Ze zkušeností penetračního testera

část II

Vnitropodnikové sítě

V předchozí části článku[1] jsme se věnovali otázce bezpečnosti systémů, které jsou přímo dostupné z Internetu, bezdrátovým sítím a nelichotivé situaci ohledně webových aplikací. Zbývá uvést, jaké možnosti se otevírají útočníkovi při útoku na vnitropodnikové sítě.

Při tzv. interním penetračním testu se snažíme o simulaci útoku v prostředí vnitropodnikové sítě. Potenciálním útočníkem je tedy např. vlastní zaměstnanec nebo zaměstnanec (sub)dodavatele, který má přístup do vnitřního prostředí. Tyto testy jsou obvykle prováděny tzv. se znalostí (scénář „zaměstnanec“), kdy konzultant dostane k dispozici standardní pracovní stanici, běžný uživatelský účet a základní informace o vnitřním prostředí nebo procesech. Tento test lze samozřejmě provádět i ve variantě „bez znalosti“, kdy útočník získává k dispozici např. jen síťovou zástrčku (scénář „uklízečka“).

Cílem je získat v dané situaci co nejvyšší možná privilegia. V rámci typického většího podniku, kde prakticky bez výjimek dominuje platforma Microsoft Windows, to znamená, že v ideálním případě je získána plná kontrola nad doménovým řadičem. Pokud máte kontrolu nad řadičem, kontrolujete obvykle dostatečně velké množství počítačů, takže je relativně pohodlně možné získat kontrolu i nad těmi zařízeními, která nejsou přímo s doménou propojena. Stačí si jen uvědomit, že i pracovní stanice správců sítě (ze kterých se na daná zařízení přistupuje) jsou obvykle členy domény.

Bezpečnostní slabiny, s nimiž se se železnou pravidelností ve vnitropodnikových sítích setkáváme (ať už se jedná o banky, energetické společnosti nebo třeba státní instituce), prakticky přesně korelují s doporučeními, která platí již snad od počátků vzniku počítačových sítí. Měla by se používat kvalitní hesla (a mělo by s nimi být patřičně opatrně zacházeno), měly by se aplikovat bezpečnostní záplaty, systémy by měly být co nejjednodušší a měly by se od sebe navzájem co nejvíce izolovat. A samozřejmě by měla být stanovena nějaká pravidla používání (bezpečnostní politika) a také prováděna kontrola, zda se tato pravidla dodržují. Jaká je praxe?

Hesla

Na samotných doménových řadičích bývá většinou nastavena přísná politika hesel, která neumožňuje nastavit jakémukoli uživateli nekvalitní heslo. To však nemusí platit pro účty, které byly vytvořeny ještě před touto politikou. V praxi se tak setkáváme s tím, že v doméně existují různé „technické“ účty s triviálními hesly, které jsou v rozporu s nastavenou politikou. Nezřídka bývají i privilegované, neboť slouží pro účely vyžadující nadstandardní oprávnění (příp. tato vyšší privilegia přiřadil administrátor tak nějak „pro jistotu“, aby měl zaručeno, že „to bude fungovat“). Pro tyto účty často platí, že administrátoři vlastně ani nevědí, co by se stalo, kdyby heslo změnili – kde všude by ho museli přepsat a co všechno by přestalo fungovat.

Běžnou praxí bývá i používání (stejných) výchozích hesel pro nově vytvářené účty. Uživatel je sice při prvním interaktivním přihlášení na pracovní stanici donucen si toto heslo změnit (v souladu s politikou), ovšem mezitím v některých případech uběhne dlouhá doba a občas zřejmě účet ani není nikdy použit. „Užitečná“ je i skutečnost, že je změna hesla vynucována jen při interaktivním grafickém přihlášení. V případě přístupu ke službám typu sdílené disky nebo RPC je i opakovaný přístup s „dočasným“ heslem umožněn, aniž by byla změna hesla vynucena, neboť tyto protokoly změnu ani neumožňují.

[1] DSM 3/2010 s. X–Y.

