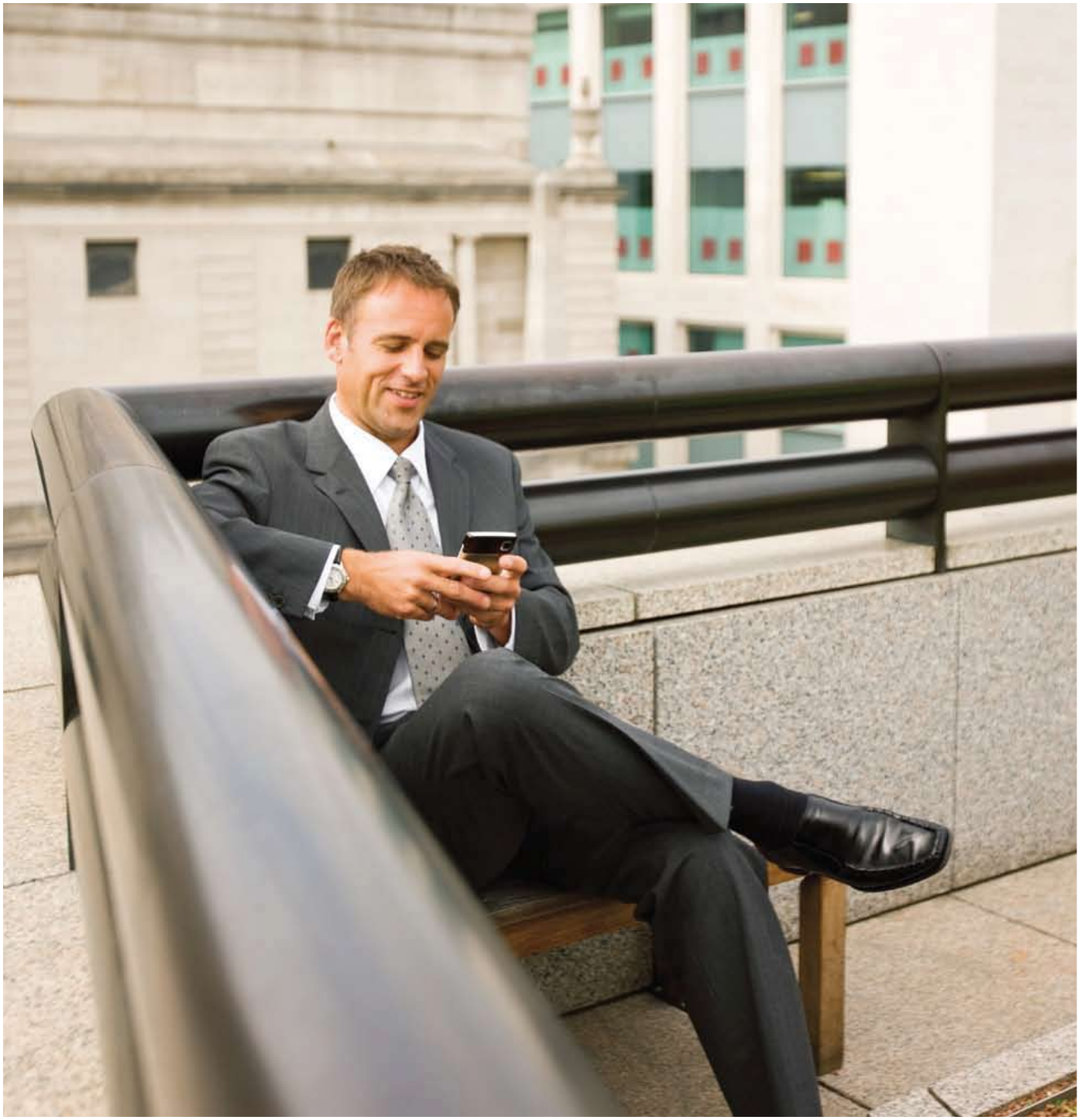
Guide de dépannage Cisco

Pour tirer pleinement parti du système informatique : les dix conseils essentiels concernant la sécurité de votre entreprise



Si vous exercez une activité professionnelle, vous êtes forcément concerné par la sécurité. La sécurité de vos informations est primordiale, tout comme celle de vos locaux et de vos données clients, même si cette activité ne fait pas partie de la mission principale de votre entreprise.
La difficulté réside dans le fait que le nombre d'informations est extrêmement élevé, et que ces informations ne sont pas toutes utiles. Les non-spécialistes sont constamment amenés à se poser des questions telles que : On me dit que j'ai besoin d'un pare-feu, mais Windows est désormais doté d'un pare-feu intégré. Alors en ai-je vraiment besoin ?

