IT Essentials : Matériel et logiciel informatique version 5.0

Chapitre 10 : Sécurité

Speaker

Cisco | Networking Academy®
Mind Wide Open™

Objectifs du chapitre 10

- 10.0 Explication des raisons de l'importance de la sécurité
- 10.1 Description des menaces de sécurité
- 10.2 Identification des procédures de sécurité
- 10.3 Identification des techniques de maintenance préventive courantes pour la sécurité
- 10.4 Dépannages en matière de sécurité

Importance de la sécurité

- Des informations privées, des données confidentielles d'entreprise, des données financières, des équipements informatiques et des éléments de sécurité nationale sont soumis à des risques si les procédures de sécurité appropriées ne sont pas respectées.
- Les responsabilités principales d'un technicien incluent la sécurité des données et des réseaux.

Menaces de sécurité

Menaces potentielles contre la sécurité informatique :

- Menaces internes
  - Les employés peuvent causer une menace malveillante ou accidentelle.
- Menaces externes
  - Des utilisateurs externes peuvent attaquer d'une manière non structurée ou structurée.

Types d'attaques de sécurité informatique :

- Physique
  - Vol, dommage ou destruction d'équipement informatique
- Données
  - Suppression, corruption, déni d'accès, accès non autorisé ou vol d'informations

Logiciels publicitaires, logiciels espions et hameçonnage

Un logiciel malveillant (malware) est un logiciel conçu pour endommager ou perturber un système :

- **Adware -** Un logiciel publicitaire est un programme qui affiche de la publicité sur votre ordinateur (fenêtre pop-up).
- **Spyware -** Se copient à l'insu des utilisateurs et sans leur intervention. Il surveille l'activité de l'ordinateur et envoie les informations recueillies à l'organisation ou à l'individu qui l'a lancé.
- **Phishing -** L'hameçonnage a lieu lorsqu'un pirate prétend représenter un organisme légitime, comme une banque. La victime potentielle est contactée par e-mail, par téléphone ou par SMS. Le pirate demande des informations telles qu'un nom d'utilisateur ou un mot de passe.
- **REMARQUE** : il est rarement nécessaire de donner des informations personnelles sensibles ou financières en ligne.
- **Voir exercice: 10.1.1.1**

Virus, vers, chevaux de Troie et rootkits

- **Un Virus** est un code logiciel délibérément créé par un pirate. Les virus peuvent collecter des informations sensibles ou modifier, voire détruire, des informations. (email, ftp, instant mail): Exple: *Revealer Keylogger*, *Raila Odinga*
- **Un vers** est un programme autopropageable qui utilise le réseau pour dupliquer son code à des hôtes du réseau. Dans le meilleur des cas, les vers consomment de la bande passante.
- **Un cheval de Troie** est, techniquement, un vers et tire son nom de la méthode qu'il utilise pour contourner les défenses des ordinateurs en prétendant être un programme utile.
- **Les logiciels antivirus** sont conçus pour détecter, désactiver et supprimer les virus, vers et chevaux de Troie avant qu'ils n'infectent un ordinateur.
- **Un rootkit** est un programme malveillant qui cherche à obtenir un accès complet à un système informatique l est très difficile de détecter un rootkit, car celui-ci peut contrôler et modifier les programmes de sécurité

Sécurité sur Internet

Les outils utilisés pour rendre les pages Web polyvalentes et plus puissantes peuvent également fragiliser les ordinateurs face aux attaques:

- **Active X** - technologie créée par Microsoft pour contrôler l'interactivité des pages Web.
- **Java** - langage de programmation permettant d'exécuter des applets dans un navigateur Web.
- **Java Script** - langage de programmation développé pour interagir avec le code source HTML.
- **Adobe Flash** - outil multimédia utilisé pour créer des contenus Web interactifs. Flash est utilisé pour intégrer des animations vidéos et des jeux
- **Microsoft Silverlight** - outil utilisé pour créer des contenus Web interactifs et enrichis. Silverlight possède de nombreuses fonctionnalités similaires à Flash

la plupart des navigateurs disposent de paramètres qui contraignent l'utilisateur à autoriser le téléchargement ou l'utilisation de ces outils:

- **Filtre ActiveX**
- **Bloquer de fenêtre Pop-up**
- **Filtre SmartScreen (Internet Explorer, détecte les sites d'hameçonnage)**

La navigation “InPrivate”

- **La navigation InPrivate** Permet d’éviter à votre navigateur d’enregistrer vos traces lorsque vous accèdez à Internet:
- Cette fonctionnalité interdit au navigateur de stocker les informations suivantes :
  - Noms d'utilisateur
  - Mots de passe
  - Cookies
  - Historique de navigation
  - Fichiers Internet temporaires
  - Données de formulaires
- Le navigateur stockera des informations (par exemple des fichiers temporaires et des cookies), mais ces fichiers seront effacés dès que la session InPrivate sera terminée.
- To start InPrivate Browsing in Windows 7:
  - Cliquez avec le bouton droit sur **Internet Explorer > Démarrer la navigation InPrivate**.

Courrier indésirable et fenêtres publicitaires intempestives

- **Un courrier indésirable** est un e-mail qui peut envoyer des liens malveillants ou un contenu trompeur.
- **Les fenêtres publicitaires intempestives** sont des fenêtres qui s'ouvrent automatiquement et qui sont conçues pour attirer votre attention et vous conduire à des sites publicitaires.

Utilisez *un logiciel antivirus*, *les options du logiciel de messagerie électronique*, *des bloqueurs de fenêtres publicitaires intempestives* et quelques indices connus pour combattre ces menaces.

Certains messages passent entre les mailles du filet. Soyez vigilant et vérifiez les éléments suspects suivants : *message sans objet, lien trop long, email mal rédigé, Email demandant des infos sur le compte,etc*.

Attaques TCP/IP

La suite de protocoles TCP/IP est utilisée pour contrôler toutes les communications sur Internet. certaines fonctionnalités des protocoles TCP/IP peuvent être détournées et créer des failles.

