percymiller

Les pratiques pour garantir sa sécurité informatique

Les pratiques pour garantir sa sécurité informatique

Face aux nouvelles menaces, l'installation de logiciels de sécurité est indispensable, mais pas suffisante. Différentes mesures doivent être prises pour protéger les actifs des entreprises.

Depuis la création, en 1983, d'un des premiers virus par Fred Cohen — considéré comme l'un des pères de la virologie grâce à ses travaux menés dans les années 80 lorsqu'il était étudiant à l'université de Californie — il en existe des dizaines de milliers.

Jusqu'à présent, les systèmes d'exploitation sous Windows étaient les principales cibles des développeurs de ces codes malveillants. La situation commence à évoluer avec des attaques virales visant les ordinateurs fonctionnant sous MacOS d'Apple, mais aussi des serveurs sous GNU/Linux.

Personne n'est donc épargné et les menaces sont devenues multiples. Les responsables informatiques des entreprises doivent donc connaitre les techniques employées par les pirates pour mettre en place les protections les mieux adaptées.

Il faut d'abord rappeler qu'il existe différentes catégories de codes malveillants. Les quatre principales sont les suivantes :

- Les virus

- Le cheval de Troie

- Les vers

- Les bombes logiques

1. Les virus

Malgré la diversité des codes malicieux, les virus restent la technique la plus employée pour infecter un poste de travail ou un réseau. Ils sont classifiés selon leurs fonctionnalités. Les deux principaux sont :

- Les virus de démarrage (ou virus de boot) : ils visent ou utilisent les organes destinés à amorcer le système d'exploitation comme le BIOS (Basic Input/Output system) et le secteur de démarrage maître (MBR – Master boot record). Principal intérêt de ce programme malicieux : en intervenant avant le lancement du système d'exploitation (comme Windows) et donc de tout logiciel (dont l'antivirus), il est impossible (ou très difficile) d'interrompre son démarrage.

- Les macros virus : ils ciblent plus précisément les suites Office de Microsoft, mais aussi les suites bureautiques comme OpenOffice et LibreOffice. Leur principe de fonctionnement est le suivant : lors de l'ouverture d'un document infecté (par défaut, les macros ne sont pas désactivées), le code viral se copie dans certains modèles et notamment le « normal.dot » pour Word.

2. Les vers

Un ver (ou worm) est capable de se dupliquer et de se diffuser tout seul par le biais des services de messagerie instantanée ou de courrier électronique.
Aujourd'hui, les vers sont très évolués et peuvent passer à travers les mailles des logiciels de sécurité (antivirus et pare-feu).

3. Les bombes logiques

Il s'agit d'un programme infectant qui s'installe dans le système d'exploitation et attend un évènement (date, action, donnée...) pour exécuter sa fonction offensive. C'est la raison pour laquelle les antivirus ont beaucoup de difficultés à les repérer avant qu'ils n'agissent.
Face aux différentes menaces, il existe des solutions logicielles !

A. L'antivirus : le surveillant principal

Son rôle consiste à débusquer tous les virus qui essaient de s'installer dans l'ordinateur. Mais attention : ces programmes ne peuvent repérer QUE les codes malveillants qu'ils connaissent, c'est-à-dire qui sont répertoriés dans leur base de données.

Reconnaissant que cette méthode a montré ses limites (la simple modification d'une ligne de code d'un virus suffit à le rendre indétectable aux yeux de nombreux antivirus...), les éditeurs ont intégré les analyses heuristique et comportementale. Mais les antivirus sont loin d'être parfaits et sont incapables de détecter une attaque ciblée, c'est-à-dire s'appuyant entre autres sur un code malveillant spécialement développé à cet effet.

B. Le pare-feu (ou firewall) : il surveille les connexions

Sa fonction est plus réduite que celle d'un antivirus, mais elle est, finalement, plus importante. Il filtre en permanence toutes les connexions entrantes et sortantes d'un ordinateur.

Rien ne vaut la mise en place de bonnes pratiques
Mais aucune solution logicielle ne peut prétendre à une sécurité absolue. Pour réduire les risques d'infection, il est indispensable de respecter deux mesures essentielles.

La première est de mettre à jour (de façon automatique) tous les logiciels et les systèmes d'exploitation. Tous les postes de travail (y compris les PC portables des salariés nomades) doivent être mis à jour. Régulièrement, les éditeurs publient des correctifs permettant de colmater une brèche dans laquelle pourrait s'engouffrer un code malveillant. Il existe différents programmes gratuits et payants qui peuvent scanner tous les logiciels installés afin de vérifier leur actualisation.

La seconde mesure indispensable est d'utiliser différents mots de passe « forts », c'est-à-dire difficiles à trouver rapidement. C'est la même chose que pour une porte et une serrure : un cambrioleur ne va pas s'acharner plus de 15 minutes. S'il n'arrive pas à ouvrir rapidement une porte, il s'attaquera à une autre cible.

Concernant l'informatique c'est le même principe. Pour rendre difficile la tâche du pirate, il faut créer des mots de passe composés de lettres en majuscule, minuscule, de chiffres et de symboles. Exemple : mT74jz+gH*!. Par ailleurs, les responsables informatiques doivent sans plus tarder supprimer tous les codes d'accès d'un collaborateur qui ne travaille plus dans l'entreprise. Autre précaution indispensable : surveiller attentivement les accès des intervenants extérieurs (dépanneurs, sous-traitants...).

Ces pratiques sont indispensables, mais elles ne sont pas suffisantes en cas de désastre, qu'il soit naturel (dégât des eaux, incendie...) ou dû à une infection virale touchant une bonne partie du système d'information de l'entreprise.