Podobným typickým nešvarem je opakované používání stejných hesel pro různé účty (třeba i do zcela jiných systémů). V některých případech se jedná „jen“ o účty spravované jedním člověkem, nezřídka se však setkáváme s případy, kdy administrátoři záměrně takové „superheslo“ mezi sebou sdílejí, aby si zjednodušili práci.

Ještě horší je obvykle situace v případě hesel do systémů/aplikací, která nepoužívají doménovou autentizaci. Běžná jsou naprosto triviální (často i prázdná) hesla k Microsoft SQL databázím (účet, resp. role sa). Pro útočníka jsou užitečná v tom, že použitím xp_cmdshell() procedury komfortně získává plnou kontrolu nad operačním systémem. Nezřídka se setkáváme i s počítači, které jsou členy domény s kvalitní politikou hesel a zároveň mají triviální heslo pro lokálního administrátora.

V oblasti problematiky hesel by bylo možné pokračovat ještě dlouho. Je sice poznat, že trendem je snaha zavádět přísné politiky hesel (ať již formou technických vynucení či na papíře), tato snaha však není téměř nikdy důsledná a většinou zcela chybí kontrolní mechanismy. Při troše snahy (a jisté opatrnosti vzhledem k automatickému zamykání účtů) však nebývá problémem najít i v prostředí, kde je zavedena přísná politika hesel, právě ty výjimky a na nich útok postavit.

Zde je nutné uvést, že pro útočníka může mít hodnotu prakticky jakýkoli počítač v rámci Windows domény. Windows totiž implementují několik mechanismů, kterými si ukládají autentizační (a jiné citlivé) údaje. Např. cached logon credentials slouží k tomu, aby se uživatel mohl ke stanici přihlásit i v případě, že není dostupný řadič (a nelze tedy ověřit platnost autentizačních údajů). Výchozím nastavením počtu takto „zachycených“ hesel (v zahashované podobě) je hodnota 10 (!). Obvykle je vysoká pravděpodobnost, že některé z těchto hesel patří privilegovanému uživateli, např. proto, že v minulosti řešil na daném počítači nějaký problém (servisní účet) anebo je tam již od prvotní instalace (z „obrazu“ předkonfigurovaného systému).

Ovládnutím systému samozřejmě získáte i hashe hesel lokálních uživatelských účtů. Těch sice nebývá mnoho (často se jedná jen o jeden účet lokálního administrátora), výhodou pro útočníka však bývá skutečnost, že hesla jsou obvykle uložena ve zcela zastaralém hashovacím formátu LM, který lze i v případě velmi kvalitního hesla prolomit v řádu jednotek minut (za použití rainbow tables) nebo v řádu jednotek hodin (za pomoci konvenční hrubé síly). Pokud se to spojí s faktem, že systémy jsou instalovány z předpřipravených obrazů, toto heslo je typicky platné i na všech okolních stanicích. Následky samozřejmě bývají fatální.

Dalším zdrojem cenných informací po ovládnutí konkrétního systému jsou různá jiná bezpečná úložiště (např. tzv. LSA secrets), která Windows používají k ukládání citlivých informací. Pokud někdo třeba v minulosti na daném systému naplánoval nějakou úlohu pomocí at pod doménovým účtem (opět, zcela typicky privilegovaným), systém si zapamatuje jeho heslo v otevřené podobě (potřebuje ho kvůli možnosti přihlášení k cílovému účtu). Podobným způsobem je např. uloženo i heslo doménového účtu, pokud je pod ním spuštěna systémová služba. Nezřídka si do tohoto úložiště různá hesla odkládají i jiné speciální aplikace třetích stran (často aniž by to bylo v jejich dokumentaci zmíněno). Takto získaná hesla pochopitelně nemusí být zcela aktuální a v mezičase mohla expirovat, často se však jedná o technické účty s příznakem „Password Never Expire“.

V praxi se pak stává, že po kompromitaci jediného, třeba i zcela nedůležitého člena domény lze získat dostatek informací k efektivnímu ovládnutí celé domény. Kupodivu není až tak výjimečné, že k takové totální kompromitaci postačí již samotná pracovní stanice, neboť na ní (resp. na stanici, na které byl vytvářen obraz vzorové instalace) byl v minulosti použit privilegovaný doménový účet.

