NEBEZPEČÍ ZVANÉ HACKING

Autor článku: **Karel Miko – DCIT, s.r.o.**
http://www.dcit.cz

Článek zveřejněn v časopise **Business World** 8/2003
http://www.businessworld.cz

Tento článek si klade za cíl přiblížit svět počítačového podsvětí, který bývá často démonizován a je obvykle popisován s nádechem senzačnosti a navíc způsobem, který ne vždy odráží skutečnou realitu.

Osobně nepatřím k žádným ilegálním živlům, nevedu dvojí život hackera pod skrytou identitou, spíš bych se chtěl podělit se o informace, osobní názory a několikaleté zkušenosti, které z této oblasti mám jako bezpečnostní specialista.

Co vůbec chápeme pod pojmem Hacking – obecně se jedná o aktivity související s počítačovou kriminalitou, jejichž míra nebezpečnosti se může dramaticky lišit případ od případu. V širším slova smyslu hacking zahrnuje záležitosti sahající od zneužívání či napadání telefonních systémů – obvykle s cílem bezplatného volání apod. (tzv. pheaking), dále přes shromažďování a šíření nelegálního software (tzv. warez), překonávání různých ochran komerčních SW produktů, DVD disků ap. (tzv. crackování) až po „tradiční“ průniky do počítačových systémů nebo sítí. V tomto článku budu pojem hacking používat právě pro ono „tradiční“ napadání a pokusy o neautorizovaný přístup k počítačovým systémům.

Rád bych hned v úvodu rád zdůraznil, že Hacking je ilegální a i české zákony již řadu let obsahují patřičné instrumenty pro postihování těchto aktivit. Ovšem jak už to v životě chodí i nezákonné věci se prostě dějí a nezbývá než se s tím vyrovnat.

Historické ohlédnutí

Hacking je záležitost stará téměř jako samotné počítače, začátek lze vysledovat zhruba v šedesátých letech, kdy za hackery byli považováni extrémně schopní programátoři, kteří na tehdejších mainframech dokázali věci, které byly považovány za téměř nemožné (nikoli však ilegální).

Sedmdesátá léta byla především ve znamení zneužívání telefonních sítí, zejména s cílem bezplatného telefonování. V průběhu této dekády se začaly objevovat první organizované skupiny hackerů.

V osmdesátých letech se začal rozvíjet ARPANET, jenž se postupně přeměnil v dnešní Internet. Význačným momentem z hlediska současných hrozeb byl rok 88, kdy Robert Moris vyrobil a vypustil The Internet Worm, jednalo se sebereplikujícího se červa napadajícího UNIXové systémy a automaticky se šířícího – vzpomeneme-li červa SQL-Slammer z počátku roku 2003 musíme bohužel konstatovat, že z některých věcí jsme se dodnes nepoučili.

V devadesátých letech získal Hacking podobu, ve které ho známe dnes tj. pronikání do systémů zneužitím chyb a slabin v programech či operačních systémech, typicky prostřednictvím počítačových sítí. Přišli rovněž nové viry, červi, DoS útoky apod.
Z mediálně nejznámějších Hackerů tohoto období zmíním legendu Kevina Mitnicka odsouzeného v roce 95 za zcizení cca 20 tisíc čísel kreditních karet.

Z prostředí nám bližšího bych uvedl skupinu CzERT působící v letech 96-98 v Čechách a na Slovensku, která je dodnes zastřena nejasnostmi a pokud vím nebyla a asi nikdy nebude odhalena.

Když se řekne Hacker

Nebudu zde plýtvat místem a opisovat psychologický a mentální profil hackera jako zneuznaného génia, samotáře trávícího 24 hodin denně u počítače a zcela neschopného vést jakýkoli společenský život či trpícího frustracemi z nedostatku sexu. Myslím, že toto je pouze jakýsi mediální obraz hackera, který se snaží vytvořit psychologové na základě svých dedukcí, případně pokus o zobecnění závěrů učiněných na základě několika jedinců, které se podařilo odhalit.

Osobně si troufnu tvrdit, že hackeři nejsou identifikovatelní podle vzhledu či jiných vnějších projevů. Tito lidé pracují často u velkých zavedených IT či Telco firem (nikoli nutně jako odborníci na bezpečnost), mají partnera/ku, vedou běžný společenský život jako kdokoli jiný. Svoji druhou identitu hackera navenek pochopitelně neinzerují – na první pohled řadu z nich rozhodně nezařadíte do kategorie hacker.

Obecně je hacker člověk spíše mladý, vysoce schopný a znalý, dámy prominou, ale obvykle muž, který může těmto aktivitám věnovat dostatek svého času.

Kromě uvedených schopností a času hacker potřebuje rovněž aktuální znalosti a patřičné nástroje – obojí lze do jisté míry získat z dostupných internetových zdrojů, pokud je navíc hacker členem nějaké uzavřené skupiny, sdílí s ostatními nejrůznější „exkluzivní“ informace či nástroje, které běžně na Internetu nenajdete.