Dans ce guide, nous aborderons un certain nombre de points que vous devez étudier et nous vous fournirons différents renseignements dont vous aurez probablement besoin. Nous examinerons également certaines questions relatives à la gestion, plutôt que d'ordre technique, que se posent les personnes chargées de protéger leur entreprise.

Dix Conseils Essentiels

1. L'antivirus :

Un logiciel antivirus est indispensable, mais certains ne sont pas assez efficaces. Comme vous le savez peut-être, ces logiciels ont recours à une base de données qui tient compte de l'évolution des menaces en temps réel. Vous devez donc impérativement mettre à jour régulièrement votre logiciel antivirus.

Toutefois, cela signifie que si votre antivirus ne « connaît » pas un virus spécifique, il n'offre pas une protection totale. C'est pourquoi Cisco conseille d'utiliser, en plus d'un antivirus, un système de prévention des intrusions. La différence est double : tout d'abord, un système de prévention des intrusions inspecte des paquets complets d'informations, à la recherche de tout élément à bloquer. En outre, il surveille le comportement suspect des différents logiciels installés sur votre ordinateur. En d'autres termes, il recherche non seulement les virus qu'il connaît, mais il bloque également toute portion de code tentant d'effectuer une action inhabituelle (supprimer d'autres fichiers ou inspecter votre base de données clients, par exemple). Les spécialistes de la sécurité appellent ceci une attaque de type « jour zéro », signifiant qu'elle exploite une vulnérabilité ou une faille avant que le fabricant ne l'ait identifiée. Nous pouvons bloquer ce type d'attaque si nous surveillons le comportement inhabituel plutôt que le code connu.

Il existe différents niveaux de systèmes de prévention des intrusions : les systèmes basés sur l'hôte et ceux basés sur le réseau. S'il est basé sur le réseau, le système est situé sur le point d'entrée de votre réseau. S'il est basé sur l'hôte, il réside sur votre ordinateur portable et non sur le réseau. Par conséquent, lorsque vous êtes connecté à un autre réseau externe, vous êtes tout de même protégé.

2. Le pare-feu :

Il ne suffit pas de se dire « Je suis équipé d'un pare-feu ». Bien au contraire. Certains sont intégrés dans le système d'exploitation tandis que d'autres sont placés sur d'autres ordinateurs du réseau.

Le plus important est de connaître les éléments que le pare-feu est chargé de surveiller. Un grand nombre d'entre eux surveillent ce qu'ils considèrent comme des attaques sur le réseau, ce qui couvre la majeure partie de vos besoins. Chez Cisco, nous proposons également une protection au niveau des applications, de façon à détecter les situations dans lesquelles une portion de code semble agir sur un programme pour qu'il se comporte bizarrement. En fait, il est primordial de disposer d'un pare-feu ne résidant pas réellement sur votre ordinateur mais sur un autre ordinateur, un routeur ou autre périphérique tenant le rôle de passerelle vers votre réseau. S'il s'agit de la seule passerelle par laquelle le trafic doit passer pour pénétrer dans votre système informatique, il est logique de la doter d'un système de surveillance. L'offre Cisco propose de nombreux niveaux de sécurité.

3. Les employés :

Avant d'étudier plus en détail la technologie, il peut être utile d'évaluer la proportion du risque pour l'entreprise qui n'est pas de nature technique. Voici quelques circonstances dans lesquelles les employés ont perdu des données ou dans lesquelles ces dernières ont été mises en péril :

* Des règles strictes ont été mises en place concernant les données à surveiller lorsqu'elles sont stockées de façon électronique, mais ces règles n'ont pas été appliquées aux documents papier, qui peuvent être oubliés dans un train, le hall d'un hôtel, etc.

* La direction n'a pas assez insisté auprès des employés quant à la nécessité d'éteindre leur écran lorsqu'ils quittent leur poste. Les visiteurs peuvent ainsi consulter des informations confidentielles sur leurs moniteurs. Sachez, d'ailleurs, que les économiseurs d'écran consomment de l'électricité inutilement et qu'il y a bien longtemps qu'ils ne protègent plus l'écran contre toutes menaces.

* On oublierait presque la vieille rengaine, mais elle est toujours d'actualité : le nom de votre conjoint, de votre rue ou de votre chien ne constitue pas un mot de passe sécurisé, tout comme « motdepasse ».

* L'entreprise ne dispose pas d'un règlement clair concernant les actions à entreprendre pour sécuriser le réseau, les personnes en charge de ces actions et les sanctions appliquées en cas d'inexécution de ces actions. Traitez les individus en tant qu'adultes intelligents et vous serez surpris de la rapidité avec laquelle ils souhaitent coopérer.

* Ce règlement doit prévoir que les employés ne sont pas autorisés à télécharger les logiciels de leur choix. Un grand nombre de ces logiciels sont sans doute inoffensifs, mais vous devez contrôler les licences logicielles et vous prémunir contre le risque de logiciels malveillants.