Stanici lze obvykle ovládnout zavedením alternativního operačního systému z výměnných médií nebo přepojením ethernetového kabelu do vlastního přenosného počítače a zavedením alternativního systému z takto improvizované „sítě“ pomocí PXE. V případě naprosté nouze, pokud ani tato varianta není v zaheslovaném BIOSu povolena, lze samozřejmě otevřít počítač a heslo k BIOSu resetovat (alternativně si „vypůjčit“ disk).

Byl bych nerad, kdyby výše uvedené skutečnosti byly brány jako kritika samotné technologie doménové správy v prostředí Windows. Pokud se používá správně, může naopak výrazně pomoci k dosažení velmi dobré úrovně zabezpečení. Pro většinu výše uvedených problémů existují relativně jednoduchá a přímočará protiopatření.

OK System

Struktura vnitřní sítě

Jinou kapitolou je samotná podoba interní sítě. Bohužel se v interních sítích firewally používají obvykle jen sporadicky. Je zcela typické, že v prostředí s řádově stovkami až tisíci zaměstnanci (resp. uživateli) jsou z běžné pracovní stanice v okolní síti dostupné řádově stovky až tisíce ostatních zařízení. Jedná se o další stanice, servery, tiskárny, směrovače, UPS zařízení, přepínače a různá jiná speciální zařízení, např. kamery nebo čtečky karet u vstupních dveří. Všude jsou pak obvykle dostupné řádově desítky služeb (otevřených portů) a každá je potenciálním rizikem. Důkladně proskenovat takovou síť zabere řádově jednotky hodin, výsledek však obvykle stojí za to.

Je-li ve společnosti velká snaha udržovat bezpečnost jednotlivých systémů na solidní úrovni, v tomto množství je prakticky vyloučeno, aby automat nenašel nějaké závažné problémy. Jedná se většinou o chybějící aktualizace, nevhodné konfigurace či výchozí přístupová hesla. Typické jsou např. různé testovací/vývojové verze serverů, které jsou z hlediska zabezpečení podceňovány, je na nich však (např.) nastaveno stejné heslo lokálního administrátora jako na ostrém serveru.

Penetrační testy ukazují, že stejného výsledku lze často dosáhnout nezávisle na tom, zda je takto v síti nalezeno velké nebo malé množství chyb. Opět platí, že někdy stačí jediná slabina (např. chybějící patch), a bezpečnost celé domény se zhroutí jako domeček z karet.

S opravdu pečlivě izolovanými stanicemi a skutečně důkladnou separací jednotlivých funkčních celků sítě se setkáváme jen velmi výjimečně. Zde je vhodné zmínit i časté používání nešifrovaných protokolů v interních sítích, slabiny vyplývající z používání přepínaného Ethernetu nebo špatně nakonfigurovaných VLAN, ale to už bychom zabíhali do přílišných detailů.

Sdílené disky a jejich obsah

Dalším smutným pozorováním, které úzce souvisí s tím předchozím, je typické obrovské množství sdílených disků a na nich dostupných souborů, jejichž kompletní jmenný seznam (rekurzivní výpis) mívá řádově milióny položek. Většinou jde samozřejmě o zcela nezajímavý „balast“, při troše snahy však lze najít i soubory se zajímavými jmény nebo příponami.

Pomineme-li soubory typu „hesla.txt“, typickým příkladem jsou různé „dočasně“ odložené zálohy poštovních schránek,

adresářů, příp. i celých serverů, jejichž originální kopie jsou samozřejmě chráněné a nepřístupné. Tímto způsobem lze získat informace prakticky stejné, jako kdyby došlo ke kompromitaci původního systému (pokud je záloha aktuální). Uživatelé nebo i správci si volnou dostupnost mnoha sdílených disků často vůbec neuvědomují, příp. zapomínají jejich obsah pravidelně „uklízet".

Detekce útoků

Poněkud překvapivá je i skutečnost, že činnosti penetračního testera ve většině případů nejsou vůbec odhaleny. V některých případech je detekováno masivní plošné skenování zranitelností pomocí síťových nástrojů typu Nessus (vulnerability scanner), a to dost často jen díky náhodě – jeden ze správců řešil nějaký jiný (běžný provozní) problém a podíval se ve správnou dobu do nějakého logu, ve kterém činnost podobného, masivně pracujícího skeneru lze jen těžko přehlédnout.

