Avec les compliments de TREND MICRO

Sécurité informatique

POUR

LES NULS™

Edition Trend Micro pour les PME-PMI

Protégez votre entreprise

A mettre dans toutes les poches!

Astuces gratuites sur dummies.com

Sécurité informatique

POUR

LES NULS™

EDITION PME-PMI

de Trend Micro

WILEY

A John Wiley and Sons, Ltd, Publication

Sécurité informatique pour les nuls™, edition PME-PMI

Publié par
John Wiley & Sons, Ltd
The Atrium
Southern Gate
Chichester
West Sussex
PO19 8SQ
Angleterre

Pour obtenir des informations détaillées sur la création d'un livre Pour les Nuls personnalisé pour votre entreprise ou organisation, veuillez contacter CorporateDevelopment@wiley.com. Pour obtenir des informations sur la licence de la marque Pour les Nuls pour des produits ou services, veuillez contacter BrandedRights&Licenses@Wiley.com.

Visitez notre site Internet à www.customdummies.com

Wiley édite également ses livres sous divers formats électroniques. Certains contenus publiés peuvent ne pas être disponibles au format électronique.

ISBN : 978-0-470-66694-4

Imprimé et relié en Grande-Bretagne par Page Bros, Norwich

10 9 8 7 6 5 4 3 2 1

Introduction

Vous avez pu constater l'impact des virus, spams et logiciels espions sur les ordinateurs ; ils infectent les fichiers, bloquent les e-mails et, dans certains cas, détruisent même des machines qui étaient en parfait état de marche. Mais quelles sont les répercussions sur une entreprise ? Vous avez instauré des mesures de sécurité informatique de base, mais sont-elles suffisantes ? Et si quelque chose de dangereux est en train de se produire sur vos réseaux, êtes-vous en mesure de le détecter ?

Étant donné la tendance grandissante des entreprises à obtenir davantage à un coût moindre, la sécurité peut descendre de quelques crans sur la liste des priorités. Vous devez vous concentrer sur tellement de sujets différents ! Mais, étant donné que les menaces pour votre sécurité informatique arrivent de tous les côtés, la sécurité devient une dépense de plus en plus incontournable.

Nous allons nous répéter tout au long de ce livre et nous nous en excusons par avance, mais vous ne devez jamais l'oublier : une petite entreprise est particulièrement vulnérable aux menaces informatiques car elle ne dispose pas d'un personnel informatique dédié pour chapeauter l'ensemble. Mais ne vous inquiétez pas : vous protéger est probablement plus facile que vous ne le pensez. Et en lisant ce livre, vous avez fait le premier pas pour atteindre cet objectif.

En d'autres termes, consacrer du temps et des efforts à la protection de votre entreprise vous évitera des coûts et des problèmes par la suite et préservera le succès futur de votre entreprise. Ce livre présente quelques principes de sécurité essentiels pour le chef d'une petite entreprise, examine les principales menaces actuelles et à venir, et présente certaines solutions nouvelles au problème grandissant de la gestion de la sécurité informatique.

Comprendre les menaces auxquelles son entreprise est confrontée, leur impact potentiel et les réglementations à

respecter est le minimum qu'un chef d'entreprise se doive d'assurer. En passant à l'étape suivante et en rédigeant une politique de sécurité (et peut-être même des politiques d'utilisation acceptable pour les employés concernant les e-mails et Internet), vous pourrez vous protéger un peu mieux.

À propos de ce livre

Le présent livre indique qu'un investissement dans la sécurité informatique n'a pas besoin d'être particulièrement élevé ou chronophage. En fait, il est probable que vous ayez déjà mis en place la plupart des mesures de sécurité nécessaires ; vous devez simplement vérifier que les différents outils et mesures de protection fonctionnent de manière coordonnée.

Il n'est pas nécessaire que les dépenses en sécurité soient élevées ; en fait, la sécurité se simplifie et devient meilleur marché.

Tous les jours, vous entendez parler d'attaques de cybercriminels. Ils ne s'intéressent plus uniquement aux grandes entreprises, mais se tournent de plus en plus vers les petites. En effet, les petites entreprises ne disposent pas de défenses aussi solides et ne peuvent pas se payer les conseillers professionnels qui pourraient les aider à les renforcer. Toutefois, les petites et moyennes entreprises s'appuient également sur la Technologie : supprimez leur serveur Internet ou volez leur liste de diffusion et elles se trouvent dans l'embarras.

La bonne nouvelle, c'est que le contrôle et la gestion de la sécurité informatique deviennent plus simples et moins chers. De plus, les contrôles techniques intégrés, proposés par les fournisseurs, deviennent de plus en plus sophistiqués et performants, et différentes solutions émergent pour correspondre aux budgets des entreprises de toutes tailles.

Conventions utilisées dans ce livre

Les livres *Pour les Nuls* ont leurs propres pratiques d'excellence. Par exemple, lorsque ce livre a été imprimé, certaines adresses Internet, qui apparaissent en police pour les faire ressortir, peuvent être coupées et apparaître sur deux lignes de texte. Dans ce cas, soyez certain que nous n'avons pas ajouté de caractères supplémentaires (comme des traits d'union) pour indiquer cette rupture. Ainsi, lors de l'utilisation de l'une de ces adresses Internet, tapez exactement l'adresse qui apparaît dans ce livre en prétendant que la rupture n'existe pas.

Les livres *Pour les Nuls* emploient également des icônes dans les marges pour mettre en lumière des informations spécifiques. Les icônes de ce livre sont :

Les informations situées à côté de cette cible peuvent être utilisées immédiatement.

Cette icône indique des informations à garder à l'esprit pendant la lecture de ce sujet.

Cet icône signale des pratiques particulièrement dangereuses.

Structure du livre

Les domaines qu'une petite entreprise doit prendre en compte afin de gérer les menaces pour la sécurité informatique sont couverts dans les six chapitres de ce petit livre. Nous espérons que les titres vous indiqueront ce que vous devez savoir sur le contenu :

- Chapitre 1 : Évaluer les menaces pour la sécurité
- Chapitre 2 : Initier une politique de sécurité
- Chapitre 3 : Établir une défense coordonnée
- Chapitre 4 : Connaître votre ennemi

- Chapitre 5 : Concevoir des solutions pratiques
- Chapitre 6 : Les dix principales mesures de sécurité informatique pour les petites entreprises

N'ayez pas peur. Ce livre n'est pas un manuel technique (nous laissons cela à d'autres et à vos experts en technologie). Lancez-vous et commencez à découvrir comment améliorer la sécurité de votre petite entreprise !

Chapitre 1

Évaluer les menaces pour la sécurité

Dans ce chapitre

- Découvrez les différentes menaces informatiques auxquelles une petite entreprise est confrontée
- Évaluez leur impact potentiel sur votre entreprise
- Commencez à accorder la priorité aux principaux problèmes
- Consultez les réglementations que vous devez respecter
- Évaluez la réactivité de l'industrie de la sécurité

Le présent chapitre identifie les problèmes fréquents : les menaces pour la sécurité qui viennent consommer les ressources de l'entreprise. Nous observons également l'impact possible de ces menaces sur votre entreprise (de la panne du réseau à la perte financière et aux répercussions négatives sur votre réputation auprès des partenaires et clients).

Sans céder aux prédictions de catastrophisme sur la débâcle imminente de la Technologie de l'Information (TI), il existe certains risques dont vous devez être conscient et des réglementations que vous devez respecter. En planifiant à l'avance un désastre potentiel, vous ne paniquerez pas s'il survient réellement.

Reconnaître les principales menaces

Depuis que les systèmes informatiques et les réseaux sont entrés dans les petites entreprises à la fin des années 1980, plusieurs menaces ont plané au-dessus de leur tête. Si vous êtes du genre à voir le verre à moitié plein et que vous pensez que ces dangers sont exagérés, ou que vous êtes un adepte de la théorie de la conspiration qui pense qu'elles ont été minimisées, ce qui est certain, c'est qu'elles ne disparaîtront pas.

Une enquête sur la sécurité informatique a indiqué que les petites entreprises ont déclaré en moyenne six incidents par an, voire plus pour certaines. Ce chiffre peut paraître insignifiant, mais si votre entreprise compte moins de 50 employés et ne dispose d'aucun service informatique dédié, chaque faille de sécurité ne constitue pas uniquement un problème en soi, elle peut également épuiser vos ressources de manière considérable.

Comprendre ces menaces est le premier pas à faire pour les affronter. En cette période d'usurpation d'identité, de spams et de logiciels espions (logiciels indésirables qui surveillent secrètement l'activité d'un utilisateur dans l'intention d'enregistrer des informations personnelles et de les transmettre), vous pourriez être surpris d'apprendre à quel point certaines de ces menaces, comptant parmi les plus graves, peuvent être dangereuses.

Selon cette enquête, les types d'incidents les plus graves auxquels sont confrontées les entreprises sont les suivants, classés par ordre de fréquence :

- Panne du système ou corruption des données
- Infection virale ou logiciel destructeur
- Mauvais usage des systèmes d'information par le personnel
- Accès non autorisé par des tiers (y compris des tentatives de piratage)
- Vol physique de l'équipement informatique

- Vol ou fraude à l'aide d'ordinateurs
- Vol ou divulgation non autorisée d'informations confidentielles

Glossaire des principales menaces

Savoir différencier un *botnet* d'un *Cheval de Troie* est un savoir important dans le royaume de la sécurité informatique. Vérifiez donc les définitions de la liste suivante :

- **Logiciel publicitaire (*adware*) :** logiciel qui affiche des bannières publicitaires dans les navigateurs comme Internet Explorer et Mozilla.
- **Porte dérobée (*backdoor*) :** application qui permet à des systèmes distants d'avoir accès aux ordinateurs.
- **Botnet ou Bot :** cheval de Troie contrôlé à distance qui infecte des hôtes Internet ; une collection est connue sous le nom de réseau de zombies (*botnet*).
- **Attaque par saturation (*denial of Service – DoS*) :** cheval de Troie qui interrompt ou empêche le flux entrant et sortant des données du système, rendant ce dernier inutile au final. Tout programme malveillant qui arrête le fonctionnement normal d'un système ou d'un réseau.
- **Enregistreur de frappe (*keylogger*) :** logiciel espion qui indique les frappes sur les touches ; souvent utilisé pour collecter le nom d'utilisateur et le mot de passe.
- **Programme malveillant (*malware*)** : abréviation de **mal**icious soft**ware** ; tout programme, logiciel ou code malveillant.
- **Hameçonnage (*phishing*)** : technique employée pour duper les utilisateurs à l'aide d'e-mails d'apparence légitime afin de collecter des données personnelles sur un site Internet factice.
- **Accès frauduleux aux privilèges Root (*rootkit*)** : collection d'outils qu'un pirate utilise pour masquer son intrusion et avoir accès à un réseau ou un système.
- **Courrier non sollicité (*Spam*) :** E-mail à risque non sollicité ; peut contenir des liens vers un code malveillant.
- **Spoofing** : programmation d'ordinateurs pour usurper l'identité de quelqu'un d'autre. Le spoofing IP utilise une fausse adresse IP pour accéder à un réseau.
- **Logiciel espion (*spyware*)** : logiciel indésirable qui surveille secrètement l'activité d'un utilisateur et enregistre en général

(continu)

(continu)

des informations personnelles pour les transmettre.

- **Cheval de Troie (*trojan*)** : programme apparemment inoffensif, mais dont l'intention cachée est malveillante.
- **Virus :** code écrit afin de se répliquer. Un virus tente de se répandre d'un ordinateur à l'autre en infectant d'autres fichiers.
- **Ver (*Worm*) :** type de *virus* qui peut répandre des copies de lui-même ou de ses segments sur les réseaux.
- **Vulnérabilité Jour Zéro (*Zero-day exploit*) :** programme malveillant qui exploite une faille récemment découverte dans un système avant qu'un correctif ne soit disponible.

Et, avant que vous ne soyez certain que votre entreprise est protégée contre toutes ces menaces, nous soulignerons l'évolution constante des attaques informatiques. L'infection virale était notamment la menace la plus sérieuse il y a quelques années, représentant la moitié de tous les incidents de sécurité dans cette étude. Mais aujourd'hui, elle ne représente que 21 %, et les dangers les plus graves sont les pannes de systèmes / corruption de données. Qui sait quel sera le problème numéro un dans quelques années ou dans quelques mois ? Dans le Chapitre 5, nous vous proposons des conseils afin de maintenir la flexibilité de votre système pour qu'il s'adapte aux problèmes futurs.

Alors que la TI gagne en sophistication, n'oubliez pas de prendre en compte les menaces fondamentales. Le mauvais usage des systèmes par les employés est une menace prioritaire de la liste actuelle. Avec la sophistication grandissante des systèmes de sécurité informatique, certaines entreprises oublient peut-être simplement de fermer les accès par les fenêtres et les portes.

Impact des failles de sécurité

Les failles de sécurité peuvent avoir de graves conséquences pour votre entreprise, de la perte financière aux atteintes à la réputation de votre entreprise.

Selon l'enquête visée précédemment, le coût moyen de l'incident le plus grave pour une petite entreprise variait de 11500 à 23000 Euros. Évidemment, cette statistique implique que certaines entreprises ont perdu beaucoup plus. Les plus gros problèmes naissent souvent d'une combinaison de répercussions. Pour une petite entreprise, la continuité des affaires ou la perte de productivité constitue l'aspect le plus important.

Étant donné votre dépendance actuelle envers l'informatique, la perturbation des activités quotidiennes de votre entreprise peut être catastrophique. Examinez simplement les scénarios suivants :

- Votre réseau tombe en panne de courant ou le serveur ne fonctionne pas correctement. Quel est l'impact financier de chaque heure de productivité perdue ?
- Votre site Internet ne fonctionne plus et vous perdez une journée de commandes. Quels seront les pertes de revenus et les préjudices pour votre réputation ?
- Vos employés passent du temps à surfer sur des sites Internet qui n'ont aucun rapport avec votre activité, comme Facebook ou MySpace. Quel est le coût en termes de perte de productivité, et quels sont les risques pour votre système informatique ?

Les employés peuvent porter directement atteinte à votre réputation en consultant un contenu illicite sur Internet. Indirectement, leur navigation peut menacer l'entreprise en récoltant des programmes malveillants qui peuvent s'infiltrer sur l'un de vos ordinateurs et installer des logiciels espions ou un *botnet* pour héberger des documents restreints que des utilisateurs distants vont visualiser ou partager.

Selon l'enquête, les incidents graves deviennent encore plus sérieux. Le nombre global peut diminuer, mais il suffit d'un seul événement catastrophique pour faire faillir votre entreprise.

Observez l'impact occulté des failles de sécurité. Souvent, les problèmes les plus graves sont ceux auxquels vous ne pensez pas immédiatement, comme la perte d'une information commerciale importante dont vous avez besoin pour conclure une transaction, ou le transfert de données à un concurrent ou un criminel.

Vérifiez votre assurance pour être certain qu'elle vous couvre contre les pertes financières qu'une faille importante peut engendrer. Mettez en place des programmes de reprise sur sinistre et de continuité des affaires afin de pouvoir reprendre le travail le plus rapidement possible après un tel événement.

Les sections suivantes présentent certaines des répercussions des failles de sécurité.

