Ze zkušeností penetračního testera

část I

Jednoduchá řešení ekosystému „počítačové kriminality“ patrně neexistují a otázka vyhodnocení dosaženého pokroku je těžko uchopitelná i při pokusech o rigorózní přístup. Jak se situace jeví z pohledu několikaleté praxe penetračního testera, jehož obvyklými klienty jsou velké instituce (podniky) z česko-slovenských luhů a hájů?

Při pokusu o hledání odpovědi na otázku, zda je dosažený pokrok v zabezpečení počítačových systémů a používaných technologií dostatečný, lze narazit na množství materiálů propagačně-marketingového rázu, které popisují nové technologie z hlediska řešení problémů těch předchozích. Zde lze pozorovat (jistý) pozitivní vývoj, v praxi však zjišťujeme, že nové technologie často přináší i nové problémy (příp. neřeší ty staré) a že je nelze posuzovat zcela v izolaci, neboť se mění i svět, s kterým tyto technologie interagují.

Slabiny dříve zanedbatelné mohou nabývat na závažnosti díky změně chování uživatelů (nebo útočníků), jejich množství a obecně způsobu, kterým je daná technologie využívána a co všechno je na ní závislé. Často se rovněž setkáváme s případy, kdy technologie nějakou možnost ochrany nabízí, v praxi však není využívána, např. z neznalosti nebo kvůli pohodlí.

Počítání chyb, patchů nebo reakčních dob

Další mediálně poměrně oblíbenou metodou je „počítaní chyb“ nebo oprav (záplat, patchů) za různá časová období, případně měření průměrných reakčních dob jednotlivých výrobců. Tímto způsobem jsou porovnávány konkurenční produkty (typicky operační systémy nebo webové prohlížeče) či je demonstrován jakýsi trend, zda v daných časových obdobích dochází ke zlepšení nebo zhoršení. Obvykle jsou pro tyto účely používány veřejně dostupné databáze slabin (CVE, OSVDB) nebo veřejně dostupné bezpečnostní bulletiny relevantních výrobců.

Netvrdím, že jsou tyto statistiky zcela nezajímavé a že z nich nelze vyvodit žádné praktické poznatky, naši obecnější otázku však dostatečným způsobem neřeší. Pomineme-li již samotnou problematičnost srovnávání jednotlivých chyb, výsledné statistiky bývají zkresleny tím, že na produkty s vysokou penetrací trhu je kladena větší pozornost (ze strany útočníků) a také výrazně větší nároky než např. na produkt, který je z hlediska trhu prakticky irelevantní (a počtem objevených chyb se tedy může jevit jako značně kvalitnější).

Statistiky rovněž jen těžko zohledňují, jak náročné je případné praktické zneužití konkrétních slabin. Bezpečnostní aktualizace často tiše opravují i slabiny, které nejsou veřejně známy (to ale nemusí vůbec znamenat, že nejsou reálně zneužívány) a v bezpečnostních bulletinech nejsou vůbec zmíněny (open source software je z toho hlediska „znevýhodněn“). Měření reakčních dob mezi zveřejněním slabin zase obvykle vůbec nezohledňuje dobu mezi tím, kdy je vlastně samotná slabina (chyba) do kódu zanesena, a tím, kdy je opravena – tedy jakou dobu byl uživatel vystaven riziku. Z hlediska těchto statistik navíc prakticky nikdy není zohledněna skutečnost, jak velké procento uživatelů a s jakým zpožděním bezpečnostní aktualizace konkrétních produktů skutečně aplikuje.

A nakonec asi ty nejvážnější výhrady obecnějšího charakteru – velké množství skutečně závažných bezpečnostních problémů vlastně ani nesouvisí s konkrétními (opravitelnými) chybami v konkrétních produktech, ale jsou jakýmsi způsobem generické (např. slabá hesla) nebo souvisejí s nevhodným způsobem používání či zcela nevyhovujícími konfiguracemi (ať už výchozími či záměrně oslabenými). Podobným způsobem není nijak zachycena ani bezpečnost speciálních (na míru šitých) aplikací, jakou jsou např. internetová bankovnictví či jiné webové aplikace.

