AVG V PRÁCI

Small Business Průvodci zabezpečením

Počítačoví zločinci a rady, proti komu se chránit.

Pět kroků pro zabezpečení webových stránek vašeho podniku a jejich obsahu

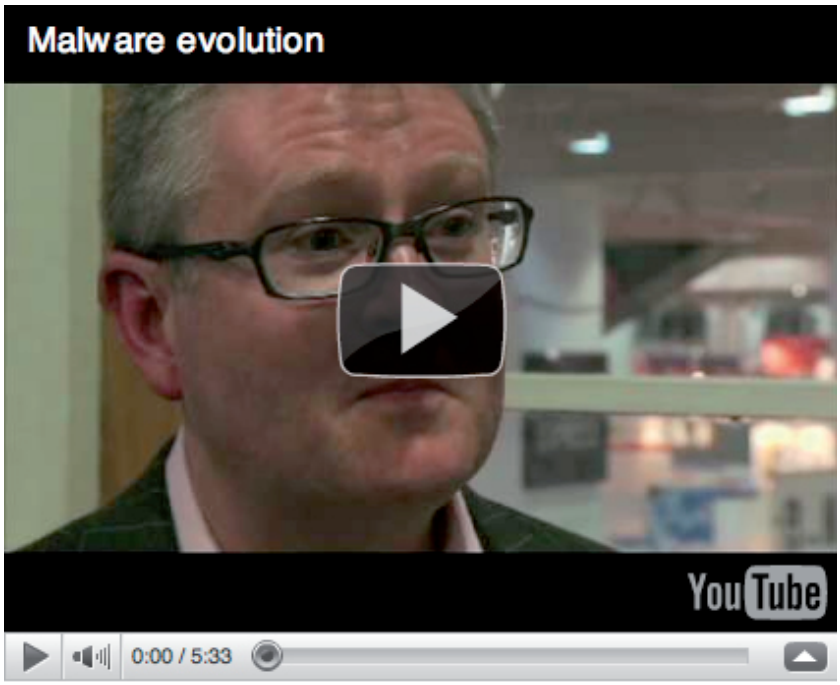
Své počítače používáme k práci i k hraní. Nakupujeme, provádíme bankovní transakce, hrajeme hry online dokonce i v práci, a naopak pracujeme, i když jsme doma. Web slouží jako nástroj pro vyhledávání i jako centrum zábavy, umožňuje nám přístup k hudbě, televizním pořadům a mnoha dalším zdrojům. Přitom ukládáme do počítačů užitečné informace, přičemž často se jedná o důležité soukromé či osobní informace.

Proto je nutné tyto informace ukládat správně a zajistit jejich bezpečnost. Počítače je rovněž nutné chránit před zneužitím a ztrátou dat. Proč? Protože existují zločinci, kteří se snaží vaše informace získat.

Zločinci? Ano, často mluvíme o zločincích, ale koho si pod tímto pojmem vlastně představit?

Při budování obrany proti bezpečnostním útokům a vniknutí zločinců vám jistě pomůže, pokud budete vědět, na koho si dávat pozor. Jen tak budete schopni správně nastavit úrovně ochrany.

Ve skutečnosti lze zločince rozdělit do několika jednoznačných kategorií, na které je třeba si dát pozor. Používáme různá označení jako hackeři, crackeři, script kiddie, počítačoví zločinci, počítačoví špioni, počítačoví vyděrači, počítačoví aktivisté, cyber počítačoví teroristé, počítačoví válečníci, ale může se jednat i o neeticky jednající kolegy či zaměstnance. Z technického hlediska představuje počítačový zločin jakékoli úmyslné porušení zabezpečení počítače prostřednictvím Internetu či jinou nelegální činnost , které Internet umožňuje.