4. Les périphériques :

Il s'agit des périphériques qui entrent et sortent d'un bâtiment : si vous travaillez pour le Ministère de la défense, par exemple, vous devrez laisser votre téléphone mobile ou votre baladeur numérique à l'entrée et le récupérer à la sortie. Ce n'est pas par crainte que les employés passent leur temps à téléphoner ou à écouter de la musique au lieu de travailler, mais parce que les téléphones, appareils photo et autres appareils similaires peuvent contenir des données. Un iPhone 3G (très en vogue actuellement) peut contenir 16 Go d'espace dans certaines configurations. Un individu peut se connecter au port USB d'un ordinateur et quitter le bâtiment après avoir transféré votre liste de clients sur l'appareil qu'il transporte avec lui. En outre, un individu peut introduire un virus dans votre système.

Il n'est peut-être pas nécessaire d'interdire purement et simplement tous types de système de stockage de données personnelles sur le lieu de travail, mais vous pouvez prendre des précautions :

* Les ordinateurs peuvent être configurés pour ne pas accepter les périphériques USB.

* Les logiciels de surveillance intelligents, tels que ceux qui sont intégrés dans tous les produits Cisco, permettent de détecter toute activité suspecte sur votre réseau et de vous la signaler.

* Si des invités se connectent à votre réseau, leur équipement (s'ils utilisent leur propre ordinateur portable) doit faire l'objet d'une analyse antivirus et doit être aussi sécurisé que le vôtre. Nous rappelons que les équipements Cisco contrôlent ces ordinateurs et autres périphériques lors de la connexion, à la recherche de virus connus mais également de toute activité suspecte.

5. La sécurisation des données des télétravailleurs :

Il est évident que la sécurisation de votre réseau en interne est inutile s'il commence à perdre des informations dès que l'utilisateur se trouve en dehors de vos locaux. Cette affirmation se traduit par différents principes à respecter. Tout d'abord, vous devez vérifier que toute liaison entre Internet et votre réseau est effectuée par le biais d'un réseau privé virtuel adapté, comportant toutes les fonctionnalités de sécurité dont il a besoin. Ensuite, assurez-vous que les aspects non techniques de l'activité de vos employés sont soumis aux mêmes règles de sécurité, qu'ils se trouvent dans les locaux ou non. Par exemple, s'ils ne sont pas autorisés à imprimer certains documents ou à transférer des fichiers sur une clé USB lorsqu'ils sont au bureau, ils ne doivent pas s'imaginer que ces activités sont autorisées depuis leur domicile.

Pour respecter ces principes de sécurité, il convient d'installer un réseau intelligemment commuté dans les locaux de l'entreprise et de sécuriser sa passerelle à l'aide des produits Cisco appropriés.

6. Les réseaux sans fil :

L'un des aspects de la sécurisation des données des télétravailleurs consiste à examiner les paramètres des réseaux sans fil, aussi bien en interne qu'en externe lorsque vous pouvez y accéder. Ne vous fiez pas à la mention « réseau sécurisé » qui apparaît lorsqu'un ordinateur portable ou un smartphone le détecte. Cela signifie généralement qu'il est protégé par une clé WEP, or cette technologie est devenue presque obsolète et n'importe quel pirate informatique expérimenté peut la contourner.

Dans les locaux de l'entreprise, tout l'équipement mis en réseau fourni par Cisco dispose d'une fonctionnalité de sécurité intégrée en version standard, qui peut être configurée par nos partenaires experts. En dehors de l'entreprise, vos employés peuvent être amenés à utiliser leur propre équipement sans fil. Il convient d'insister pour qu'ils le sécurisent de la façon suivante :

* Si l'équipement dispose d'une configuration WEP, l'utilisateur doit adopter la technologie WPA.

* Les mots de passe par défaut configurés dans l'équipement doivent être modifiés.

* L'ordinateur et le routeur disposent d'un identifiant, appelé SSID, qui se trouve dans le menu de configuration du routeur. Modifiez-le et désactivez la diffusion du SSID, de sorte que des tiers ne puissent voir votre ordinateur s'ils recherchent des réseaux à pirater.

* Désactivez la connexion automatique aux réseaux Wi-Fi de sorte que l'utilisateur se connecte uniquement aux réseaux que vous considérez comme fiables.

* Attribuez une adresse IP statique à vos machines. Sinon, votre réseau attribue ces adresses de façon aléatoire et vous risquez d'avoir des problèmes si vous souhaitez exclure un équipement particulier.

* Votre routeur est probablement équipé d'un pare-feu. Vérifiez qu'il est activé, car un certain nombre de ces systèmes sont livrés désactivés par défaut.