Reprise après une panne d'ordinateurs, du réseau ou du site Web

La majeure partie des incidents de sécurité entraîne un temps d'arrêt, sous une forme ou une autre. Un incident majeur peut entraîner l'arrêt complet d'un ordinateur, d'un réseau ou d'un serveur Web. Même un problème moins grave, comme une *attaque par saturation* (une tentative pour empêcher les utilisateurs d'accéder à un système ou un réseau) peut transformer votre réseau en tortue.

Le temps peut être un élément critique ; si votre ordinateur tombe en panne pendant que vous travaillez sur une nouvelle transaction très importante, qui peut dire quel sera le coût final de cette interruption ? De même, si votre site Internet n'est pas disponible quand un client veut passer une commande ou envoyer une demande, ce client pourrait ne jamais revenir.

Un ralentissement du système teste entièrement l'efficacité de vos plans de secours. Avec de bons plans de reprise après sinistre ou de continuité des affaires, vous pouvez restaurer les données perdues ou passer sur une machine ou un réseau redondant, et continuer à travailler comme si rien ne s'était passé.

Dommages, destruction ou vol de données

Vous n'en avez peut-être pas conscience, mais la plupart des entreprises dépendent des données pour bien fonctionner.

Que cela vous plaise ou non, les données graissent les rouages de votre entreprise, de la simple liste de noms et d'adresses de clients aux droits de propriété intellectuelle fondamentaux qui rendent vos produits et services uniques, en passant par l'administration des paiements et factures. Quand ces données confidentielles sont endommagées, détruites ou volées, les problèmes peuvent être considérables.

Le vol des informations clients peut s'avérer extrêmement préjudiciable. Combien de fois un vendeur a-t-il quitté son entreprise en emmenant ses clients les plus importants avec lui ? Ou, dans le cas des droits de propriété intellectuelle, combien de directeurs ont quitté une entreprise pour en créer une autre qui finit par lui ressembler étrangement ? Des données incomplètes ou manquantes peuvent provoquer des dommages tout aussi importants, et leur absence est souvent constatée uniquement après les faits, quand il s'agit de faire appliquer des contrats ou de réaliser des tâches administratives.

Les grandes entreprises ont mis en place des garde-fous pour éviter ce type de problèmes. Pour les petites entreprises, ces scénarios se produisent bien trop souvent.

Selon la dernière étude de TrendLabs, les programmes de vol de données sont l'une des catégories de menaces dont l'évolution est la plus rapide aujourd'hui. Ils peuvent prendre plusieurs formes et vous pouvez ne pas vous rendre compte du moment où cela se produit. L'objectif principal est de capter des données sensibles sur les ordinateurs des utilisateurs et de les envoyer à des opérateurs criminels pour une exploitation directe ou une vente sur le marché noir.

Usurpation d'identité et vol de mot de passe

Nous connaissons tous les dangers d'une usurpation d'identité dans l'environnement de consommation actuel. Mais vous ne savez peut-être pas qu'elle est tout aussi dangereuse sur le plan commercial. En volant des mots de passe et des codes d'entrée, les fraudeurs peuvent se faire passer pour les représentants officiels d'une entreprise.

Étant donné que les comptes d'une entreprise fonctionnent souvent à l'aide de crédits, les imposteurs se faisant passer

pour des directeurs peuvent contracter des dettes considérables avant d'être démasqués. Ensuite, au moment de régler les factures à la fin du mois, l'entreprise a une surprise très désagréable. Dans 88 % des failles les plus graves, aucune perte financière n'a été subie. Mais ne s'agit-il pas d'un déni de la part des entreprises ?

Selon le groupe de sécurité en ligne *Get Safe Online*, l'usurpation de l'identité d'une entreprise peut prendre de nombreuses formes, notamment :

- Création d'un compte marchand au nom de votre entreprise, puis acceptation de nombreux achats à l'aide de cartes de crédit volées et dépôt des recettes sur le compte bancaire des criminels. Quand vous recevez les plaintes des clients et que la société de cartes de crédit vous contacte au sujet des factures, les voleurs ont disparu.
- Fouille des poubelles pour obtenir les noms, les informations bancaires et autres informations sensibles sur les employés.
- Commande de marchandises auprès de votre site d'e-commerce avec des cartes de crédit volées ou par téléphone avec de fausses informations bancaires (destinées à ressembler à une vraie société).
- Piratage de votre site Internet pour présenter des informations factices ou dommageables, ou détournement de votre site pour diffuser de la pornographie.
- Utilisation d'un programme de vol de données pour collecter les noms d'utilisateurs et les mots de passe de votre compte bancaire et transférer vos fonds vers un autre compte.

Selon l'étude 2009 du Centre de recherche pour l'étude et l'observation des conditions de vie (CREDOC), l'usurpation d'identité coûte à l'économie française 4 milliards d'euros par an.

Vol financier

Les vols financiers déclarés par les entreprises sont en réalité assez rares. L'enquête de 2008 sur les failles de sécurité de l'information indique qu'aucune perte financière n'a été subie dans 88 % des failles les plus graves. Toutefois, ce chiffre

relativement faible peut découler du fait que les entreprises gèrent les vols internes en leur sein, ou nient simplement ces vols. Après tout, personne n'aime avouer s'être fait voler de l'argent.

Cependant, si l'on considère les failles de sécurité sous un autre angle, la plupart des attaques actuelles sont motivées par l'argent, un paiement financier quelconque constituant l'objectif final. Ainsi, si votre entreprise ne perd pas d'argent, il est probable qu'une autre personne sera flouée en aval.

Coûts de la réactivité

La mise en place d'une réaction à un incident de sécurité peut coûter très cher, bien que l'évaluation de toutes les dépenses liées à celle-ci soit difficile.

Certains de ces coûts ne seront pas immédiatement perceptibles, notamment :

- **Temps d'arrêt de travail :** étant donné que le personnel représente le coût le plus élevé d'une entreprise, les perturbations subies par les employés représentent l'impact le plus important d'un incident. Et il ne s'agit pas uniquement du temps passé par le personnel qui réinstalle les systèmes d'exploitation et restaure les données, mais également du coût de toutes les personnes incapables de travailler pendant la restauration des systèmes.
- **Perte d'opportunités :** dans le monde des affaires, le temps, c'est de l'argent, et le *coût d'une opportunité perdue* (le revenu potentiel que vous auriez pu dégager si vous n'aviez pas subi cet incident) est un autre facteur à prendre en compte.

En moyenne, selon l'enquête précédemment citée, les entreprises dépensent entre 1200 et 2300 euros pour reprendre leurs activités après un incident grave, en plus des coûts liés au personnel.

Préjudice pour votre réputation

Dans le cadre d'une faille de sécurité, l'image de votre entreprise auprès des clients est l'un des aspects intangibles d'une

faille de sécurité les plus difficiles à quantifier. Les clients et les partenaires se moquent probablement de savoir que vous étiez occupé à réparer une faille de sécurité. Tout ce qu'ils savent, c'est que vous n'avez pas été en mesure de fournir le service qu'ils attendaient. Les clients, les partenaires et les investisseurs peuvent par la suite vous considérer comme une entité à risque.

En outre, le comportement de vos employés envers ce qu'ils considèrent comme une perte de temps inutile peut avoir une influence sur leur engagement et leur productivité.

En tant que petite entreprise, vous pensez peut-être que votre réputation n'est pas affectée par un incident de sécurité. Mais si un client se demande s'il fait bien de travailler avec un petit fournisseur, les problèmes de sécurité réguliers confirmeront ses suspicions et l'inciteront à travailler avec un acteur plus grand qui sera en mesure de gérer ces attaques.

Évaluer l'ampleur de la menace pour votre entreprise

Il est évident que l'ampleur des menaces affectant la sécurité de l'information varie d'une entreprise à l'autre. Pour une start-up dans le domaine des hautes technologies disposant d'actifs numériques en grande quantité, le défi consiste à protéger le protocole IP et à gérer sa réputation et ses relations avec les fournisseurs et les acheteurs. Pour une société plus traditionnelle, comme une société de taxis, la sécurité informatique consiste principalement à gérer son infrastructure de communication et les ordinateurs de son réseau.

Certaines menaces sont universelles : le vol physique du matériel informatique affecte toutes les entreprises car le remplacement des produits volés a un coût. Mais il est également nécessaire de penser aux vulnérabilités spécifiques de votre entreprise et aux menaces qui peuvent vous concerner. Utilisez le tableau 1-1 pour consulter les principales menaces et vérifier les vulnérabilités de votre entreprise dans la première colonne (les coches représentent les domaines dans lesquels les principales menaces pourraient avoir un impact).

Tableau 1-1 Vérifier les vulnérabilités et les menaces

	Panne système	Infection virus/ logiciels malveillants	Mauvaise utilisation par le personnel	Accès non autorisé	Vol physique	Vol d'ordinateurs	Vol d'informations
Site Internet	✓	✓		✓	✓		
Données confidentielles				✓	✓		✓
Infrastructure de communication critique	✓				✓		
Traitement critique pour une mission	✓	✓	✓	✓	✓	✓	✓
Communications par e-mails	✓						
Autre							

Une évaluation formelle des risques, par un tiers indépendant qui notera les points vulnérables de votre configuration informatique et soulignera les risques auxquels vous pourriez être confronté, est un exercice nécessaire. Certains fournisseurs réaliseront cette étude à prix réduit dans l'espoir d'un contrat futur. Chaque configuration est différente. Il convient donc de faire appel à un expert pour une étude personnalisée ; vous pourriez être surpris des résultats.

Responsabilités légales

Il existe de nombreuses lois que vous devez garder à l'esprit quand vous évaluez vos responsabilités en matière de sécurité informatique. Votre organisation doit essentiellement se préoccuper de ses responsabilités en matière de vie privée et de communications électroniques, ainsi que du traitement du personnel, tout en tenant compte de la vague de réglementations de la Commission Européenne.

Respect de la vie privée et des communications

La responsabilité d'une entreprise qui traite des données personnelles est établie par la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés. Cette loi stipule que les entreprises doivent respecter certains principes. Ainsi, toute donnée détenue doit :

- Être traitée de manière équitable et légale
- Être traitée pour des raisons limitées
- Être adéquate, appropriée et non excessive
- Être précise et à jour
- Ne pas être conservée plus longtemps que nécessaire
- Être traitée en accord avec les droits de la personne
- Être protégée
- Ne pas être transférée vers d'autres pays sans protection appropriée.

La Loi accorde également aux individus un droit d'accès aux informations qu'une entreprise détient sur eux.

Par ailleurs, la Directive « Vie privée et communications électroniques » de 2002 établit également le traitement des messages de marketing non sollicités, que ce soit par téléphone, par télécopie, par e-mail ou par courrier. Si vous désirez passer des appels téléphoniques, envoyer des télécopies ou des e-mails automatisés, vous devez obtenir le consentement du souscripteur, bien que les e-mails soient autorisés si l'adresse a été reçue dans le cadre d'une relation commerciale. Cette Directive de la Commission Européenne (CE) permet au consommateur de refuser d'être contacté. Elle régit également l'emploi des cookies, ces petits fichiers placés sur le système des utilisateurs lorsqu'ils visitent un site Internet.

Traitement légal du personnel

Les responsabilités des entreprises envers leurs employés sont traitées dans un vaste ensemble de réglementations, notamment :

- Loi Informatique et Libertés de 1978
- Directive « Vie privée et communications électroniques » de 2002
- Loi sur le secret des correspondances émises par la voie des communications électroniques de 1991qui limite l'interception des télécommunications

- Les Droits de l'Homme, tels qu'établis dans la Déclaration des Droits de l'Homme et du Citoyen de 1789 et dans la Convention Européenne des Droits de l'Homme
- L'article 226-1 du Code Pénal qui interdit l'interception des communications des employés sans leur consentement.

Chaque texte aborde un aspect spécifique, mais le grand principe de base est la confidentialité des contrats entre l'organisation et l'employé, et la sécurisation des données personnelles.

Un certain nombre de directives européennes supplémentaires et de réglementations locales sont actuellement en phase d'examen, y compris des directives sur l'utilisation inappropriée des informations sur le personnel.

La réponse de l'industrie de la sécurité

Dans les premiers temps de la sécurité informatique, les fournisseurs privilégiaient le domaine des logiciels antivirus et des pare-feux. Mais ce secteur commence aujourd'hui à s'élargir car les entreprises se rendent compte qu'elles ont besoin d'une défense coordonnée contre les attaques mettant à mal la sécurité de leurs informations.

Les pare-feux et les technologies de lutte contre les programmes malveillants sont devenus plus sophistiqués et ont été regroupés dans des suites logicielles, intégrant d'autres fonctionnalités comme les programmes antispam et anti-logiciel espion. La *sécurité des Terminaux*, axée exclusivement sur les ordinateurs ou autres dispositifs utilisés au niveau de l'utilisateur final, se voit complétée par certaines capacités de la *sécurité de la passerelle* (la sécurité placée devant la connexion Internet) en vue de bloquer spécifiquement les menaces du Web avant qu'elles n'atteignent leurs cibles. La nouvelle tendance consiste à instaurer une protection en couche, à la fois au niveau de la passerelle Internet et des terminaux.

L'émergence des services de sécurité hébergés est un autre développement bienvenu pour les petites entreprises. Ils réduisent les frais informatiques, à la fois en termes de

matériel et de gestion, et ils sont plus fiables car les éléments de la solution sécuritaire sont hébergés sur les serveurs du fournisseur de sécurité. Nous aborderons ce sujet plus en détail dans le prochain chapitre.

Vous pensez peut-être avoir besoin de solutions de sécurité installées sur site, mais beaucoup d'entreprises utilisent désormais des services hébergés sous la forme de Webmail, ou encore des logiciels de gestion de la relation client (GRC, ou CRM en anglais). Ne sous-estimez pas l'utilité du service de sécurité hébergé : les entreprises qui développent les logiciels sont les mieux placées pour les gérer, et elles disposent de capacités de traitement que vous ne pouvez même pas imaginer.

Le modèle de facturation « à l'utilisation » permet également de prévoir le coût mensuel pour votre bilan sans avoir à vous inquiéter du coût des mises à jour futures au fil de l'évolution de la sécurité informatique.

Chapitre 2

Initier une politique de sécurité

Dans ce chapitre

- Comprendre la nécessité d'une politique de sécurité
- Connaître les normes et les pratiques d'excellence
- Gérer la sécurité
- Appliquer des contrôles techniques

Après avoir reconnu les menaces et adopté les principes d'une bonne sécurité informatique (voir Chapitre 1), votre prochaine question pourrait bien être : par où commencer? Si vous avez déjà évalué la nature des risques auxquels votre entreprise est exposée, la première étape consiste à établir une politique de sécurité pour votre entreprise et à la communiquer à vos employés.

Ensuite, vous devez réfléchir à la méthode d'application de cette politique, notamment la technologie déjà en place pour contrôler les risques sécuritaires, et aux éventuelles failles que vous devez combler. Cependant, la technologie n'est qu'une partie de la solution, qui englobe également les individus, les procédures et les politiques.

Ce chapitre aborde également les différentes pratiques d'excellence que les entreprises peuvent utiliser et ce que nous pouvons en apprendre.

Formuler une politique de sécurité

La politique de sécurité d'une entreprise est la fondation sur laquelle repose une bonne sécurité informatique. Une *politique de sécurité* est une déclaration d'intention concernant les méthodes envisagées pour protéger vos actifs numériques et surveiller l'organisation. Elle représente un référentiel d'informations central pour la gestion, le personnel et les tiers, et regroupe tout, des processus et procédures à une description des mesures techniques en place et des méthodes de reprise sur sinistre, en passant par les fonctions et responsabilités des employés.