Lze bezpečnost měřit lépe?

Pokud bychom chtěli na otázku skutečných trendů v praktické bezpečnosti odpovědět rigorózně, museli bychom nejprve přesně definovat, co si vlastně pod samotným pojmem „bezpečnost“ vůbec představujeme, což může být z formálního hlediska značně komplikované. Dále bychom museli vybudovat nějakou dostatečně vypovídající metriku, kterou bychom byli schopni úroveň bezpečnosti měřit, a nakonec bychom pravděpodobně velmi tvrdě narazili při snaze získat dostatečné množství kvalitních dat, která by umožnila dobrat se smysluplného a (statisticky) vypovídajícího výsledku.

Metoda penetračních testů

Pokusím se však subjektivně zachytit trendy, které během několikaleté praxe v oboru bezpečnostních konzultací v našem týmu penetračních testerů pozorujeme (penetrační testy viz Box 1). Bezpečnost můžeme posuzovat z hlediska toho, jak velký odpor při penetračních testech testované systémy kladou a jakých výsledků se při těchto útocích daří dosahovat.

Netvrdím, že je tato metodika dokonalá, protože penetrační testy neodpovídají přesně tomu, jakým způsobem jsou vedeny skutečné útoky reálnými útočníky. Není ani vyčerpávající, neboť penetrační testy nepokrývají veškeré oblasti bezpečnostní problematiky. Navíc se omezíme hlavně na oblast větších (převážně podnikových) sítí, což samozřejmě v některých ohledech nemusí souviset např. s problémy běžných koncových uživatelů a jimi používaných technologií (např. mobilních telefonů). Přesto si troufnu tvrdit, že výsledky penetračních testů mohou o celkové úrovni bezpečnosti a trendech vypovídat více než výše diskutované metody.

Co je to penetrační test? BOX 1

Při penetračním testu externí konzultant (na základě objednávky klienta) simuluje činnost potenciálního útočníka. Cílem je v daném časovém intervalu identifikovat bezpečnostní slabiny a demonstrovat jejich zneužití (aniž by se však způsobila reálná škoda). Výstupem testu je zpráva, ve které jsou identifikované slabiny detailně popsány včetně postupu vlastního průniku.

Při klasickém penetračním testu je snahou dosáhnout co nejhlubšího průniku a získat co nejvyšší privilegia. Pro klienta, který za test platí, však obvykle mají největší hodnotu informace o nalezených slabinách, samotná demonstrace průniku mu příliš velkou hodnotu nepřináší. Průniky však mohou často doložit skutečnou závažnost identifikovaných problémů, příp. odhalit fundamentální problémy, které by při povrchní analýze zůstaly skryty. Mohou rovněž ospravedlnit nutnost investic do zabezpečení či celkovou změnu přístupu před vedením společnosti.

V praxi tudíž bývá při penetračních testech (vzhledem k obvyklým časovým omezením) kladen větší důraz na množství nalezených slabin a pokrytí co největšího množství možných testovaných oblastí na úkor prostoru pro samotné zneužití nalezených slabin a rozsahu (hloubky) následného průniku (jakéhosi bonusu). Tím se oblast penetračního testování v praxi výrazně přibližuje spíše oblasti „vulnerability assessmentu“.

Testy internetových služeb – externí penetrační testy

Při tzv. externím penetračním testu se snažíme o simulaci útoku na klienta prostřednictvím slabin na zařízeních a službách, které jsou veřejně dostupné z internetu. Potenciálním útočníkem je tudíž kdokoli s přístupem k internetu. Tento test je obvykle prováděn tzv. bez znalosti, neboli útočník před vlastním testem nemá žádné interní informace o testované síti.