- **Denial of Service (DoS)** - forme d'attaque qui empêche les utilisateurs d'accéder normalement à des services tels que la messagerie électronique ou un serveur Web.
- **Distributed DoS (DDoS)** - utilise un grand nombre d'ordinateurs contaminés, appelés des **zombies** ou des **botnets**, pour lancer une attaque**.**
- **Inondation SYN-** La requête SYN est la communication initiale envoyée pour établir une connexion TCP. Attaque de type DoS
- **Mistification-** Il s'agit de l'usurpation, ici, une hôte utilise une fausse adresse IP et/ouMAC pour se faire passer pour un autre afin d'accéder au système.
- **Man-in-the-Middle -** intercepte les communications entre plusieurs ordinateurs pour voler les informations en transit sur le réseau..
- **Rejeu-** les transmissions de données sont interceptées et enregistrées par un pirate. Ces transmissions sont ensuite envoyées à l'ordinateur de destination.
- **Empoisonnement DNS -** Modifier les enregistrements dans les serveurs

Rafraîchissement Mémoire

1. Définition: Menace externe, menace interne, attaque physique, virus, hameçonnage, cheval de trois, grayware, adware, spyware, pop-up, SPAM, DoS, DDoS, Spoofing, botnets, zombies
2. Quelles différences faites vous entre une attaque de type physique et une attaque dirigé sur les données?
3. Comment combattre efficacement les menaces liés aux virus, vers, cheval de trois, et autre programme malveillant? (citez au moins 2 méthodes et commentez).
4. Quelle différence faites-vous entre un virus et un vers?
5. Enumérez quatre conséquences liées à une attaque par des programmes malveillants.
6. Enumérez tout en définissant, quatre outils utilisés pour rendre les pages web plus attractives et qui peuvent être des sources de menaces en matière de sécurité.
7. En quoi consiste le filtre SmartScreen?
8. En quoi consiste le terme Navigation InPrivate, quel type de navigateur offre cette fonctionnalité? Cette fonctionnalité existe-t-elle dans d'autres navigateurs? Si oui donnez quelques exemples.
9. Listez en définissant les différentes types d'attaques qui résulte des faille de la pile de protocole TCP/IP
10. 10.1.1.7 Fiche de travail – Atteintes à la sécurité

Piratage psychologique

- **Un pirate psychologique** réussit à accéder à un équipement ou à un réseau en trompant ses victimes, pour qu'elles lui fournissent les informations d'accès nécessaires.
- Voici quelques précautions de base pour vous protéger contre la manipulation psychologique :
  - Ne divulguez jamais votre mot de passe.
  - Vérifiez toujours l'identité des inconnus.
  - Limitez l'accès des visiteurs.
  - Accompagnez tous les visiteurs.
  - N'affichez jamais votre mot de passe dans votre espace de travail.
  - Verrouillez votre ordinateur si vous quittez votre bureau.
  - Ne laissez personne vous suivre derrière une porte qui nécessite une carte d'accès.

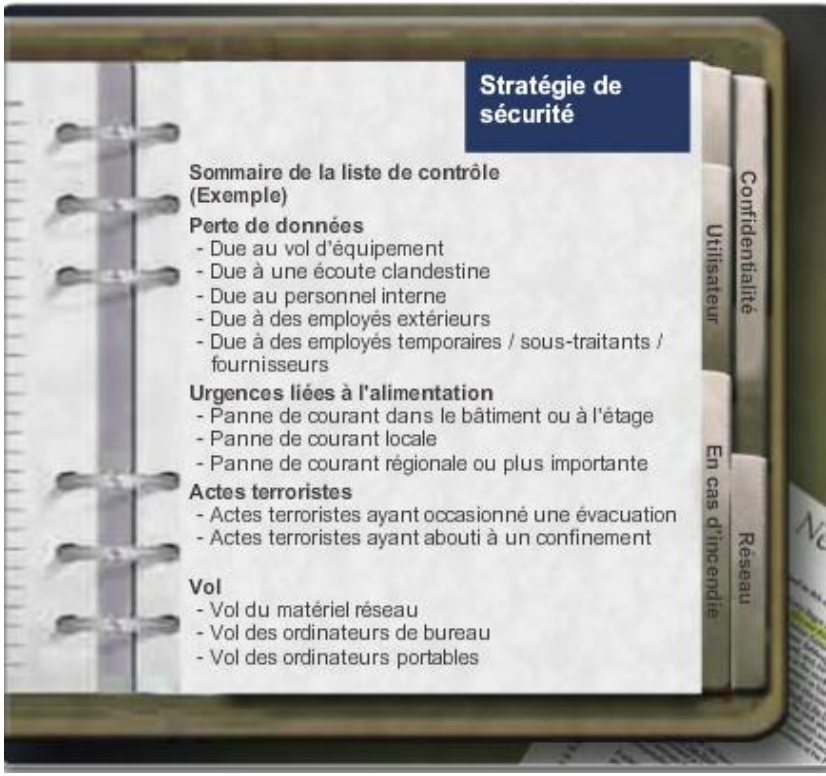
Effacement des données, destruction des disques durs et recyclage

- Pour que la récupération des données soit impossible, il faut effacer entièrement le contenu du disque dur au moyen d'un logiciel spécial.
- **L'effacement** des données, ou effacement sécurisé, est une procédure visant à supprimer définitivement les données du disque dur. Souvant effectué sur les DD contenant des données sensibles.
- La **démagnétisation** consiste à perturber ou à éliminer le champ magnétique d'un disque dur qui permet le stockage des données. Un outil de démagnétisation coûte très cher.
- Pour garantir avec certitude que les données d'un disque dur ne pourront pas être récupérées, il faut briser soigneusement les plateaux avec un marteau et éliminer convenablement les morceaux.
- Pour s'assurer que les données ne peuvent pas être récupérées sur un disque SSD, CD, disquette, DVD, effectuez un écrasement sécurisé ou broyez le disque en petites pièces.
- **Recyclage des Disque durs-** Les disques durs qui ne contiennent pas de données sensibles peuvent être réutilisés dans d'autres ordinateurs. Le lecteur peut ainsi être **reformaté** et un nouveau système d'exploitation installé.

Stratégie de sécurité

- Une stratégie de sécurité est un ensemble de règles, de directives et de listes de contrôle
- Une stratégie de sécurité doit impérativement prévoir la gestion des problèmes de sécurité.
- Questions à se poser lors de la mise en place d'une stratégie de sécurité:
  - Quelles ressources doivent être protégées ?
  - Quelles sont les menaces possibles ?
  - Que faire si une faille est détectée ?
  - Quelle formation est proposée aux utilisateurs ? **Exercice: 10.2.1.2**

Liste de contrôle dans la stratégie de sécurité



REMARQUE : une stratégie de sécurité est efficace uniquement si elle est appliquée et respectée par tous les employés.

