

## Optimiser la sécurité Internet : une défense par couches successives

## Introduction

Les porte-avions appliquent une stratégie de défense complète par couches successives, qui commence par la détection proactive. Le radar constitue ainsi une première ligne de défense, détectant les attaquants dès leur approche. Lorsqu'il identifie une menace, le porte-avions déploie un mécanisme de défense appropriée - missile surface-air ou mitrailleuse radioguidée - pour assurer la protection du vaisseau face aux attaques. Ces différentes défenses viennent s'ajouter les unes aux autres, pour que la défaillance de l'une d'entre elles n'entraîne pas la perte du vaisseau.

De leur côté, les Responsables Informatiques se doivent également de déployer une stratégie complète de défense par couches successives. Les menaces Web n'utilisent pas de pistolets, de missiles ou autres armes de guerre, mais des applications logicielles malveillantes, regroupées sous le terme malware. Les malwares incluent les virus, spyware (logiciel espion), vers, chevaux de Troie, backdoors (portes dérobées) et keyloggers (enregistreurs de frappe), qui se propagent par e-mail et sur le Web. Ces dernières années, on a constaté la montée en puissance des menaces mixtes, combinaison de deux ou trois types de malware.

Les responsables informatiques utilisent depuis longtemps des applications bureautiques antivirus, anti-spyware et autres solutions de sécurité du poste de travail, pour se protéger des menaces véhiculées par le Web. À une époque, cette solution offrait une protection suffisante, mais depuis quelques années, le paysage des menaces informatiques s'est considérablement transformé.

En 2000, les experts en sécurité ont reçu environ 500 000 échantillons différents de malware. Un chiffre estimé à 15 millions pour 2008. De même, de nouveaux types de menaces et de vecteurs d'attaque ne cessent d'apparaître. C'est pourquoi les responsables informatiques doivent impérativement mettre en oeuvre des mesures de sécurité complètes, qui prennent en compte toute la diversité des menaces. Tout comme un porte-avions, le réseau d'une entreprise nécessite une stratégie de défense par couches successives pour se protéger efficacement.

### Les menaces

Les professionnels de la sécurité informatique le savent, le catalogue des menaces est en évolution constante. Les malwares sont toujours plus différents, toujours plus complexes. Les premières menaces qui sont apparues s'attaquaient uniquement au poste de travail, leur champ d'application et leurs possibilités étaient limités. En revanche, les malwares actuels mettent en oeuvre une multitude de techniques et de vecteurs d'attaque sur plusieurs niveaux : l'e-mail et le Web permettent d'atteindre les postes de travail et les serveurs des entreprises.

Au début, les malwares se limitaient à tout ce qui pouvait être transporté par disquette ou autre moyen rudimentaire, et nécessitaient l'intervention de l'utilisateur pour se propager d'un ordinateur à un autre. Au contraire, les menaces actuelles font appel à tout un panel de techniques de propagation, exploitant au maximum la connectivité offerte par Internet. Selon une récente étude de l'institut Gartner, le nombre de menaces hébergées sur le Web a augmenté de 800 % en 2007<sup>1</sup>. Entre-temps, l'utilisation de l'e-mail pour attirer les utilisateurs vers la menace s'est généralisée. Les failles de sécurité des logiciels, des systèmes d'exploitation et des plug-ins des navigateurs sont autant de moyens à la disposition des pirates pour diffuser leurs menaces rapidement et avec efficacité. La banalisation des connexions Internet permet également aux pirates d'exporter discrètement des identifiants et autres données confidentielles des systèmes infectés.

Les motivations des pirates sont également un paramètre essentiel de l'évolution du paysage de la menace informatique. Pendant longtemps, les programmeurs ont conçu des menaces informatiques pour impressionner leurs amis ou la communauté des programmeurs. Aujourd'hui, les pirates sont avant tout des criminels, financièrement intéressés. Ces criminels sont les acteurs du marché souterrain en pleine croissance de la menace informatique, estimé à 100 milliards de dollars. Ce sont des programmeurs talentueux payés pour écrire le code nécessaire à l'attaque, les membres du crime organisé dont le but est de dérober des informations confidentielles sensibles, les détenteurs des listes d'e-mail ou d'autres méthodes de diffusion.

Avec le développement constant de ce marché parallèle, les entreprises qui ne sont pas protégées sont plus que jamais en danger, les pirates motivés par le gain s'attaquant désormais aux informations sensibles et aux données clients.

