exploitation Windows l'installe par défaut lors de la phase d'installation.

L'utilisateur peut contrôler le type des données échangées avec l'ordinateur en ouvrant ou en bloquant les ports sélectionnés. Les pare-feu peuvent bloquer les connexions réseau entrantes et sortantes, sauf si des exceptions ont été définies pour ouvrir et fermer les ports requis par un programme.

Systèmes de détection d'intrusions basés sur l'hôte

Un système de détection d'intrusions basé sur l'hôte (ou HIDS) est un logiciel qui s'exécute sur un ordinateur chargé de surveiller toute activité suspecte. Ce logiciel doit être installé sur chaque serveur ou ordinateur qui doit bénéficier d'une protection. Le système HIDS surveille les appels système et l'accès au système de fichiers pour s'assurer que les requêtes ne sont pas dues à une activité malveillante. Il peut également surveiller les paramètres du Registre système. Le Registre conserve les informations de configuration relatives à l'ordinateur.

Le système HIDS stocke toutes les données de journal en local. Ce logiciel étant particulièrement gourmand en ressources, son utilisation peut également nuire aux performances du système. Nota : le système HIDS ne peut pas surveiller le trafic réseau qui n'atteint pas le système hôte. En revanche, il surveille le système d'exploitation et les processus système critiques qui sont propres à cet hôte.

Communications sécurisées

Lors de la connexion au réseau local et du partage de fichiers, la communication entre les ordinateurs s'effectue dans les limites du réseau. Les données sont sécurisées, car elles ne sont pas accessibles depuis d'autres réseaux ou depuis Internet. Pour communiquer et partager des ressources sur un réseau non sécurisé, les utilisateurs ont recours à un réseau privé virtuel (VPN).

Il s'agit d'un réseau privé qui utilise un réseau public, par exemple Internet, pour connecter des sites ou des utilisateurs à distance. Le type de VPN le plus courant est l'accès à un réseau privé d'entreprise. Un VPN utilise des connexions sécurisées dédiées qui sont acheminées via Internet depuis le réseau privé de l'entreprise jusqu'à l'utilisateur distant. Une fois les utilisateurs connectés au réseau privé de l'entreprise, ils sont intégrés à celui-ci et peuvent accéder à tous les services et ressources dont ils bénéficieraient s'ils étaient physiquement connectés au réseau local de l'entreprise.

Un client VPN doit être installé sur les ordinateurs des utilisateurs distants pour qu'il soit possible d'établir une connexion sécurisée avec le réseau privé de l'entreprise. Le client VPN chiffre les données avant de les envoyer sur Internet vers la passerelle VPN du réseau privé de l'entreprise. Les passerelles VPN établissent, gèrent et contrôlent les connexions du réseau privé virtuel, également appelées « tunnels » du réseau privé virtuel.

Les systèmes d'exploitation intègrent un client VPN que l'utilisateur configure pour établir une connexion VPN.

Partie 2 : Renforcement du serveur

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.

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.

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.

Comptes avec privileges

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.

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

Activer les journaux et les alertes

Un journal 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

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.

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.

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.

Partie 3 : Sécurité physique

Biométrie

a 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).

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.