Z hlediska těchto testů lze pozorovat dva velmi silné trendy. Jedním je ten, že v průběhu posledních deseti let se výrazně snížila hustota z internetu dostupných služeb (otevřených portů) v testovaných sítích. V podnikových sítích je již obvykle bráno jako zcela samozřejmé, že každou jednotlivou, do internetu vystavenou službu je třeba podrobit zásadní analýze, zda je opravdu nezbytně nutné, aby byla veřejně dostupná. Je poznat i úbytek různých nestandardních/netypických protokolů a služeb typu vzdálené správy. Zároveň s touto minimalizací je znatelná i pozornost věnovaná vlastnímu zabezpečení jednotlivých služeb. Druhým poměrně zajímavým trendem je silný pokles poptávky po tomto typu testů. Zatímco před 5–10 lety patřily externí penetrační testy k těm nejčastějším, nyní je to spíše naopak. (Oproti tomu znatelně stoupla poptávka po penetračních testech webových aplikací a interních testech vnitropodnikových sítí.)

Pomineme-li webové aplikace (viz dále), situace se na první pohled jeví jako značně pozitivní.

Testy webových aplikací

Při těchto testech je pozornost věnována jen vybraným webovým aplikacím a jejich bezprostřednímu okolí. Zde máme na mysli především specifické aplikace šité na míru konkrétním provozovatelům. Testy jsou prováděny jak ve variantách „bez znalosti“ (tedy z pohledu anonymního uživatele), tak i v obvyklejších variantách „se znalostí“, při kterých má útočník k dispozici uživatelský účet.

Situaci a trendy lze pravděpodobně shrnout velice snadno. Z technologického hlediska sice dochází k jistým zlepšením, a to zejména z hlediska vestavěných podpor pro bezpečnostní protiopatření na úrovni vývojových a runtime prostředků, v praxi však bohužel v hotových aplikacích nacházíme stále ty samé kategorie problémů. Moderní webové aplikace jsou totiž řádově složitější a rozsáhlejší, než byly před 5–10 lety. Nalézt a zneužít v nich ekvivalentní slabiny sice bývá pracnější, výsledky

však zůstávají stejné nebo i horší, neboť webové aplikace nabývají na důležitosti.

Rozeberme si to na příkladu jedné z typických slabin. Před několika lety (pokud aplikace pracovala s databází) bylo obvykle možné nalézt SQL injection slabiny prakticky ve všech zpracovávaných vstupech a jejich zneužití bylo často velmi přímočaré. V modernějších aplikacích nebývá koncentrace SQL injection tak vysoká a nalezení nedostatečně ošetřeného vstupu bývá pracnější. Navíc již není obvyklé, že by aplikace prozrazovala detailní chybové výstupy, takže vlastní zneužití může být značně složitější.

Ofensivní technologie a kolektivní know-how však v případě SQL injection v průběhu posledních přibližně pěti let pokročily natolik, že ve výsledku se situace nijak zásadně nezměnila. Neomezený přístup k databázi lze dnes téměř rutinně realizovat i pomocí tzv. blind SQL injection, např. za použití postranních časových kanálů. Není zcela neobvyklé, že se tímto způsobem podaří eskalovat privilegia a získat přístup k operačnímu systému, na kterém je databáze provozována.

Chyby typu SQL injection navíc často odhalí i typické fundamentální slabiny již v samotných architekturách webových aplikací, ve kterých je přístup k databázi řešen pomocí „všemocných databázových uživatelů“, jejichž privilegia obvykle zcela zásadně převyšují skutečné potřeby dané aplikace.

