Počítačová kriminalita

Autor: Mgr. Jaromír JUŘEK

1. Počítačová kriminalita

Mezi nejvýraznější projevy počítačové kriminality patří:

Podvody, zpronevěry - především se týkají finanční sféry. Příkladem počítačové zpronevěry je zaměstnanec banky, který zná veškerá přístupová data, která využije ve svůj prospěch, aby získal finanční prostředky banky. Samozřejmě jeho velkým pomocníkem bude počítač. Do této oblasti také patří průniky do počítačových systémů a elektronického bankovnictví zvenčí. Bankovní elektronické systémy jsou ovšem natolik zabezpečené, že tyto případy nastávají málokdy.

Padělání - i tento trestní čin dokáží informační technologie usnadnit. Dříve padělání prováděli nejzručnější kreslíři a rytci, v dnešní době může padělání peněz provádět i člověk bez kreslířského talentu. S rozšířením IT je to jen otázka techniky. K tomuto trestnému činu je potřeba jen příslušného grafického software na vytvoření peněz, dále je potřeba vlastnit kvalitní tiskárnu, nejlépe laserovou nebo sublimační. Jediným problémem je tedy použití správného papíru, což v současné době není nepřekonatelné, proto tato situace vyžaduje maximální ochranu při výrobě peněz, cenin a jiných důležitých listin, jako jsou např. vysokoškolské diplomy. Obnovování ochrany musí být časté, jelikož vývoj technologií užívaných v této oblasti je neustálý.

Elektronická msta a pomluvy - tato trestná činnost je stará jako lidstvo samo. Vždy existovaly pomluvy a msty, ovšem se vznikem IT je jejich provedení značně nebezpečnější a existuje mnoho způsobů, jak to provést. Páchání této trestné činnost není ani zase tak složité, jelikož každý, kdo má počítač a přístup k Internetu, se jí může dopustit. Jedním ze způsobů provedení je šíření nepravdivých informací po Internetu, jehož cílem je pošpinění cti určité osoby nebo osob, kdy může dojít i k zásahu do osobního nebo pracovního života. Dalším způsobem, jak se někomu pomstít prostřednictvím Internetu je zanesení jeho údajů, konkrétně telefonního čísla a adresy, do erotických seznamovacích služeb. Výsledkem je pak telefonické obtěžování, v nejhorším případě i návštěvy v místě bydliště.

Hoaxes - neboli nepravdivá varování. Zatímco dříve nebyly metody šíření těchto poplašných zpráv tolik efektivní, neboť se jednalo o ústní šíření nebo šíření pomocí bulvárních médií, dnes a s pomocí Internetu je tento úkol o mnoho jednodušší. Obsahem těchto zpráv může být cokoliv, důležité je, aby svým sdělením působily na strach uživatelů, protože v tom je schovaná efektivita těchto zpráv. Takováto zpráva je schopná ovlivnit spoustu uživatelů a způsobit paniku. Jedná se například o poplašnou zprávu, že v poštovních obálkách se šíří virus, který je lidskému životu nebezpečný apod. Více informací i databázi už známých hoaxů lze nalézt na www.hoax.cz

Mezi počítačovou kriminalitu můžeme řadit i **používání nelegálního software**, či **porušování autorských práv na vytvořená díla** (dokumenty, fotografie, apod.)

Počítačové bankovní krádeže

Bankovní krádeže uskutečněné pomocí počítače jsou zatím u nás řídké, ale ve světě se začínají stále více vyskytovat. Známé jsou následující tři typy bankovních krádeží.

Phishing (někdy převáděno do češtiny jako rybaření) je podvodná technika používaná na Internetu k získávání citlivých údajů (hesla, čísla kreditních karet apod.) v elektronické komunikaci. K nalákání důvěřivé veřejnosti komunikace předstírá, že pochází z populárních sociálních sítí, aukčních webů, on-line platebních portálů nebo od IT administrátorů. Principem phishingu je typicky rozesílání e-mailových zpráv nebo instant messaging, 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. Phishing je příkladem techniky sociálního inženýrství používané k oklamání uživatelů za využití slabých míst současných bezpečnostních technologií (jejich implementací). Ochrana proti rostoucímu množství nahlášených případů phishingu zahrnuje legislativu, trénování uživatelů, veřejnou osvětu a technická opatření.

Pharming (někdy překládáno do češtiny jako farmaření) je podvodná technika používaná na Internetu k získávání citlivých údajů od obětí útoku. Principem je napadení DNS a přepsání IP adresy, což způsobí 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 (na rozdíl od příbuzné techniky phishingu).

IP spoofing označuje v informatice vytvoření IP datagramu s falešnou zdrojovou IP adresou, který je následně odeslán počítačovou sítí k cílovému počítači, před kterým má být zatajena totožnost odesílatele.

Obsah