Slovník pojmů, se kterými se setkáte při výběru antivirového programu

Výkonná ochrana, super zabezpečení, vaše data budou jako v sejfu! Tak přesně s takovými větami se setkáte, při výběru antivirového programu. Jenže pak se objeví výrazy jako malware, phishing, anti-theft atd..Ztrácíte se v této části popisků produktů? Pak právě pro vás máme super pomocníka. Takový slovník s vysvětlením jednotlivých pojmů. A začneme pěkně od začátku abecedy!

Address Harvester

Robot, který je naprogramovaný tak, aby navštěvoval jednotlivé webové stránky, fóra nebo třeba blogy a hledal. Hledal cokoliv, co vypadá jako platná e-mailová adresa. Nakonec získá spoustu e-mailových adres, které využije k zasílání e-mailů nakažených virem nebo je může majitel prodat. Po takových elektronických adresách se poptávají především rozesílatelé spamu.

Adware

Speciální a velice nenápadný program. Jeho instalace do počítače proběhne, aniž byste o tom věděli. Obsahují ho například neprověřené programy, které můžete zdarma stáhnout na pochybně vypadajících stránkách na internetu zdarma. Adware si můžete představit jako takovou nepatrnou část, která je součástí takto stahovaného programu. Ovšem jakmile se do počítače dostane, může napáchat velké škody. Může totiž nainstalovat další skryté programy, které o vás sbírají nejrůznější detaily. Jako např. vaši e-mailovou adresu, webové stránky, které navštěvujete apod. Takto získané informace může autor tohoto viru poskytnout za slušný peníz zadavatelům reklamy. Ti pak zahltí vaši e-mailovou schránku reklamou a spamem (nevyžádanou poštou).

Anti-Phishing

Zabraňuje podvodným internetovým stránkám získat citlivá data (uživatelské jméno, heslo k poštovním účtům a bankovnictví, detaily o kreditní kartě atd.).

Antispam (spam filter)

Soubor programů, které zkoumají příchozí e-maily. A to podle různých pravidel i filtrů (porovnávají je s databází spamů, blocklisty, bayesiánskými filtry aj.). Na základě těchto pravidel oddělují spam (tedy nevyžádanou poštu) od pošty, kterou skutečně očekáváte. Takže se nevyžádaná pošta nedostane do e-mailové schránky adresáta.

Antispyware

Program kontroluje všechna data, která stahujete nebo jinak přenášíte do PC (například přes USB). Během kontroly vyhledává spywarový software (*označení pro škodlivé počítačové programy zaměřené na sledování -špionáž- napadeného počítače*). A pokud odhalí hrozbu, znemožní jí přístup. Takže nemůže váš počítač ohrozit. Zároveň sestavuje seznam podezřelých položek, které mají být vymazány.

Antivirus

Software navržený tak, aby ochránil počítač před útoky počítačových virů. Antivirus automaticky kontroluje váš počítač. A to nonstop. Mimo obrany při brouzdání na internetu, například scanuje všechny soubory, které na webu používáte. Zároveň můžete manuálně spustit podrobný test všech souborů na disku počítače. Tyto testy mohou trvat i několik hodin, ale občasný scan se doporučuje. Mezi nejznámější antiviry patří AVG, ESET, Norton či Kaspersky.

Anti-Theft

Aplikace, která umožní najít váš ztracený telefon, tablet nebo třeba notebook. A to pomocí GPS, WiFi nebo mobilní sítě. Zároveň je schopný na dálku uzamknout váš telefon. Takže zabrání přístupu k vaším osobním datům a nastavením nepovolané osobě. V případě krádeže telefonu a vložení nové SIM karty, může být nové číslo a poloha telefonu odeslána na zařízení některého z vašich přátel.

Bezpečnostní údaje

Hromadný pojem pro bezpečnostní prvky, jako například klientské číslo či heslo. Ty jsou automaticky přiděleny každému uživateli bankovnictví. S cílem jeho jednoznačné identifikace.

Botnet

Hlavní hnací silou pro tvorbu botnetu je uznání a finanční zisk. Čím větší botnet je, tím větší "prestiž" má majitel napříč komunitou. Ten také pronajímá část třetím stranám například k rozesílání spamu a DDoS útokům. Díky velkému množství počítačů, jež jsou součástí botnetu, je schopen vygenerovat velký síťový provoz ať už jako útok nebo spam

Bulk

Označení pro e-mail, který je poslán velkému množství adresátů.

