Počítačová bezpečnost

Lukáš Rychnovský, ÚVT MU

Počítačová bezpečnost se postupem času stává problémem, který je nucen řešit stále větší počet uživatelů. Zatímco dříve se tento problém příliš neřešil nebo byl doménou odborníků, dnes se těmito problémy musí zabývat i koncový uživatel. Tento článek je úvodem k seriálu článků věnovaných počítačové bezpečnosti, který bude vycházet v tomto ročníku Zpravodaje ÚVT MU.

Když počátkem 70. let vznikal Internet (tehdejší Arpanet), byla počítačová bezpečnost pojímána jinak než dnes. V roce 1972 bylo k Arpanetu připojeno asi 50 počítačů, převážně armádních. Ke strojům měli přístup pouze prověření lidé a počítačová kriminalita neexistovala. Během několika let se však čistě armádní projekt začal rozrůstat o další, převážně akademická pracoviště, čímž se Internet dostával do rukou větší skupině uživatelů. Stále však byl vyhrazen pouze odborníkům k čistě akademickému využití (75% veškeré komunikace byly e-mailové zprávy). Nicméně problémy na sebe nenechaly dlouho čekat. 27. října 1980 vyřadil virus celý Arpanet z provozu. V roce 1981 Ian Murphy (alias Captain Zap) pronikl do počítačové sítě firmy AT&T a pozměnil čas jejich vnitřního systému. Tím se hovory s noční tarifní sazbou účtovaly jako denní a opačně. Byl prvním člověkem trestaným za počítačovou kriminalitu. 2. listopadu 1988 Robert Morris vypustil prvního internetového červa který se rychle rozšířil na více než 6.000 počítačů (z tehdejších přibližně 60.000).

To však byla počítačová kriminalita ještě v plenkách, velké ryby teprve přišly. V roce 1990 Kevin Poulsen pronikl do telefonní sítě jednoho amerického rádia a zajistil si pozici 102. volajícího, aby vyhrál Porsche 944 S2. Vladimir Levin, mladý student Petrohradské univerzity, se svými kolegy připravil americkou Citibank o 10 milionů dolarů. Nejslavnějšího hackera Kevina Mitnicka a jeho protihráče Tsutomu Shimomuru není jistě odborníkům nutné připomínat. Ovšem ani v této době se obětmi počítačové kriminality nestávali obyčejní lidé, ale spíše bohaté společnosti. Tento stav se však pozvolna mění od počátku 90. let, kdy začal Internet pronikat mezi širší vrstvy uživatelů.

V dnešní době můžeme počítačové piráty zhruba rozdělit do tří kategorií.

Script kiddies – jsou označováni převážně mladí hackeři s průměrnými znalostmi programování a počítačů. K útokům používají předpřipravené nástroje (skripty), do kterých stačí zadat adresu vzdáleného počítače. Jsou většinou schopni pronikat do systému pouze významnými a dlouho známými bezpečnostními děrami. Po proniknutí do systému většinou data vymažou a nechají vzkaz typu „Byl jsem tu. Fantomas“. Žádné techniky pro maskování útoku a zahlazení stop většinou nepoužívají a je proto hned jasné, co se děje a jak k tomu došlo.

Střední třída – hackeři s většinou výbornými programovacími zkušenostmi a znalostí operačních systémů. K útokům také používají předpřipravené nástroje, avšak podle typu operačních systémů a úrovně zabezpečení lehce použijí vhodný nástroj k dosažení svého cíle. Po proniknutí do systému se snaží nepozorovaně sledovat celou síť pro získání dalších informací a přístupu k okolním systémům. Někteří podnikají průniky pro svoje pobavení, jiní pro slávu nebo peníze. Stačí například uživatelská data zašifrovat nebo přesunout jinam a za navrácení (rozšifrování) požadovat malou sumu (v řádu stovek dolarů).

Top class – elitní hackeři s excelentními znalostmi. Předpřipravené nástroje vytvářejí a prodávají. Do systému pronikají pomocí komplexních útoků a nedávno objevenými bezpečnostními děrami. Po průniku používají drahé maskovací nástroje (v řádu tisíců dolarů) a v systému mohou nepozorovaně působit i několik let. Jejich snahou je ovládnutí celého systému k vlastnímu prospěchu. Jejich útok je většinou organizovaný a dotyčnou společnost stojí velké množství prostředků, případně je spojený s únikem osobních dat, čísel platebních karet nebo zdrojových kódů vyvíjených programů.

Obyčejný počítačový uživatel se naštěstí s třetím typem hackerů nepotká. Potká se však s prvními

dvěma typy a je dobré vědět, jak se proti jejich útokům bránit.

Před útokem typu „script kiddie“ váš počítač ochrání dodržování základních úkonů, jako je pravidelná aktualizace a správně nastavený firewall (více podrobností najdete v článku [1]).

Útoky druhého typu hackerů jsou daleko promyšlenější a rafinovanější. Nejedná se vždy o útok na váš operační systém, ale útočník se obecně snaží získat kontrolu nad vaším e-mailovým nebo bankovním účtem, získat vaše osobní data, případně další zpeněžitelné informace. Může se o to pokoušet například některým z následujících způsobů nebo jejich kombinací.

