Bezpečnosť informačných systémov

Podľa výskumov, na každého používateľa je v priemere každých päť minút pripojenia na internet spáchaný minimálne jeden útok z internetu. Bez vhodnej ochrany môže akýkoľvek útok spôsobiť značné škody.

Zabezpečenie počítačových systémov je zložitá problematika. Spoločnosti vynakladajú nemalé finančné prostriedky na previerky bezpečnosti (bezpečnostný audit) - firmám, ktoré sa na takúto úlohu špecializujú. Cieľom takejto činnosti je vypracovanie bezpečnostného projektu firmy.

Cieľom tohoto projektu je docielenie takého stavu, aby úsilie, riziko odhalenia a finančné prostriedky potrebné na narušenie bezpečnostného systému boli adekvátne v porovnaní s hodnotou, ktorú chráni bezpečnostný systém. Každý bezpečnostný projekt pozostáva z troch hlavných častí:

- prevencia - hovorí o predchádzaní bezpečnostných rizík
- detekcia - hovorí o spôsobe odhaľovania narušenej bezpečnosti
- náprava - hovorí o odstraňovaní škôd a zamedzení opakovania v prípade zistenia narušenia bezpečnosti

Spôsoby ochrany:

- Obmedzenie počtu osôb, ktoré budú mať prístup k počítaču a poučenie osôb, ktoré so systémom pracujú.
- Nastavenie zavádzania z pevného disku zabezpečenie systému BIOS heslom a zapnutie signalizácie otvorenia skrinky počítača.
- Nastavenie hesla do zavádzača operačného systému
- Nastavenie overenia totožnosti používateľa napríklad heslom alebo biometrickými údajmi
- Nastavenie politiky hesiel - akú minimálnu dĺžku musí mať heslo, z akých znakov sa musí skladať, ako často je potrebné heslo meniť
- Nastavenie uzamykania obrazovky šetričom.
- Nastavenie šifrovania údajov na disku
- Zálohovanie dát

Firewall

Firewall je sieťové zariadenie a/alebo softvér, ktorého úlohou je oddeliť siete s rôznymi prístupovými právami (typicky napr. Internet a Intranet) a kontrolovať tok dát medzi týmito sieťami.

Kontrola údajov prebieha na základe aplikovania pravidiel, ktoré určujú podmienky a akcie. Podmienky sa stanovujú pre údaje, ktoré možno získať z dátového toku (napr. zdrojová, cieľová adresu, zdrojový alebo cieľový port a rôzne iné). Úlohou firewallu je vyhodnotiť podmienky a ak je podmienka splnená, vykoná sa akcia. Dve základné akcie sú "povoliť dátový tok" a "zamietnuť dátový tok".

Spamy

V angličtine existujú dva spisovnejšie výrazy pre spam vo forme elektronickej pošty:

- Unsolicited Bulk Email (UBE) - nevyžiadaná masová pošta.
- Unsolicited Commercial Email (UCE) - nevyžiadaná komerčná pošta.
  E-mailové adresy, ktoré sú cieľom pre spamming, sa získavajú z rôznych zdrojov. Medzi tradičné patria internetové fóra a chaty. Ďalším zdrojom adries sú formulárové registrácie rôznych služieb,

kde zákazník musí poskytnúť osobné údaje vrátane e-mailovej adresy. Používajú sa aj programy na filtrovanie diskusných fór, ktoré dokážu e-mailové adresy vyfiltrovať.

Nevyžiadanú elektronickú poštu môžeme rozdeliť do troch kategórií:

- spam reklamný – patria sem všetky nevyžiadané ponuky tovarov a služieb,
- spam priateľský – pošta zasielaná s dobrým úmyslom (nadácie, žartíky), ale taktiež spadá do kategórie spamu,
- spam so zlým úmyslom – spam s cieľom poškodiť, patria sem napríklad maily s počítačovými vírusmi, maily podvodné (s cieľom získať osobné údaje),
- spam poplašný (hoax) - je poplašná správa posielaná e-mailom, ktorá na svoje šírenie využíva ľudskú dôverčivosť.

Počítačová kriminalita

Počítačová kriminalita je relatívne novým druhom závažnej trestnej činnosti. Od klasickej kriminality sa odlišuje celým radom osobitných charakteristík a zvláštností. Trestný čin môže byť spáchaný v anonymite na diaľku, sprostredkovane a to všetko v priebehu niekoľkých sekúnd bez toho, aby poškodený zaregistroval spáchanie takéhoto trestného činu a niekedy sa o tom vôbec dozvedel. Internet, anonymita a nedostatočná legislatíva, robia z počítačovej kriminality mocný nástroj na páchanie domácich a medzinárodných trestných činov veľakrát závažného charakteru s priamym dopadom na ekonomiku krajiny a jej bezpečnosť.