Exigences en matière de stratégies de sécurité

Lorsque vous élaborez une stratégie de sécurité, voici les points principaux à prendre en compte:

- Procédure de traitement des incidents de sécurité du réseau
- Procédure d'audit de la sécurité sur le réseau existant
- Cadre général de sécurité pour l'implémenter sur le réseau local.
- Comportements autorisés
- Comportements interdits
- Que consigner et où stocker les journaux : Observateur d'événements, fichiers journaux système ou fichiers journaux de sécurité
- Accès aux ressources via le réseau grâce aux autorisations des comptes
- Technologies d'authentification pour l'accès aux données : noms d'utilisateur, mots de passe, biométrie, cartes à puce

Noms d'utilisateur et mots de passe

- Les mots de passe permettent de se protéger contre le vol de données et les autres actes malveillants.
- Stratégie en matière de nom d'utilisateur et de mot de passe:
  - Modifier les noms d'utilisateur par défaut pour les comptes administrateur ou invité, car ils sont connus de tous.
  - l'administrateur système définit une convention d'attribution des noms d'utilisateur lors de la création des sessions de réseau..
- Trois niveaux de protection par mot de passe sont recommandés :
  - **BIOS**
  - **Ouverture de session**
  - **Réseau**

Exigences en matière de mots de passe

Conseils pour la création de mots de passe forts :

- **Longueur** : utilisez au moins 8 caractères.
- **Complexité** : utilisez une combinaison de lettres, de chiffres, de caractères spéciaux et de signes de ponctuation. Il est important d'utiliser des caractères variés et pas uniquement des lettres ou des chiffres.
- **Modification** : modifiez souvent le mot de passe. Paramétrez des rappels de modification des mots de passe de messagerie, de compte bancaire et des sites sur lesquels vous utilisez votre carte bancaire en moyenne tous les trois ou quatre mois.
- **Variété** : utilisez un mot de passe différent pour chaque site et chaque ordinateur.

Autorisations d'accès aux fichiers et aux dossiers

- Les niveaux d'autorisation sont configurés pour limiter l'accès d'un utilisateur ou d'un groupe d'utilisateurs à des données particulières.
- **NTFS** – (SGF utilisant les fichiers de journalisation qui sont des fichiers spéciaux où les changements effectués sur les fichiers sont inscrits avant d'être effectués.
  - peuvent consigner les accès par utilisateur, date et heure.
  - Capable de chiffrer les données.
- **FAT 32** - Le système de fichiers FAT32 ne dispose pas de toutes les possibilités de journalisation ni de chiffrement.
- **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. .
- **Restriction des autorisations attribuées aux utilisateurs**. Lorsqu'un utilisateur ou un groupe n'est pas autorisé à accéder à un partage réseau, cela remplace toute autre autorisation concédée.

Comparaison de FAT32 et NTFS

	FAT32	NTFS
Sécurité	Faible niveau de sécurité	Autorisations au niveau des fichiers et des dossiers, chiffrement
Compatibilité	Compatible avec toutes les versions de Windows	Compatible avec toutes les versions de Windows
Taille des fichiers	Limitée à des fichiers de 4 Go / volumes de 32 Go.	Limitée à des fichiers de 16 To / volumes de 256 To
Fichiers par volume	4,17 millions	4,29 milliards
Efficacité de la taille des fichiers	Les grands clusters gaspillent de l'espace	Des clusters plus petits utilisent mieux l'espace disponible ; compression intégrée pour optimiser l'espace
Fiabilité	N'effectue pas le suivi des modifications apportées au système de fichiers	Inclut la journalisation qui permet de reconstruire le système de fichiers après une panne de l'ordinateur ou une panne d'électricité

Protection des données

La valeur d'un matériel informatique est souvent très inférieure à la valeur des données qu'il contient. Diverses méthodes de protections peuvent être implémentées

- Un pare-feu logiciel
- Les cartes à puce
- La sécurité Biométrie
- Sauvegardes de données
- Chiffrement des données

Chiffrement des données

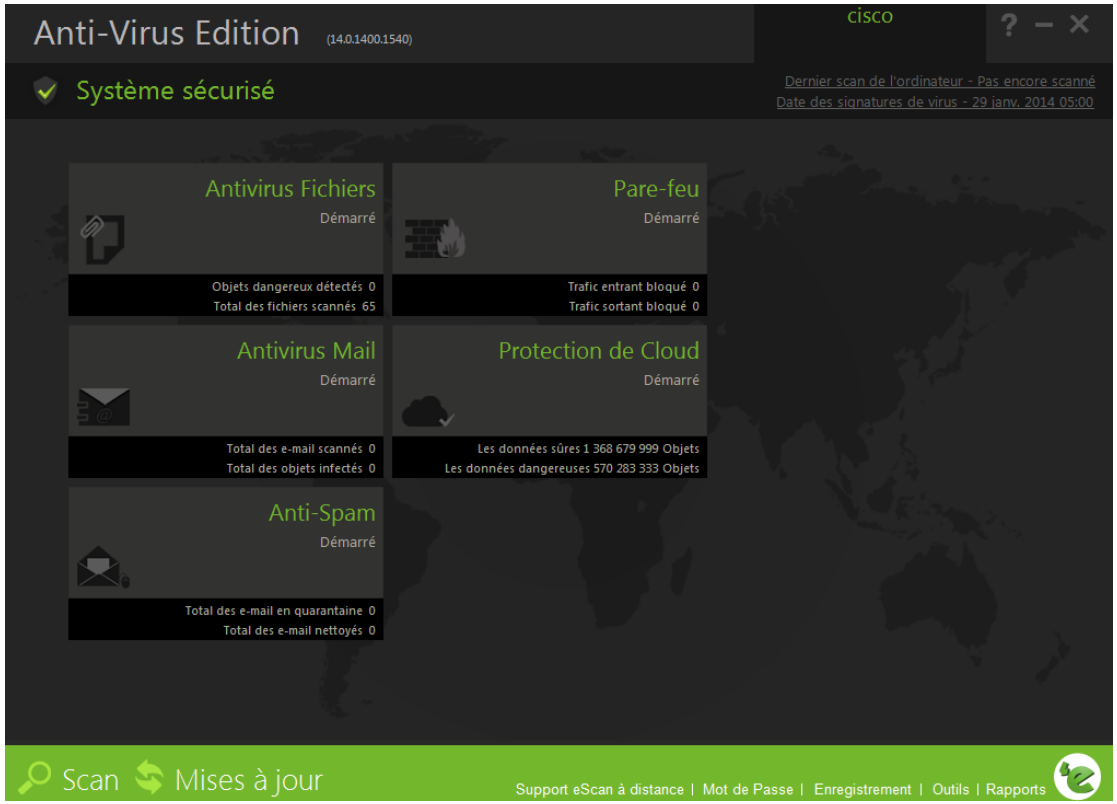
- Le chiffrement est souvent utilisé pour protéger les données. Il consiste à transformer celles-ci à l'aide d'un algorithme complexe visant à les rendre illisibles.
- **Encrypting File System (EFS)** Cette fonction est directement liée à un compte d'utilisateur. Seul l'utilisateur ayant chiffré les données pourra à nouveau y accéder.
- **BitLocker** permet de chiffrer un volume complet. Il est fourni avec Windows 7, Windows Vista Édition Intégrale et Windows Vista Entreprise. Le volume système ne peut pas être chiffré et doit faire au moins 100 Mo.
- **Trusted Platform Module (TPM)** Il s'agit d'une puce spécialisée qui est installée sur la carte mère d'un ordinateur et qui est utilisée pour l'authentification matérielle et logicielle.
  - Le TPM stocke des informations spécifiques au système hôte, telles que les clés de chiffrement, les certificats numériques et les mots de passe.