Základy pro podniky:

Definice

Hackeři

Byly doby, kdy hackeři chovali dobré úmysly. Ilegálně pronikali do počítačů, aby o nich zjistili podrobnosti, nebo hledali bezpečnostní mezery v počítačích či v sítích, ke kterým jsou počítače připojeny. Neprováděli však nic škodlivého a byli pyšní na kvalitu proniknutí, které nezanechalo žádné stopy.

Crackeři

Hackerské prostředí se později změnilo a převládli crackeři – lidé, kteří záměrně pronikali do počítačů či sítí s úmyslem způsobit škodu či odcizit data. Hackeři i crackeři jsou obvykle velmi zruční v práci s počítači a v síti a dokážou vyvíjet skripty a programy, které jim umožňují napadat počítačové systémy a sítě.

Script kiddie

Hackerské nástroje se mohou dostat do rukou uživatelům označovaným jako „script kiddie“, kteří je poté používají, často bez plného vědomí možných následků. Tito uživatelé mají obvykle omezené dovednosti a často se jedná o nedospělé osoby, které se snaží provést co nejvíce útoků za účelem upoutání pozornosti.

Počítačoví zločinci

Termín „počítačový zločinec“ se obvykle používá pro ty, kteří používají Internet nelegálním způsobem nebo umožňují nelegální či podvodné činnosti.

Přesněji se „počítačoví zločinci“ snaží umístit malware do systému za účelem získání cenných informací, například čísel platebních karet a přihlašovacích údajů k bankovním účtům. Jedná se o krádež identity a původci často získané informace využívají k podvodům či je prodají jiným zločincům.

Mezi počítačové zločince patří rovněž podvodníci využívající phishing a podvodné e-maily, jimiž se snaží vylákat peníze. Mohou vás požádat o převod velkých peněžních částek nebo vám sdělit, že jste vyhráli cenu v loterii, které jste se však neúčastnili. Někdy se jedná o podvodný e-mail slibující dědictví po bohatém příbuzném, kterého neznáte.

Někteří počítačoví zločinci nelegálně distribuují software, hudbu či filmy a porušují zákony na ochranu autorských práv. Mohou rovněž prodávat ilegální druhy pornografie. Jejich aktivity jsou obvykle zaměřeny pouze na zisk. V případě kyberšikany či kybergroomingu jsou však motivy jiné.

Ne všichni počítačoví zločinci mají kvalitní schopnosti práce s počítači a v síti. Velká většina počítačových zločinců dnes využívá nástroje a sady škodlivého softwaru prodávané jejich tvůrci za účelem zisku.

Ve většině případů se tak jedná o novodobé uživatele typu „script kiddie“, kteří jsou však motivováni ziskem, nikoli získáním pozornosti. Odpovídající skripty si dnes může téměř kdokoli koupit za cenu přibližně 400 dolarů a po několika hodinách provádění požadovaných postupů se stát počítačovým zločincem. To je děsivé.

Kybernetický špion

Obvykle se jedná o osobu, která se snaží získat informace o společnostech nebo státních organizacích. Útoky na podniky jsou obvykle vedeny za účelem zisku, zatímco v případě útoků na státní organizace se jedná o mezinárodní špionáž.

Internetový vyděrač

Osoba, která se věnuje vyděračství prostřednictvím Internetu. Příkladem je hrozba zveřejnění důvěrných informací, pokud vydíraná osoba či společnost nevyplatí velkou peněžní částku. Internetoví vyděrači mohou například použít distribuovaný útok DDoS proti webu nebo síti společnosti a vymáhat platbu za jeho zastavení. Mohou vás podvodně přimět ke stažení a instalaci malwaru/scarewaru/scamwaru, například podvodného antivirového softwaru, a poté požadovat platbu za jeho odstranění.