Od nástupu informačného veku je stále veľké množstvo právnych noriem zastaraných alebo v praxi nevymožiteľných. Vznikli nové oblasti, s ktorými žiadny právny systém pred pár rokmi nepočítal. Jedná sa najmä o zákony, súvisiace s uplatňovaním autorských práv a zákony súvisiace s pohybom informácií.

V oblasti autorského práva to bola digitalizácia, ktorá spôsobila revolúciu a umožnila lacné vytváranie kópií digitálnych dokumentov. Veľa spoločnosti, kopíruje a vymieňa digitálne dokumenty, chránené autorským právom (film, hudba, program) v dokonalej kvalite za účelom finančného profitu.

Prejavy internetovej kriminality

Šírenie pornografie. Okrem porušovania autorských práv a hackingu patrí táto oblasť medzi najčastejšie nelegálne aktivity páchané prostredníctvom počítača a internetu. Pred internetom sa táto aktivita rozvíjala a šírila formou časopisov a video nahrávok. Vďaka nadnárodnému pôsobeniu internetu sú stránky s nelegálnym obsahom viditeľné po celom svete. V SR je trestná výroba a distribúcia pornografických materiálov, v ktorých sú znázornené násilné a ľudskú dôstojnosť ponižujúce činnosti, styky s deťmi a zvieratami, prípadne iné patologické sexuálne praktiky. Rovnako je trestné sprístupňovanie pornografických materiálov maloletým.

Hacking je útok vo forme prieniku so zámerom skompromitovania počítača. Snaha vykonať veci ku ktorým používateľ nemá oprávnenie, ale **hackeri väčšinou získané dáta nezneužívajú**. Hacking so svojou bohatou históriou je najvýraznejšou oblasťou počítačovej kriminality. Nebezpečie, pokusu o prienik hackera do domáceho počítača je veľmi malé. Väčšinou sa pokúšajú preniknúť do firemných počítačov a serverov. Známe sú aj prípady tzv. násilného hackingu. Jedná sa o priamy fyzický útok na osobu s administrátorským právom v systéme, ktorú násilím alebo vyhrážkami donútia vyčleniť prístupové heslo, prípadne vykonať požadovanú operáciu pre útočníka. Podľa historických štatistík hackingu, organizáciám hrozí väčšie nebezpečenstvo od ľudí oprávnených pohybovať sa v systéme ako od anonymných hackerov.

Carding alebo zneužívanie platobných kariet. Vznik súvisí s rozvojom internetu. Platobná karta sa stala bežným platobným nástrojom. Jej zabezpečenie nie je vždy dostatočné. Krádežou karty, alebo jej čísla sa vykonáva veľa druhov trestnej činnosti. Jeden z prvých bol kreditný nákup (nákup

tovaru bez platenia v hotovosti). Páchatelia na zistenie čísla kreditnej karty používajú generátory čísiel. Osobné údaje získavajú od majiteľov účtu rôznymi spôsobmi. Medzi najčastejšie parí sociálne inžinierstvo kde sa páchateľ vydáva napr. za zamestnanca banky, v ktorej bola karta vydaná a predstiera problémy v bankovom systéme. Ďalšími spôsobmi sú, hľadanie vyhodených výpisov z bankomatov, inštalovanie kamery nad bankomat, zistenie PIN čísla karty pomocou tenkej klávesnice a následné okradnutie obete, falošné bankomaty, pri platbe cez internet z účtu zákazníka strhnúť viac, ako bola zverejnená cena za tovar.

Prienik do počítačového systému

Najobávanejším druhom počítačovej kriminality je útok na počítačový systém. Človek zaoberajúci sa touto činnosťou sa v počítačovom slangu nazýva Hacker.

V minulosti sa termín hacker spájal s vyjadrením vysokého stupňa odbornosti a šikovnosti na úrovni počítačového experta. Dnes verejnosť označuje za hackerov všetkých, ktorí neoprávnene prenikajú do cudzích počítačov a sietí.

Typológia hackerov:

- **Hacker** - počítačový expert, dobrý programátor, hľadajúci bezpečnostné diery v systémoch, za účelom zlepšenia ich bezpečnosti. O nájdených chybách a nedostatkoch informuje autorov programov, správcov systému aj verejnosť.
- **Cracker** - má technické schopnosti ako hacker, ktoré ale používa vo svoj prospech,väčšinou ilegálne. Patria sem aj takzvaní softvéroví, filmoví a hudobní piráti, lovci čísiel kreditných kariet a iní. Najčastejším motívom je pre nich uznanie v komunite a peniaze. Jedná sa o plánovanú a premyslenú činnosť.