Bullying (cyber bullying, kyberšikana)

Moderní doba přináší bohužel i moderní styl šikanování. Kyberšikana se rozmohla zejména mezi mladistvými. Bullying může mít více podob sahajících od posměchu přes urážky až k bití. Takový útok se nahraje a následně sdílí přes mobilní telefon, e-mail, internet či blog, mluví se o „e-bullyingu" nebo častěji o „cyber bullyingu" (kyberšikaně). Ovšem pozor! Terčem kyberšikany se může stát také například učitel ve škole. Žáci například stáhnou učitelovu fotografii a vytvoří z ní "vtipnou" koláž a tak podobně.

Cracker

Osoba, která se nelegálně nabourává do počítačových systémů cizích lidí či firem.

Cyberstalking

Použití mobilního telefonu, e-mailu, tabletu počítače, notebooku atd... cizího uživatele k obtěžování jiného uživatele.

Červ

Další speciální druh viru. Tento ale sám sebe kopíruje a může se samovolně šířit na velké množství počítačů, napadat sítě, snižovat rychlost připojení počítače k internetu, vypnout počítač apod.

Download (stahování)

Ukládání souborů z internetu do vlastního počítače. Ke stahování dochází i při běžném surfování po internetu (tedy prohlížení webových stránek). Pro zobrazení jakékoliv webové stránky, je totiž třeba

nejprve stáhnout její obsah ze serveru. Stahovat je možné i celé soubory, jako např. dokumenty, programy, hudbu nebo filmy.

E-mail

Elektronická pošta. Nejrozšířenější způsob internetové komunikace. E-maily (elektronické dopisy) mohou obsahovat nejen text, ale také např. různé dokumenty, obrázky či videa přiložené v příloze. E-mail je závislý na připojení k internetu. Bez něj není možné mejly posílat a ani přijímat.

Exploit Blocker

Blokuje hrozby, které se jinak úspěšně vyhýbají detekci. Eliminuje malware, který zamyká obrazovku a brání přístupu do systému. Chrání před útoky na webové prohlížeče, PDF čtečky a další aplikace.

Firewall

Kontroluje komunikaci mezi sítěmi a sloužící ke kontrole jejich důvěryhodnosti. Firewall může zakázat komunikaci na základě předem určených pravidel. Může také povolit komunikaci pouze mezi nastavenými adresami.

Firmware

Je v současných elektronických zařízeních běžně používán. Nesprávně provedená aktualizace firmware může vést k tzv. „bricku" (zařízení je nadále nepoužitelné).

Grooming (lákání na schůzku)

Pojem, který označuje jednání pedofilů. Ti se představují dětem jako jejich vrstevníci a pokoušejí se je vylákat na schůzku. Během psaní zpráv zjišťují informace o místě jejich pobytu, zájmech, koníčcích a sexuálních zkušenostech.

Hacker

Osoba, která neoprávněně proniká na nejrůznější webové stránky a nebo se snaží nabourat do počítačového systému. Cílem hackerů bývají často informace z firem menších, středních ale třeba i vládních organizací nebo bank (např. různé adresáře e-mailových kontaktů). Ty pak prodávají rozesílatelům spamu.

Hash Buster

Označení způsobu, jakým se rozesílatelé spamu mohou vyhýbat tomu, aby jejich nevyžádané e-maily nezachytil spam filtr. Může to fungovat například tak, že vloží náhodně vybraný obsah do každého nevyžádaného e-mailu. Častokrát v podobě částí slov v kolonce předmět. To může spam filtry zmást.

HIPS (Host-based Intrusion Prevention System)

Nabízí lepší nastavení a kontrolu chování systému. Umožňuje definovat pravidla pro systémové registry, procesy, aplikace a soubory a detekuje hrozby na základě chování systému.

Homebanking

Služba, kterou poskytuje banka klientovi a spočívá v komunikaci s bankou (včetně zadávání platebních příkazů) prostřednictvím sítě internet. K tomu, aby tato komunikace mohla fungovat, je třeba do PC nainstalovat speciální program. Ten nabízí přímo banky. A právě tím se homebanking odlišuje od internetového bankovnictví, kde se speciální program nepožaduje.

Hyperlink

Odkaz na jiný dokument na internetu nebo na jiné místo v dokumentu. Často se označuje jako link a po kliknutí se uživateli otevře dokument, na který odkazuje.