Motivace hackera může být různá – od „zábavy“ na různé etické úrovni, přes zviditelnění se v rámci komunity, prezentaci osobních postojů či protestů („hacktivism“) až po přímý osobní prospěch (hackera či třetí osoby).

Zcela jistě by se našly i jiné motivy, každopádně já osobně nevěřím občas prezentovaným ušlechtilým cílům hackerů tvrdících, že lidem svými činy v podstatě pomáhají, že chtějí jen upozornit na problémy, a snažících se jako šlechetní hackeři odlišit od škodlivých crackerů. Srovnal bych to s případem, kdy ekologové zničí drobnému českému zemědělci lán geneticky modifikované kukuřice a vyvěsí na místě transparent „zachraňte deštné pralesy“.

Ovšem ne každý kdo si říká hacker je opravdový hacker. Laciného efektu lze snadno dosáhnout tím, že si stáhnete již hotový program pro napadení systému (tzv. exploit), který napsal někdo jiný a prostě ho jen spustíte na oběť svého útoku, asi není třeba dlouho diskutovat, že k tomuto příliš velké znalosti nepotřebujete. Tito rádoby hackeři, kteří nejsou sami příliš odborně zdatní, ale umí šikovně využít práce jiných, bývají nazývání „script kiddies“.

Bílé vs. černé klobouky

V současné době se ustálilo nepsané rozdělení hackerské scény na Bílé a Černé klobouky, sami jistě tušíte, kteří jsou „ti dobří“ a kteří „ti zlí“.

- White Hats – někdy též etičtí hackeři, nezávislí experti a konzultanti, uznávané individuality, komerční security laboratoře či jiní bezpečnostní profesionálové. Slabiny, které tito lidé odhalí jsou obvykle zveřejňovány, na téma bezpečnost často publikují, řada z nich se bezpečností živí.
- Black Hats – uzavřená společnost hackerů (nikoli jedna celosvětová, ale řada drobných skupin), jejichž cílem je nalezení bezpečnostních slabin a jejich vyžití pro „vlastní potřebu“. Řadu bezpečnostních slabin odhalí dříve než bílé klobouky, téměř nikdy je nezveřejňují. Právě zde lze spatřovat počítačový underground s opravdovými e-zločinci.

Jen pro doplnění bych rád uvedl, že i když sledujete na Internetu různé hackerské zdroje o bezpečnosti (jako např. oblíbená konference Bugtraq), téměř s jistotou si troufnu tvrdit, že se stále pohybujete ve sféře bílých, neboť do sféry černých se pouhým klikáním po Internetu nedostanete.

Metody průniků

Prakticky každý útok hackera zneužívá nějakou slabinu, kterou může být:

- chyba výrobce (přímo v aplikaci, operačním systému)
- chyba dodavatele nebo administrátora (špatné nastavení)
- chyba uživatele – tato „slabina“ se narozdíl od předchozích dvou velmi obtížně řeší

Nechci zde podrobně popisovat technické detaily konkrétních typů útoků, uvedu pouze základní informace o některých z nich:

- Buffer Overflow (BOF) – poměrně velký okruh slabin, jejichž příčinou je programátorská chyba díky níž dochází za jistých okolností k nežádoucímu přepsání paměti, čehož lze zneužít pro spuštění vlastního kódu.
- Zneužití chyb ve WWW aplikacích – nejčastěji SQL injection či podobné variace, kdy opět díky chybě programátora lze prostřednictvím manipulace s dynamickými parametry WWW stránek (příp. cookies) proniknout na sever či neoprávněně získat data.
- Síťové techniky – Sniffing (odposlech síťové komunikace), Spoofing (předstírání cizí identity, obvykle IP adresy).
- Denial of Service (DoS) útoky – Flooding (zahlcení linky, zahlcení systému požadavky, zahlcení e-mailovými zprávami, …), distribuované DoS (při současných technologiích prakticky není obrany).
- Útoky na heslo – hádání/lámání hesel. Bohužel na rozdíl od výkonu počítačů schopnosti lidí pamatovat si delší hesla stagnuje, proto tato velmi stará metoda je stále velmi účinná.

Osobně považuji za největší slabinu v drtivé většině případů lidský faktor (tj. vlastní zaměstnance), z konvenčních hrozeb vidím jako nejzákeřnější chyby ve WWW aplikacích či jiných systémech vyvíjených na zakázku – jedná se o jedinečné chyby programátora (vlastní zaměstnanec, či pracovník dodavatele), které žádný běžně dostupný scanner obsahující databázi jen těch nejrozšířenějších chyb neodhalí a často je vytvořena falešná iluze bezpečí.

Bezpečnost je především business

Nesouhlasím s často používaným tvrzením, že bezpečnost je investice, která se vrátí. Je to prostě náklad, který je potřeba účelně vynaložit. Za trefný považuji příměr k air-bagům – taky si za ně řada lidí k ceně auta ráda připlatí, přičemž minimum z nich zažilo air-bag v akci.

