Guides de sécurité pour les petites entreprises

Les cybercriminels et ceux contre qui il faut se protéger

AVG AU TRAVAIL

Cinq étapes pour sécuriser le site Web de votre entreprise et son contenu

Aujourd'hui, la plupart des ordinateurs sont connectés à Internet. Cela signifie qu'ils communiquent avec d'autres ordinateurs – ce qui implique un risque.

Nous utilisons nos PC aussi bien pour travailler que pour nous divertir. Nous faisons des achats, des transactions bancaires et jouons en ligne - même lorsque nous sommes au bureau - mais nous travaillons aussi à domicile. Le Web est un outil de recherche et un centre de loisirs, qui nous permet d'accéder à de la musique, des films, des émissions de télévision, etc. Ainsi, nous stockons sur nos PC des informations utiles et même des informations privées et personnelles essentielles.

Par conséquent, il est extrêmement important de stocker vos informations correctement et de les maintenir sécurisées. Il est également indispensable de protéger vos PC contre les utilisations impropres, les abus et les pertes de données.

Pourquoi ? Parce qu'il y a quelque part des cybercriminels qui cherchent à faire main basse sur vos informations.

Des bandits ? Oui, nous utilisons fréquemment ce terme, mais savez-vous réellement qui sont les bandits ?

Avant de pouvoir vous armer correctement contre une attaque et/ou une brèche de sécurité par les bandits, il est utile de savoir de qui vous devez vous méfier, afin de pouvoir mettre en place les couches de protection appropriées.

Il existe en réalité plusieurs catégories uniques de criminels dont nous devons nous méfier. On les appelle parfois pirates, voleurs de scripts, cybercriminels, cyber-espions, cyber-escrocs, cyber-activistes, cyber-terroristes, cyber-guerriers, et même amis ou collègues sans scrupules. D'un point de vue technique, un cyber crime est toute brèche délibérée de la sécurité d'un ordinateur via Internet ou une autre action illégale facilitée par Internet.

Les bases de l'entreprise : Définitions

Pirates

À une certaine époque, les « pirates » portaient des chapeaux blancs. Ils accédaient illégalement à des ordinateurs pour en savoir plus à leur sujet ou pour chercher des lacunes de sécurité dans l'ordinateur ou dans le réseau auquel il était connecté. Ils ne faisaient rien de mal et étaient fiers de la qualité de leurs actes qui ne laissaient aucune trace d'intrusion.

Pirates malfaisants

Ensuite, le paysage du piratage a évolué et on a commencé à assister à une domination des pirates malveillants – des personnes qui accèdent intentionnellement à un ordinateur ou à un réseau d'ordinateurs pour leur nuire, les endommager ou voler des données. Généralement, les deux types de pirates possèdent des connaissances très poussées de l'informatique et des réseaux, ce qui leur permet de développer des scripts ou des programmes grâce auxquels ils attaquent les systèmes et les réseaux informatiques.

Voleurs de scripts

Les outils de piratage se retrouvent parfois entre les mains de « voleurs de scripts » qui les utilisent, souvent, de manière aléatoire et sans comprendre réellement leurs conséquences ni s'en préoccuper. Les voleurs de scripts ne possèdent généralement que des connaissances limitées de l'informatique et peuvent manquer de maturité, cherchant souvent à déclencher une multitude d'attaques pour accéder à la notoriété et attirer l'attention.

Cyber criminels

Nous utilisons généralement le terme « cyber criminel » pour décrire une personne utilisant Internet de manière illégale ou facilitant des activités illégales ou frauduleuses.

Plus précisément, les cybercriminels sont des personnes qui cherchent à implanter des logiciels malveillants sur votre système afin d'obtenir des informations précieuses telles que les données de cartes de crédit et de comptes bancaires, les noms d'utilisateur et les mots de passe. Il s'agit d'un vol d'identité et ceux qui en sont responsables utilisent ces informations pour voler quelqu'un ou les vendent à une autre personne qui se livrera à des vols.

Les cybercriminels sont également des escrocs et des hameçonneurs qui tentent de vous inciter à leur envoyer de l'argent. Ils peuvent vous inviter à transférer des sommes importantes ou vous faire croire que vous avez gagné un prix dans une loterie à laquelle vous n'avez jamais participé. Parfois, ils promettent un héritage fabuleux provenant d'un richissime parent dont vous n'avez jamais entendu parler.

Certains cybercriminels vendent illégalement des logiciels, de la musique ou des films au mépris des lois sur le copyright. Il leur arrive même parfois de vendre des formes illégales de pornographie. Le profit est généralement leur unique motivation. Toutefois, dans le cas du cyber-harcèlement et du cyber-groupage, les mobiles sont différents.