Votre politique de sécurité doit s'appuyer sur l'analyse des risques mentionnée dans le chapitre précédent et sur une connaissance des menaces les plus sérieuses auxquelles vous êtes confronté.

Pour qu'elle fasse autorité, une politique de sécurité doit être approuvée par la direction supérieure et révisée quand les circonstances changent. Nul besoin d'entrer dans les détails sur chaque sujet. Considérez la politique de sécurité comme un plan d'action qui décrit dans les grandes lignes les informations critiques de la société et les méthodes de protection de celles-ci.

Il vaut mieux adopter une approche par couches pour composer une politique de sécurité en commençant par énoncer une mission de haut niveau, puis en approfondissant avec les appareils physiques, les fonctions et les responsabilités du personnel, en intégrant notamment des références à l'usage acceptable, à la gestion des incidents, etc. Elle permet également de préciser les plans de continuité des affaires et de reprise après sinistre.

Éléments à intégrer

Si les politiques de sécurité varient d'une entreprise à l'autre, elles doivent néanmoins toujours comprendre les éléments suivants :

- Une explication claire des principes de la politique, notamment les objectifs finaux et l'importance stratégique de la sécurité de l'information pour l'entreprise.
- Une déclaration de soutien de la direction supérieure, démontrant son engagement envers la sécurité de l'information.
- De la formation pour permettre aux employés de comprendre la sécurité de l'information et les risques.
- Une explication sur les normes de sécurité minimales mettant l'accent sur les procédures à suivre dans les domaines particulièrement importants pour l'entreprise. Chaque politique de sécurité devrait notamment aborder les précautions élémentaires en matière de virus informatiques, les directives sur le comportement à adopter sur Internet, et les instructions pour créer des mots de passe.
- Des définitions des fonctions et responsabilités au sein de l'entreprise en matière de sécurité de l'information.
- Les procédures à adopter concernant les incidents de sécurité : déclaration, traitement et résolution.
- Les plans de continuité des affaires qui expliquent comment l'entreprise peut continuer à fonctionner en cas de panne due à une catastrophe comme un incendie ou une inondation.
- Des références aux documents de support, comme les politiques du personnel, les procédures, les directives ou les spécifications et normes sur la sécurité. Par exemple, si vous désirez expliquer en détail la politique Internet, vous pouvez inclure :
    - L'utilisation d'Internet par l'entreprise et les menaces associées
    - Les services Internet qui peuvent être utilisés et ceux qui sont interdits
    - La personne qui autorise les connexions Internet
    - La personne responsable de la sécurité informatique
    - Les normes, directives et pratiques à suivre.

La protection des mots de passe est souvent l'un des maillons faibles de la chaîne de sécurité d'une entreprise car les utilisateurs notent leurs mots de passe sur un post-it collé à côté de leur machine ou conservent le mot de passe par défaut. Votre politique de sécurité doit les mettre en garde contre ce type de comportement risqué et établir des protocoles sécurisés pour la protection des mots de passe.

Par ailleurs, il peut être souhaitable d'établir une *politique d'utilisation acceptable* au sein de la politique de sécurité. Elle précisera ce que l'entreprise considère comme acceptable et inacceptable.

Vous pouvez intégrer des politiques d'utilisation acceptable distinctes pour l'accès à Internet, pour les e-mails et pour l'utilisation de tous les actifs informatiques de votre entreprise. Nous aborderons les politiques d'utilisation acceptable de façon plus détaillée dans la section suivante.

Ne vous lancez pas dans des descriptions minutieuses des politiques et procédures applicables à chaque actif informatique. Une politique de sécurité vise essentiellement à faire comprendre aux employés les objectifs principaux, les raisons de l'instauration de certaines mesures et les conséquences d'une infraction.

Définir l'utilisation acceptable

La protection de vos actifs informatiques commence par les employés à qui vous devez communiquer des directives claires sur l'utilisation acceptable, la confidentialité et les normes de sécurité. Une *politique d'utilisation acceptable* stipule ce qui est autorisé et ce qui est interdit pendant les heures de travail et en utilisant les ordinateurs de l'entreprise, et explique les répercussions du non-respect de cette politique.

Sans directive claire, les employés peuvent exposer l'entreprise à des programmes malveillants, partager des informations confidentielles sur Internet ou faire sortir de l'entreprise des informations sensibles sur des ordinateurs portables ou des clés USB.

Les politiques d'utilisation acceptable peuvent sembler draconiennes, mais, tant qu'elles établissent un équilibre entre pragmatisme et contrôle et que l'entreprise communique clairement les risques qu'elle tente d'éviter, les employés comprendront son importance. Vous pouvez même intégrer les employés dans le processus de conception de ces politiques, obtenant ainsi leur adhésion dès le premier jour, et les encourager à communiquer leur opinion sur le fonctionnement ou non de certaines restrictions.

En liant les politiques d'utilisation acceptable aux contrats des employés et aux procédures disciplinaires, vous les intégrez pleinement dans la culture de l'entreprise.

Naviguer sur Internet sans mettre en danger l'entreprise

Vos employés ont besoin d'Internet dans leur travail. Il arrive cependant qu'Internet fasse diminuer la productivité et expose votre entreprise à des menaces.

Dans une politique Internet, vous pouvez inclure ce qui suit :

- Les délais acceptables et inacceptables d'une utilisation privée d'Internet. Vous pouvez notamment interdire aux employés d'aller sur Facebook pendant les heures de travail.
- Les types de contenu interdit (pornographie, obscénité, haine raciale, etc.).
- Les méthodes de gestion des informations confidentielles : ne pas les partager en dehors du réseau privé de l'entreprise par exemple.
- Les méthodes de traitement des biens de l'entreprise, comme les ordinateurs portables.
- Les directives sur le téléchargement et l'installation de logiciels.
- Les directives sur la sécurité, comme les réglages de sécurité des navigateurs.
- Une interdiction sur le partage et le téléchargement de documents protégés par des droits d'auteur.
- Les informations détaillées sur toute activité de surveillance mise en place par l'entreprise.
- Les conséquences d'un non-respect de cette politique.

Comment faire appliquer cette politique ? Un programme de filtrage des sites Internet peut permettre d'éviter ou de détecter certains problèmes.

Modèle d'une politique d'utilisation acceptable

Ce texte établit une politique d'utilisation acceptable pour Internet. Vous pouvez le copier et l'adapter à vos besoins.

L'utilisation d'Internet par les employés de [nom de l'entreprise] est autorisée et encouragée quand une telle utilisation soutient les buts et objectifs de l'entreprise. Toutefois, [nom de l'entreprise] a instauré une politique quant à l'utilisation d'Internet selon laquelle les employés doivent s'assurer de :

- *Respecter la législation en vigueur*
- *Utiliser Internet de manière acceptable*
- *Ne pas créer de risques inutiles pour l'entreprise par une mauvaise utilisation d'Internet.*

Comportement inacceptable

Les points suivants sont en particulier considérés comme une utilisation ou un comportement inacceptable des employés :

- *Visiter des sites Internet qui contiennent des documents obscènes, haineux, pornographiques ou autre contenu illicite*
- *Utiliser l'ordinateur pour perpétrer une fraude quelconque ou un piratage de logiciel, de film ou de musique*
- *Utiliser Internet pour envoyer des documents offensants ou harceler d'autres utilisateurs*
- *Télécharger un logiciel commercial ou tout document protégé par des droits d'auteur qui appartient à des tiers, sauf si ce téléchargement est couvert ou autorisé par un accord commercial ou toute autre licence*
- *Pirater des zones non autorisées*
- *Publier des documents diffamatoires et/ou sciemment mensongers à propos de [nom de l'entreprise], de vos collègues et/ou de nos clients sur des sites de réseau social, des blogs (journaux en ligne), des sites Wiki (forums de discussion en ligne) et sous tout autre format de publication en ligne*
- *Entreprendre délibérément des activités qui visent à gâcher les efforts du personnel ou les ressources du réseau*

- *Introduire un logiciel malveillant sous quelque forme que ce soit sur le réseau de l'entreprise.*

Informations de l'entreprise détenues sur des sites Internet tiers

Si vous produisez, collectez et/ou traitez des informations commerciales pendant votre travail, lesdites informations restent la propriété de [nom de l'entreprise]. Ces informations regroupent les données stockées sur des sites Internet tiers, notamment des fournisseurs de service d'e-mail et des sites de réseau social comme Facebook et LinkedIn.

Contrôle

[nom de l'entreprise] reconnaît qu'Internet est un outil commercial important. Toutefois, une mauvaise utilisation de cet outil peut avoir un impact négatif sur la productivité des employés et la réputation de l'entreprise.

Par ailleurs, toutes les ressources de l'entreprise associées à Internet sont fournies pour des raisons commerciales. Par conséquent, l'entreprise se réserve le droit de contrôler le volume du trafic Internet et du réseau, conjointement aux sites Internet visités. Le contenu spécifique de toute transaction ne sera pas contrôlé sauf en cas de suspicion d'utilisation inappropriée.

Sanctions

Si un employé est suspecté d'avoir enfreint la présente politique, il sera soumis à la procédure disciplinaire de l'entreprise. S'il est prouvé que l'employé a enfreint la politique, une sanction disciplinaire sera prise qui peut aller d'un avertissement oral à un licenciement. La sanction réellement appliquée dépendra de certains facteurs comme la gravité de l'infraction et le dossier disciplinaire de l'employé.

Note : *les procédures disciplinaires doivent être spécifiques à votre entreprise et refléter vos procédures opérationnelles et disciplinaires normales. Créez des procédures disciplinaires dès le début et intégrez-les dans votre politique d'utilisation acceptable.*

Acceptation

Tous les employés, sous-traitants ou personnel temporaire de l'entreprise qui ont obtenu le droit d'utiliser l'accès à Internet de l'entreprise ont l'obligation de signer le présent accord, confirmant qu'ils comprennent et acceptent la présente politique.

Politique sur les e-mails

L'e-mail est devenu la principale méthode de communication commerciale. Vous devez donc faire connaître à vos employés les procédures de sécurité et vous assurer qu'ils les respectent. Parmi les problèmes à aborder :

- Utilisation d'une mise en garde dans les e-mails (« ce message est privé et ne représente pas l'opinion de l'employeur... »).
- Directives sur l'ouverture et la visualisation des pièces jointes aux e-mails.
- Directives supplémentaires, le cas échéant, en rapport avec la Loi Informatique et Libertés
- Méthodes de gestion des informations confidentielles envoyées par e-mail et les circonstances dans lesquelles les e-mails doivent être cryptés en accord avec les directives de l'entreprise.

Assurer le fonctionnement de la politique

De trop nombreuses politiques de sécurité prennent la poussière sur une étagère ou restent sur un disque dur ; elles sont négligées, impopulaires et, surtout, inappliquées. Pour qu'une politique de sécurité produise un effet, elle doit être un document vivant auquel la direction et les employés ont accès et peuvent se référer.

De plus, vous devez vous assurer de faire connaître et de faire comprendre la politique de sécurité à vos employés, la direction supérieure de votre entreprise montrant clairement qu'elle prend cette politique au sérieux en assurant sa pertinence et sa mise à jour constantes.

Les convenances sociales sur l'utilisation acceptable peuvent facilement évoluer au fur et à mesure que les services Internet disponibles arrivent à maturité et changent. Il est donc nécessaire d'établir une analyse périodique de votre politique de sécurité afin qu'elle reste pertinente : un document au format d'un navigateur Internet que l'entreprise n'utilise plus rend l'ensemble de la politique moins efficace.

Normes et pratiques d'excellence

La norme ISO/IEC 27001 est une référence incontournable en matière de gestion de la sécurité de l'information. Cette norme vous permet de profiter d'années de réflexion et d'expérience pratique sur la meilleure méthode à adopter pour établir et gérer un système de gestion de la sécurité de l'information. Pour plus d'informations, veuillez consulter le site `www.bsigroup.fr/fr/Services-daudit-et-de-certification/Systemes-de-management/Normes-et-programmes/ISOIEC-27001/`.

La certification du système de gestion d'une société est probablement trop onéreuse pour la plupart des petites entreprises sauf si vous opérez dans un secteur où vous souhaitez prouver à vos clients vos références en matière de sécurité de l'information. Mais tout un chacun peut profiter des exigences de cette norme, dont la plupart sont abordées dans ce livre.

Si vous cherchez de l'aide pour la création d'une politique et d'un système de sécurité informatique, Trend Micro (`www.trendmicro.com`) propose un éventail de ressources.

Gérer la politique de sécurité

Après avoir établi la politique de sécurité de votre entreprise en fonction d'une évaluation des menaces auxquelles vous êtes confronté, vous devez définir la procédure de gestion de la sécurité. Elle incombe à différentes personnes et nécessite différentes politiques, procédures et technologies, chacun de ces éléments jouant un rôle essentiel pour assurer la sécurité globale.

Plus les machines clientes qui équipent votre entreprise sont nombreuses, plus la configuration de votre réseau est complexe, et plus la sécurité informatique devient difficile à assurer. Cela étant dit, la plupart des petites entreprises n'ont pas besoin d'embaucher du personnel supplémentaire pour gérer les systèmes de sécurité informatique. En général, elles attribuent ces responsabilités aux directeurs existants et éventuellement à un conseiller externe, fournisseur de services informatiques.

Si vous faites appel à un conseiller externe pour créer votre système de sécurité, assurez-vous que ce conseiller transmet des rapports par le biais de la hiérarchie existante. Ne laissez pas votre sécurité entre les mains d'un étranger.

Un conseiller sur la sécurité informatique va créer un *registre des actifs* qui mentionne tous les actifs informatiques que possède l'entreprise (ordinateurs, routeurs, disques durs externes) et enregistre les normes et les procédures utilisées par l'entreprise pour leur assurer la plus grande sécurité possible. Ce registre des actifs prend toute son importance quand vous modifiez les composants de votre configuration informatique. En cas d'incident, il peut vous aider à trouver l'origine du problème.

Une planification préalable est essentielle pour établir un système de sécurité de l'information, en imaginant les pires scénarios et les solutions de reprise. En outre, il est beaucoup plus facile de planifier un incident avant qu'il ne survienne plutôt que d'attendre d'être au cœur de la tempête pour tenter d'avoir accès aux bonnes ressources pour restaurer les systèmes, afin que le personnel puisse reprendre le travail.

Rôle des contrôles techniques

Le rôle de la technologie commence avec les actifs informatiques que vous avez identifiés, puis passe aux systèmes de protection dont vous disposez.

Pour s'attaquer à la conception de systèmes de protection et de reprise efficaces, posez-vous les questions suivantes :

- Qui est chargé d'assurer la mise à jour des systèmes et l'application des correctifs pour éviter toute attaque ? Qui s'occupe des licences des logiciels que vous utilisez ?
- Comment gérez-vous la sauvegarde des données ? Vérifiez que les tâches sont séparées. Ainsi, toute la charge n'incombera pas à une seule personne et vous serez toujours protégé si cette personne est malade ou en congé.

