

L'utilisation d'Internet met votre entreprise en danger

Introduction

Aujourd'hui, l'Internet joue un rôle toujours plus important au coeur de l'activité quotidienne des petites et moyennes entreprises. Il permet d'accéder très rapidement à l'information et de communiquer à tout moment avec le monde entier. Pourtant, malgré ses avantages indéniables, ce média véhicule également toute une variété de menaces susceptibles de porter atteinte à la sécurité des entreprises. Le simple fait de naviguer sur le Web expose l'utilisateur à quantité d'attaques dont le nombre grandit à mesure que se développent les activités en ligne.

Une utilisation inadaptée

Les entreprises qui n'ont mis en place aucun système de filtrage ou de contrôle de l'utilisation d'Internet par leurs collaborateurs risquent d'en ressentir l'impact sur la productivité, la réputation et la sécurité de leur réseau. Le temps passé sur l'Internet, pour des raisons personnelles ou professionnelles, peut représenter une part impressionnante dans la journée de travail d'un salarié. Nombreux sont ceux qui font des achats en ligne, échangent des fichiers peer-to-peer, naviguent sur les réseaux communautaires - voire même sur des sites de rencontre ou des sites pour adultes. Toutes ces activités font perdre du temps à l'entreprise, et exposent son réseau aux menaces qui se propagent via l'Internet.

Par exemple, il est bien connu que les sites pour adultes hébergent des programmes malveillants. Ce type de sites est facile et peu coûteux à mettre en ligne, leur contenu attire de nombreux visiteurs, et ils sont suffisamment tabous pour que les visiteurs qui les soupçonnent d'avoir infecté leur ordinateur n'en disent rien à personne. Autant de caractéristiques qui en font un média idéal pour diffuser des programmes malveillants.

Les sites de shopping en ligne sont tout aussi réputés que les sites pour adultes quant au risque qu'ils font courir à leurs visiteurs. La plupart de ces sites sont truffés de logiciels espions. De plus, bien souvent, lorsque l'utilisateur clique sur un lien de ce type de site, il est transféré à son insu vers un autre site. Ainsi, même si le site principal est fiable, l'utilisateur peut difficilement savoir s'il se trouve sur le site "propre" ou sur celui d'un tiers qu'il ne connaît pas...

Selon une enquête annuelle sur les atteintes à la sécurité des informations, réalisée par PricewaterhouseCoopers pour le compte du BERR (Ministère britannique de l'entreprise et de la réforme législative), une entreprise sur six déclare avoir eu connaissance d'une mauvaise utilisation des systèmes d'information par son personnel au cours de l'année écoulée. Dans 36% des cas, les collaborateurs ont consacré un temps excessif à la navigation sur Internet, et 41% ont visité des sites Web inappropriés. Bien que cela soit plus rare, des entreprises ont également fait état de certains accès à des contenus illégaux.

Cette utilisation inappropriée de l'Internet, y compris les comportements répréhensibles ou à risque, est due pour une large part à l'attitude désinvolte de nombreux collaborateurs vis-à-vis de l'équipement de leur employeur. Beaucoup naviguent sur Internet en considérant que l'ordinateur ne leur appartenant pas, ils n'ont pas à se soucier de la sécurité. De même, de nombreux utilisateurs estiment que la sécurité relève du service informatique, et qu'ils peuvent donc adopter un comportement à risque en toute impunité.

Un vecteur des menaces extérieures

Même bien utilisé, l'Internet constitue la principale source de menaces pour l'ordinateur, avec notamment les spywares, les chevaux de Troie, les robots, les portes dérobées (backdoor) et rootkits. Souvent, il suffit de visiter le site Internet pour être infecté. Cette méthode de propagation, que l'on appelle "drive-by download" (téléchargement intempestif) intervient en arrière-plan des activités normales de l'utilisateur en ligne, à son insu et sans aucune action de sa part.

Selon les études menées par NETGEAR ProSecure, 79% de ces menaces ont été identifiées sur des sites légitimes, victimes de pirates qui y ont injecté subrepticement une menace. Pour ce type d'attaques, les pirates exploitent certaines failles de sécurité pour infecter les sites qui n'ont pas encore appliqué le patch correspondant. Par conséquent, n'importe quel site est susceptible d'être la cible d'une attaque. Rien que sur le premier trimestre 2008, des milliers de sites Internet appartenant à des entreprises figurant au classement Fortune 500, à des organisations gouvernementales ou à certains établissements scolaires ont été la victime de malwares. Même des fournisseurs réputés de solutions de sécurité comme Symantec, Trend Micro et Computer Associates ont été concernés.

Téléchargements intempestifs

Les téléchargements intempestifs "drive-by download" font partie des menaces web. Cette menace est sensiblement différente de celles évoquées précédemment, en ce sens qu'elle compte sur la victime pour venir à elle, plutôt que d'attaquer le système de la victime. Dans le cas d'un drive-by download, une menace de type spywares, logiciel publicitaire ou cheval de Troie est installée sans que l'utilisateur ne le sache et sans aucune action de sa part. Lorsque l'utilisateur visite un site Web infecté, la menace est automatiquement téléchargée en arrière-plan. Le site infecté peut être un site malveillant, développé par un concepteur malintentionné pour offrir une apparence respectable, ou bien un site légitime victime d'un piratage puis d'une infection par cette menace. En tous cas, l'utilisateur n'est même pas conscient d'avoir été infecté.