Hypertext

Speciální skrytý text, který obsahuje hyperlinkové propojení na jiný dokument nebo na jiné místo v dokumentu. Odkazy v takovém textu jsou obvykle zobrazovány modrým písmem a ještě podtrženy. Uživatel, který na takto označený text klikne, bude mít možnost otevřít dokument nebo webovou stránku, na nějž text odkazoval. Hypertext usnadňuje například orientaci v rozsáhlých textech a publikování odkazů.

Internetové bankovnictví

Bankovní služba. Ta klientovi umožňuje komunikaci s bankou (včetně zadávání platebních příkazů). A to pouze pomocí internetu. Klient nepotřebuje instalovat žádné speciální programy, postačí mu pouze internetové připojení.

Instant messaging

je internetová služba, která uživatelům umožňuje zjistit, kteří jejich přátelé jsou právě připojeni k internetu. A dle potřeby jim posílat zprávy, přeposílat soubory a obecně vzájemně komunikovat. Hlavní výhodou oproti používání např. e-mailu spočívá v principu odesílání zpráv v reálném čase, zpráva je doručena ve velmi krátké době od odeslání.

Internet

Je označení pro celosvětovou počítačovou síť, která propojuje jednotlivé sítě. Internet slouží k přenášení informací a poskytování mnoha služeb (např. e-mail, chat, www stránky atd.)

Internet service provider (poskytovatel internetového připojení)

Firma nebo organizace, která poskytuje přístup na internet a další příbuzné služby.

Internetová stránka

Představuje soubor webových stránek s informačním obsahem textů, obrázků, videí a dalších digitálních položek na internetu. Přístupná je z mobilních telefonů, počítačů stolních i notebooků nebo tabletů. První internetová adresa se objevila v roce 1991.

Internetové fórum/internetová diskuse

je stránka na internetu, na které naleznete názory, reakce a dotazy dalších uživatelů. Internetová diskuse se vyznačuje tím, že přispěvatelé nemusí být ke stránce připojeni současně, ale mohou reagovat i s časovým odstupem.

IP adresa

je jednoznačná identifikace konkrétního počítače v internetu. Zkratka „IP" značí "*internetový protokol*". To je způsob, jak spolu komunikují všechna zařízení v internetu.

Junk Mail

Označení pro nevyžádanou reklamu.

Logging

Proces, který zprostředkovává přístup uživateli do počítačového systému. Log-in je označení pro identifikaci uživatele, která je nutná při vstupu do systému (obvykle obsahuje uživatelské jméno, heslo

atd.). Naopak označení log-out se používá pro opuštění systému uživatelem (předtím co do něj vstoupil pomocí log-in).

Mail Loop (e-mailová smyčka)

Označení pro vir, kdy jeden automatický e-mail spustí další a ten opět spustí ten první e-mail k odpovědi atd., Tím vzniká takzvaná e-mailová smyčka (*mail loop*).

Malware

Malware je jakýkoli typ škodlivého softwaru, který se snaží infikovat počítač, telefon nebo tablet. Hackeři využívají malware pro různé účely. Jedním z těch nejčastějších je získávání osobních údajů, krádež peněz nebo firemních dat. Mohou tak získat i přístup k napadenému zařízení.

Mobilní bankovnictví

Další z podob přímého elektronického bankovnictví. Funguje tak, že klient ke komunikaci s bankou (včetně zadávání platebních příkazů) používá speciální program v mobilním telefonu - oproti běžnému telefonnímu bankovnictví poskytuje vyšší míru ochrany klienta.

Mousetrap (past na myši)

Jednoduchý prográmek (*JavaScript*). Jeho úkolem je ztížení procesu opuštění webové stránky. Pokud uživatel zkusí ze stránky odejít, objeví se okénko, které ho vrátí zpět na stránku a brání mu v kliknutí na tlačítko Zpět. Používá se, například v momentě, kdy je zadavatel reklamy placen za počet osob, které kliknou na klientovu webovou stránku.

Nelegální obsah

To je označení pro takový obsah internetových stránek, který je podle zákonů daného státu protiprávní. Většinou jde o obrázky sexuálního zneužívání dětí, protiprávní aktivity na chatu (např. grooming - lákání na schůzku) nebo publikování materiálů nenávistného charakteru.

Nevyžádaná pošta (spam)

Stejné zprávy posílané najednou na e-mailové adresy mnoha lidí, kteří o ně nemají zájem.

Newsletter (zpravodaj)

Jednoduchá forma novin nebo informačního letáku. Ten má za cíl komunikovat s cílovou skupinou. Zpravodaje jsou většinou legitimní a uživatel musí s jejich zasíláním souhlasit - většinou je možné se k nim přihlásit. Stejně tak musí být možné zasílání zpravodaje odhlásit.