- Comment contrôlez-vous l'accès à l'équipement et aux données de la TI ? Comment vous assurez-vous que le personnel respecte vos politiques, notamment la navigation sur Internet ? Comptez-vous sur leur honnêteté pour qu'ils respectent les règles ? Ou instaurez-vous des technologies de filtrage appropriées ?
- Disposez-vous d'une procédure pour vous assurer que les modifications apportées au matériel et aux logiciels ne dégradent pas les politiques de sécurité déjà en place ?
- Avez-vous établi un plan de reprise après sinistre ? Quelles mesures avez-vous instaurées pour reprendre les activités après un incident grave comme un incendie ou une coupure du réseau ?
- Quelle est votre politique sur l'utilisation par les employés de leur propre équipement informatique et le transfert des données à l'extérieur et à l'intérieur de l'entreprise ?

Certaines questions de cette liste peuvent être résolues à l'aide de solutions automatisées qui allègent les tâches administratives pour le personnel. Par exemple, vous pouvez utiliser la gestion des identités pour protéger le contrôle d'accès, en remettant des jetons de sécurité au personnel qui se connecte au réseau de l'entreprise. Vous aurez probablement installé des filtres antispam pour vos e-mails. Les mises à jour des programmes anti-logiciels espions seront certainement automatisées dans une certaine mesure.

Vous pouvez bloquer des domaines particulièrement sensibles de l'architecture informatique à l'aide de pare-feux. Vos plans de continuité des affaires peuvent inclure une sauvegarde automatique vers un magasin de données en ligne sécurisé. Et vous pouvez employer le cryptage automatique des données dès qu'elles quittent l'entreprise. Vous pouvez également mettre en œuvre une solution de filtrage des URL (adresse d'une ressource du Web) et des sites Internet pour permettre au personnel d'avoir accès uniquement aux sites Internet adaptés au travail qu'ils doivent effectuer, en réduisant non seulement les failles de sécurité, mais en augmentant également la productivité du personnel. S'ils ne peuvent aller sur MySpace, ils ne peuvent pas perdre leur temps à actualiser leurs profils.

Sous-traitance des fonctions de sécurité – La solution hébergée

La gestion de la sécurité ne doit pas se traduire par une tâche technique. C'est là que l'hébergement entre en jeu, quand le fournisseur informatique gère le logiciel pour le compte du client, en fournissant en général un accès *via* Internet. La sécurité hébergée ne convient pas à tous les secteurs, mais elle fonctionne très bien dans deux domaines que nous explorons dans les sections suivantes.

Sécurité hébergée de la messagerie électronique

Protéger l'entreprise contre les spams est une méthode évidente pour atténuer les frais d'administration.

Environ 95 % des e-mails envoyés dans le monde sont des spams. Régler ce problème peut donc accaparer les employés, réduire la productivité et occuper la bande passante du réseau et l'espace de stockage. Le spam est également très utilisé pour diffuser des programmes malveillants, soit par le biais d'e-mails d'hameçonnage contenant des liens vers des sites Internet compromis, soit en intégrant des pièces jointes douteuses.

Les systèmes de sécurité hébergés filtrent les e-mails avant qu'ils n'atteignent le réseau, évitant une perte de temps pour le personnel informatique et l'utilisateur final, et un gaspillage du matériel et des ressources du réseau. Ils libèrent votre bande passante et réduisent l'impact sur le serveur de messagerie car les spams ne parviennent jamais jusqu'à votre entreprise.

Un mot d'avertissement sur la sécurité hébergée des e-mails. La seule chose qui est pire que de tenter de récupérer un e-mail que votre filtre a défini par erreur comme un spam, c'est de ne pas réaliser que vous avez reçu cet e-mail en premier lieu. Il peut s'agir d'un message important comme une proposition d'affaires. Vous devez vous assurer que le fournisseur de sécurité hébergé que vous choisissez a un bon taux (faible) en matière de *faux positifs* : des e-mails

qu'il considère comme des spams, mais qui n'en sont pas en réalité. Le fournisseur peut même proposer un accord de niveau de service en fonction d'un faible taux de faux positifs. Ainsi, vous pouvez obtenir un dédommagement financier si le taux de faux positifs dépasse la limite convenue.

Sécurité hébergée des terminaux

La gestion de la sécurité des terminaux (la protection de multiples ordinateurs, portables, serveurs de fichiers et autres appareils des utilisateurs) est un autre domaine dans lequel la sécurité hébergée peut également profiter à l'entreprise. La plupart de ces systèmes sont vendus avec des solutions de sécurité informatiques préinstallées, destinées aux particuliers. Cependant, il faut savoir que non seulement ces produits sont conçus pour une utilisation domestique, sans les fonctions nécessaires à un environnement commercial, mais qu'ils doivent également être gérés séparément.

En effet, des dates d'expiration et des licences différentes, ainsi que divers réglages de configuration, impliquent que votre administrateur système doit être capable de maîtriser plusieurs types de produits. Plus important : ils impliquent une protection instable d'une machine à l'autre. Dans certains cas, les utilisateurs peuvent gérer les produits de leurs propres ordinateurs et ne pas installer des mises à jour essentielles, exposant inutilement votre entreprise à des menaces. Et quand ils emportent leurs portables à la maison, la gestion de la sécurité devient totalement incontrôlable.

Une bonne solution pour résoudre ce cauchemar administratif, en particulier pour les petites entreprises, consiste à choisir une solution de sécurité informatique hébergée. Elle est facile à appliquer sur de multiples machines, l'utilisateur pouvant en un simple clic télécharger la protection pour son ordinateur qui sera opérationnelle au bureau et à la maison. Vous n'avez pas besoin de gérer un serveur de sécurité, et chacun dispose d'une protection constante, à jour et sophistiquée.

Ce type de solution vous permet également d'avoir une vue centrale de la gestion par le biais d'une console hébergée sur Internet qui permet de voir l'état de chaque machine, les menaces qui ont été détectées, etc.

Chapitre 3

Établir une défense coordonnée

Dans ce chapitre

- Concevoir des systèmes de sécurité pour protéger vos systèmes
- Réfléchir à une protection physique
- Éduquer les employés

La robustesse de la sécurité ne dépend pas d'une technologie ou d'une discipline particulière ; il s'agit d'une combinaison de mesures qui protègent vos systèmes contre les attaques. Certaines que vous avez probablement depuis plusieurs années, d'autres que vous ne connaissez pas. Mais elles sont toutes d'importance égale pour créer une protection globale.

La plupart des entreprises n'ont pas de défense coordonnée contre les menaces informatiques, incluant des contrôles techniques intégrés qui permettent de faire appliquer au plus haut niveau les mesures convenues. Vous pouvez disposer d'une protection extrêmement efficace dans certains domaines, comme un pare-feu d'entreprise qui bloque le moindre élément suspect et l'empêche de pénétrer ou de quitter l'entreprise. Dans d'autres secteurs, les utilisateurs sont protégés par des solutions pour particuliers, comme les logiciels antivirus préinstallés sur les ordinateurs. Mais si ces éléments ne sont pas tous coordonnés, notamment par des contrôles sur les droits d'annulation des réglages du pare-feu et par une console centrale de gestion de la sécurité (hébergée éventuellement par le fournisseur de support informatique pour les petites entreprises), vos mesures de sécurité non coordonnées peuvent vous donner une fausse impression de sécurité.

Ce chapitre présente chacun de ces domaines en détail. Nous ne cherchons pas à fournir une explication exhaustive sur un élément quelconque, mais plutôt à présenter une vision globale et une compréhension de leur assemblage.

Contrôle d'accès

Les *systèmes de contrôle d'accès* contrôlent l'identité réelle des utilisateurs qui ont accès à vos systèmes, vérifient que les tâches qu'ils réalisent sont autorisées, les empêchent d'infecter vos systèmes avec des virus et autres programmes malveillants, et de voler des informations confidentielles ou d'y accéder. Les outils d'accès regroupent des systèmes pour l'authentification, la gestion des identités, les autorisations, les noms d'utilisateurs et les mots de passe.

Sans contrôle d'accès, un pirate peut très facilement s'introduire dans une organisation. Mais si vous n'êtes pas une société de négociation de marchandises de haute valeur, n'en faites pas votre préoccupation majeure.

Délimiter le périmètre

Les directeurs de la TI et des transactions consacrent énormément de temps et d'énergie à ériger de grandes barrières autour de leurs systèmes informatiques. Ils achètent des pare-feux et des systèmes de prévention d'intrusion et, dans certains cas, configurent des réseaux privés virtuels afin que les utilisateurs puissent se connecter en toute sécurité aux systèmes de l'entreprise quand ils ne sont pas au bureau.

Cependant, la consolidation du périmètre constitue uniquement la défense la plus éloignée, et aucun périmètre informatique n'est imperméable. Il y aura toujours des failles dans ces défenses, comme le port HTTP (80) qu'un serveur Web utilise.

Vérifier l'identité à l'entrée

Si vous érigez des défenses considérables, comme des pare-feux et autres dispositifs similaires, vous devez vous assurer que les personnes que vous laissez entrer ne sont pas des pirates déguisés.

C'est là qu'intervient le contrôle d'accès. C'est l'équivalent de « Qui va là ? » avant de baisser le pont-levis.

Le contrôle d'accès n'a pas besoin d'être composé de biométries complexes, comme un lecteur d'empreinte rétinienne et manuelle, bien que ces méthodes deviennent de plus en plus courantes dans les grandes entreprises. Toutefois, la plupart des petites entreprises adoptent une approche plus pragmatique, et abordable, pour gérer les identités.

Aujourd'hui, les noms d'utilisateurs et les mots de passe sont les clés qui ouvrent les portes du royaume informatique. Vous avez besoin de ces deux éléments pour accéder à la machine que vous souhaitez utiliser, deux autres pour aller sur le réseau de l'entreprise, deux autres pour des applications particulières comme le système de comptabilité, et peut être même deux autres pour un secteur de données sensibles de l'entreprise. C'est ça le contrôle d'accès.

Évidemment, vous devez toujours vérifier que, si une personne se connecte à l'entreprise de l'extérieur, elle ne s'est pas approprié le nom d'utilisateur de quelqu'un d'autre. Même une personne à l'intérieur de l'entreprise peut tenter de regarder quelque chose qui ne la concerne pas, comme le salaire et les avantages du patron.

L'authentification de l'identité d'un utilisateur repose habituellement sur quatre facteurs :

- Quelque chose qu'il connaît : un mot de passe ou NIP (numéro d'identification personnel ou PIN)
- Quelque chose qu'il a : une carte à puce intelligente ou un jeton de sécurité
- Quelque chose qu'il est : une personne avec une empreinte rétinienne ou manuelle
- Un emplacement connu : à l'intérieur des locaux de l'entreprise.

La protection d'une entreprise est d'un bon niveau si chaque utilisateur peut passer deux de ces quatre tests. Après tout, votre banque vous fait confiance pour retirer de l'argent avec une carte et un code. Exiger trois des quatre tests indique que votre système est paré à l'épreuve des balles.

Choisir et préserver les bons mots de passe

Étant donné que les noms d'utilisateurs et les mots de passe représentent le niveau le plus fondamental de la sécurité informatique, il est important d'encourager tous les employés à choisir des mots de passe difficiles à pirater. Voici une liste de règles à suivre :

- Une association de lettres majuscules et minuscules, et de chiffres
- Une longueur de huit caractères ou plus.

Vous devez également vérifier que chaque utilisateur protège ses mots de passe. Quelques mesures élémentaires de précaution :

- N'écrivez pas les mots de passe ou ne laissez pas des papiers à côté de la machine utilisée pour l'accès.
- Ne laissez jamais les réglages usine pas défaut. L'utilisation du terme « mot de passe » comme mot de passe est bien trop facile à craquer.
- N'utilisez pas des données personnelles faciles à deviner, comme le nom de votre premier enfant ou de votre animal domestique.
- Ne communiquez jamais votre mot de passe à un tiers, même une personne de votre entreprise. Seul l'administrateur informatique doit avoir accès à ces données.

Limiter les actions

Après s'être identifiés et authentifiés, les utilisateurs peuvent avoir besoin de passer une autre étape d'autorisation pour définir les actions qu'ils peuvent entreprendre : sont-ils autorisés à modifier des fichiers ou simplement à les visualiser ?

Dans une entreprise, vous pouvez configurer l'accès en fonction des postes, de la même manière que vous le feriez pour approuver des dépenses. Si vous êtes le directeur des ressources humaines (DRH), vous pouvez visualiser et modifier les informations sur les employés ; si vous êtes juste un employé du service RH, vous pouvez visualiser les fichiers sans avoir le droit de les modifier.

Quand le DRH part en vacances ou qu'une autre personne reprend ses fonctions, celle-ci bénéficie des mêmes droits d'accès aux archives RH.

Sécuriser vos téléphones et vos réseaux informatiques

La sécurité du réseau ou de la passerelle Internet fait l'objet de nombreux débats. Toutefois, certaines entreprises ne prennent pas en compte le fait qu'elles n'ont pas un seul réseau à protéger, mais plusieurs. Conjointement au réseau Internet, vous avez le réseau téléphonique, un intranet et parfois un extranet. De plus, vous disposez probablement d'un réseau sans fil (WIFI), et éventuellement d'un réseau privé virtuel (RPV) ou d'une autre méthode pour permettre aux employés extérieurs d'appeler.

Chaque réseau dispose probablement d'un certain niveau de sécurité associé. Mais est-ce le bon niveau ? C'est l'interconnexion de ces différents réseaux qui rend le paysage si complexe. Par le passé, quand votre connexion réseau tombait en panne, vous preniez le téléphone et continuiez à travailler ainsi. Mais si vous avez un système *Voix sur IP* (*VoIP*) qui fait fonctionner le service téléphonique par le biais de votre connexion Internet, vous perdez également ce service.

Protéger vos réseaux téléphoniques

Les services téléphoniques ordinaires (STO) et, en particulier, les commutateurs privés (PBX) ont toujours fait l'objet d'un piratage et présenté un risque d'écoute téléphonique. Mais rares étaient les criminels qui avaient les compétences ou les techniques pour orchestrer de telles attaques.

De nos jours, la plupart des entreprises transfèrent cependant leurs réseaux téléphoniques sur le VoIP, pour profiter d'économies considérables sur les factures téléphoniques et des capacités de partager le même réseau que celui des données, réduisant ainsi les coûts d'infrastructure et la gestion.

Le VoIP est plus facile à pirater ou à perturber car il fonctionne sur le même réseau que les systèmes informatiques. Les systèmes VoIP peuvent être ouverts à :

- **La fraude :** un cybercriminel pénètre sur vos systèmes VoIP et passe de nombreux appels vers des numéros à revenus partagés, vous laissant régler la facture.
- **Les attaques par saturation :** comme pour les sites Internet, un cybercriminel tente de mettre à mal votre service téléphonique et d'empêcher quiconque de l'utiliser.
- **Les attaques par spams et hameçonnage :** à nouveau, tout comme les systèmes informatiques, les ordinateurs de synthèse de la parole appellent constamment de nombreux numéros dans l'espoir qu'une personne décroche le téléphone et soit incitée à faire un achat frauduleux ou à gaspiller son temps à répondre à un appel bidon.

Le fait que vous utilisiez des protocoles Internet indique que vous pouvez adopter la même protection que vous le feriez pour les systèmes informatiques. Toutefois, prenez en compte le risque associé à une panne de téléphone et décidez si vous souhaitez isoler votre système VoIP de vos systèmes informatiques.