Un PSI : pour redémarrer rapidement

Trop souvent négligé, un Plan de Secours Informatique (PSI) est indispensable. Le principal objectif étant une reprise très rapide de l'activité, il implique une parfaite organisation, une évolution par paliers et une synergie renforcée entre les différents services.

Les pratiques pour garantir sa sécurité informatique

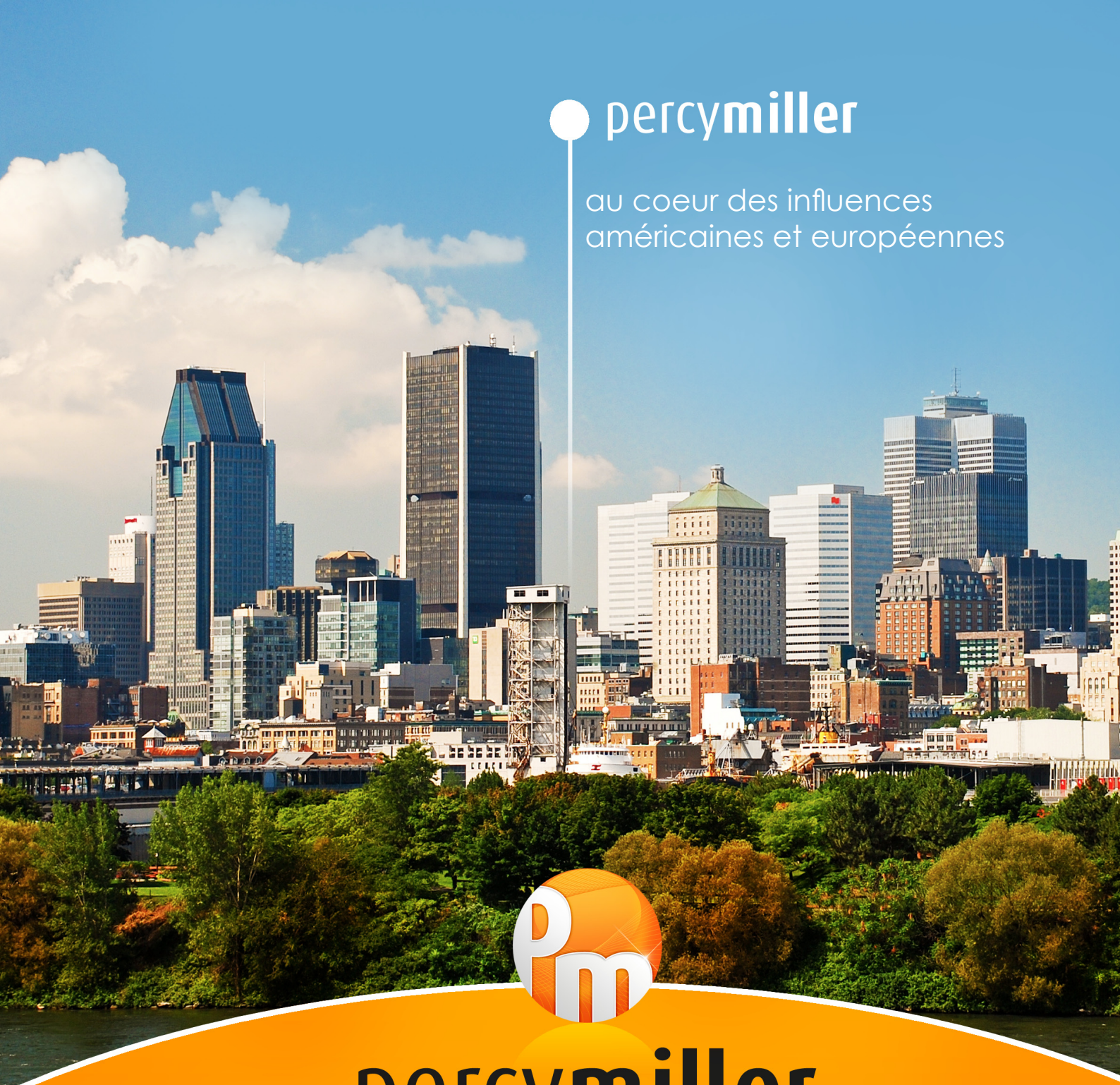
Un PSI efficace exige d'avoir une bonne vision de l'ensemble du patrimoine applicatif.
Les PSI sont devenus très complexes. Établir la liste des applications critiques touchées par un sinistre, par exemple, est très difficile, car les technologies informatiques ont beaucoup évolué et sont multiplateformes.

La mission première est donc de déterminer quels salariés et quelles applications sont critiques. Les entreprises doivent ainsi établir leurs exigences en matière de continuité et la DSI en tenir compte avec des architectures à résilience appropriée.

Pourtant, les bénéfices d'un PSI vont au-delà des aspects purement techniques. Il fait évoluer les mentalités et améliore la documentation (consignes de travail opérationnel, procédures de redémarrage...) et l'industrialisation du SI.

En conclusion, chaque collaborateur est concerné !

Dans les situations de crise, il est essentiel que les choses soient bien
« huilées ». Cela nécessite un important travail de conception des processus, de finalisation des chaînes de décision avec des personnes qui ont compris ce qu'elles avaient à faire.



percymiller

au coeur des influences
américaines et européennes

percymiller

400 Boul. De Maisonneuve Ouest - Suite 850
Montréal H3A 1L4
(Québec) Canada

Tél. : +1 514 908 75 68
Tél. France : +33 (0) 1 73 00 20 40
Fax : +1 514 908 75 72

contact@percy-miller.com

www.percy-miller.com