Podobná situace je i v případě ostatních nejběžnějších slabin webových aplikací, jako jsou např. cross-site scripting, slabiny v implementacích autentizačních metod nebo metodách řízení uživatelských seancí. Stejně tak běžné jsou i problémy s řízením přístupu na úrovni aplikační logiky, kdy vhodnou manipulací se vstupními parametry lze často obejít zamýšlenou aplikační logiku a dosáhnout přístupu k datům jiného uživatele nebo k „nedostupné“ funkci. Často se totiž spoléhá pouze na prezentační vrstvu – vychází se z naivního předpokladu, že pokud se uživatel k daným datům nebo funkci ve standardním prohlížeči „nemůže doklikat“ (položka není v menu, vstupní pole je „nezměnitelné“, tlačítko je „vypnuté“ atp.), tak tuto funkci nebude schopen využít.

V oblasti webových aplikací dle našich zkušeností k obecnému zlepšení nedochází, troufneme se říct, že je to spíše naopak. Webové aplikace dnes programuje kdekdo, aniž by měl byť jen základní povědomí o souvisejících bezpečnostních problémech. S podobným přístupem se bohužel setkáváme i u některých zavedených softwarových dodavatelů, kteří si aplikace vyvíjené na míru zákazníkům někdy nechávají programovat u zcela nekompetentních subdodavatelů, zřejmě kvůli nízkým cenám. Dle našich pozorování dochází ke zlepšení prakticky jen u těch dodavatelů, kteří si aplikace nechávají pravidelně testovat a z výsledků předchozích testů se poučují.

Testy bezdrátových sítí

Při penetračních testech bezdrátových sítí na bázi protokolů 802.11 (běžně nazývaných WiFi) se obvykle snažíme zmapovat dostupnost bezdrátových sítí z vnějšího prostředí, zejména mimo oblast perimetrické ochrany společnosti, např. z veřejného parkoviště před budovou, parku, přilehlých ulic atp. Dále bývá prováděn odposlech a analýza síťového provozu. Případné další útoky lze vést na dostupnost sítě (denial of service), připojení do sítě (prolomení ochran na přístupových bodech), příp. vůči k síti připojeným klientským stanicím.

Penetrační testy bezdrátových sítí neděláme příliš často (maximálně jednotky případů ročně), přesto je patrný pozitivní trend. Se slabými šifrovacími metodami založenými na WEP nebo TKIP se v podnikových sítích na rozdíl od minulosti dnes téměř vůbec nesetkáváme. Pokud ano, jedná se většinou o nějaké „pokročilejší“ implementace rozšířené o časté automatizované výměny klíčů s detekcí běžných typů útoků včetně aktivních protiopatření. I tyto technologie jsou však na ústupu.

V podnikových sítích se prakticky vůbec nesetkáváme s použitím tzv. pre-shared klíčů, které by umožňovaly zaútočit na přístupové údaje pomocí slovníkových metod nebo hrubé síly. Z hlediska přímých útoků jsou tedy současné bezdrátové sítě velmi odolné.

Z hlediska zabezpečení klientských stanic připojených do bezdrátových sítí se situace nijak zásadně nemění. Je pravda, že nejnovější operační systémy (resp. software, který bezdrátová spojení řídí na klientských stranách) již tak často do éteru nešíří jména všech svých přednastavených sítí a ochota „naivně“ se připojit do falešné sítě pouze na základě shodného SSID (jméno sítě) je na ústupu.

Na druhou stranu jsou útoky založené na pasivním odposlechu jména sítě (do které je nebo naposledy byl klient připojen) a vytvoření falešného přístupového bodu se stejným jménem stále poměrně účinné. V typické konfiguraci větší podnikové sítě se klient k falešné síti obvykle ochotně připojí, obzvláště pokud má silnější signál. Tímto způsobem sice není přímo získán přístup k původní bezdrátové síti, umožňuje to však provést přímý útok na klientský počítač (osobní firewall bývá často v případě připojení do podnikové sítě vypnutý nebo velmi benevolentně nastavený) anebo aktivní manipulaci s jeho síťovým provozem (např. vložení „exploitů“ do HTML stránek přenášených tímto spojením). Pokud se následně podaří získat kontrolu nad klientským počítačem, otevírá se možnost přístupu do původní (skutečné) podnikové sítě.