Protéger vos réseaux sans fil

Avec la première génération de connexions sans fil, les utilisateurs se sont montrés très négligents en matière de sécurité des routeurs et des points d'accès, en partie car cette procédure était décrite comme complexe, mais également par un manque de connaissance des risques.

Aujourd'hui, vous devez savoir que les connexions sans fil WIFI impliquent des risques de sécurité isolés qui leur sont propres. Ces derniers entrent dans plusieurs catégories :

- **Accès à califourchon :** d'autres utilisateurs s'invitent sur votre connexion pour avoir accès à Internet, réduisant la performance et disposant d'un accès complet au réseau et à ses ressources. Ce problème survient quand aucune mesure d'authentification ou de cryptage n'est activée.

- **Mystification de l'adresse MAC :** les pirates obtiennent l'adresse MAC (contrôle d'accès au support) de votre réseau et l'utilisent pour accéder au trafic réseau et l'intercepter.
- **Attaque par saturation :** un cybercriminel empêche les utilisateurs légitimes d'accéder au réseau sans fil.
- **Attaque de l'homme du milieu :** un pirate crée un point d'accès factice à partir duquel il peut lire l'ensemble de votre trafic et insérer des communications factices, mais d'apparence réelle.

L'ancienne norme pour la sécurité sans fil a désormais été remplacée par la protection WPA et WPA2 (*Wi-fi Protected Access*). Tant que vous configurez votre système avec des mots de passe sécurisés que vous protégez, les connexions de votre réseau devraient être suffisamment protégées. Les cryptages WPA et WPA2 authentifient les utilisateurs pour vérifier que leur accès est autorisé, et ils encryptent les données transmises entre l'utilisateur et le réseau.

Mieux encore, les fabricants d'équipement ont réellement simplifié la configuration de ce protocole de sécurité. Il vous suffit donc de suivre quelques étapes simples pour sécuriser votre réseau sans fil.

Protéger vos réseaux informatiques

Les réseaux informatiques des petites entreprises ont toujours été ouverts aux attaques et les mesures de sécurité sont en général assez efficaces. Selon certaines estimations, 80 à 90 % des entreprises ont investi dans des pare-feux, et 50 à 60 % dans des systèmes de détection et de prévention d'intrusion. L'intégration de cette technologie dans les systèmes d'exploitation Microsoft a encore augmenté ce nombre.

Un *pare-feu* empêche un accès non autorisé au réseau, tandis qu'un *système de détection / prévention d'intrusion* contrôle l'activité du réseau à la recherche d'un comportement malveillant ou anormal, et réagit pour l'interrompre.

Malheureusement, avec les technologies de sécurité informatique, quand vous bloquez vos ordinateurs afin que votre entreprise soit totalement sécurisée et que vous prenez chaque alerte pour une tentative de piratage, vous pouvez empêcher l'entreprise de fonctionner normalement. Adoptez l'attitude extrême inverse et il devient presque inutile d'installer cette technologie. L'astuce consiste essentiellement à s'habituer aux capacités de la technologie, et les fabricants de ces produits simplifient les choses pour les administrateurs de réseaux.

Les pare-feux des réseaux et les systèmes de détection / prévention d'intrusion sont de plus en plus regroupés et associés à des capacités supplémentaires sur un dispositif de gestion unifiée des menaces (UTM). Ils reposent souvent sur des unités autonomes matérielles qu'une petite entreprise peut littéralement acheter, brancher et laisser travailler dans leur coin.

Une entreprise dont certains utilisateurs désirent se connecter à distance au réseau du bureau, ou une entreprise cherchant à connecter des bureaux satellites à un réseau principal, peut configurer un *réseau privé virtuel* (RPV) qui emploie différentes méthodes pour établir une connexion sécurisée. À l'aide d'un éventail de protocoles de sécurité, en général une extension de sécurité pour le protocole IP (IPSec) pour l'accès d'un site à un autre et un protocole SSL pour l'accès des utilisateurs distants, un RPV est en général hautement sécurisé par un cryptage des données qui circulent sur le réseau à travers un "tunnel" de communication sécurisé.

Vous devez réfléchir à la configuration des connexions utilisateurs et à la méthode d'authentification des utilisateurs d'un RPV. Que se passe-t-il si un utilisateur oublie son ordinateur portable dans un train ? Un étranger pourrait-il prendre l'ordinateur et avoir accès au réseau de votre entreprise ?

Gestion de la sécurité

La majeure partie de ce qui constitue la sécurité informatique concerne une administration de base : s'assurer de réaliser les tâches de maintenance essentielles requises dans l'environnement informatique de l'entreprise. Certaines de

ces tâches consistent à s'assurer que le logiciel est à jour et que les correctifs sont appliqués ; une discipline importante car le nombre de bugs découverts dans les différents systèmes et logiciels augmente constamment. De même, il peut être nécessaire que les gestionnaires de la sécurité vérifient que les utilisateurs obtiennent la toute dernière version des mises à jour de la sécurité.

Éviter les attaques Jour Zéro

Les *attaques de sécurité Jour Zéro*, qui exploitent les vulnérabilités des logiciels avant que le fournisseur puisse diffuser un correctif, sont de plus en plus nombreuses. Les navigateurs Internet sont devenus un point d'attaque privilégié car ils concernent un nombre important d'utilisateurs et peuvent être exploités directement, dès qu'un utilisateur arrive sur un site Web infecté. Microsoft a adopté pour politique d'émettre des mises à jour une fois par mois, le deuxième mardi de chaque mois (le « Patch Tuesday »), ce qui donne aux cybercriminels un mois entier pour exploiter une vulnérabilité avant qu'un correctif ne soit diffusé.

Au-delà d'une bonne maintenance, les possibilités à la disposition des gestionnaires pour se protéger contre les attaques Jour Zéro sont peu nombreuses bien que se tenir informé des principales vulnérabilités et menaces et appliquer les correctifs intermédiaires puisse aider.

La majeure partie de l'administration de la sécurité peut désormais être automatisée, y compris les correctifs par l'intermédiaire de *Windows Update*, le service automatisé de Microsoft pour assurer la mise à jour de ses logiciels et l'actualisation automatique des bases de données de virus et de logiciels espions. Vous pouvez même faire appliquer certaines des règles contenues dans votre politique de sécurité en bloquant notamment l'accès à certaines applications pour un type d'utilisateurs donné.

Limiter l'accès utilisateur

Vous pouvez également intégrer des restrictions dans votre politique d'utilisation d'Internet, qui précise par exemple une interdiction d'accès aux sites de socialisation pendant les heures de travail, de 9h00 à 13h00 et de 14h00 à 18h00. Nous

proposons un exemple de politique d'utilisation acceptable dans le Chapitre 2. Mais comment la faire appliquer ? Vous ne pouvez pas patrouiller dans les bureaux pour épier ce que les gens regardent. Le filtrage des URL, avec un haut niveau de souplesse et de catégorisation des différents sites Web, peut bloquer l'accès à un contenu inapproprié en fonction d'une politique établie, économisant éventuellement des heures de productivité perdues.

La politique de sécurité contient également des informations sur les fonctions et responsabilités ; en d'autres termes, un tableau de maintenance. Au sein d'une petite entreprise, il est rare que cette tâche soit la fonction principale d'une personne. Il est donc important de s'assurer que le travail est réalisé comme spécifié.

Contrôler la technologie

L'administration de la sécurité consiste également à contrôler la technologie de lutte contre les programmes malveillants (anti-virus et anti-logiciel espion) et les spams. Les logiciels de lutte contre les programmes malveillants sont présents dans plus de 95 % des petites et des grandes entreprises. Il s'agit également d'une technologie très mature, les principaux produits étant difficiles à différencier.

L'administration des protections contre les programmes malveillants constitue l'avantage actuel, avec des fonctions comme :

- Actualisation constante des bases de données hors site pour réduire la charge sur les systèmes de l'entreprise, couplée à des solutions hébergées pour la sécurité des terminaux et des e-mails. Informations complémentaires à cet égard dans le Chapitre 5.
- Mise en correspondance automatique des menaces potentielles avec les menaces contenues dans la base de données hors site.
- Déploiement central des systèmes et mises à jour sans avoir à visiter chaque ordinateur.
- Gestion centralisée et rapports.
- Compatibilité améliorée avec les anciens systèmes d'exploitation et matériels.

- Suppression / mise en quarantaine automatisée des programmes malveillants et envois de rapports aux administrateurs systèmes.

La majeure partie de l'infection par des programmes malveillants provient des téléchargements des utilisateurs, consciemment ou inconsciemment. Ils peuvent notamment penser mettre à jour une application et découvrir une alerte d'usurpation car ils ont téléchargé un ver ou autre virus.

Les administrateurs système aimeraient vraiment verrouiller l'environnement des ordinateurs afin que les modifications de la configuration apportées par les utilisateurs soient minimes et que tout changement réalisé soit effacé à la fin d'une session. Cet *état vierge* permet aux administrateurs de rester plus facilement maîtres des mises à jour logicielles et, en théorie, d'éradiquer la majeure partie des infections potentielles.

Les environnements verrouillés conviennent aux lieux publics et aux machines à utilisation partagée, aux environnements à bureaux flexibles (les employés travaillent sur différents postes) et peut-être même aux utilisateurs mobiles. Quant à savoir s'ils conviennent à une entreprise plus vaste, c'est une autre question.

Les entreprises doivent établir une politique concernant l'emprunt des ordinateurs portables par les employés ; le verrouillage de l'environnement de bureau peut notamment permettre de faire appliquer cette politique. Mais vous devez vérifier que vous ne risquez pas d'entraver la productivité des employés.

La protection des données

Les mesures de protection des données contrôlent l'accès aux données confidentielles et les protègent contre toute corruption. Elles font les gros titres quand les politiciens et les fonctionnaires oublient leurs portables dans les trains et les avions, laissant des informations personnelles et publiques à la vue de tous.

Mais, derrière ces gros titres, les inquiétudes des entreprises sont plus prosaïques concernant les coordonnées de

leurs clients et leur responsabilité légale de maintenir la confidentialité des données personnelles de leurs employés.

Comprendre la portée des bases de données

Étant donné l'interconnexion des systèmes actuels, vous ne pouvez pas espérer que les données soient sécurisées sur un système séparé. La base de données elle-même doit être sûre, comme toutes les applications qui lui sont connectées.

Les cybercriminels sont parvenus à exploiter les bases de données par le biais des applications Web qui emploient un code et des outils obsolètes. Pensez-y : si votre base de données est connectée à une application Internet, toute personne qui peut avoir accès à cette base par le biais d'une faille de l'application peut alors envoyer une requête et fouiller vos données.

Ce type de problèmes est peu connu car il n'est dans l'intérêt de personne de les admettre. Toutefois, ils peuvent avoir des conséquences catastrophiques pour l'entreprise et inciter les directeurs d'entreprise à avoir recours à une censure très stricte.

Limiter les menaces visant les e-mails

La messagerie e-mail est un champ de mines potentiel pour les données car il n'est protégé en général que par un nom d'utilisateur et un mot de passe. On peut cependant se rassurer en pensant que la recherche d'un e-mail sensible revient à chercher une aiguille dans une meule de foin étant donné le volume de messages.

La messagerie e-mail est par nature peu sécurisée et, pour les e-mails commerciaux sensibles, le cryptage est toujours la solution. Le *cryptage des e-mails* utilise des clés pour authentifier les utilisateurs et protéger, en même temps les informations sensibles.

La confidentialité des e-mails des employés au travail a fait l'objet de nombreux débats. Les e-mails sont-ils la propriété personnelle du destinataire ou de l'entreprise ? Mais une politique et une mise en garde sur les e-mails sensibles devraient protéger l'entreprise contre la plupart des problèmes. Consultez le Chapitre 2 pour connaître les politiques d'utilisation acceptable.

Protection des données

La perte des données survient souvent quand les informations circulent au sein d'une entreprise sur une clé USB ou quand une personne prend une partie des données en vue d'une analyse et les laisse sur un portable.

La fuite de données survient en général quand les données sont en phase de transfert ou quand les employés ne respectent pas les politiques établies par l'entreprise.

L'automatisation peut à nouveau être utile à cet égard. Vous pouvez par exemple automatiser le cryptage des données pendant leur transfert vers une clé USB ou utiliser une solution pour assurer le cryptage automatique des données sur un portable.

La sécurité physique

La protection des locaux, des installations, du personnel, des systèmes informatiques et autres actifs de l'entreprise constitue certainement le travail de sécurité le plus pratique. Si vous pensez que la sécurité physique n'a pas sa place dans un livre sur la sécurité informatique, détrompez-vous.

La sécurité physique représente la première ligne de défense des systèmes informatiques et une condition préalable essentielle car l'accès physique est le moyen le plus facile pour un cybercriminel de voler des données ou de compromettre des systèmes.

La protection de vos locaux est probablement un facteur que vous avez déjà planifié et mis en place, et les risques pour les actifs informatiques ne changeront pas vos dispositions à cet égard. Toutefois, après avoir réalisé un audit des actifs

informatiques de votre entreprise, vous pouvez décider que certains secteurs nécessitent une couche de protection supplémentaire, non seulement en raison de leur valeur financière, mais également à cause des données qui résident sur ces machines et des perturbations qui surviendraient en cas d'incident.

Une sécurisation de l'accès à la salle des serveurs, si vous en avez une, est essentielle. Vous devez filtrer toutes les personnes qui entrent et sortent pour vérifier qu'elles n'ont pas une unité amovible sur laquelle copier des données.

Verrous, coffres-forts, systèmes d'alarme et gardes de sécurité sont des méthodes de sécurité éprouvées, et certains dispositifs électroniques plus modernes peuvent également aider :

- Des caméras en circuit fermé dirigées sur des points d'accès particuliers peuvent être reliées à des réseaux d'ordinateurs pour enregistrer et visualiser depuis n'importe quel endroit.
- Écrans, câblage, contrôleurs et autres dispositifs sont de plus en plus abordables pour les petites entreprises.
- Les prix des systèmes d'alarme, non seulement autour du bâtiment, mais également dans des lieux particulièrement sensibles, baissent également, et la plupart peuvent désormais être installés par l'acheteur.
- Les systèmes de contrôle d'accès, avec cartes, numéros d'identification personnels ou interphones, autrefois réservés aux grandes entreprises, sont aujourd'hui essentiels pour tous.

Prévoir les conséquences

Aucun plan de sécurité n'est complet sans un plan de continuité des affaires et de reprise sur sinistre. La planification de la continuité des affaires face à un désastre, qu'il soit technique comme la perte du site Internet, ou naturel comme un incendie dans les locaux, est une priorité absolue pour toutes les entreprises. La *continuité des affaires* consiste à assurer le fonctionnement de l'entreprise lors d'un tel événement, tandis que la *reprise sur sinistre* concerne la restauration des systèmes informatiques après une catastrophe.

La planification de la continuité des affaires consiste souvent à réfléchir au pire scénario possible et aux solutions éventuelles. En fait, étant donné qu'il est peu probable que vous subissiez une catastrophe naturelle ou une attaque terroriste pendant la durée de vie de votre entreprise, il vaut mieux penser aux scénarios possibles dans la vie quotidienne, comme les pannes électriques et la disparition d'un fournisseur, ou les inondations et les tempêtes.