Nutno ovšem podotknout, že i když do bezpečnosti nainvestujete, nemáte vyhráno, neboť bezpečnost není jednorázová záležitost, je to nekonečný cyklus. Navíc řada problémů není řešitelná technicky, ale záleží na lidech, vnitřních procesech, firemní kultuře apod.

V souvislosti s náklady na bezpečnost bych rád uvedl, že úroveň bezpečnosti rozhodně není přímo úměrná ceně technologie. Doporučuji volit především zavedené technologie, které mají nějakou historii a jsou usazené, takové najdete jak mezi komerčními, tak free/opensource produkty. Ve výsledku bývá podle mé zkušenosti nakonec rozhodující kvalita konkrétních lidí (interních či externích), kteří technologii v daném prostředí nasazují, i špičkovou technologii lze provozovat nebezpečně.

Bohužel ani u renomovaných dodavatelů není zabezpečení dodávaných řešení samozřejmostí, často garantují funkčnost jen na „své“ konfiguraci a instalací nového patche (byť kritického z hlediska bezpečnosti) porušíte garanční podmínky a ztrácíte nárok na záruční servis.

Několik poznatků z praxe

Ač s tím nemusíte souhlasit, hacking se týká opravdu každého, neboť globalizace není v této oblasti jen prázdné heslo, ale realita. Rychlost a způsob šíření některých virů a červů je asi jednoznačným důkazem, že prakticky kdokoli v dnešním propojeném světě může být obětí nejnovějšího útoku. Z vlastní zkušenosti můžu potvrdit, že pokud připojíte na Internet nové zařízení nebude trvat více než několik hodin než ho některý z automatických prohledávačů objeví (co s ním udělá nechávám stranou).

Možná mi budete oponovat, že jste pro hackera nezajímavý objekt. Řada útoků ale nemá za cíl se prolomit do jednoho konkrétního systému, ale plošně prohledává kusy Internetu a na vybrané oběti opět plošně aplikuje připravený útok, a to bez ohledu na to jedná-li se o banku či úschovnu zavazadel.

Dále je nutno si uvědomit, že bezpečnostní slabiny nevznikají, existují v systémech již léta jen se o nich neví, v horším případě je znají jen někteří (Black Hats). Taky nepodléhejte iluzi, že nabourat server znamená změnit WWW stránky, Vaší opravdovou hrozbou jsou průniky bez viditelných projevů – často je Váš systém napaden jen proto, aby mohl být použit jako přestupní stanice pro další útoky.

Pro řadu lidí to bývá překvapení, ale nabourat se do systému a plně ho ovládnout lze přes jeden jediný otevřený port, byť je to např. šifrovaný přístup k WWW (443/tcp) – zde Vám ani sebelepší firewall nepomůže, neboť komunikace s tímto portem prostě musí být povolena.

Útok však nemusí přijít z vnějšku, prakticky v každém prostředí, které znám a nějakým způsobem jsem se účastnil hodnocení jeho bezpečnosti byly identifikovány vážné slabiny umožňující úspěšný průnik do interních systémů zaměstnancem. Dá se do jisté míry spoléhat na to, že toho vaši uživatelé nejsou schopni, nicméně je třeba si uvědomit, že v běžně používaných systémech může uživatel jediným neuváženým kliknutím poskytnout veškerá svá práva nějakému spustitelnému kódu (podstrčenému s Internetu, z elektronické pošty, reklamního CD apod.), který už bude vědět kudy na to.

Jak se bránit

V oblasti ochrany před útoky hackerů se nabízí tradiční technické prostředky jakými jsou firewally, které jsou v současnosti prakticky téměř nutnost. Dále například Intrusion Detection Systémy (IDS), které jsou především monitorovacím nástrojem umožňující včasnou identifikaci podezřelých aktivit. IDS sice často nabízí i reakční mechanizmy, jejich praktické využití a efektivita je však často přeceňována.

Zdánlivě nesouvisející oblastí obrany proti útokům jsou produkty z oblasti Content security (nejen antiviry). Je totiž podstatně jednodušší uživateli nějakým způsobem podstrčit škodlivý program (virus, červ, trojský kůň) a např. odposlechnout jeho heslo přímo z klávesnice než složitě luštit zašifrovanou komunikaci.

Existuje taky řada kontrolních nástrojů jako například bezpečnostní audity na různé úrovni detailu. Nejrozšířenější slabiny můžete poměrně jednoduše odhalit vlastními silami s využitím scannerů zranitelností (komerční ISS, Netrecon, Retina; free/opensource Nessus). Případně lze využít služeb externích firem a na důkladné prověření svého systému si můžete „etického hackera“ najmout (tzv. penetrační test).

Z hlediska budoucnosti bohužel nelze očekávat obrat k lepšímu, statistiky vývoje počtu bezpečnostních incidentů nemilosrdně pokračují ve strmém růstu.