et cifom

CPLN Ecole technique

Sécurité

Module 146

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Présentation

À cause de la présence continue de vers, virus et autres menaces pour les ordinateurs, la sécurité des réseaux est toujours l'une des principales préoccupations des dirigeants d'entreprises, même ceux qui utilisent des réseaux simples.

Protéger le réseau de votre entreprise		
Tâches simples	Tâches plus compliquées	Tâches d'un professionnel
Installer un logiciel antivirus	Restreindre l'accès au matériel	Installer un pare-feu matériel
Utiliser des outils de mise à jour des logiciels	Définir des niveaux de permission	Configurer un réseau privé virtuel (VPN)
Installer un programme anti-espion	Supprimer l'accès des anciens employés au réseau	Configurer les fonctions de sécurité sans fil
Installer un pare-feu logiciel	Créer une stratégie d'activité pour Internet et le courrier électronique	Créer des procédures de sauvegarde et de restauration
Installer un logiciel de filtrage du courrier indésirable (spam)	Insister pour que les employés utilisent des mots de passe sûrs	Détection d'attaques - Surveillance des journaux d'événements

1. Tâches simples de sécurité

1.1 Installer et mettre à jour un logiciel antivirus

Les logiciels antivirus effectuent des contrôles permanents pour éviter les infections qui pourraient endommager ou détruire les données de votre réseau.

Sachez toutefois que votre logiciel antivirus ne sera efficace que s'il peut détecter les menaces les plus récentes.

Paramétrez donc votre logiciel antivirus afin qu'il télécharge automatiquement les mises à jour pour vous protéger contre les nouveaux virus.

1. Tâches simples

1.2 Installer et mettre à jour un logiciel antivirus

Les S.E. comme Microsoft disposent d'outils intégrés gratuits que vous pouvez utiliser pour mettre à jour vos logiciels afin de les rendre plus sûrs.

La fonction de mise à jour automatique permet à Windows de rechercher automatiquement les dernières mises à jour en ligne et de les installer, afin de prévenir les menaces de sécurité.

Une fois que vous avez paramétré et activé la fonction de mise à jour automatique, le logiciel se met à jour lui-même.

Un logiciel comme Microsoft Office est également équipé d'un outil de mise à jour automatique.

1. Tâches simples

1.3 Installer une protection anti-espion

Installez et mettez régulièrement à jour un programme anti-espion («anti-spyware»).

Ce programme détecte les logiciels qui tentent de découvrir à votre insu vos mots de passe et numéros de compte.

Le S.E. Windows propose un programme (Windows Defender) et un outil de suppression des logiciels malveillants , que vous pouvez utiliser pour débarrasser vos PC des logiciels indésirables.

1. Tâches simples

1.4 Installer un pare-feu logiciel

Le pare-feu examine les données qui entrent dans votre réseau et les écarte si elles ne répondent pas à certains critères. Il existe des pare-feu logiciels ou hardware.

Les pare-feu logiciels, comme le pare-feu intégré de Windows, protègent non seulement l'ordinateur sur lequel ils sont installés mais constituent également de bons alliés de défense pour les pare-feu matériels.

1. Tâches simples

1.5 Installer un logiciel de filtrage du courrier indésirable (spam)

Le spam est l'ensemble des courriers publicitaires non sollicités qui infiltrent les boîtes aux lettres électroniques.

Ces messages comportent un risque lorsqu'ils contiennent des pièces jointes qui, si elles sont ouvertes, peuvent libérer un virus.

Les courriers indésirables de type phishing incitent leurs destinataires à fournir des mots de passe ou d'autres informations.

Installer un produit de filtrage du spam, ou configurer les filtres de courrier indésirable intégrés dans Outlook, permet de lutter efficacement contre le spam.

2. Tâches de sécurité plus compliquées

Ces tâches requièrent davantage d'expertise technique ou de gestion continue de vos stratégies et procédures de sécurité.

2.1 Restreindre l'accès au matériel

Il est possible d'améliorer la sécurité en restreignant l'accès physique à vos serveurs et équipements réseau, comme les routeurs et les commutateurs.

Si possible, placez ces machines dans une pièce fermée à clé et assurez-vous que seules les personnes habilitées à travailler sur ce matériel en aient les clés.

2. Tâches de sécurité plus compliquées

2.2 Définir des niveaux de permission

Vous pouvez attribuer différents niveaux de permission aux différents utilisateurs des réseaux.

Au lieu de donner un accès « Administrateur » à tous les utilisateurs, ne leur accordez que l'accès à des programmes spécifiques et définissez quels privilèges d'accès sont octroyés pour accéder au serveur.