Si vous vous demandez s'il est vraiment important d'établir un plan de continuité des affaires, il vaut mieux savoir qu'une partie des petites entreprises qui subissent le pire scénario n'y survivent pas :

- Sur les 350 entreprises affectées par les attaques du World Trade Center de New York en 1993, 150 n'ont pas survécu. Toutefois, celles qui ont bien survécu, et il existe certains exemples remarquables à cet égard, étaient en mesure de fonctionner avec des perturbations minimales quelques jours après l'événement.
- L'incendie, en 2005, du dépôt pétrolier de Buncefield près de Londres (le plus important en Europe depuis la Seconde Guerre Mondiale), a engendré d'importantes perturbations pour les entreprises. Le bureau de Northgate Information Solutions situé à Hemel Hempstead, juste à côté du dépôt, a été entièrement détruit, et certains des sites Internet du secteur public qu'il exploitait ont été temporairement mis hors service. Mais les plans de continuité des affaires de Northgate ont permis aux clients de ne pas trop souffrir, et vers la fin du mois, la société avait restauré la totalité de ses systèmes internes et la grande majorité de ses données.

Les attaques des pirates et la corruption des données doivent sembler insignifiantes en comparaison. Toutefois, à cause des perturbations qu'elles provoquent pour le fonctionnement continu de l'entreprise, elles comptent actuellement parmi les menaces les plus graves.

Les menaces courantes pour la continuité des affaires comprennent :

- Les catastrophes naturelles (inondations, tremblements de terre, incendies, etc.)
- Les attaques informatiques

- Le sabotage interne
- Les pannes des services publics
- Le terrorisme
- Les maladies (comme une épidémie de grippe)
- Les pannes de disques durs.

Après avoir identifié les menaces, analysé leurs répercussions et établi des plans de continuité des affaires, assurez-vous de tester vos systèmes et de les maintenir à jour. La plupart des entreprises s'arrêtent après avoir formulé le plan et pensent qu'elles sont protégées. Elles se trompent. Les tests et la maintenance des plans sont d'une importance cruciale pour l'efficacité de ces derniers en cas de catastrophe.

Les plans de reprise sur sinistre, quand ils sont en place, sont la méthode la plus adaptée quand l'événement survient, alors que les plans qui concernent les pannes de système, les attaques des sites Web et l'infection par des programmes malveillants sont moins efficaces, car moins rigoureux peut-être.

Communiquer vos plans aux utilisateurs

La communication aux employés de l'existence des plans, des politiques et procédures applicables au personnel, et des autorisations et interdictions relatives à la sécurité informatique, représente une étape vitale pour l'efficacité de ces plans.

La plupart des petites entreprises ne précisent ni ce qu'elles entendent par utilisation acceptable, ni ce qui constitue un mauvais mot de passe. Par conséquent, alors que vous pensez appliquer des pratiques d'excellence, vos employés ne savent pas en quoi elles consistent. Si vous ne leur dites pas quels sont les plans et politiques, comment sont-ils supposés les respecter ?

Rares sont ceux qui tentent délibérément de nuire à leur entreprise ou de l'exposer à des risques inutiles, mais les employés peuvent mettre l'entreprise en danger par leur ignorance de ces politiques. Une navigation inoffensive sur Internet ou un transfert de données apparemment

anodin peuvent entraîner des défaillances alarmantes que les cybercriminels peuvent exploiter. Alors que vous allez nommer des personnes pour contrôler et gérer la sécurité de l'entreprise, la responsabilité à cet égard incombe finalement à chaque employé.

Les employés sont souvent le maillon faible d'un système de gestion de la sécurité informatique. La formation et la connaissance continues sont la cerise sur le gâteau, la pièce trop souvent manquante du puzzle, le dernier obstacle dans la course à l'excellence de la sécurité informatique.

La plupart des délits informatiques visent à embobiner les utilisateurs pour qu'ils réalisent une activité qui compromet leur entreprise. Il s'agit d'une activité qu'ils n'auraient pas faite s'ils avaient réfléchi. Quelques exemples :

- Cliquer sur un lien dans un e-mail qui est un spam
- Visiter un site Web qu'ils ne devraient consulter en aucun cas
- Transmettre des informations personnelles ou des données sur l'entreprise à une tierce partie non identifiée
- Sortir des données confidentielles de l'entreprise
- Négliger les mises à jour de la sécurité ou les sauvegardes pour gagner du temps.

La communication initiale sur la sécurité et les politiques applicables aux employés, couplée à une formation sur leur importance, permet d'en assurer le respect, au moins dans les grandes lignes. La formation doit mettre l'accent sur le niveau de confiance le plus bas. Si vous avez le moindre doute sur une pièce jointe, ne l'ouvrez pas.

Mais la connaissance et la formation continues sont également importantes pour semer les cybercriminels. Cet aspect est particulièrement important pour l'évolution des politiques et pour démontrer clairement au personnel l'engagement constant de la direction envers un niveau élevé de protection. Les cybercriminels sont toujours en quête de nouveaux moyens pour persuader les utilisateurs de faire des choses qu'ils ne devraient pas faire. Il est donc essentiel de s'assurer que chacun reste sur ses gardes. Ce qui semble suspect l'est probablement.

Chapitre 4

Connaître votre ennemi

Dans ce chapitre

- Vue générale sur l'évolution des menaces
- Comprendre les principales menaces auxquelles est confrontée votre entreprise aujourd'hui
- Connaître l'histoire de certaines attaques informatiques
- Explorer le monde souterrain de la cybercriminalité

Les menaces ont évolué de manière stupéfiante au cours des dix dernières années, depuis les événements de masse qui ont fait la une des journaux au début de la décennie jusqu'aux menaces Internet combinées et plus secrètes d'aujourd'hui. Le volume des menaces a également progressé de manière considérable. La société de recherche anti-virus AV-Test identifie actuellement jusqu'à 700 000 nouveaux programmes malveillants par mois. Ce volume colossal rend les menaces plus difficiles à suivre et à combattre. En outre, la nature du monde souterrain de la cybercriminalité a changé, d'un groupe d'amateurs en quête de gloire à une industrie de professionnels motivés par l'argent.

Les petites entreprises sont davantage ciblées par les attaques car souvent, elles ne disposent pas des ressources informatiques nécessaires pour se protéger contre de tels assauts et ont du mal à réagir.

Afin de pouvoir vous défendre contre ces menaces changeantes, la meilleure stratégie consiste à connaître votre ennemi ; ce chapitre examine en détail les menaces et les criminels modernes.

Petite histoire des cyber-menaces

Avant et pendant les années 2000, les épidémies de virus, vers et chevaux de Troie constituaient les principales menaces. Le virus Melissa, découvert en 1999, tentait de s'envoyer lui-même en masse par e-mail en utilisant les 50 premières entrées du carnet d'adresses d'un utilisateur. Le ver ILOVEYOU, arrivé en mai 1999 et considéré comme la menace la plus préjudiciable à cette date en termes financiers, s'envoyait également tout seul en utilisant toutes les entrées du carnet d'adresses d'un utilisateur, avec une « lettre d'amour » jointe qui provoquait des dommages importants à l'ouverture. Code Red en 2001, et SQL Slammer et Sasser ont suivi en 2003.

De nombreuses variantes des vers et des virus ont continué à apparaître et à exploiter différentes failles, principalement dans les systèmes Microsoft (en raison de leur ubiquité) pendant les années suivantes. Cependant, au fil du temps, cette charge virale a été limitée en partie par l'expansion à grande échelle et l'efficacité grandissante des logiciels antivirus, et en partie par une meilleure information des utilisateurs.

Traquer l'épidémie de Spams

Les cyber-terroristes se sont tournés vers l'envoi de spams en masse entre 2001 et 2003 à l'aide des *techniques de hameçonnage* qui consistaient à envoyer des e-mails d'apparence légitime pour duper des utilisateurs qui ne se doutaient de rien et obtenir leurs coordonnées bancaires et autres données personnelles.

Le problème du spam a atteint des proportions épidémiques en 2004 quand 70 à 80 % des e-mails entrant dans les entreprises pouvaient être classés comme des spams ; à cette époque également, les auteurs de virus ont commencé à joindre des charges virales aux e-mails.

De nouveau, la vague de spams a été quelque peu ralentie par les filtres antispam qui sont devenus plus sophistiqués, supprimant non seulement les e-mails dont la barre de message ou l'expéditeur paraissait suspect, mais également en fonction du type de contenu. La technologie antispam hébergée résout encore mieux ces problèmes : en éliminant les spams et autres menaces reposant sur les e-mails avant qu'ils n'atteignent le réseau, elle veille à ce que le volume colossal de e-mails indésirables ne bloque pas les serveurs de courrier et les réseaux.

Attention aux logiciels espions !

En 2004, le *logiciel espion* ou *Spyware* (logiciel téléchargé à l'insu

de l'utilisateur et qui enregistre son activité informatique) a été ajouté à l'arsenal du cybercriminel ; une menace bien plus sinistre et difficile à traquer. Selon une étude de 2004 réalisée par AOL et National Cyber-Security Alliance, 80 % des ordinateurs des ménages étaient infectés à leur insu par une forme quelconque de logiciel espion.

Le développement du logiciel espion a été d'autant plus grave que, lors de son apparition, les fournisseurs étaient concentrés sur les logiciels antivirus. Or, les produits antivirus traditionnels ne pouvaient pas détecter les logiciels espions, dont les caractéristiques sont totalement différentes des virus. Par la suite, le logiciel espion a été largement intégré dans les suites de sécurité tout-en-un, et la plupart des entreprises sont désormais protégées.

La guerre contre les botnets

Ensuite, le logiciel espion a laissé la place au bot (abréviation de robot). Les bots sont des ordinateurs compromis, connus sous le nom de *botnet* quand ils sont regroupés, qui sont prêts à exécuter les ordres de leur maître, des attaques par saturation aux envois de spams en masse.

Les botnets disposent d'une puissance de calcul qui est cent à mille fois supérieure aux attaques informatiques traditionnelles et peuvent provoquer de graves dommages lors d'initiatives concentrées et ciblées. Certains experts pensent que les techniques modernes de calcul distribué ont permis l'expansion des botnets, qui peuvent rapidement infecter un grand nombre d'ordinateur par le biais du partage de fichiers et des réseaux poste à poste.

Protection contre les menaces Internet combinées d'aujourd'hui

Si le développement des menaces au cours des dix dernières années nous donne une indication (voir l'encadré « Petite histoire des cyber-menaces »), c'est bien la suivante : dès que vous bouchez une faille dans vos défenses, vous devez en surveiller une autre. Aujourd'hui, les frontières entre les différents types de programmes malveillants sont devenues troubles, et ce qui était par le passé une attaque linéaire relativement simple est devenu un assaut combiné, souvent soutenu.

Auparavant, la méthode d'attaque indiquait le programme malveillant (et souvent la défense associée), mais les cybercriminels évoluent de jour en jour. Ils s'appuient sur les charges virales les plus puissantes de la génération précédente, tout en intégrant de nouvelles méthodes, et ils modifient constamment leurs points d'attaque pour éviter toute détection. Leurs nouvelles attaques associent un certain nombre de caractéristiques dommageables pour des résultats potentiellement désastreux.

Ces menaces combinées sont dénommées *menaces Internet* car elles reposent en majeure partie sur le Web. Une étude de 2008 de TrendLabs (le laboratoire de la sécurité de Trend Micro), qui détermine les origines d'un grand nombre d'infections informatiques, a découvert que plus de 90 % d'entre elles atteignaient leurs cibles via Internet. Le transfert de fichiers arrivait en deuxième place et concernait les supports amovibles comme les clés USB.

Le Web est l'endroit parfait pour lancer des attaques informatiques. Il représente une masse considérable de victimes potentielles, et les cybercriminels peuvent masquer, dans une certaine mesure, leur véritable identité à l'utilisateur. Évidemment, les attaques sont également faciles à suivre car elles proviennent d'une URL spécifique, qui peut être bloquée. Mais cela oblige simplement les criminels à passer à leur proie suivante.

Des combinaisons mortelles

Les menaces Internet combinées comportent souvent des étapes multiples, qui semblent bénignes au premier abord, par exemple un e-mail avec un lien qui, lorsqu'il est activé, relâche une charge virale. Quelques étapes possibles :

- Un programme malveillant est installé par le biais d'une pièce jointe à un e-mail ou d'un site Web compromis.
- Un canal de communication ouvert est établi (une porte dérobée) en général par l'intermédiaire d'un cheval de Troie
- Un programme malveillant supplémentaire est téléchargé, modifiant éventuellement la forme du logiciel malveillant d'origine.

Les menaces combinées regroupent plusieurs variétés et niveaux de menaces. Elles sont :

- **Multivariantes :** multitude de menaces combinées créées sur une même base, incorporant des variations minimes mais infinies, d'une variante à l'autre. La variété est un moyen d'éviter constamment la détection.
- **Multi-protocoles :** attaquant plusieurs systèmes à la fois. Une menace peut arriver par le biais d'une URL intégrée dans un e-mail, des essais de vulnérabilités dans un navigateur, ou une attaque via des protocoles de messagerie électronique (e-mail ou messagerie instantanée).
- **Distribuées :** répartissant leur charge virale sur de nombreux hôtes, à nouveau en petites quantités sur chaque hôte.

La combinaison de l'attaque est potentiellement mortelle, utilisant des spams pour une diffusion à grande échelle, l'Internet comme média de masse parfait et les programmes malveillants pour une activité destructrice. Chaque partie de ce puzzle peut sembler bénigne, mais considéré dans son ensemble, la puissance de l'assaut combiné devient évidente.

Étude de cas d'une cyber-menace : le ver Conficker

Le ver Conficker ou WORM_DOWNAD est un bon exemple des méthodes employées par les cybercriminels pour combiner les tactiques d'infection de masse traditionnelles aux mécanismes plus modernes de l'attaque combinée, couplées à l'infrastructure de « contrôle-commande ».

Ce ver a exploité une faille d'un service de Windows pour infecter les ordinateurs équipés de ce système. Ensuite, il s'est répandu sur les réseaux Windows ; une variante consécutive a réussi à forcer l'entrée des serveurs de réseaux et des lecteurs amovibles, réinfectant les ordinateurs précédemment infectés. Il est considéré comme le ver le plus rapide depuis SQL Slammer en 2003, car en janvier 2009, il avait infecté entre 9 et 15 millions d'ordinateurs.

Le ver bloque l'accès aux sites antivirus, désactive les mises à jour

(continu)

(continu)

de Windows et autres services du système d'exploitation et verrouille les comptes utilisateurs. Il génère une liste de noms de domaines auxquels il se connecte et télécharge une charge virale supplémentaire.

Microsoft a publié un correctif en urgence en octobre 2008 pour combler cette faille et a créé un groupe d'urgence pour lutter contre les répercussions de Conficker en offrant une récompense de 250 000 dollars pour des informations permettant l'arrestation de ses créateurs. Mais de nombreuses machines n'ont pas bénéficié de ce correctif.

La charge virale finale a donné lieu à de nombreuses spéculations car le botnet du ver s'est relancé le 1er avril 2009. Mais, à la date de rédaction de ce livre, il a provoqué des dommages limités.

L'ingénierie sociale

Au cours de l'année écoulée, les criminels ont employé de plus en plus les *techniques d'ingénierie sociale* (en fait, le cyber-mensonge) pour atteindre leurs buts. Ils surfent sur les problèmes publiés dans les médias ou prétendent être votre banque ou une société de livraison pour vous persuader d'ouvrir un fichier malveillant. Ils utilisent les e-mails d'hameçonnage (*fishing*) pour tenter de soutirer des données personnelles aux utilisateurs, en leur demandant par exemple de remplir un questionnaire en échange d'une récompense financière. Ils peuvent aussi se faire passer pour des sites de réseaux sociaux, voire des fournisseurs de logiciels antivirus.