Logiciels de protection contre les programmes malveillants

- **Logiciel malveillant** est un programme qui s'installe sur un ordinateur à l'insu et sans permission de l'utilisateur.
- On peut être emmené à exécuter des programmes de recherche de virus et de logiciels espions afin de détecter et supprimer ces programmes indésirables.
- Les utilitaires de protections sont: **Protection contre les virus**, **Protection contre les logiciels espions**, **Protection contre les logiciels publicitaires**, **Protection contre l'hameçonnage.**
- **Faux antivirus**
- Sur Internet, il est courant de voir des publicités concernant des produits et des logiciels. Ces publicités peuvent être utilisées pour contaminer l'ordinateur d'un utilisateur.

Mises à jour des fichiers de signatures

- De nouvelles attaques sont découvertes tous les jours. Les éditeurs de logiciels doivent créer et distribuer régulièrement de nouveaux correctifs.

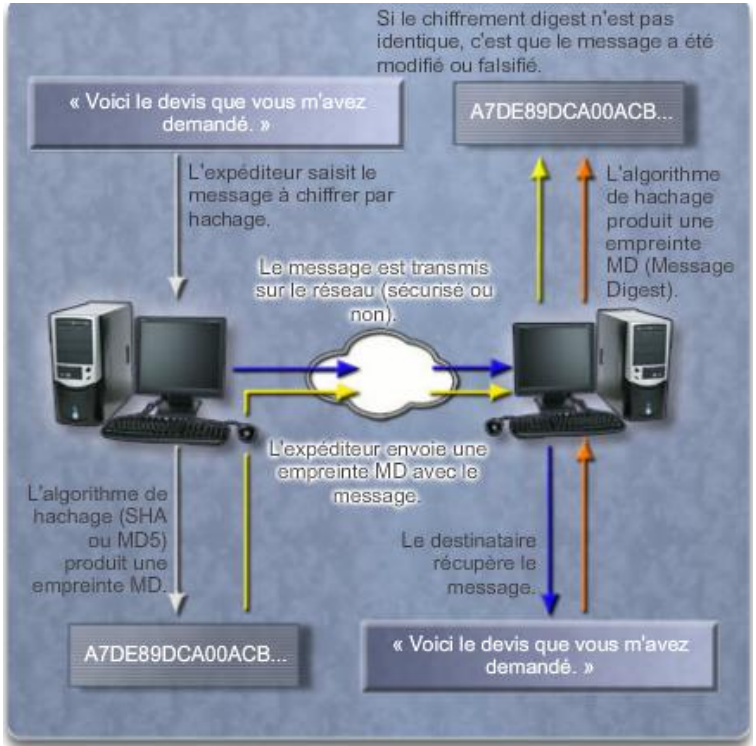


Rafraîchissement Mémoire

1. Démagnétisation, Recyclage, formatage de bas niveau, formatage de haut niveau, stratégie de sécurité, mot de passe, NTFS, FAT32, biométrie, chiffrement, BitLocker, système EFS, TPM, Faux antivirus
2. Pour quelle raison à votre avis l'on peut être emmené à supprimer les données sur un disque dur? Quelles sont les bonnes pratiques pour détruire un disque?
3. Existe-t-il des logiciels permettant de récupérer des fichiers et dossiers même après leur suppression sur un disque? Si oui donne en 2 exemples.
4. En quoi consiste une stratégie de sécurité? Quelles sont les bonnes questions à se poser pour l'élaboration d'une tel stratégie?
5. Enumérez 5 principaux point à prendre en compte lors de la mise en place d'une stratégie de sécurité.
6. Quelles sont les quatre principales exigences auxquelles doit se plier un mot de passe qualifié de « fort »? En quoi consiste chacune d'elle? Donner un exemple de mot de passe « fort ».
7. Lister les 3 niveaux de sécurités dans un système d'information où l'on pourrait utiliser un mot de passe. Quelles sont les bonnes pratiques (02) pour sa gestion?
8. Dressez le tableau de comparaison qui existe NTFS et FAT32.
9. En dehors des mots de passe, citez cinq (05) autres méthodes pouvant être utilisées pour protégées un données dans un système d'information. Décrivez en quoi chacun d'eux consiste.
10. Pourquoi est-il important qu'un technicien s'assure que les logiciel d'antivirus installés dans les ordinateurs se mettent à jour?