Vous pouvez par exemple autoriser certains utilisateurs à lire certains fichiers stockés sur le serveur, sans toutefois pouvoir les modifier.

2. Tâches de sécurité plus compliquées

2.3 Supprimer l'accès des anciens employés au réseau

Faites en sorte que les anciens employés ne puissent plus se connecter à votre réseau.

N'attendez pas trop pour supprimer les privilèges d'accès et d'utilisateur des anciens employés, mais car cela pourrait permettre à d'anciens employés malveillants d'endommager ou de voler des fichiers.

2. Tâches de sécurité plus compliquées

2.4 Créer une stratégie d'utilisation pour Internet et le courrier électronique

De nombreux messages électroniques sont infectés par des virus ou autres programmes susceptibles d'endommager vos ordinateurs.

Créez une stratégie Internet au niveau de toute l'entreprise, comprenant l'obligation pour les employés de ne pas ouvrir les pièces jointes dont ils ne sont pas sûrs.

Cette stratégie doit également prendre en compte les activités en ligne risquées et interdire le téléchargement d'utilitaires et autres programmes gratuits.

2. Tâches de sécurité plus compliquées

2.5 Insister pour que les employés utilisent des mots de passe sûrs

Les mots de passe faciles à deviner peuvent permettre à des personnes non autorisées d'accéder à votre réseau.

Pour prévenir ce risque, exigez que les mots de passe contiennent à la fois des chiffres et des lettres. Cela peut être

Les mots de passe doivent être changés régulièrement, mais pas trop souvent : Si les employés ont du mal à se les rappeler, ils pourraient les écrire sur papier et les coller sur leurs moniteurs!

3. Tâches de sécurité d'un professionnel

3.1 Installer un pare-feu de périmètre

Le pare-feu de périmètre est un périphérique matériel qui se branche sur votre réseau et protège l'ensemble des ordinateurs.

L'une de ses caractéristiques est de vous permettre de fermer les ports réseau. Les ports réseau permettant d'établir la communication entre les ordinateurs et les serveurs du client.

Il est possible de renforcer la sécurité de votre réseau et d'empêcher les accès non autorisés en fermant les ports non utilisés.

3. Tâches de sécurité d'un professionnel

3.2 Sécuriser un réseau privé virtuel

Le fait de relier des utilisateurs hors site au réseau de votre entreprise par l'intermédiaire d'Internet leur permet de consulter leurs messages et d'accéder aux fichiers partagés.

Les réseaux privés virtuels (VPN) vous permettent de faire cela avec davantage de sécurité.

Il est préférable de faire appel à un professionnel de la sécurité, car il peut être difficile de configurer un VPN efficace.

3. Tâches de sécurité d'un professionnel

3.3 Configurer les fonctions de sécurité sans fil

Toute personne située dans la zone radio d'un réseau sans fil a la possibilité d'écouter ou de transmettre des données sur le réseau.

Si vous envisagez d'utiliser un réseau sans fil, il faut vous assurer que les fonctions de sécurité soient bien activées et que le cryptage sans fil et les fonctions de contrôle d'accès soient bien configurés.

3. Tâches de sécurité d'un professionnel

3.4 Créer des procédures de sauvegarde et de restauration

Vous pouvez simplement sauvegarder vos fichiers de données sur un support externe (DVD, bandes magnétiques, HD ou SSD) et le stocker ensuite dans un endroit sûr.

Si vous avez besoin que vos données soient accessibles à tout moment, vous ajouterez à votre système du matériel de redondance, afin de dupliquer les fichiers sur un autre disque dur à chaque enregistrement. De cette façon, en cas d'arrêt définitif d'un disque dur, le système de sauvegarde entre en jeu et vous récupérez toutes vos données.

Il est conseillé de sauvegarder les fichiers au moins une fois par semaine et de les restaurer régulièrement, afin de vérifier que le système fonctionne bien.

3. Tâches de sécurité d'un professionnel

3.5 Détection d'attaques - Surveillance des journaux d'événements (ou d'activités)

Un des meilleurs moyens de détecter les intrusions consiste à surveiller les journaux d'événements (en anglais «logs»).

Il s'agit de fichiers où les serveurs stockent une trace de leur activité et en particulier des erreurs rencontrées.

Lors d'une attaque informatique il est rare que le pirate parvienne à compromettre un système du premier coup. Il agit la plupart du temps par tâtonnement. La surveillance des journaux permet de détecter une activité suspecte.

Il est en particulier important de surveiller les journaux d'activité des dispositifs de protection, car il se peut qu'ils soient un jour la cible d'une attaque.