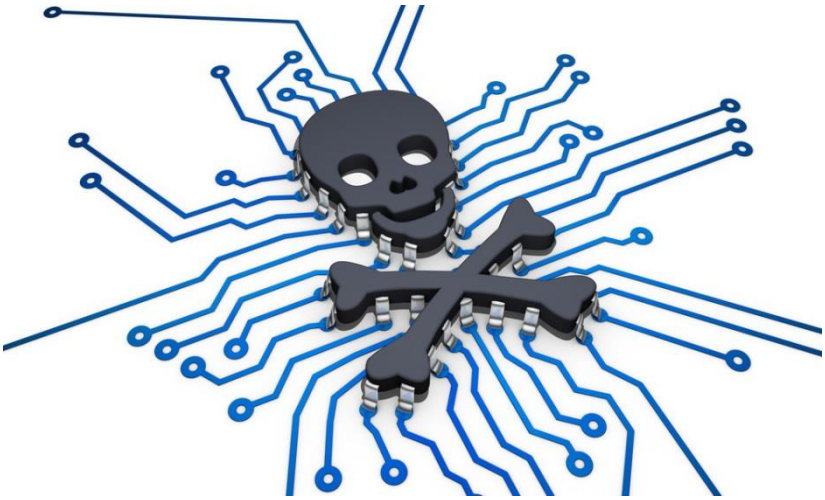
Les 9 menaces informatiques les plus courantes

Un article écrit par les experts de TELUS

Toutes les entreprises craignent les attaques informatiques, sans toujours savoir quelles formes celles-ci peuvent prendre. Ces menaces insidieuses sont variées, mais on peut facilement identifier les plus courantes par leur mode d'opération.

Logiciel malveillant

Un logiciel malveillant est un terme générique englobant ces différentes menaces qui visent toutes à nuire à un système informatique, qu'il s'agisse d'un ordinateur, d'un téléphone ou d'une caisse enregistreuse. Peu importe sa forme, un logiciel malveillant peut corrompre, effacer ou voler les données des appareils et réseaux d'une entreprise. Il peut subtiliser des données confidentielles, comme les numéros de carte de crédit de clients.



Virus informatique

De son côté, un virus informatique est un type de logiciel malveillant caché dans un logiciel légitime. Chaque fois qu'un utilisateur ouvre le logiciel infecté, il permet au virus de se propager. Il agit discrètement et se réplique à une vitesse fulgurante grâce aux échanges de données, que ce soit par une clé USB ou un réseau informatique.

Ver informatique

Le virus ne doit pas être confondu avec un ver informatique, qui se répand sur le réseau Internet. Ce dernier peut s'installer sur un ordinateur à partir d'un courriel, par téléchargement d'un fichier ou par messagerie instantanée. Il est beaucoup plus courant que le virus informatique de nos jours.

Logiciel espion ou cheval de Troie

Les virus classiques ont cédé le pas depuis une dizaine d'années à un type particulier de logiciel malveillant, les logiciels espions ou chevaux de Troie. Ceux-ci infectent silencieusement l'ordinateur grâce à une application en apparence légitime. Une fois dans l'ordinateur, le logiciel peut faire ce qu'il veut : enregistrer les mots de passe ou accéder à la caméra pour enregistrer les moindres faits et gestes de l'utilisateur. De quoi donner froid dans le dos…

Pourriel

En tant que tels, les pourriels sont inoffensifs, mais si on les ouvre ou si l'on clique sur leur lien, ils peuvent implanter un ver informatique sur l'ordinateur.

Vol d'appareils portatifs ou mobiles

Le vol de matériel est encore une réalité courante pour bien des entreprises, 42 % l'ayant vécu en 2013. Petits et faciles à transporter, les téléphones et tablettes sont particulièrement susceptibles d'être subtilisés d'un sac à main ou oubliés sur un banc de métro.

S'il n'est pas adéquatement protégé, il est facile d'extirper le contenu d'un appareil tombé entre de mauvaises mains ou de l'utiliser pour accéder aux réseaux de l'entreprise. Ceux-ci ne sont habituellement verrouillés que par un mot de passe de quatre chiffres, une protection trop faible la plupart du temps. Un malfaiteur peut aussi simplement effacer son contenu et revendre l'appareil sur le marché noir, jetant à la poubelle tout le travail qu'il contenait, une perte parfois considérable pour une entreprise.

Ces risques de perte et de vol sont accentués par la tendance appelée, en anglais, Bring your own device (BYOD), où les employés utilisent leurs appareils personnels au travail. De plus, les données personnelles se mélangent aux données professionnelles, rendant les employés réfractaires à des mesures de sécurité accrues.

Hameçonnage

La fraude par hameçonnage est plus facile à identifier. Il s'agit d'un courriel qui ressemble à s'y méprendre à celui d'un service connu, comme une institution bancaire. Le fraudeur tente d'obtenir des informations personnelles en incitant l'utilisateur à cliquer sur un lien, par exemple pour vérifier l'identification d'un compte de carte de crédit. Les banques le répètent pourtant : jamais elles ne demandent de renseignements personnels à leurs clients de cette manière.

Accès non autorisé à l'information

Même s'il est préoccupé par les menaces extérieures, tout directeur TI devrait porter une attention particulière à l'accès des employés aux informations confidentielles de l'entreprise. Par exemple, la secrétaire d'un cabinet médical n'a pas besoin de consulter les dossiers des patients à distance, mais cela peut être justifié pour les médecins.

Les comptes d'utilisateurs inactifs ou d'anciens employés sont des points faibles qui peuvent être facilement exploités. Un employé mécontent pourrait divulguer de l'information à la concurrence.

Lorsque des milliers de documents internes de la multinationale Sony ont été rendus publics en 2014, la faute a initialement été attribuée à des pirates nord-coréens, qui exigeaient que le film The Interview ne soit pas diffusé au cinéma. Peu à peu toutefois, des indications ont pointé vers la participation d'un ancien employé de Sony frustré, qui aurait aidé les pirates dans leur cyberattaque.

Les tiers partis ayant accès aux réseaux et systèmes de l'entreprise accentuent le potentiel de brèches informatiques, car peu d'entre eux utilisent des pratiques de sécurité optimales. Ils se connectent le plus souvent à distance, rendant le réseau vulnérable à ses points d'accès. Les entreprises américaines Target et Home Depot se sont d'ailleurs fait voler les numéros de carte de crédit et les courriels personnels de millions de clients, car des pirates informatiques avaient subtilisé les codes d'identification de leurs tiers partis. Les fraudeurs ont ainsi pu accéder directement à leur réseau.

Attaque par déni de service

L'attaque par déni de service est causée en inondant un serveur ou un site web de requêtes dans le but de le rendre indisponible. L'attaque par déni de service peut être perpétrée par un petit nombre de ressources. Un pirate peut utiliser son seul ordinateur pour contrôler des zombies, c'est-à-dire d'autres ordinateurs infectés qui obéiront à ses commandes. Ces ordinateurs peuvent avoir précédemment été infectés par des virus ou des vers.

Même si seulement 15 % des entreprises en ont été victimes, selon l'étude TELUS-Rotman, une telle cyberattaque peut causer de lourdes pertes financières si elle vise un site web transactionnel, par exemple. Des raisons politiques peuvent aussi animer les pirates informatiques, comme en témoigne l'attaque contre les sites du gouvernement du Canada en juin 2015, revendiquée par le collectif Anonymous en réponse à l'adoption du projet de loi C-51.

Face à la variété des menaces, adopter des mesures de sécurité proactives permet de prévenir ces attaques plus efficacement qu'en colmatant les brèches une à une.