### L'absence de solution globale

Une enquête réalisée en juin 2008 a révélé qu'il manquait au moins un composant essentiel de sécurité à 81 % du parc informatique des entreprises, dont le système était donc vulnérable aux attaques. Les enquêteurs ont évalué le niveau de sécurité de 580 systèmes, en notant le statut des correctifs installés, des pare-feu au niveau du système, et des logiciels de sécurité côté client. Sur 63 % des systèmes, il manquait au moins un correctif de sécurité critique Microsoft ; le pare-feu était désactivé sur 51 % d'entre eux ; enfin, sur 15 % de systèmes, le logiciel de sécurité était désactivé ou bien n'avait pas été correctement mis à jour.

Les utilisateurs finaux ne sont pas les seuls à mettre en cause. D'autres enquêtes ont abouti à un résultat comparable en ce qui concerne l'administration des systèmes : un niveau de protection inférieure à la moyenne sur les serveurs e-mail, serveurs Web et serveurs d'applications. Le problème est surtout visible dans les petites entreprises, qui ne disposent pas d'un service informatique dédié, à plein temps. Comme la plupart de ces entreprises ne possèdent pas le niveau d'expertise et de sécurité nécessaire pour combattre efficacement les différentes menaces, elles peuvent courir un risque sans en avoir conscience.

## Un équilibre délicat

Par définition, sécurité totale et facilité d'utilisation s'opposent. Une solution de sécurité infaillible consisterait à couper toutes communications avec l'extérieur. Efficace, certes, mais pas très pratique. De même, autoriser la totalité du trafic entrant et sortant sans régulation d'aucune sorte offrirait sans aucun doute aux utilisateurs toute la liberté dont ils ont besoin, mais dans le même temps, cela exposerait largement l'organisation aux attaques extérieures. Aussi la solution adoptée devra-t-elle impérativement proposer un compromis entre sécurité et liberté d'utilisation.

'Enquête Gartner n°158459, "Pourquoi il est nécessaire de filtrer les malwares au niveau de la passerelle Web", 26 Août 2008.

## Ne pas se limiter au poste de travail

Pour s'assurer que l'organisation est protégée contre les menaces provenant du Web, tout en apportant aux collaborateurs la souplesse de communication dont ils ont besoin, il est essentiel d'adopter une approche plus globale. Le modèle de sécurité par couches successives permet au personnel des services informatiques de commencer par évaluer les points d'entrée potentiels, puis de mettre en oeuvre une solution de sécurité spécifique ad hoc.

Naturellement, il est important de commencer par installer un logiciel de sécurité sur l'ordinateur des utilisateurs, mais cela ne suffit certainement pas à garantir l'intégrité des actifs du réseau de l'entreprise. Il y a principalement deux raisons à cela :

1. Il est impossible de contrôler le système d'un utilisateur final de manière appropriée. Ainsi que l'a démontré l'étude mentionnée plus haut, il est fréquent que les utilisateurs finaux désactivent leur logiciel de sécurité, ou qu'ils oublient de le mettre à jour régulièrement. Le personnel d'un service informatique permanent peut déclencher manuellement les mises à jour de sécurité. Cependant, les utilisateurs sont de plus en plus mobiles, ce qui diminue considérablement l'efficacité de cette solution car les mises à jour peuvent être effectuées uniquement lorsque ces utilisateurs se connectent au réseau. Si un ordinateur portable est victime d'une infection alors qu'il n'est pas connecté au réseau de l'entreprise, cette infection pourra se diffuser dans toute l'organisation dès que le client se connectera de nouveau, bien avant que le service informatique n'ait pu activer la mise à jour.
2. La passerelle Web constitue le point d'entrée principal. Lorsque l'utilisateur final est connecté au réseau de l'entreprise, les menaces Web et e-mail sont forcées de transiter en premier lieu par la passerelle Internet de l'organisation, avant de pouvoir atteindre les différents postes de travail. Il est donc plus efficace et proactif de bloquer les menaces au niveau de la passerelle Internet. Cela garantit également au service informatique une meilleure maîtrise de la sécurité, car il assure lui-même le management de cet équipement, sans dépendre de l'intervention des utilisateurs finaux.

Si l'on tient compte de ces paramètres, il apparaît vital que les organisations sécurisent leur passerelle Internet pour se protéger efficacement contre les menaces véhiculées par Internet.