Dans le pire des scénarios, ces criminels ne se concentrent pas uniquement sur le monde virtuel. Des tentatives récentes dans le monde physique cherchent à faire venir les gens sur des sites infectés. À titre d'exemple, ils placent des papillons sur les voitures dans les parkings, déclarant que la personne a reçu une amende pour un stationnement non autorisé et qu'elle doit aller sur un site Internet pour confirmer les informations sur son véhicule. Lors de la visite du site Internet, un programme malveillant est installé sur l'ordinateur.

Une tendance plus sophistiquée d'utilisation des spams consiste à employer un *spam de rétrodiffusion* qui permet aux criminels d'envoyer en masse des e-mails à un grand nombre

de destinataires en se faisant passer pour un expéditeur différent. Le tiers reçoit alors une charge complète de messages d'erreurs ou en absence.

On monte le volume

La croissance du volume des programmes malveillants généré aujourd'hui est phénoménale. Selon AV-Test, en 1988, il existait 1 738 menaces isolées. Ce chiffre a doublé *chaque année* jusqu'en 2005. Mais au cours des dernières années, le nombre de nouvelles menaces a explosé. Les statistiques qui suivent font froid dans le dos :

- Au début de l'année 2008, le nombre total de menaces isolées en circulation a dépassé 10 millions ; vers la fin de l'année 2008, il avait atteint 20 millions ; il a donc doublé en moins d'un an !
- En moyenne, plus de 2 000 programmes malveillants isolés et nouveaux arrivent toutes les heures sur Internet.
- Aujourd'hui, une semaine suffit pour créer la production complète de programmes malveillants de l'année 2005.

Dans certaines catégories spécifiques, une montée massive des spams et des bots est survenue en 2008, les deux étant intrinsèquement liés car les botnets sont la principale source d'expédition de spams. De janvier à novembre 2008, 34,3 millions d'ordinateurs ont été infectés par des programmes malveillants provenant de sources couramment associées aux bots.

Le monde souterrain de la cybercriminalité

Contrairement à l'économie du monde réel, l'économie du cybercrime est en plein boom. Selon certaines estimations, le monde souterrain de la cybercriminalité génère désormais des bénéfices impressionnants de 100 milliards de dollars par an. Alors que les enchères montent, ce monde souterrain se professionnalise et se structure davantage comme une

entreprise. Par conséquent, les individus se spécialisent et offrent des services malveillants particuliers. Tout peut pratiquement s'acheter ou se louer.

Conjointement aux offres groupées, les cybercriminels peuvent employer les services de programmateurs malveillants dédiés en vendant un code en ligne, comme le ferait une société de conception de logiciels dans le monde réel.

Les bénéfices financiers

Les informations volées représentent un commerce colossal, les cybercriminels négociant les données personnelles, notamment les noms d'utilisateurs pour les e-mails, les numéros de cartes de crédit, les numéros de sécurité sociale, les mots de passe d'accès à un compte, les numéros d'identification et les mots de passe des sites de jeux. Les cybercriminels font des affaires avec les pirates et les fournisseurs de botnet, négociant ces produits avec des vendeurs de programmes malveillants, qui à leur tour collaborent avec des vendeurs de programmes d'anti-détection et de boîtes à outils. Les programmeurs pirates, spammeurs et maîtres chanteurs travaillent côte à côte ou collaborent parfois avec des hommes d'affaires indépendants dans ce qui devient une industrie de plus en plus consolidée.

Les prix sur le marché noir de la cybercriminalité sont cependant très abordables : 50 à 3 500 dollars pour l'achat d'un programme malveillant prêt à l'emploi selon un article du journal anglais *The Independent* ; et 25 à 60 dollars par mois seulement pour une souscription à un service qui contrôle les développements des logiciels antivirus et peaufine les programmes malveillants en conséquence. Selon ce même article, une heure d'utilisation d'un réseau botnet comptant 8 000 à 10 000 ordinateurs coûte environ 200 dollars. Une recherche menée en 2007 par TrendLabs sur l'économie numérique souterraine a découvert que, pour seulement 100 dollars par jour, vous pouvez disposer d'une attaque par saturation distribuée, tandis qu'il vous faudra 1 000 dollars pour acheter 10 000 ordinateurs compromis. Les attaques par saturation visent à éliminer des ressources en ligne en les bombardant de demandes de service.

Une palette d'outils

La disponibilité des outils leur permettant de se lancer et d'agir rapidement est une des raisons du succès grandissant des cybercriminels. Ces outils vont des kits de hameçonnage prêts à l'emploi et gratuits, obtenus auprès d'entités telles que « Mr Brain » (un groupe de fraudeurs marocains qui fait la publicité de kits faciles à utiliser ayant lancé des attaques sur de nombreuses banques Tier One), aux modèles de spams gratuits qui répliquent avec précision l'apparence des sites bancaires populaires.

Les failles de la protection des données augmentent : selon le rapport d'Identity Theft Resource Center de 2008, 656 failles avaient été déclarées à la fin de l'année 2008, une augmentation de 47 % par rapport aux 446 failles de 2007, ce qui représente un total de 35 millions de données compromises.

La croissance des programmes automatisés de création de logiciels malveillants est tout aussi inquiétante. Ils peuvent utiliser une version d'un programme malveillant et en générer des centaines de variantes, chacune ayant une empreinte unique, échappant ainsi à la détection traditionnelle du fichier signature.

Chapitre 5

Concevoir des solutions pratiques

Dans ce chapitre

- Submergé par des menaces en constante augmentation?
- Lutter contre les menaces qui arrivent de toutes parts
- Considérer une protection hébergée dans le nuage informatique
- Se relier à un « réseau de protection intelligent »

Face à la croissance exponentielle chaque année du nombre de menaces informatiques, les fournisseurs de sécurité ressemblent parfois au roi Canut qui tente d'ordonner aux vagues d'arrêter de déferler sur la plage. Bien que les entreprises reçoivent en général le message sur la sécurité informatique et mettent en œuvre les mesures dont nous avons parlé dans le Chapitre 3, les moyens de protection traditionnels ne seront plus adaptés dans l'avenir.

Les mises à jour des fichiers signatures, expliquées ultérieurement, ne gagnent pas seulement en importance et en fréquence, elles perdent également en efficacité car les cybercriminels modifient constamment leurs attaques et utilisent des menaces Internet combinées pour déguiser leurs intentions.

Peut-être est-il temps de se tourner vers l'informatique hébergée sur Internet, aussi appelée « informatique dans le nuage » (*in-the-cloud*), pour sauvegarder votre sécurité informatique ; elle est adoptée pour héberger hors site des solutions informatiques qui doivent conserver et maintenir à jour, en permanence, de vastes banques de données. Elle facilite aussi considérablement les frais d'administration pour les petites entreprises.

Envisager un réseau de protection intelligent (*Smart Protection Network*), dont nous parlerons plus en détail par la suite, va encore plus loin en reprenant l'idée de l'informatique dans le nuage, tout en reliant tous les nuages. Ce type de ressource partagée répond exactement à la demande informatique moderne : un plan de surveillance groupée pour la sécurité informatique.

Tenter vainement d'arrêter le déferlement des vagues

L'accroissement du volume des programmes malveillants a été phénoménal ces dernières années. Mais la situation va empirer dans les années qui viennent. TrendLabs a remarqué une augmentation de 1 731 % des nouvelles menaces entre 2005 et 2008. D'ici à 2015, le laboratoire de la sécurité prévoit de traiter 26 598 menaces par heure, comme l'indique la Figure 5-1.

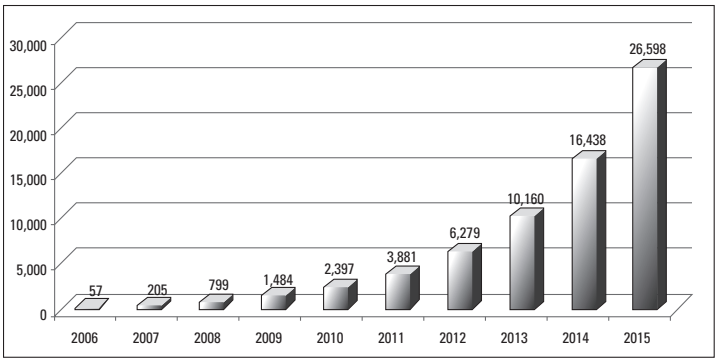

Figure 5-1: augmentation anticipée des nouvelles menaces malveillantes.

Le cercle vicieux dans lequel les réseaux informatiques sont aujourd'hui englués explique en partie pourquoi les analystes sont tellement convaincus de l'amplification constante de la marée des logiciels malveillants. En dépit d'une activité importante et de mesures de réglementation pour lutter contre les spams, ces derniers continuent d'augmenter aux États-Unis alors que de nouvelles techniques d'hameçonnage

et de spam apparaissent. Les États-Unis sont toujours très loin devant les autres pays, avec 22,5 % de l'ensemble des spams. Et l'augmentation inévitable du nombre de bots conduira à des attaques de spams, par saturation et autres, toujours plus nombreuses.

Les fichiers signatures ne peuvent pas suivre

La prolifération des menaces ne permet pas aux garde-fous traditionnels, comme les mises à jour des fichiers signatures, de suivre le rythme. La plupart des systèmes antivirus modernes détectent les virus en scannant les ordinateurs à la recherche d'une signature particulière et la mettent en correspondance avec les fichiers signatures de leurs bases de données. Dès qu'une correspondance de signature est découverte, l'élément incriminé peut être placé en quarantaine ou complètement supprimé.

En 1988, quand les menaces n'atteignaient que 1 738 programmes isolés, les professionnels de la sécurité les avaient regroupées dans 30 familles ou modèles. Ils devaient émettre 30 signatures pour trouver les logiciels malveillants. Les modèles totalement nouveaux n'ont émergé que lentement alors que les auteurs de virus découvraient une nouvelle méthode pour répandre leurs charges virales.

Aujourd'hui, des milliers de nouveaux modèles émergent toutes les heures, et les cybercriminels, comprenant les limites auxquelles sont confrontés les fournisseurs de mises à jour, créent constamment de nouvelles variantes de leurs logiciels malveillants. Ils modifient souvent leur logiciel malveillant dans les heures qui suivent pour conserver leur avance.

L'industrie de la sécurité a réagi à ce problème en publiant des mises à jour plus fréquentes, certains fournisseurs rafraîchissant les mesures de sécurité deux fois par jour, voire toutes les heures. Chaque nouvelle mise à jour contient un volume élevé de modèles alors que les fournisseurs de sécurité tentent d'endiguer la marée des cyber-menaces.

L'effet McColo

S'il vous faut des preuves supplémentaires de la prédominance continue des menaces, l'affaire McColo, survenue en 2009, devrait vous en convaincre. McColo Corp était un hébergeur de sites Internet de San José en Californie qui était considéré comme hébergeant toutes sortes d'opérateurs cybercriminels (du spammeur à l'infrastructure de contrôle-commande) pour certains des botnets identifiés les plus importants du monde. Ces botnets contrôlaient des milliers d'ordinateurs impliqués dans des activités de spams, de pornographie infantile, de vol de carte de crédit, de fraude et d'escroqueries du type « devenez riche rapidement ».

Après des années d'enquête, McColo a finalement été fermé en novembre 2008, entraînant une chute mondiale des spams de 50 à 75 % en une nuit. Toutefois, la déconnexion de McColo n'a eu qu'un effet temporaire ; le niveau des spams a progressivement redémarré, et l'un des plus grands botnets qui était censé être hébergé par McColo semble gagner en robustesse, étant contrôlé à partir d'un autre lieu.

Mais les mises à jour fréquentes des fichiers signatures posent des problèmes. Elles peuvent :

- Étrangler la bande passante du réseau pendant la mise à jour des machines clientes
- Ralentir la performance des ordinateurs individuels
- Donner des maux de tête supplémentaires aux administrateurs de réseaux qui doivent vérifier que les machines sont bien actualisées.

Le rythme et le volume de mises à jour des fichiers signatures encombrent les réseaux des entreprises, occupant une bande passante précieuse qui devrait servir à des tâches commerciales importantes, et affectant la performance des machines des utilisateurs. Rien n'est plus agaçant que de devoir attendre que votre ordinateur ait terminé d'appliquer une mise à jour quand vous le démarrez le matin et que vous souhaitez vous mettre immédiatement au travail.

Le nouveau défi des menaces combinées

Certaines indications laissent supposer que les mesures de sécurité des entreprises et leur protection contre les menaces dangereuses pour les affaires s'améliorent. L'enquête sur les failles de sécurité informatique citée dans le chapitre 1 a indiqué notamment que, parmi toutes les entreprises :

- 99 % sauvegardent les systèmes et les données critiques
- 98 % disposent d'un programme de lutte contre les logiciels espions
- 97 % filtrent les e-mails entrants à la recherche des spams
- 97 % protègent leur site Internet avec un pare-feu
- 95 % scannent les e-mails entrants à la recherche de virus
- 94 % cryptent les informations envoyées et reçues sur leur réseau sans fil.

Et il ne s'agit pas uniquement d'une amélioration des contrôles techniques. Cette enquête a montré que 55 % des entreprises disposent d'une politique de sécurité documentée (contre 27 % l'année précédente) et 40 % assurent une formation continue des employés sur la reconnaissance des menaces (contre 20 % l'année précédente).

Ces chiffres proviennent essentiellement des grandes entreprises qui disposent de ressources plus importantes à consacrer aux contrôles, à la documentation et à la prise de conscience de la sécurité. Ils restent toutefois encourageants.

Croissance des menaces multiples

Les mesures de sécurité informatique traditionnelles traitent des problèmes de sécurité traditionnels. Qu'en est-il des menaces les plus récentes qui évitent ces contrôles techniques, comme le *programme de vol de données* qui infecte les réseaux des entreprises et s'installe en silence pour dérober les informations commerciales en vue de commettre des fraudes ? Le programme de vol de données représente un type de menace Internet combinée, constitué en général d'un certain nombre

de menaces, fusionnant dans une activité apparemment inoffensive avec une charge virale, comme illustré à la Figure 5-2.

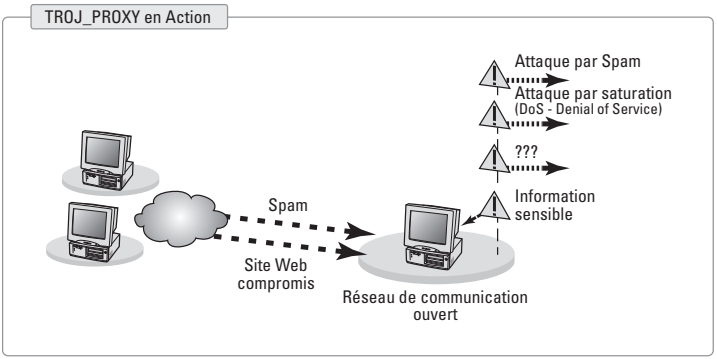

Figure 5-2: menace Internet combinée de spams et de sites Internet malveillants

Les menaces Internet combinées peuvent changer de forme, passant d'un programme apparemment inoffensif à une charge malveillante, évitant ainsi le scannage des fichiers. Elles arrivent souvent par le biais d'un port de protocole Internet ouvert, évitant ainsi les systèmes de détection d'intrusion comme les pare-feux, ou via un lien intégré dans un e-mail.