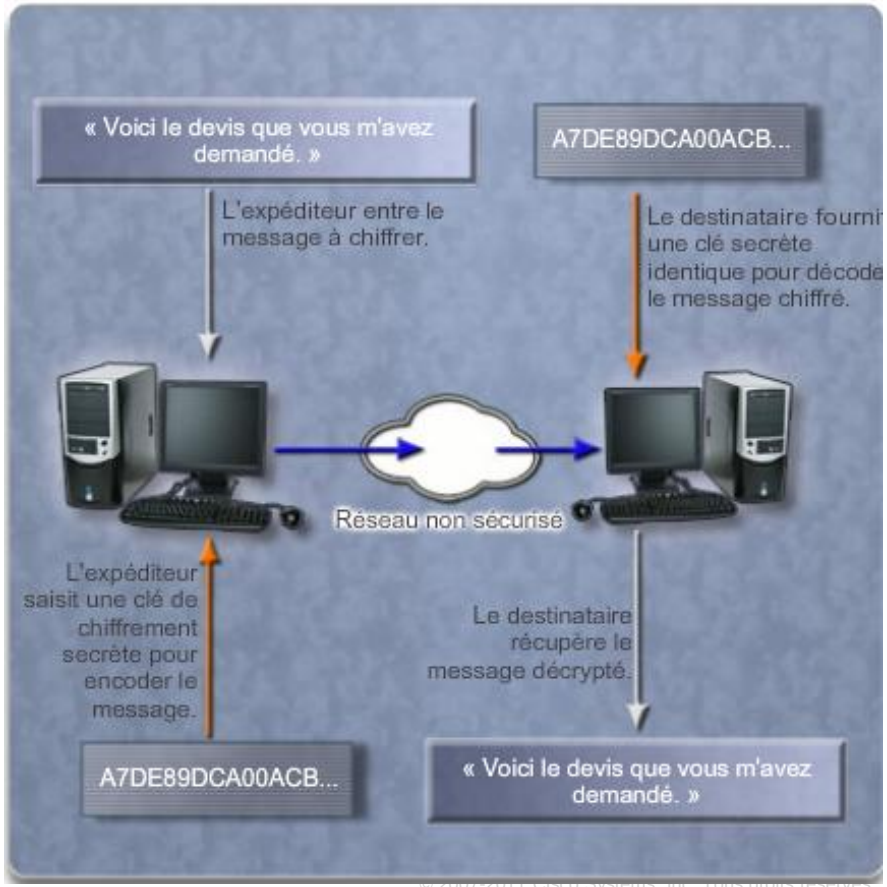
Méthodes courantes de chiffrement des communications

- **Hachage** Le hachage garantit que les messages ne sont pas endommagés ni modifiés au cours de leur transmission. Cette technique utilise une fonction mathématique (**Algorithme MD**) pour créer une valeur numérique unique pour les données. Les algorithmes de hachage les plus répandus sont le SHA (Secure Hash Algorithm), le MD5 (Message Digest 5) et le DES (Data Encryption Standard).



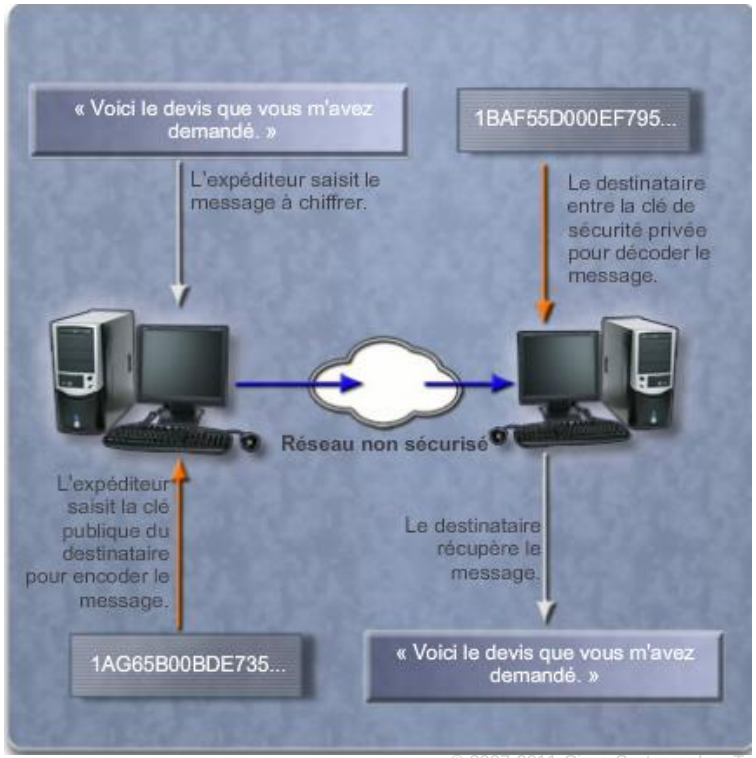
Méthodes courantes de chiffrement des communications

- **Chiffrement symétrique** : Il exige que les deux interlocuteurs d'une conversation chiffrée utilisent une clé de chiffrement pour coder et décoder les données. **DES** et **3DES** sont des exemples de chiffrement symétrique.



Méthodes courantes de chiffrement des communications

- **Chiffrement asymétrique:** Il exige deux clés, l'une **privée** et l'autre **publique**. Le destinataire prévu est le seul à disposer de la clé privée, qui sert à déchiffrer les messages. Exemple de fonctionnement de l'Adresse eMail. Le chiffrement asymétrique **RSA** est l'exemple le plus répandu