## Analyser les e-mails

L'e-mail demeure le vecteur privilégié de tout un ensemble de menaces. Le spam, les attaques de phishing (hameçonnage) et les pièces jointes frauduleuses sont autant de méthodes couramment employées pour introduire une menace en milieu professionnel. Il est également possible d'utiliser un poste de travail infecté pour envoyer une quantité incroyable de spam, à l'insu de l'utilisateur. Pour cette raison, il est très important d'analyser et de filtrer à la fois le trafic e-mail entrant et sortant au niveau de la passerelle.

L'analyse du trafic e-mail entrant peut aider l'organisation à contrer de façon proactive une large gamme de menaces véhiculées par e-mail, parmi lesquelles le spam, les virus, les spywares, les attaques de phishing et les contenus inappropriés. Il s'agit d'un aspect critique de la solution de sécurité, car cette analyse constitue une véritable ligne de défense qui garantit que la menace ne parvient jamais jusqu'à l'utilisateur final.

L'analyse du trafic e-mail sortant, souvent négligée par les organisations, joue également un rôle dans la stratégie de sécurité par couches successives d'une entreprise. En effet, elle peut être la seule indication d'une infection sur le réseau.

## Se protéger du Web

L'utilisation de l'Internet fait désormais partie de notre quotidien, et il ne fait aucun doute qu'il existe de nombreux usages légitimes du Web pour les entreprises. Pourtant, le Web constitue également une base de lancement idéale pour les malwares, entre autres attaques. 79 % de toutes les menaces véhiculées par le Web ont été identifiés sur des sites légitimes, piratés pour y injecter ensuite des applications malveillantes. Également, certains sites inappropriés contiennent des spywares, d'autres adoptent une apparence légitime pour attirer un trafic conséquent de visiteurs via les moteurs de recherche et les attaques de phishing, notamment.

Pour autoriser les utilisations légitimes de l'Internet tout en maintenant un niveau de sécurité suffisant dans l'entreprise, il faut mettre en place un système de détection efficace des virus et autres malwares, ainsi qu'un filtrage des URL. Comme pour les e-mails, il est essentiel d'analyser à la fois le trafic entrant et le trafic sortant. L'analyse du trafic entrant permet de détecter une tentative d'intrusion par malware, une tentative de téléchargement frauduleux d'un programme malveillant, ou bien de repérer qu'un utilisateur télécharge un malware par inadvertance. L'analyse du trafic sortant ajoute une ligne de défense supplémentaire, en permettant de détecter toute tentative d'envoi à une personne malintentionnée de données sensibles récupérées par un spyware sur l'ordinateur d'un l'utilisateur.

## Conclusion

Les menaces hébergées sur l'Internet occupent une place centrale et de plus en plus importante parmi les différentes menaces informatiques. Elles peuvent adopter des formes variées, utiliser de nombreuses techniques de propagation, rendant inefficace le seul recours à une solution de sécurité au niveau du poste de travail. C'est pourquoi les responsables informatiques doivent impérativement mettre en place des politiques de sécurité globale pour se protéger contre ces menaces. En adoptant une approche de défense par couches successives, en complétant la solution bureautique par une analyse du trafic Web et e-mail entrant et sortant, les responsables informatiques pourront protéger efficacement leur entreprise contre la menace des attaques véhiculées par Internet.

---

## NETGEAR ProSecure STM : Solution de management des menaces Web et E-mail

Le boîtier ProSecure STM fait appel à une technologie exclusive qui détecte et bloque les attaques de façon appropriée à la rapidité et à l'étendue de leur propagation. Par cette approche, il est possible de détecter le spam et les attaques de malwares dès leur apparition, et de bloquer en temps réel tous les messages associés.

Le boîtier ProSecure STM intègre la technologie Netgear de Stream Scanning (Scan à la Volée), en attente de brevet, qui permet d'analyser les flux de données au moment où ils entrent sur le réseau. Grâce à la technologie Stream Scanning, les boîtiers NETGEAR STM peuvent traiter un volume important de données en temps réel, une seule analyse suffisant pour identifier le spam, les malwares, les atteintes à la sécurité ou les applications inappropriées. Il est ainsi possible de garantir aux utilisateurs du réseau un contenu e-mail et Web sûr, sans temps d'attente.

Le boîtier ProSecure STM utilise un système de défense comportemental et proactif qui supprime l'intervalle existant jusqu'alors entre l'exploitation d'une vulnérabilité et sa correction. La solution NETGEAR intègre une analyse chirurgicale qui permet d'identifier les caractéristiques suspectes du trafic réseau entrant et sortant, et de les neutraliser jusqu'à ce qu'elles puissent être examinées de manière approfondie.