Les pirates ont également appris à utiliser un site légitime comme appât, pour tromper les utilisateurs et les amener à cliquer sur un lien ou une pièce jointe par e-mail. En décembre 2008, le site du célèbre réseau communautaire Facebook a été utilisé comme vecteur pour une attaque de ce type. Les utilisateurs ont reçu un courrier électronique ayant pour objet "You look funny in this new video" (Tu as l'air marquant dans cette nouvelle vidéo). L'e-mail invitait le destinataire à cliquer sur le lien du message pour regarder la vidéo. L'utilisateur était alors redirigé sur un site de vidéo n'appartenant pas à Facebook, sur lequel on l'informait que son lecteur Flash devait être mis à jour. En cliquant sur le lien correspondant à l'action recommandée, l'utilisateur déclenchait l'installation d'un vers sur son système. Ce vers comportait un spyware et ouvrait une porte dérobée permettant l'envoi d'informations confidentielles à partir du système mais également d'installer ultérieurement un code supplémentaire.

Les menaces restantes (21%) sont dues à la navigation involontaire sur un site malveillant. Ce type de site a été conçu pour offrir une apparence respectable afin d'attirer tout particulièrement les utilisateurs peu méfiants. Bien souvent, les sites malveillants font appel au marketing sur les moteurs de recherche ou bien à des bannières publicitaires pour augmenter le nombre de visites.

S'ils implantent leur menace sur un site légitime, les pirates bénéficient d'un public acquis. S'ils développent leur propre site malveillant, ils peuvent mieux contrôler la diffusion de leur menace. Dans tous les cas, il semble évident qu'un simple blocage des sites en fonction du contenu n'est plus suffisant pour protéger l'entreprise des risques de l'Internet.

Protégez votre entreprise

Les pirates considèrent le système de l'utilisateur comme une faille, un accès jusqu'à leur véritable cible : le réseau de l'entreprise. C'est pourquoi la plupart des malwares pénètrent le réseau via le système des utilisateurs, pour ensuite se propager librement. Une fois à l'intérieur, ces menaces peuvent accaparer une part importante du débit du réseau, dérober des données sensibles appartenant à l'entreprise et à ses clients, endommager les systèmes de fichiers. Elles peuvent même pirater les actifs de l'entreprise pour servir de base de lancement à une campagne de spam ou autre menace véhiculée par e-mail.

Pour cette raison, la première ligne de défense contre les menaces qui se propagent par Internet consiste à définir et à faire appliquer une politique de bonne pratique de l'Internet. Cette politique identifierait clairement quels sont les sites autorisés ou non, et indiquerait une limite acceptable pour le temps passé sur Internet. Pour autant, la plupart des entreprises tolèrent à un certain niveau les activités personnelles sur le Web utilisant l'équipement de l'entreprise, et accordent à leurs collaborateurs une liberté trop grande, mettant ainsi en danger sa sécurité. La politique de bonnes pratiques ne doit pas seulement définir le temps que les salariés sont autorisés à passer sur Internet pour des raisons personnelles, mais également le type de sites autorisés.

En complément des politiques d'utilisation, il est absolument essentiel que l'entreprise mette en place d'importants moyens de sécurité au niveau de la passerelle, avec notamment un filtrage des URL et du contenu, ainsi qu'un contrôle bidirectionnel du trafic. Par le filtrage des URL et du contenu, le système de sécurité permet l'application de la politique de l'entreprise en bloquant les URL interdites et les contenus inappropriés. Lorsqu'un salarié tente de se connecter à un site proscrié, ou qui comporte des contenus que l'entreprise a interdits, la transmission réseau est bloquée et un rapport est envoyé au Responsable Informatique.

Il ne faut pas oublier que le filtrage protège l'entreprise d'une partie relativement limitée des menaces potentielles. Pour bénéficier d'une protection plus complète, le système doit impérativement réaliser également un contrôle bidirectionnel du trafic en temps réel pour assurer une protection proactive contre les malwares diffusés par les sites qui n'ont pas été spécifiquement bannis. On ajoute ainsi un rideau de défense essentiel qui apporte une protection efficace à l'entreprise contre les infections contractées involontairement par la navigation sur un site Web légitime piraté ou bien sur un site conçu pour offrir une apparence respectable. Le contrôle bidirectionnel concerne à la fois le trafic entrant et le trafic sortant chaque fois qu'un collaborateur se connecte à une URL. Si cette personne se retrouve par inadvertance sur un site infecté, le trafic entrant déclenche le système, et la transmission réseau est immédiatement bloquée.

Conclusion

Toute entreprise connectée à Internet doit faire face à certaines menaces pesant sur sa sécurité, qui se propagent au cours des activités normales de ses collaborateurs sur le Web. Si cette entreprise n'a pas mis en place des mesures de sécurité stricte au niveau de la passerelle, le risque d'infection s'accroît de façon exponentielle. Pour limiter ce risque, il est essentiel de définir et d'appliquer des bonnes pratiques pour l'utilisation d'Internet, associées à un contrôle bidirectionnel du trafic en temps réel.

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.