Tous les cybercriminels ne possèdent pas des connaissances de pointe de l'informatique et des réseaux. Aujourd'hui, la grande majorité des cybercriminels utilisent simplement les outils et kits malveillants commercialisés à des fins lucratives par ceux qui les élaborent.

Par conséquent, la plupart des cybercriminels ne sont rien d'autre que des voleurs de scripts perfectionnés, mais désormais, ils cherchent l'argent et pas seulement la célébrité. Moyennant environ 280 euros, pratiquement n'importe qui peut acheter des scripts appropriés et au bout de quatre heures passées à suivre les instructions, être parfaitement équipé pour se livrer à la cyber criminalité. C'est assez effrayant.

Cyber-espions

Il s'agit le plus souvent de personnes qui tentent d'obtenir des informations à propos d'entreprises ou d'administrations. L'attaque vise en général une entreprise à but lucratif, tandis qu'on parle plutôt d'espionnage international lorsque la cible visée est une administration.

Les bases de l'entreprise : Définitions

Cyber-escroc

Il s'agit d'une personne qui se livre au chantage via Internet. Par exemple, elle peut menacer de révéler des informations confidentielles si une personne ou une entreprise ne lui verse pas une somme importante. Les cyber-escrocs peuvent mettre en place une attaque distribuée en déni de service (DDoS) contre le site Web ou le réseau d'une entreprise et exiger un paiement pour arrêter l'attaque. Ils peuvent vous persuader de télécharger et d'installer des logiciels malveillants/effrayants/illégaux, tels que des antivirus piratés, puis exiger un paiement pour les retirer.

Cyber-activistes

Il s'agit de personnes qui utilisent Internet pour accélérer leurs communications afin d'organiser des manifestations publiques, parfois liées à des collectes de fonds, regrouper des communautés, se livrer au lobbying et à l'organisation des foules. C'est le cas des Iraniens qui ont utilisé Twitter pour organiser des manifestations de masse en 2009.

Cyber-terroristes

Il s'agit de cybercriminels qui utilisent Internet pour détruire des ordinateurs ou perturber des services connectés à Internet et ce, pour des raisons politiques. À l'instar d'une attaque terroriste classique, le cyber-terrorisme requiert généralement des individus compétents, beaucoup d'argent et une planification minutieuse. On peut citer l'exemple des centaines d'attaques en DDoS organisées en 2007 et qui ont failli détruire Internet en Estonie.

Il semble que de nombreux pays, parmi lesquels les États-Unis et la Chine, aient décidé qu'Internet est un outil valide pour mener une guerre contre leurs ennemis. Même si Internet peut être utilisé pour renforcer considérablement une puissance militaire et économique, il présente également des vulnérabilités pour les adversaires actuels et futurs. Par conséquent, les gouvernements recrutent et forment des cyber-guerriers à l'utilisation d'Internet pour mener des attaques et pour nous protéger contre ce type d'attaques menées par d'autres. Triste, mais vrai.

En nous connectant, nous sommes tous à la merci des bandits. Il est donc indispensable que les entreprises comme les particuliers sécurisent leurs informations afin que les criminels ne puissent pas y accédert.

Comment protéger votre entreprise et vous-même

- Installez sur tous les PC que vous utilisez un logiciel de sécurité Internet à jour et correctement configuré, par exemple **AVG Internet Security Businnes Edition 10**
- Comprenez qui peut chercher à traverser vos défenses et comment il peut procéder. On peut espérer que les informations que nous vous avons fournies ici vous aideront en ce sens.
- Regardez cette vidéo pour voir comment la protection AVG a aidé ces entreprises

AVG SMB group :
bit.ly/AVGSMB

Devenez fan d'AVG:
facebook.com/avgfree

Lisez nos blogs :
blogs.avg.com

Suivez-nous sur :
twitter.com/
officialAVGnews

Devenez un affilié AVG :
avg.com/affiliate

Regardez notre chaîne :
youtube.com/officialAVG

AVG Technologies France
1, Place de la Chapelle
64600 Anglet
France
www.avg.fr

AVG Technologies CZ, s.r.o.
Lidická 31, 602 00 Brno
République Tchèque
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
États-Unis
www.avg.com

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Royaume-Uni
www.avg.co.uk

AVG Technologies GER GmbH
Bernhard-Wicki-Str. 7
80636 München
Allemagne
www.avg.de

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosie, Chypre
www.avg.com

AVG AU TRAVAIL