Sociotechnika – termín zavedený Kevinem Mitnickem označuje činnost přesvědčování lidí, aby dělali věci, které se pro neznámé lidi obvykle nedělají. Může to být například požadavek na číslo mobilního telefonu kolegy, spuštění cizího programu ve vašem počítači nebo třeba vypnutí firewallu na malou chvíli z důvodu testování. Poskytnutí mobilního čísla se může zdát jako drobnost, ale když pak kolegovi někdo zavolá a řekne, že ztratil heslo a od vás má číslo, že mu máte poskytnout nějaké informace ke kterým se bez hesla nedostane, míra důvěryhodnosti jeho tvrzení značně stoupne. Spouštění cizích programů (například humorných animací nebo šetřičů obrazovky) ve vašem počítači je jedna z nejnebezpečnějších věcí pro váš systém a tímto způsobem obvykle dochází k průnikům. Spuštěním útočníkova programu ve vašem počítači poskytnete hackerovi například přístup k souborům na vašem disku (i k bankovnímu certifikátu na disketě). Stejně tak může útočník odchytávat stisknuté klávesy na vašem počítači a získat hesla pro přístup k citlivým informacím.

Podvržení identity – pro hackera není problém zfalšovat e-mailovou zprávu tak, aby vypadala, že vám ji poslal například váš šéf nebo kamarád. Dokonce lze zprávu nastavit tak, aby odpověď šla zpět do jeho rukou.

Phishing – technika velice podobná předchozímu. Je doplněna zpravidla o žádost o navštívení nějaké webové stránky a dalších úkonů. Běžné jsou například podvržené zprávy od provozovatele vašeho emailového účtu, že je nějaký problém a máte se co nejdříve přihlásit pomocí vašeho hesla na uvedené adrese. Tato adresa však patří útočníkovi a lehce odchytí vaše heslo.

Podobně se může vyskytnout e-mail od provozovatele vašeho bankovního účtu s popisem problému a podobnou žádostí. Aby však útočník vyvrátil jakékoliv podezření, odkazovaná stránka je přesná kopie bankovního systému. Dokonce po zadání hesla je zobrazena stránka s vaším účtem. Jak? Na pozadí se vaše heslo použije pro skutečné přihlášení k bankovnímu systému a informace se přenesou na stránky útočníka.

Hromadné použití phishingu (z původního slova fishing – rybaření) je pro útočníka velice jednoduché. Stačí rozeslat dostatek e-mailů a jen čekat. Další podrobnosti lze najít například na `www.antiphishing.org`.

Odcizení identity (identity theft) – technika oblíbená především v USA. Využívá toho, že při prokazování identity po Internetu je vyžadováno ověření zpravidla jedním způsobem. Stačí tedy získat například číslo sociálního pojištění (v USA něco jako rodné číslo u nás, což není veřejný údaj, ale také není tajný) nebo číslo kreditní karty.

Všechny popsané metody se stávají obyčejným uživatelům, jsou velmi nebezpečné a v poslední době i časté. I v ČR bylo zaznamenáno několik případů odčerpání nemalých částek z účtů klientů bank. Bohužel v současné době banky u nás přesouvají zodpovědnost za úniky informací a finanční ztráty na koncové uživatele bez dostatečné informační kampaně. Zavedení doplňkových bezpečnostních prvků je pomalé nebo nedostatečné.

Ovšem vaše bankovní konto není jediným cílem hackerů. Lákavé jsou jakékoliv zpeněžitelné či jinak využitelné informace. Od lékařských záznamů přes osobní nebo ekonomická data až po například právní informace a různé smlouvy. Časté také bývá zneužití napadených počítačů pro rozesílání spamu či šíření ilegálních materiálů po Internetu. V tomto případě je samozřejmě právně postižitelná osoba zodpovědná za napadený počítač.

Z předchozího textu by se mohlo zdát, že obětmi počítačové kriminality jsou spíše velké firmy, než akademické obce. Opak je spíše pravdou. Akademické sítě jsou pro „škodnou“ velmi atraktivní, a to z řady důvodů. Zejména však kvůli svému výkonu, větší otevřenosti (plynoucí z přirozené povahy akademického prostředí) i zpravidla velkému množství počítačů, které je objektivně velmi obtížné mít v každém okamžiku na 100 % bezpečnostně zajištěné. Pokud zůstaneme jen na půdě MU, tak během posledního roku bylo odhaleno několik závažných hackerských průniků, přičemž poslední z nich kompletně ochromily dění na dvou fakultách a vyžádaly si kompletní reinstalaci všech stanic a serverů daných fakult (kvůli závažné hrozbě zneužití citlivých osobních i služebních dat). V některých případech se jednalo i o dlouhodobější průniky v délce trvání i několik let. Odhalení takovýchto průniků je velice obtížné a vyžaduje znalosti, zkušenosti a zdroje mnohdy nad rámec jednotlivých fakult. V takovych případech se velmi osvědčuje spolupráce na mezifakultní úrovni. V daných dvou případech například došlo k odhalení a eliminování těchto průniků právě díky polupráci specialistů z ÚVT MU.

Jak se bránit? Důležitá v tomto případě je především osvěta (na její podporu byla i na stránkách Zpravodaje publikována řada článků – viz např. [2]). Informovanost uživatelů a zdravý rozum pomohou odhalit mnoho problémů. Počítačovou bezpečnost se dnes nevyplatí nikomu podceňovat. Konzultacemi s odborníky a dodržováním jejich rad si lze ušetřit velké množství problémů.

Literatura

[1] L. Rychnovský, R. Peša. Deset rad pro zabezpečení MS Windows 2000/XP. Zpravodaj ÚVT MU. ISSN 1212-0901, 2004, roč.15, č.2, s.5-8

[2] Série článků o počítačové bezpečnosti: Zpravodaj ÚVT MU. ISSN 1212-0901, roč.12, č.4, duben 2002 □