Le filtre de messagerie va scanner les pièces jointes. Mais, si un utilisateur est amené à cliquer sur un lien contenu dans un e-mail, il ouvre un site factice dirigé par un cybercriminel, qui commence alors à télécharger un programme malveillant.

De plus, les cybercriminels élargissent sans cesse leurs cibles pour intégrer les téléphones portables, spécifiquement Windows Mobile PocketPC, Symbian OS et Palm OS. L'emploi grandissant de ces appareils par les entreprises va provoquer de nouveaux maux de tête pour les gestionnaires de systèmes.

Les cybercriminels testent constamment leur nouveau programme malveillant par rapport aux solutions de protection. Ainsi, leurs attaques sont si efficaces que la plupart des solutions de protection des entreprises sont incapables de les détecter. Étant donné l'évolution constante des menaces et des modèles d'attaque, le scannage reposant sur la signature ou le comportement d'un fichier est inefficace.

Lutter contre les dangers d'Internet

Les sites Internet commerciaux sont de plus en plus compromis par les cybercriminels, équipés d'outils automatisés, qui surfent sur Internet à la recherche de failles.

Évidemment, les grands sites comme eBay et Google sont des cibles de choix. Cependant, les cybercriminels s'attaquent également aux sites des petites entreprises. Il s'agit souvent de sites anciens qui utilisent des outils et des logiciels obsolètes car, à nouveau, l'entreprise ne dispose pas des ressources nécessaires pour les actualiser.

Les sites Internet sont de plus en plus compromis. Les derniers chiffres de WhiteHat Security indiquent que 64 % des sites présentent une faille importante ou critique tandis que, selon Websense, 70 % des 100 plus grands sites contiennent un contenu malveillant ou une redirection cachée.

Rester au fait des sites compromis dans les différentes régions du monde quand ils sont infectés à une vitesse aussi alarmante est l'un des défis les plus difficiles auxquels l'industrie de la sécurité est confrontée aujourd'hui.

En sécurité dans le nuage

L'informatique « dans le nuage » (Cloud Computing) est un regroupement de ressources informatiques partagées, maintenu en général en dehors du site de l'entreprise, et auquel on accède par le biais d'Internet. Les services informatiques offerts « *in-the-cloud* » comprennent des solutions telles que la sécurité de messagerie hébergée, ou de larges bases de données de réputation de sites Web, ou encore de vastes banques de données informatiques. Relisez le Chapitre 2 pour de plus amples informations sur les services d'hébergement. Déplacer et héberger les bases de données des fichiers signatures et autres ressources de sécurité dans le nuage, représente une solution pour la gestion de la marée montante des menaces.

L'avantage de l'utilisation de l'informatique dans le nuage pour gérer de grands groupements de ressources repose sur la gestion du « nuage » informatique par des experts. Vous n'avez donc pas à vous inquiéter d'une gestion en interne. Elle est également :

- Évolutive, elle peut donc grandir au fur et à mesure de l'augmentation des ressources à héberger.
- Virtualisée, autrement dit, elle utilise au mieux les ressources informatiques sur lesquelles elle fonctionne et, à cet égard, elle est moins gourmande en ressources.
- Plus fiable car vous ne comptez pas sur la mise à jour de votre propre réseau. Tant que vous disposez d'une connexion Internet, vos machines peuvent se mettre à jour toutes seules.
- Moins chère que des ressources locales, bien que le coût dépende du nombre d'utilisateurs et de la taille de la base de données que vous utilisez.
- Efficace sur de multiples terminaux. Ainsi, vous pouvez facilement connecter des utilisateurs nomades, différents appareils mobiles et autres sans avoir à vous rendre sur place pour les actualiser. Ainsi, la sécurité ne dépend plus d'un emplacement particulier.
- Plus sécurisée. Les débats quant à la sécurité des plateformes informatique dans le nuage ont été nombreux. Mais réfléchissez : le fournisseur de sécurité héberge son propre logiciel, vous évitant d'avoir à l'exploiter sur vos propres systèmes. Vous n'avez peut-être plus le contrôle, mais c'est obligatoirement plus sûr.

En outre, l'informatique dans le nuage présente un avantage supplémentaire pour la sécurité : vous pouvez associer différents services dans le nuage et leur permettre de communiquer entre eux. Cela permet de lutter contre la menace supplémentaire qu'impliquent les menaces Internet combinées en détectant les modèles dans les combinaisons elles-mêmes. Choisissez l'informatique dans le nuage pour sauver votre sécurité informatique !

Un réseau de protection intelligent

Se tourner vers un Réseau de Protection Intelligent (*Smart Protection Network*) est une nouvelle approche qui exploite les technologies les plus récentes.

Les ressources de sécurité étant déjà étirées au maximum et les menaces devenant chaque jour plus difficiles à combattre, la technologie de protection dynamique en temps réel d'un réseau de protection intelligent (*Smart Protection Network*), est conçue pour s'adapter à la nature de la menace et réduire son impact sur le réseau et les ressources informatiques d'une entreprise, contrairement aux offres traditionnelles.

Un réseau de protection intelligent repose sur l'informatique *in-the-cloud* et est composé de trois éléments :

- Gestion de la réputation des e-mails (évalue l'authenticité des adresses électroniques en fonction d'adresses similaires détenues dans un fichier)
- Gestion de la réputation des sites Web (ou protection contre les menaces Internet)
- Gestion de la réputation des fichiers (ou scannage intelligent).

Ce réseau vous apporte :

- Une corrélation croisée entre les événements. Ainsi, si un spam renvoie vers un site Web particulier, le réseau ajoute cette URL à la liste noire, analyse le programme malveillant caché sur ce site et rédige une signature pour l'identifier et l'intercepter.
- Une population croisée entre les bases de données à l'échelle mondiale, actualisant les informations sur les failles de sécurité entre, par exemple, le marché asiatique et le marché européen.
- Une boucle de rétroaction dont bénéficient tous les utilisateurs à l'échelle mondiale, assurant à tous un partage efficace des informations sur les menaces qu'ils rencontrent.

Le fournisseur de sécurité entretient le réseau global de renseignements sur les menaces, ajoutant des millions d'adresses IP, d'URL et de fichiers douteux chaque jour. Et, étant donné qu'il est hébergé, le réseau peut traiter des milliards de demandes par jour, assurant une vaste protection contre tous les types de menaces, y compris les nouvelles menaces Internet.

La corrélation est un concept important dans la lutte contre les menaces combinées. C'est l'association des trois éléments définis ci-dessus qui fait du réseau de protection intelligent un réseau si puissant dans la lutte contre les menaces Internet. Ce réseau peut relier différents événements, permettant d'obtenir une image globale et assurant finalement une meilleure base de données des menaces informatiques.

Un réseau de protection intelligent utilise des boucles de rétroaction globales pour suivre une menace de sécurité et isoler sa cause, reliant des centres de recherche, des utilisateurs, des produits et des services :

- Quand un programme malveillant est détecté, le réseau génère la rétroaction qui conduit à la recherche de l'URL source, et actualise le réseau de protection intelligent en conséquence.
- L'e-mail est, par la suite, bloqué au niveau de la passerelle du réseau car il contient une URL qui est désormais sur la liste noire de la base de données sur la réputation des sites Web.
- Les téléchargements futurs sont bloqués car le fichier signature est ajouté à la base de données de réputation des fichiers, et l'expéditeur de l'e-mail est ajouté à la base de données de réputation des e-mails, rompant la chaîne d'infection le plus rapidement possible.

L'utilisation du *Cloud Computing* accélère également le processus car vous n'avez pas à attendre que les ordinateurs téléchargent les dernières mises à jour sur les modèles de fichiers.

Le réseau de protection intelligent est parfois comparé à une version en ligne de la surveillance de quartier dans lesquels les citoyens se protègent les uns les autres en temps réel et réagissent avant que les problèmes ne surviennent.

L'avenir de la sécurité

Les ressources de sécurité étant déjà étirées au maximum et la situation devenant chaque jour plus pénible, l'association de la technologie dans le nuage (*in-the-cloud*) et des méthodes de protection traditionnelles dessine l'avenir de la sécurité et, dans les tests, elle apporte le meilleur niveau de protection.

Dans un rapport de comparaison de logiciels antispam réalisé en 2009 par West Coast Labs, la solution de sécurité hébergée des e-mails permettait notamment d'obtenir le meilleur taux de détection (à 96,71 %) par rapport à neuf autres solutions, ainsi qu'un taux de faux positifs négligeable.

Autre exemple : en novembre 2009, NSS Labs a testé les dernières solutions de sécurité. Le test a démontré l'efficacité de l'association d'une protection hébergée dans le nuage et d'une protection hébergée localement sur les terminaux. La meilleure solution offrait un taux de protection de 96,4 % contre les menaces informatiques modernes.

Différentes technologies et approches seront bientôt regroupées pour écrire l'avenir de la protection informatique. Pour les petites entreprises, il ne s'agit pas uniquement de protéger mieux leurs actifs, cette solution facilite également la gestion de la sécurité, réduit les coûts et les problèmes.

Chapitre 6

Les dix principales mesures de sécurité informatique pour les petites entreprises

Dans ce chapitre

- Savoir contre quoi vous luttez
- Connaître les méthodes de défense

Ce court chapitre présente les pratiques essentielles que chaque petite entreprise doit adopter pour préserver l'efficacité de ses systèmes de sécurité informatique. Nous sommes convaincus que votre entreprise obtiendra une note de dix sur dix !

Identifier les menaces

Chaque entreprise disposant d'une connexion Internet (en fait, chaque personne ayant une connexion Internet) est la proie potentielle des cybercriminels. Pour protéger parfaitement votre technologie et votre entreprise, vous devez déterminer quelles sont les menaces les plus inquiétantes. Le Chapitre 1 vous permet d'évaluer vos domaines à risque pour identifier les événements qui pourraient affecter votre entreprise et sa réussite continue.

Réaliser une étude d'impact

Après avoir identifié les menaces, vous devez déterminer les dommages potentiels en cas d'attaque. Réfléchissez à tous les scénarios possibles pour pouvoir déterminer les méthodes de reprise si ces événements se concrétisent. Allez au Chapitre 1 pour obtenir des conseils sur la réalisation de cette étude.

Formuler une politique de sécurité

Les mesures que vous avez instaurées pour sécuriser votre entreprise constituent la politique de sécurité à l'origine de vos pratiques commerciales et du comportement de vos employés. Le Chapitre 2 couvre ce sujet en profondeur.

Identifier les actifs et les facteurs de risque

Vous devez connaître les actifs de valeur dont vous disposez pour pouvoir trouver un moyen de les protéger. Et en étudiant les risques qui menacent chaque actif, vous pouvez concevoir des méthodes de protection.

Rédiger une politique d'utilisation acceptable

Votre entreprise fournit aux employés les outils dont ils ont besoin pour travailler. Vos employés doivent savoir quelles sont les pratiques d'utilisation acceptable et inacceptable de chacun de ces outils. Vous pouvez notamment interdire aux employés de visiter des sites Web qui pourraient engendrer des problèmes légaux, aussi bien pour l'employé que pour l'entreprise. Cependant, comme l'explique le Chapitre 2, il ne faut pas réduire uniquement les pratiques illégales, mais également toute utilisation qui affecte la productivité et les bonnes pratiques commerciales.

Formuler une politique d'utilisation d'Internet et des e-mails

L'accès aux e-mails et à l'Internet compte parmi les principaux outils que vous mettez à la disposition de vos employés. Formulez une politique indiquant l'usage commercial approprié de ces outils par vos employés. Le Chapitre 2 propose des idées à cet égard.

Instaurer des contrôles techniques

Chaque entreprise doit mettre en place certains systèmes pour protéger ses fonctions informatiques. Assurez-vous de couvrir les fondements en installant des pare-feux et en achetant des programmes anti-virus / anti-logiciel espion. Nous discutons des méthodes de défense dans le Chapitre 3.

Coordonner les éléments sécuritaires

Vous disposez d'un éventail de moyens de sécurité pour vous protéger contre un éventail de failles. Tous ces contrôles de sécurité doivent s'imbriquer afin que l'ensemble des contrôles de sécurité, des pratiques des employés et des politiques forment un front unifié pour protéger votre entreprise. Le Chapitre 3 présente des informations supplémentaires sur le fonctionnement combiné de ces éléments.

Connaître votre ennemi

Vous devez savoir comment travaillent les cybercriminels. Et vous devez devancer les menaces émergentes, comme les menaces Internet combinées, afin de pouvoir former vos

employés à reconnaître ces menaces. Le Chapitre 4 couvre les derniers conseils et les menaces.

Tirer parti du pouvoir de l'informatique in-the-cloud

L'informatique dans le nuage (*in-the-cloud ou Cloud Computing*) vous permet d'utiliser les ressources d'un centre de données partagées, vous apporte un meilleur niveau de protection et réduit l'impact sur votre réseau et vos ressources informatiques. Nous abordons ce sujet dans le Chapitre 5.

LES MENACES WEB SONT OMNIPRÉSENTES... QUEL SOULAGEMENT DE POUVOIR COMPTER SUR WORRY-FREE

De nos jours, les menaces de sécurité sont partout
Avec un nouveau virus détecté toutes les 6 secondes, il est plus que jamais essentiel de protéger votre productivité et votre crédibilité avec Trend Micro™ Worry-Free™ Business Security.

Basée sur notre technologie avancée Smart Protection Network, cette solution détecte et neutralise les menaces en ligne, avant même qu'elles n'atteignent votre entreprise.
Plus sûre et plus intelligente, elle libère votre réseau des menaces de sécurité.

SACHEZ DECRYPTER LES SIGNES

Téléchargez dès aujourd'hui votre version d'évaluation gratuite sur **www.trendmicro.fr/pme-pmi**

TREND MICRO™
Securing Your Web World

Distinguez la réalité de la fiction

Protégez-vous des menaces informatiques

Les menaces liées à sécurité informatique sont partout, et de nouvelles semblent émerger chaque jour. Mais, si vous êtes une petite ou moyenne entreprise, vous disposez de ressources limitées pour protéger vos actifs de valeur. Ce livre vous indique les principes de base dont vous avez besoin pour être vraiment protégé. En présentant les grandes menaces et leur impact potentiel sur votre entreprise, il vous aide à créer une politique de sécurité, à constituer une défense coordonnée, et surtout, à mieux gérer votre sécurité. Les cybercriminels évoluent constamment en utilisant de nouvelles méthodes d'attaque. Voici comment endiguer cette marée montante.

Découvrez Comment:

- *Formuler une politique de sécurité*
- *Constituter votre défense*
- *Combattre en continu les menaces*

L'ESPRIT DES NULS™

- *Des explications pertinentes*
- *Des informations rapides*
- *Des icônes et d'autres aides à la lecture*
- *Un Top Ten*
- *Une bonne dose d'humour*

Allez sur @www.dummies.com!

- *Trouvez la liste de tous nos livres*
- *Faites votre choix parmi différentes catégories de sujets*
- *Inscrivez-vous pour avoir des astuces sur etips.dummies.com*

ISBN: 978-0-470-66694-4