Internetový aktivista

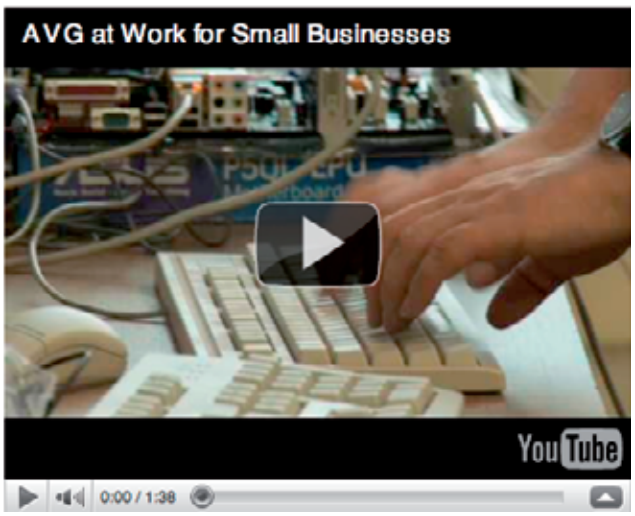
Osoba, která využívá Internet k rychlejší komunikaci při pořádání rozsáhlých demonstrací, případně získávání finančních prostředků, vytváření komunit, lobbingu či organizování. Příkladem je využití Twitteru k organizování masových protestů v Íránu v roce 2009.

Internetový terorista

Jedná se o počítačového zločince, který využívá Internet k ničení počítačů nebo narušení internetových služeb z politických důvodů. Stejně jako běžný teroristický útok vyžaduje počítačový terorismus obvykle vysoce zručné osoby, dostatek peněz na realizaci a podrobné naplánování. Příkladem mohou být stovky útoků DDoS v roce 2007, které prakticky vyřadily z provozu Internet v Estonsku.

Zdá se, že mnoho zemí, včetně USA a Číny, považuje Internet za užitečný nástroj v boji proti nepřátelům. Internet může sloužit k výrazné podpoře vojenské a ekonomické síly, avšak představuje rovněž slabé místo ideální pro útoky současných i budoucích nepřátel. Vlády států proto zaměstnávají a školí počítačové bojovníky, kteří používají Internet k útokům a zajišťují obranu proti podobným útokům ostatních. Je to smutné, ale je to pravda.

Při připojení online je útokům zločinců vystaven každý. Proto je pro podniky i jednotlivce klíčové, aby zabezpečili své informace a zabránili zločincům v přístupu k nim.



Jak chránit svůj podnik i sebe

Používejte aktuální a správně nakonfigurovaný software internetového zabezpečení ve všech počítačích, které používáte, např. AVG Internet Security Business Edition 2011.

Uvažujte, kdo může mít zájem proniknout vašimi ochrannými systémy a jakým způsobem to může provést. Věříme, že poskytnuté informace pro vás budou užitečné.

Na následujícím videu můžete vidět, jak ochrana od společnosti AVG pomáhá podnikům.

Skupinu AVG SMB najdete na adrese:
bit.ly/AVGSMB

Staňte se fanouškem společnosti AVG na adrese:
facebook.com/avgfree

Přečtěte si naše blogy na adrese:
blogs.avg.com

Sledujte nás na adrese:
twitter.com/officialAVGnews

Staňte se partnerem společnosti AVG na adrese:
avg.com/gb-en/affiliate

Sledujte náš videokanál na adrese:
youtube.com/user/officialAVG

AVG Technologies CZ, s.r.o.
Holandská 4, 639 00 Brno
Česká republika
www.avg.cz

AVG Technologies USA, Inc.
1 Executive Drive, 3rd Floor
Chelmsford, MA 01824
USA
www.avg.com/us-en/homepage

AVG Technologies UK, Ltd.
Glenholm Park, Brunel Drive
Newark, Nottinghamshire,
NG24 2EG
Velká Británie
www.avg.co.uk

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

AVG Technologies CY Ltd.
Arch. Makariou III.
2-4 Capital Centre
1505, Nicosia, Cyprus
Fax: +357 224 100 33
www.avg.com