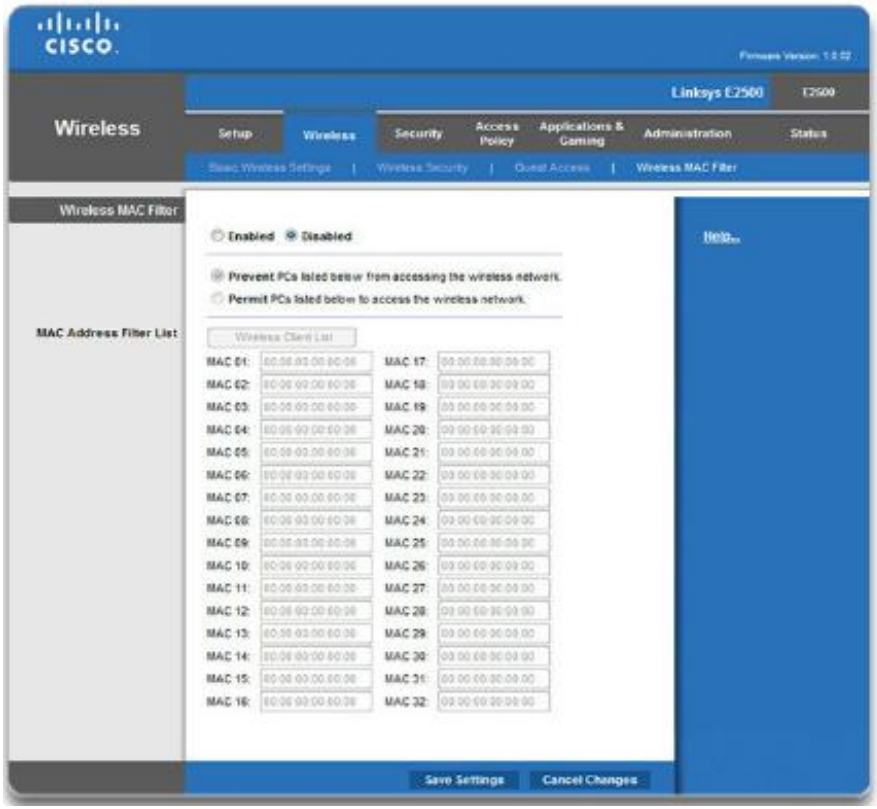


Le Service Set Identifiers

- **Le SSID** (Service Set Identifier) est le nom du réseau sans fil. Un routeur ou un point d'accès sans fil diffuse le SSID par défaut, afin que les périphériques sans fil puissent détecter le réseau sans fil.
- Pour désactiver la diffusion du SSID, procédez comme suit (voir ci-contre) :
- **Wireless > Basic Wireless Setting**, puis **Disabled** pour la diffusion SSID (SSID Broadcast) et **Save Settings > Continue.**
- La désactivation de la diffusion SSID n'améliore que très légèrement la sécurité. Si la diffusion SSID est désactivée, tous les utilisateurs voulant se connecter au réseau sans fil doivent saisir le SSID manuellement. Lorsqu'un ordinateur recherche un réseau sans fil, le SSID est diffusé.

Filtrage d'adresses MAC

- Le filtrage d'adresses MAC est une technique qui permet de déployer la sécurité au niveau des périphériques sur un réseau local sans fil (WLAN)..



Modes de sécurité pour le sans fil

- **Wired Equivalent Privacy (WEP)** – protocole de sécurité de première génération pour les communications sans fil. Les pirates informatiques ont rapidement découvert que le chiffrement WEP était facile à contourner.
- **Wi-Fi Protected Access (WPA)** – version améliorée du WEP. Il utilise un chiffrement plus fort que le chiffrement WEP.
- **Wi-Fi Protected Access 2 (WPA2)** – version améliorée du protocole WPA. Ce protocole permet d'atteindre des niveaux de sécurité plus élevés que le mode WPA. Il existe 2 versions du WPA2 : **le mode Personnel** (authentification par mot de passe) et le **mode Entreprise** (authentification par serveur)
- D'autres protocoles de sécurité ont été ajoutés au protocole WPA: TKIP, EAP, PEAP, AES

Exercice PT: 10.2.4.5

Accès sans fil

- **Antennes sans fil**
  - Évitez de transmettre des signaux en dehors de la zone du réseau en installant une antenne avec des caractéristiques adaptées aux utilisateurs de votre réseau.
- **Accès aux périphériques réseau**
  - La première fois que vous vous connectez au périphérique réseau, changez le nom d'utilisateur et le mot de passe par défaut.
- **Wi-Fi Protected Setup (WPS)**
  - Le routeur sans fil dispose d'un code PIN choisi lors de sa fabrication. Ce code est imprimé sur un autocollant ou affiché à l'écran.
  - Des logiciels ont été créés pour intercepter le trafic et récupérer le code PIN et la clé de chiffrement pré-partagée utilisés par le protocole WPS. si vous le pouvez désactivez le protocole WPS sur le routeur sans fil.

Firewalls / Pare-feu

- **Un pare-feu matériel** est un dispositif de filtrage matériel qui inspecte les paquets de données en provenance du réseau avant que ceux-ci n'atteignent les ordinateurs et les autres périphériques connectés

Hardware Firewall	Software Firewall
Dedicated hardware component	Available as third-party software, cost varies
Initial cost for hardware and software updates can be expensive	Free version included with Windows operating system
Multiple computers can be protected	Typically protects only the computer on which it is installed
No impact on computer performance	Uses the CPU, potential impact on computer performance

Redirection et déclenchement de port

- **Redirection de port** La redirection de port est une méthode basée sur des règles qui redirige le trafic entre des périphériques situés sur des réseaux distincts:
  - il est parfois nécessaire d'ouvrir des ports spécifiques pour permettre à certains programmes et applications de communiquer avec les périphériques de différents réseaux.
  - un routeur peut être configuré pour effectuer une redirection pour le port 80, lequel est associé au protocole HTTP.
- **Le déclenchement de port** autorise le routeur à transférer temporairement les données via les ports entrants vers un périphérique spécifique.
  - Par exemple, un jeu vidéo peut utiliser les ports de 27 000 à 27 100 pour les connexions avec les autres joueurs.

Méthodes de protection du matériel

- La sécurité physique est aussi importante que la sécurité des données. Lorsqu'un ordinateur est volé, son contenu l'est également. L'infrastructure du réseau peut être protégé par:
  - Salles de télécommunications sécurisées, armoires fermées pour les équipements
  - Câbles antivol et vis de sécurité pour les équipements
  - Système de détection des points d'accès sans fil non autorisés
  - Pare-feu matériels
  - Système de gestion du réseau qui détecte les changements dans le câblage et les tableaux de connexion.
- **Désactivation de l'exécution automatique**
- **Authentification à deux facteurs -** sécurisés au moyen de techniques de protection qui se cumulent pour empêcher un accès non autorisé aux données sensibles.
  - Il peut s'agir de protéger une ressource avec un mot de passe et une carte à puce.