Nezákonný obsah

Tento obsah webu je zakázán zákonem. Jedná se především o dětskou pornografii, nelegální sexuální praktiky, nabídky dětské prostituce a sdružování pedofilních zájmů.

Ochrana soukromí

Soubor nastavitelných vlastností systému. Ty mají zabezpečit ochranu soukromí uživatele a jeho osobních údajů.

Ochrana domácí sítě

umožňuje otestovat domácí router na různé zranitelnosti, jako je slabé heslo nebo neaktuální firmware. Poskytuje seznam aktuálně připojených zařízení a uživatel je může pro lepší přehlednost řadit do různých kategorií.

Ochrana webkamery

Monitoruje všechny procesy a aplikace běžící na počítači a upozorní uživatele na nestandardní použití webové kamery.

Osobní údaje

Jakékoli informace, které lze přiřadit určité osobě. Při shromažďování, zpracovávání a přechovávání osobních dat je vždy nutno přesně určit účel, pro který jsou používána.

Parental Control (rodičovská kontrola)

Způsob, jakým mohou rodiče sledovat chování dítěte při práci na počítači a případně omezit jeho aktivity na internetu. Umožňuje také rodičům nastavit jaké aplikace a internetové stránky si děti mohou prohlížet nebo používat či jaké soubory stahovat.

Pasivní transakce

Je souhrnné označení pro všechny informace poskytované prostřednictvím přímého bankovnictví.

Pharming

Přesměrování klienta na **falešné stránky** internetbankingu po napsání URL banky do prohlížeče. Tyto stránky jsou obvykle k nerozeznání od skutečných stránek banky. Ani zkušení uživatelé nemusejí poznat rozdíl.

Phishing

Představuje získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. Mejl může vypadat, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů, úřadů státní správy nebo od IT administrátorů. Principem phishingu je typicky rozesílání e-mailových zpráv, které často vyzývají adresáta k zadání osobních údajů na falešnou stránku, jejíž podoba je takřka identická s tou oficiální. Stránka může například napodobovat přihlašovací okno internetového bankovnictví. Uživatel do něj zadá své přihlašovací jméno a heslo. Tím tyto údaje prozradí útočníkům, kteří jsou poté schopni mu z účtu vykrást peníze.

Počítačový virus

Tento pojem se využívá ve spojení s jakýmkoliv napadením počítače škodlivým souborem. Ovšem není zcela správný. Protože kromě virů existují i jiné programy ohrožující počítač, jako jsou např. programy malware (určené ke vniknutí do počítačového systému a jeho poškození). Viry mohou být šířeny z jednoho počítače na druhý, pokud se jejich hostitel dostane do kontaktu s jiným, neinfikovaným počítačem např. prostřednictvím internetu nebo vyměnitelného média jako jsou CD, disketa nebo flash disk. Zatímco některé viry mohou být cíleně ničivé (mazání souborů na disku), jiné mohou jen obtěžovat.

Prohlížeč (browser)

Umožňuje prohlížení internetu. Jde o okno, ve kterém se zobrazují jednotlivé webové stránky. Prohlížeče umožňují práci s těmito stránkami (např. vyplňování formulářů, práci s obrázky, hraní jednoduchých her atd.). Mezi nejznámější patří Microsoft Internet Explorer, Mozilla Firefox, Opera či Google Chrome.

Přílohy

Složky, které posíláme spolu s e-mailovou zprávou (např. obrázky, textové dokumenty). Bohužel mohou být přílohou e-mailů od neznámých odesílatelů i škodlivé programy.

Skriptové útoky

Útoky škodlivých skriptů, které se snaží zneužít prostředí Windows PowerShell, a Javascriptové útoky ve všech běžných internetových prohlížečích. Funkce je obsažena ve všech uváděných produktech.

Řetězový dopis

Je označení e-mailu, který je poslán postupně několika lidem. Tato sdělení často obsahují přátelské pozdravy nebo naopak hrozby, co se stane, pokud neuděláte to, o co vás dopis žádá. Nejedná se přímo o spam, nicméně je mnoha lidmi za spam považován.

Sdílení souborů

Představuje formu zajištění přístupu k určitým souborům. A to hned pro více uživatelů internetu. Sdílející uživatelé mohou sdílené složky nahrávat i stahovat.