V dôsledku vplyvu najznámejších internetových stránok sa problémy objavujú aj v oblasti médií. Tieto stránky majú rovnaký mediálny vplyv ako tlačené noviny, časopisy, alebo televízia, ale štát nie je vlastníkom internetu a tým na internete nie sú obmedzené zdroje, ktoré by bolo možné prideľovať. Je to nová situácia, keď štát bude musieť nanovo definovať problém regulácie médií.

Škodlivý softvér

Malware (skratka z anglického malicious software) alebo **malvér** je všeobecné označenie škodlivého softvéru

Klasické počítačové vírusy

Počítačový vírus je program, ktorý dokáže rozmnožovať sám seba pridávaním svojho kódu do iných programov. Pre svoje rozširovanie teda podobne ako biologický vírus potrebuje hostiteľa – iný program. Z toho vyplýva, že do počítača sa môže dostať jedine tak, že spustíme nainfikovaný program. Spolu so spustením nainfikovaného programu sa aktivuje vírus v operačnej pamäti, a potom napadne i ďalšie súbory v počítači.

Špeciálnym druhom vírusov boli v minulosti tzv. Boot vírusy, ktoré namiesto bežných programov napádali miesto na nosiči dát, z ktorého sa dá zaviesť operačný systém. Najčastejšie sa prenášal pri zabudnutí diskety v disketovej jednotke pri zapínaní počítača.

Ďalším špeciálnym druhom vírusov sú Makro vírusy, rozšírené najmä v prostredí kancelárskeho balíka MS Office (Word, Excel, PowerPoint, Outlook...), prípadne aj v iných, menej rozšírených programoch. Do softvéru bola pridaná možnosť vytvárať „makrá“ – malé programy zahrnuté v dokumentoch, ktoré mali pôvodne slúžiť na automatizáciu často vykonávaných krokov. Jazyk tvorby

makier však umožňuje zahrnúť do nich aj potenciálne nebezpečné operácie ako napr. zápis na disk. Otvorením dokumentu, ktorý obsahuje makro vírus, sa telo vírusu najčastejšie skopíruje do šablóny „normal“, z ktorej sa vytvárajú všetky nové dokumenty. Každý nový dokument, ktorý potom vytvoríte, je napadnutý makro vírusom. Našťastie novšie balíky Office na prítomnosť makra upozorňujú a ich dôveryhodnosť sa dá zabezpečiť napríklad digitálnym podpisom, pomocou ktorého sa dá zistiť, kto makro vytvoril.

Podobným druhom sú i vírusy napísané pomocou skriptovacích jazykov, ako je jazyk VBScript alebo WSH (Windows Scripting Host). VBScript bol podobne ako makrá pridaný do kancelárskeho balíka Office. Jazyk WSH bol zasa vytvorený na uľahčenie práce správcom systémov Windows.

Účinky nákazy počítača vírusom sú rozličné - od vypísania "vtipných" textov až po zničenie dát uložených na diskoch alebo ich odoslanie záškodníkovi prostredníctvom Internetu - podľa toho, čo autor vírusu v ňom implementuje.

Internetové červy

V pôvodnom význame je červ tá časť vírusu, ktorá je zodpovedná za jeho šírenie. Kým klasickým súborovým vírusom trvalo mesiace až roky, kým sa rozšírili, internetovým červom na to stačí niekoľko dní až niekoľko minút. Kým súborový vírus potrebuje našu pomoc, aby sa dostal z jedného počítača na druhý pomocou diskety, CD alebo iného nosiča, internetový červ sa dokáže rozšíriť i sám pomocou počítačovej siete. Funguje tak, že sa skúša pripojiť na každý možný počítač v počítačovej sieti a na svoj prenos využiť slabé miesto zle zabezpečeného počítača (predovšetkým vďaka chybám v operačnom systéme). Na tomto počítači sa červ aktivuje a znovu sa skúša šíriť do ďalších počítačov. Počet nakazených počítačov teda stúpa lavínovite.

Šíreniu červov sa dá zabrániť dobrým zabezpečením počítačovej siete, pretože napadnutiu vnútornej siete z internetu dnes už dokážeme zabrániť pomocou firewallu a smerovačov s prekladom adries.

Trójske kone

Najzraniteľnejšia je sieť z vnútra. Túto skutočnosť využíva ďalší typ malwaru, trójsky kôň. Trójsky kôň (pomenovanie podľa trójskeho koňa z Homérovho diela Illias) je škodlivý kód, ktorý sa vydáva za užitočný. Okrem užitočných akcií vykonáva i neželané akcie, ktoré môžu mať najrôznejšie účinky (môžu i priamo ohroziť počítač podobne ako vírusy vykonaním škodlivej akcie).