Testy uživatelů – sociální inženýrství

Na rozdíl od testů, které se zabývají převážně technologickými chybami, při testech na bázi sociálního inženýrství jsou cílem zaměstnanci, které se pokoušíme přesvědčit ke spuštění trojského koně. Tyto testy jsou z praktického, etického i právního hlediska poněkud problematické, proto je aktivně nenabízíme a provádíme jen na výslovné přání zákazníka.

Za posledních několik let zde došlo jen k marginálnímu zlepšení, které souvisí především se skutečností, že dnes již obvykle nelze spustitelný kód zaslat přímo v příloze emailu a občas jej nelze ani stáhnout prostřednictvím HTTP protokolu (díky filtraci na úrovni proxy serveru). Prakticky vždy ale lze poslat e-mail s HTTPS odkazem na spustitelný kód.

Dle našich zkušeností se ve všech případech najde dostatečné množství uživatelů, kteří daný kód spustí i v případě, že se nejedná o žádný rafinovaný způsob sociálního inženýrství (např. e-mail od zcela neznámé osoby s odkazem na „vtípek“). Ve společnosti, jejíž uživatelé byli proškoleni o hrozbách tohoto typu, takto podstrčený kód spustí místo obvyklých 30–60 % uživatelů „pouze“ 5–10 %. Skutečnému útočníkovi však může stačit i jen jediný.

Pokud zcela „amatérský“ způsob nahradíme např. zasláním profesionálně zpracovaného CD-ROM disku poštou nebo rozdáváním USB klíčenek v profesionálním balení s brožurou (např. soutěž s možností výhry fotoaparátu či lístku na sportovní utkání) u vchodu do budovy, úspěšnost dramaticky vzroste i v případě silně proškolených zaměstnanců.

Podobný útok navíc vůbec nemusí být přesně zacílen na konkrétní společnost. Na pracovních stanicích bývá obvykle nainstalováno nezanedbatelné množství aplikací od třetích stran, které na rozdíl od operačního systému nejsou automaticky aktualizovány a obsahují závažné bezpečnostní slabiny. Jedná se většinou o zastaralé verze software od firmy Adobe (Reader a Shockwave/Flash), Oracle/Sun Java VM, Mozilla Firefox, WinZip/WinRAR, Winamp nebo Quicktime. Často však není aktualizován ani kancelářský balík Office nebo Internet Explorer. Útočníkovi pak stačí umístit zlomyslný kód na exponovaný webový server (nebo do reklamních bannerových systémů) a pak si jen z napadených návštěvníků vybírat ty, kteří pocházejí z potenciálně zajímavých destinací.

Závěr

Z hlediska bezpečnosti sítí přímo dostupných z internetu došlo ke znatelnému zlepšení situace. K podobnému zlepšení došlo i z hlediska zabezpečení bezdrátových sítí. Tyto pozitivní trendy jsou však často zcela eliminovány množstvím webových aplikací, které bývají výrazně nejslabším článkem v pomyslném řetězu.

Pokud chce útočník komfortně získat přístup do vnitřní sítě, absolutně nejsnazší a nejspolehlivější je útok za použití sociálního inženýrství, jehož úspěch je prakticky garantován. O tom, jak vypadá bezpečnost z hlediska interních vnitropodnikových sítí a jaké možnosti se získáním přístupu do interní sítě útočníkovi otevírají, se dozvíte v části II tohoto článku, která vyjde v čísle 4/2010 DSM.

Martin Mačok
macok@dcit.cz

Mgr. Martin Mačok

Vystudoval Matematicko-fyzikální fakultu Univerzity Karlovy (obor Informatika) a v současné době pracuje pro DCIT, a.s., jako bezpečnostní konzultant/analytik se specializací na penetrační testování.