Skutečnost, že se třeba o hodinu později penetrační tester přihlásí jako doménový administrátor přímo na doménový řadič, však bývá odhalena jen ve velmi ojedinělých případech. Zde je asi vhodné podotknout, že skutečný útočník by takové intenzivní (velmi nápadné) skeny s největší pravděpodobností vůbec neprováděl. Při penetračním testu je však vzhledem k výrazným časovým omezením (v našem případě typicky 2–3 dny) třeba rezignovat na opatrnost a nenápadnost, neboť je třeba postupovat co nejrychleji (a pokrýt co nejvíce oblastí).

Shrnutí stavu bezpečnosti vnitropodnikových sítí

V otázce bezpečnosti vnitropodnikových sítí nás bohužel napadají pouze slova typu „tragédie" či „katastrofa". Kompromitaci interních sítí lze provádět za použití prakticky stejných metod jako před pěti nebo deseti lety a přestože u většiny klientů pozorujeme mnohdy i výrazně skokové zlepšení, prakticky ve všech případech lze z pohledu útočníka tento pokrok kompenzovat zvýšenou efektivitou (lepší automatizací) starých postupů a použitím pokročilejšího (opět často volně dostupného) software z oblasti ofensivních technologií (např. Metasploit Framework). Ve více než 90 % případů z desítek testovaných vnitropodnikových sítí za poslední cca dva roky se nám podařilo získat plnou kontrolu nad doménovým řadičem nejpozději druhý den testu, přičemž není zcela výjimečné, že doménový řadič padne už během několika prvních hodin testu (autorův osobní rekord je 20 minut od zahájení testu, jeho kolegové jsou však v těsném závěsu).

Není tedy výjimkou, že klienta ve výsledné zprávě chválíme, neboť od předchozího testu dosáhl velmi výrazného zlepšení a velmi dobré úrovně ve srovnání s konkurencí, přestože jsme i v jeho případě našli v síti slabá místa a následně dosáhli plné kontroly nad doménovým řadičem. Je zřejmé, že pouhé snižování hustoty výskytu slabin je taháním za kratší konec provazu, neboť útočníkovi může k úspěchu stačit i jen jediný výskyt hledané chyby.

Závěr

Zcela nepochybně platí, že úroveň zabezpečení se prakticky ve všech oblastech u všech testovaných subjektů nějakým způsobem neustále zlepšuje. Na druhou stranu se však počítačové sítě neustále rozrůstají o další nové systémy, a to typicky větším tempem, než ubývají ty staré. Tyto nové systémy nejsou vždy z bezpečnostního hlediska lepší (alespoň ne ve svých výchozích pozicích) a nově nasazované technologie bývají z bezpečnostního hlediska často rozporuplné.

Praxe bohužel ukazuje, že útočníkům k pokrytí technologického pokroku často stačí jen nepatrně přizpůsobit své metody (příp. je pouze zefektivnit a zautomatizovat) k tomu, aby dosahovali prakticky stejných výsledků. Bohužel se nám stávající situace jeví jako téměř neřešitelná, neboť i přes velkou snahu je stále velmi těžké dosáhnout uspokojivého stavu, kdy by kompromitace podnikové sítě vyžadovala skutečně jen velmi vytrvalého, odhodlaného a rafinovaného útočníka.

Dosáhnout ideálního zabezpečení je sice prakticky nemožné, nelze to však zneužívat jako výmluvu, proč se o to nesnažit. Vyjma razantnějšího přístupu při implementaci bezpečnostních politik je třeba akceptovat realitu a současně zaměřit o něco více pozornosti směrem k detekci potenciálně úspěšných útoků a schopnosti adekvátně reagovat. Principiální chybou je vlastně i ono samotné zaměřování na konkrétní problémy. K bezpečnosti by se mělo přistupovat komplexně a vyváženě tak, aby se nestavěly neprůstřelné zdi vedle plotů ze shnilého dřeva. To je totiž výsledkem typické ideologie „bezpečnost vyřešíme tím, že si koupíme bezpečnostní produkt X".

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.