Matériel de sécurité

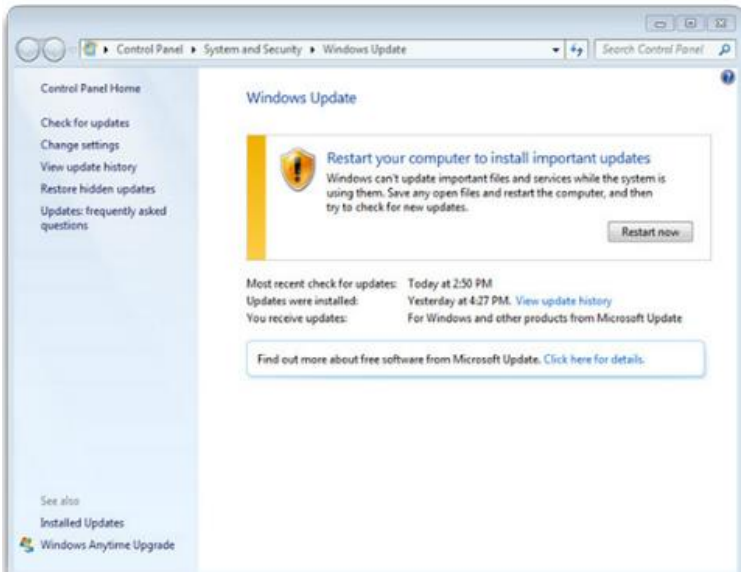
- Il existe plusieurs méthodes pour protéger physiquement l'équipement informatique:
  - Utiliser des câbles antivol pour protéger les équipements
  - Garder les salles de télécommunications fermées à clé
  - Sécuriser les équipements avec des vis de sécurité
  - Utiliser des cages de sécurité autour des équipements
  - Installer des capteurs et placer des étiquettes d'identification par radiofréquence (RFID, Radio Frequency Identification) sur les équipements
  - Installer des alarmes déclenchées par des détecteurs de mouvement
  - Utiliser des webcams avec des logiciels de détection de mouvement et de surveillance
- Plusieurs moyens permettent de protéger l'accès aux installations :
  - Cartes d'accès contenant des informations sur l'utilisateur, notamment son niveau d'accès
  - Capteurs biométriques identifiant les caractéristiques physiques d'un utilisateur, telles que son empreinte rétinienne ou ses empreintes digitales
  - Présence permanente d'un agent de sécurité
  - Capteurs, par exemple des étiquettes RFID, pour surveiller les équipements

Exercice 10.2.5.3

Rafraîchissement Mémoire.

Correctifs de sécurité et Service Packs des systèmes d'exploitation

- 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.
- les techniciens doivent savoir comment installer des correctifs et des mises à jour.
- **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
- Un **Service Pack** Combine les correctif et les mises à jour.



- Vous pouvez configurer Windows pour qu'il télécharge et installe automatiquement les mises à jour prioritaires dont votre ordinateur a besoin ou qu'il vous informe de leur disponibilité.
  - **Démarrer > Tous les programmes > Windows Update > Modifier les paramètres**

Sauvegardes de données

- Vous pouvez faire une sauvegarde manuelle de Windows ou planifier la fréquence des sauvegardes automatiques.
- Pour sauvegarder et restaurer des données sous Windows, des droits et des autorisations appropriés sont requis :
  - **Start> All Programs > Maintenance >Backup and Restore >Set up backup**

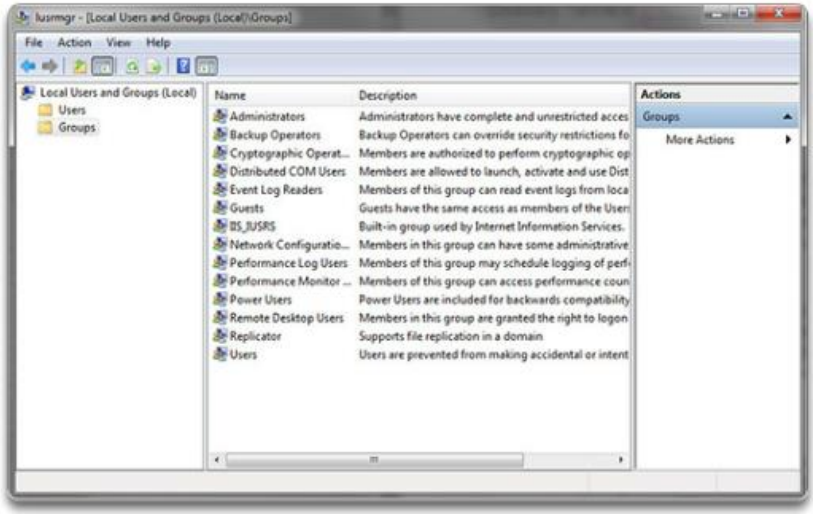
Type de sauvegarde	Description
Complète ou normale	Sauvegarde tous les fichiers sélectionnés et marque chacun d'eux comme ayant été sauvegardé.
Incrémentielle	Sauvegarde uniquement les fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde complète ou incrémentielle. La restauration des fichiers exige que vous disposiez du dernier jeu de sauvegarde complet et de tous les jeux de sauvegardes incrémentielles.
Différentielle	Sauvegarde uniquement les fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde complète. La restauration des fichiers exige que vous disposiez de la dernière sauvegarde complète et d'une sauvegarde différentielle.
Quotidienne	Sauvegarde tous les fichiers sélectionnés qui ont été modifiés le jour où la sauvegarde quotidienne a été effectuée.
Par copie	Sauvegarde tous les fichiers sélectionnés mais ne les marque pas comme ayant été sauvegardés.

Configuration des types de pare-feu

- **Un pare-feu** interdit le trafic vers un ordinateur ou un segment de réseau.
- **une stratégie de sécurité** - En ouvrant uniquement les ports requis sur un pare-feu, vous implémentez une stratégie de sécurité restrictive.
- Configuring the Windows 7 or Windows Vista firewall can be completed in two ways:
  - **Automatically** - The user is prompted to **Keep Blocking**, **Unblock**, or **Ask Me Later** for unsolicited requests.
  - **Manage Security Settings** – the user adds the program or ports that are required for the applications in use on the network.

Gestion des compte

- Les employés d'une organisation ont souvent besoin de différents niveaux d'accès aux données.
- Lorsqu'une personne quitte une entreprise, ses droits d'accès aux données et au matériel doivent être supprimés immédiatement.
- Il peut s’avérer utile de créer des comptes “Invité” pour les utilisateurs de passages.
- Pour configurer tous les types d'utilisateur et de groupe d'un ordinateur, saisissez **lusrmgr.msc** dans la zone de recherche ou Exécuter.