Server

Si představte jako počítač, který v rámci internetu neustále obsluhuje jiné počítače. Začíná pracovat v momentě, když se chcete podívat na nějaké webové stránky. Server musí komunikovat právě s jedním nebo více servery. Na některých serverech je uložený samotný obsah webových stránek (zdrojový kód, texty, obrázky nebo třeba databáze) a jiné servery zajišťují a doplňují komunikaci (např. proxy server či DNS).

Sociální síť

Je služba na internetu, která uživatelům umožňuje vzájemnou a velice rychlou komunikaci. Registrovaní uživatelé vlastní tzv. profily a následně mohou např. diskutovat, chatovat, psát si blogy, sdílet fotografie, a podobně. Jak už název napovídá, klíčové jsou vztahy a vazby - tedy vytváření „sítí" mezi přáteli, kolegy, zájmovými skupinami atd. Mezi nejznámější sociální sítě patří Facebook, Instagram nebo třeba Twitter.

Spam

nevyžádané, obtěžující reklamní e-maily.

Spambot

Program, který navštěvuje náhodné webové stránky a diskusní internetové stránky a sbírá na nich vše, co vypadá jako platná e-mailová adresa. Tu následně přidá na spam seznam, tedy seznam adres k rozesílání spamu.

Spamfilter

Filtruje všechny příchozí e-maily a třídí je. A to na normální e-maily a ty, které obsahují spam nebo takovým způsobem vypadají.

Spammer

Je označení pro člověka, který rozesílá spam.

Spamnest

Označení pro společnost nebo místo, kde se vytváří a rozesílá spam (*nebo které umožňuje jeho rozesílání*).

Spamware

Hromadné označení pro programy určené pro sbírání e-mailových adres a programy sloužící přímo k rozesílání spamu.

Spim

Nevyžádaná reklama v on-line komunikaci na ICQ, Messenger a Skype.

Spoofing

Označení pro situaci, kdy spammer nebo scammer falšuje svůj vlastní původ nebo předstírá, že je někdo jiný. Toho dosáhne např. posláním e-mailu s falešnou hlavičkou. Do této kategorie je možné zařadit také phishing maily, které mají zakrýt identitu skutečného odesílatele.

Spyware

Skupina škodlivých programů, které se zaměřují na sledování (špionáž) napadeného počítače. Jakmile spyware úspěšně infikuje počítač, může sledovat aktivitu jeho uživatele - např. jaké webové stránky si prohlíží, s jakými pracuje soubory nebo co píše na klávesnici. Spyware tedy může zjistit i velmi citlivé údaje (např. přístupová hesla) a ty pak potají odeslat svému tvůrci. Na detekci a odstraňování škodlivých programů se používá např. Ad-Aware či Spybot.

Stahování (downloading)

Získávání souborů z internetu do vlastního počítače.

Trojský kůň

Takový "balicí papír" pro škodlivé programy. Navenek se tváří jako užitečný program ke stažení zdarma. Po stažení a nainstalování do počítače se z trojského koně „vybalí" další škodlivé programy (viry, spyware, adware...).

URL (Uniform Resource Locator)

Slouží k přesnému určení umístění informací na internetu. Například URL této stránky je http://www.sw.centrum.cz/tutorialy/slovnik-pojmu-se-kterymi-se-setkate-pri-vyberu-antiviroveho-programu/

Virus

Dokáže sám sebe kopírovat a šířit se do dalších počítačů (jako virus skutečné nemoci). Existuje celá řada různých virů a většina z nich může být velice nebezpečná - některé mohou např. smazat nebo zničit soubory v počítači, jiné mohou odeslat citlivá data uživatele (např. hesla nebo dokumenty) a další mohou nakažený počítač přímo ovládat (a třeba rozesílat viry dalším lidem).

Virus Mail

Tento pojem představuje e-mail, který obsahuje počítačový program navržený tak, aby se sám kopíroval a roztahoval se z počítače do počítače. Samozřejmě aniž o tom uživatel věděl.

Vyhledávač

Webová aplikace, vytvořená tak, aby uživateli umožnila vyhledávat informace, webové stránky nebo dokumenty v internetu.

Web bug/štěnice

Jde o malou grafiku zadanou do spam e-mailu. Ta informuje spammera o tom, kdy je jeho rozesílaná zpráva přečtena nebo je do ní nahlédnuto.

Zloděj identity

Označení pro podvodné jednání, které zahrnuje krádež peněz nebo získání výhod. A to tak, že jedinec předstírá, že je někdo jiný.