* Désactivez le réseau si vous comptez ne pas l'utiliser pendant une certaine période.

7. Piratage : quelle est la part de risque ?

Jusqu'à présent, nous avons expliqué comment éviter d'être piraté et comment se protéger contre les intrusions indésirables dans son réseau informatique. Mais quelle est la probabilité qu'un individu tente de pénétrer sur votre système ? De nombreux clients de Cisco sont des petites entreprises et ils se demandent souvent qui pourrait bien s'intéresser à leur système...

Lorsque le piratage était uniquement l'œuvre d'individus, cette question était probablement plus pertinente qu'aujourd'hui. En effet, de nombreux actes de piratage et d'intrusion sont maintenant automatisés. Considérez le pirate comme l'organisateur d'une multitude de vols, qui doit rentrer par effraction dans des maisons non surveillées pour voir s'il y a quelque chose à dérober. Dans notre exemple, les maisons sont les ordinateurs et paraissent identiques. Par conséquent, le seul moyen de savoir s'ils en valent la peine est d'y pénétrer et de jeter un coup d'œil.

Cette tâche, appelée « scannage de ports », est effectuée par des « robots » automatisés sur Internet. Pour résumer, ils accèdent à la « porte » de votre réseau qui donne sur Internet et ils vérifient d'abord si elle est verrouillée. Il est clairement dans votre intérêt de vous assurer qu'elle l'est.

Et n'oubliez pas non plus de fermer les « vraies » portes de votre entreprise ! Cisco propose des caméras qui peuvent être reliées à Internet pour vous permettre de surveiller ce qui se passe dans vos locaux, où que vous soyez. Certaines se déclenchent en fonction des mouvements, ce qui vous permet d'être averti à tout moment si une personne pénètre dans un endroit interdit.

8. Les activités en ligne :

Si tout ou partie de votre activité s'effectue en ligne, vous devez impérativement protéger les informations concernant vos stocks (si elles sont confidentielles) et vos données clients. Toutes les mesures énoncées précédemment participent à cette protection, mais il en existe d'autres. Une fois encore, elles concernent aussi bien la gestion que l'aspect technique et impliquent de ne pas suivre l'exemple de certains hauts fonctionnaires et, par exemple, de ne pas laisser des CD non cryptés dans les transports en commun ! N'oubliez pas de crypter les CD, de sorte que personne ne puisse lire les données même en contournant le mot de passe.

9. Est-ce que cela porte ses fruits ?

La plupart des petites entreprises, notamment en période de crise, sont préoccupées par le niveau de rentabilité potentiel de tout investissement technologique. Cette question est un peu délicate en matière de sécurité, car il s'agit d'actifs incorporels. Vous avez probablement payé l'installation de verrous sur la porte de votre maison, mais vous n'avez jamais calculé le temps que vous avez mis à les rentabiliser. Vous savez seulement ce que vous pourriez perdre s'ils étaient forcés.

Toutefois, il existe un retour sur investissement en matière de sécurité qu'il est facile d'identifier. Si vous gérez une boutique en ligne et que vous ne pouvez pas assurer à vos clients que leurs données sont sécurisées, par exemple, votre activité ne risque pas de prospérer. Si vous avez des invités dans vos locaux et qu'ils se connectent à votre réseau, puis quittent l'entreprise avec un nouveau virus dans leur ordinateur en raison de votre configuration de sécurité, ils seront peu enclins à poursuivre les relations commerciales avec vous. Et on pourrait citer bien d'autres exemples.

Il est toutefois important de souligner qu'un petit équipement de base n'est pas spécialement onéreux. Une petite entreprise comptant quelques employés peut s'équiper d'un routeur sans fil adapté, avec un pare-feu et la sécurité complète, pour moins de 170 euros.

10. La sécurité externalisée :

Si vous ne vous sentez pas d'attaque, nous vous recommandons d'externaliser l'intégralité de votre infrastructure de sécurité. Cisco est associé à de nombreux partenaires, dont le métier consiste à rendre les petites entreprises plus sécurisées qu'elles ne l'étaient auparavant. Et comme ce sont des experts, ils offrent des économies d'échelle et des compétences que vous ne souhaitez pas prendre le temps d'acquérir. De nombreuses petites entreprises sont ravies de transférer toutes leurs données en dehors de leurs locaux, de les confier à une société fiable et qualifiée et de bénéficier ainsi d'un niveau de sécurité supplémentaire.

Comme indiqué en préambule, si vous exercez une activité professionnelle, quelle que soit votre fonction, vous êtes concerné par la sécurité, que vous le vouliez ou non. Heureusement, le point de départ de la sécurisation de votre réseau ne coûte pas les yeux de la tête et vous pouvez faire appel à de nombreux experts pour vous aider.

Bonne chance !