Procédure de dépannage de base pour la sécurité

Step 1 Identification du problème

Step 2 Élaboration d'une théorie sur les causes probables

Step 3 Test de la théorie en vue de déterminer la cause

Step 4 Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution

Step 5 Vérification du fonctionnement de l'ensemble du système et, s'il y a lieu, implémentation des mesures préventives

Step 6 Documentation des résultats des recherches et des actions entreprises

Step 1 - Identification du problème

Étape 1. Identification du problème	
Questions ouvertes	• Quand le problème a-t-il commencé ? • Quels problèmes rencontrez-vous ? • Quels sites Web avez-vous visités récemment ? • Quel logiciel de sécurité est installé sur votre ordinateur ? • Qui d'autre a utilisé votre ordinateur récemment ?
Questions fermées	• Votre logiciel de sécurité est-il à jour ? • Avez-vous récemment vérifié si votre ordinateur contenait des virus ? • Avez-vous ouvert une pièce jointe dans un e-mail suspect ? • Avez-vous changé votre mot de passe récemment ? • Avez-vous communiqué votre mot de passe à un tiers ?

Step 2 - Élaboration d'une théorie sur les causes probables

- Après avoir discuté avec le client, vous pouvez élaborer une théorie sur les causes probables:

Étape 2. Élaboration d'une théorie sur les causes probables	
Causes courantes des problèmes de sécurité	• Virus • Cheval de Troie • Ver • Logiciel espion • Logiciel publicitaire • Programme malveillant • Hameçonnage (Phishing) • Mot de passe pas assez complexe • Salles d'équipements non protégées • Environnement de travail non sûr

Step 3 - Test de la théorie en vue de déterminer la cause

Étape 3. Tester la théorie en vue de déterminer la cause	
Étapes classiques pour déterminer la cause	• Se déconnecter du réseau • Mettre à jour les signatures de l'antivirus et du logiciel anti-espion • Analyser l'ordinateur avec un logiciel de protection • Rechercher les derniers correctifs et les dernières mises à jour pour le système d'exploitation de l'ordinateur • Redémarrer l'ordinateur ou le périphérique réseau • Ouvrir une session avec un nom d'utilisateur différent afin de changer le mot de passe • Sécuriser les salles d'équipements • Sécuriser l'environnement de travail • Mettre en place une stratégie de sécurité

- Lorsqu'une procédure rapide permet de résoudre le problème, vous pouvez passer à l'étape de vérification du fonctionnement de l'ensemble du système..

Step 4 - Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution

- Après avoir déterminé la cause exacte du problème, établissez un plan d'action en vue de le résoudre et d'implémenter la solution.

Étape 4. Élaboration d'un plan d'action visant à résoudre le problème et à implémenter la solution	
Si aucune solution n'a été trouvée à l'étape précédente, des recherches complémentaires sont nécessaires pour implémenter la solution.	• Journaux des réparations du centre d'assistance • Autres techniciens • FAQ de l'éditeur • Sites Web techniques • Forums de discussion • Guides d'utilisation des ordinateurs • Guides d'utilisation des périphériques • Forums en ligne • Recherche sur Internet

Step 5 - Vérification du fonctionnement de l'ensemble du système et, s'il y a lieu, implémentation des mesures préventive

Étape 5. Vérification du fonctionnement de l'ensemble du système et, s'il y a lieu, implémentation des mesures préventives	
Vérifier le fonctionnement du système complet	• Relancer l'analyse de l'ordinateur afin de vérifier qu'il ne reste pas de virus • Relancer l'analyse de l'ordinateur afin de vérifier qu'il ne reste plus de logiciel espion • Consulter les journaux du logiciel de sécurité afin de s'assurer qu'aucun problème ne subsiste • Rechercher les derniers correctifs et les dernières mises à jour pour le système d'exploitation de l'ordinateur • Tester la connectivité réseau et Internet • S'assurer que toutes les applications fonctionnent • Vérifier l'accès aux ressources autorisées comme les imprimantes partagées et les bases de données • S'assurer que les entrées sont sécurisées • S'assurer que la stratégie de sécurité est appliquée

- Permettez au client de vérifier le fonctionnement de l’ensemble du système.

Step 6 - Documentation des résultats des recherches et des actions entreprises

Étape 6. Documentation des résultats des recherches et des actions entreprises	
Documenter les résultats des recherches et les actions entreprises	• Discuter de la solution mise en œuvre avec le client • Faire vérifier par le client que le problème a été résolu • Fournir tous les documents au client • Dans le bon de travail et dans le journal du technicien, décrire les étapes suivies pour résoudre le problème • Décrire tous les composants utilisés pour la réparation • Indiquer le temps passé pour résoudre le problème

Identification des problèmes courants et des solutions

- Les problèmes de sécurité peuvent être attribués au matériel, aux logiciels, au réseau ou à une combinaison des trois.

Problèmes courants et solutions

Symptôme	Causes du problème	Solutions possibles
Un réseau sans fil a subi une intrusion malgré l'utilisation du chiffrement WEP 128 bits.	Un pirate informatique utilise des outils de piratage de réseau sans fil aisément disponibles pour contourner le chiffrement.	• Passer au chiffrement WPA2. • Utiliser le filtrage d'adresses MAC pour les clients ne prenant pas en charge le WPA2.
Un utilisateur reçoit chaque jour des centaines ou des milliers d'e-mails indésirables.	Le réseau n'assure pas la détection ou la protection du serveur de messagerie contre les spammeurs.	Installer un antivirus ou un logiciel de messagerie permettant de filtrer les e-mails indésirables.
On voit un réparateur d'imprimantes inconnu regarder sous les claviers et sur les bureaux.	Les visiteurs ne sont pas surveillés correctement ou des informations d'identification d'utilisateurs ont été dérobées en vue de pénétrer à l'intérieur du bâtiment.	• Contacter le service de sécurité ou la police. • Conseiller aux utilisateurs de ne jamais cacher leurs mots de passe à proximité de leur espace de travail.

Résumé du chapitre 10

- L'application des procédures de sécurité appropriées protègent les ordinateurs et les équipements du réseau ainsi que les données qu'ils contiennent des dangers physiques - tels les incendies et le vol - et de la perte ou de l'endommagement résultant de l'action d'employés et de pirates.
- Les menaces de sécurité peuvent provenir de l'intérieur ou de l'extérieur d'une organisation.
- Les virus et les vers sont des menaces répandues qui attaquent les données.
- Un plan de sécurité doit être développé et mis à jour pour protéger les données et l'équipement matériel de toute perte.
- Les applications et les systèmes d'exploitation doivent être mis à jour avec les correctifs et les service packs.