Najzákernejším druhom trójskych koňov sú však droppery (vypúšťače). Tieto v pravidelných intervaloch do systému vypúšťajú najrôznejší malware. Môžu obsahovať klasické vírusy, červy ale i spyware (špionážny program). Takto vypustený červ potom napadne sieť z vnútra, pričom je veľmi ťažké odhaliť zdroj nákazy. Odhalenie trójskeho koňa sťažuje i technika nazývaná rootkits (voľne preložené ako nástroje správcu). Touto technikou trójsky kôň dokáže poprieť svoju existenciu v systéme. Túto techniku môže trójsky kôň najľahšie využiť v prípade, že ho otvoríme s oprávneniami správcu systému.

Ďalšou nebezpečnou akciou, ktorú môžu trójske kone vykonávať, je otvorenie tzv. zadných vrátok (backdoor). Cez tieto „zadné vrátka“ sa vie útočník, tzv. hacker, dostať do systému bez toho, aby poznal prístupové meno a heslo do počítačového systému.

E-mailové červy

Rozdelenie vírusov do spomínaných kategórií (klasické, červy a trójske kone) nie je úplne jednoznačné. Typickým príkladom sú e-mailové vírusy, ktoré by sa dali zaradiť medzi červy, pretože sa šíria cez internet, ale i medzi klasické vírusy a trójske kone, pretože sa aktivujú

otvorením spustiteľného programu v prílohe e-mailu. Typickým príkladom takýchto červov sú vírusy Mellisa a ILOVEYOU, ktoré sa aktivovali otvorením prílohy e-mailu (Melisa bola vytvorená ako Makro a ILOVEYOU ako VBScript).

Zásuvné moduly ActiveX a Java applety

Trójske kone a vírusy sa objavujú nielen v e-mailoch ale celkom bezpečné nie je ani surfovanie po Internete, pretože i webové stránky (predovšetkým pochybného obsahu, ako je nelegálny softvér, pornografia a pod.) môžu obsahovať zákerné programy vo forme zásuvných modulov ActiveX a Java appletov.

ActiveX je technológia firmy Microsoft, ktorá umožňuje do prehliadača Internet Explorer pripojiť zásuvný modul. Tento prvok je vlastne len inak vytvorený spustiteľný program, ktorý dokáže ovládať ktorúkoľvek službu operačného systému. I keď firma Microsoft urobila podstatné kroky aby zabezpečila túto technológiu i tak nebezpečenstvo stále hrozí. Jedným z bezpečnostných prvkov je podobne ako u makier digitálny podpis, pomocou ktorého sa dá zistiť kto ActiveX prvok vyrobil. Pre pripojením takéhoto prvku do prehliadača vás tento vždy upozorní a je na zvážení používateľa či ActiveX prvku bude dôverovať a nainštaluje ho.

Ani používatelia iných prehliadačov ako Internet Explorer nie sú v bezpečí, pretože ich môžu ohroziť Java applety, ktoré sú nezávislé na prehliadači. Java applet je program vytvorený v jazyku Java a vložený na stránku. Rovnako ako modul ActiveX i Java applet môže využiť ktorúkoľvek službu operačného systému. Na zvýšenie bezpečnosti sa používa technológia Java Virtual Machine, ktorá pred spustením overuje nebezpečnosť spúšťaného programu. Preto je dôležité mať čo najnovšiu verziu tejto technológie (pre používateľov je nazvaná Java Runtime Environment).

Spyware (spajvér)

V poslednom čase sa za škodlivé začali považovať aj programy, ktoré sú vytvorené za účelom neetického obohatenia. Bojovať proti tomuto problému sa začalo v roku 2003, keď množstvo nevyžiadanej pošty a vyskakujúcich okien s reklamou začal byť neúnosný.

Za škodlivé programy sa považujú i programy patriace do skupiny spyware. Tieto programy zisťujú informácie o počítači a jeho používateľovi a bez súhlasu odosielajú cudzej osobe. Informácie môžu byť najrôznejšieho druhu, ako napríklad zoznam emailových adries, zoznam najčastejšie navštevovaných stránok, atď. Najnebezpečnejším druhom spywaru sú tzv. keyloggery, ktoré zaznamenávajú všetky stlačené klávesy. Prostredníctvom takýchto programov sa dajú získať prístupové heslá do počítačového systému, čísla kreditných kariet, registračné kľúče k programom a ďalšie informácie.

Adware

Do tejto skupiny patria softvery, ktoré zobrazujú reklamu. Slovo adware je skrátením slov advertising-supported software. Takéto programy sú najčastejšie súčasťou iného programu, ktorý nie je škodlivý. Je to cesta, akou sa snažia programátori získať peniaze za svoj program. Nebezpečenstvo týchto programov je v tom, že integrované reklamné systémy sú často spywarom.

Zdroj: http://maturitazinf.mrazovci.eu/pocitacova-bezpecnost