Jak myslí a pracují hackeři

STUDIE SKUTEČNÉHO PŘÍPADU ZCIZENÍ DAT

MARTIN IGNJATOVIĆ

Následující studie skutečného případu zcizení dat ukazuje, že bezpečnost není jen o tom mít zabezpečený počítač, ale souvisí z mnohem více věcmi, než by si člověk pomyslel a vyžaduje mnohem širší pohled na bezpečnost informačních technologií.

BRIAN A JEHO PARTA

Mezi půlnocí a ránem není na celosvětové síti internet ani zdaleka tak mrtvo, jak by se mohlo na první pohled zdát. Jsou připojeny miliony uživatelů. Čas je díky celosvětovému charakteru sítě a časovým pásmům na zeměkouli pouze relativní. Toho si byl vědom i Brian, hlavní bezpečnostní specialista úřadu jedné velmi důležité státní organizace. Tato organizace zpracovávala velmi citlivá data, za jejichž bezpečnost byl Brian odpovědný. Ze svých zkušeností rovněž dobře věděl, že noc je ideální dobou, kdy se různí lidé snaží pronikat do cizích systémů. Mnozí z nich totiž předpokládají, že většina správců tou dobou spí nebo je jejich pozornost snížena. Brian, který dříve sloužil u zvláštních jednotek námořnictva, se naučil nic nepředpokládat. Proto i dnes, ve tři hodiny ráno chladné lednové noci, seděl u svého počítače a sledoval stav sítě. Trápila ho však jiná věc. Před několika dny byl pozván k řediteli organizace, který mu sdělil, že úřad může v nejbližších dnech čekat pokusy o krádež dat nebo o průnik do jejich počítačové sítě. Z průniku do sítě Brian strach tolik neměl. V oddělení pracovalo několik vynikajících inženýrů a Brian věděl, že svou práci odvádějí velmi dobře. Šel jim totiž příkladem. Na pracovišti byl vždy první a odcházel poslední. Nikdy po nich nechtěl to, co by neudělal on. Rovněž jim v práci dával volnost a nezasahoval do toho, co dělají. Podporoval je, pokud přišli s nějakým nápadem či řešením. Všechny změny, které měly být provedeny, nebo všechna nová zařízení, která měla být použita, s nimi konzultoval. Věděl, že jeho lidé jsou velmi schopní, ve svém oboru pracují denně a vědí tudíž mnohem více o tom, co bude fungovat, než nějaký byrokrat z logistické sekce. Nebyl typem mikromanažera, který by se šťoural v každém problému, říkal lidem co a jak mají dělat a trestal je za jejich chyby. Brian trestal lidi za to, že se z chyb nepoučí, ne za to, že se jich dopouštějí. Jeho podřízení, což neznamená lokajové, viděli jak jejich šéf tvrdě pracuje a nechává zodpovědnost na nich, a tudíž se snažili pracovat, jak nejlépe uměli. Snažili se svému šéfovi vyrovnat. Přicházeli s novými nápady a nebáli se rozumně riskovat, neboť věděli, že mají ve svém vedoucím opravdovou oporu. Zároveň věděli, že pokud selžou a nebudou na svou práci stačit, budou bez milosti propuštěni, a proto se neustále zdokonalovali, studovali a tvrdě pracovali. Spolupráce s oddělením správy sítě byla rovněž bezproblémová. Mezi oběma útvary panovala velmi dobrá komunikace, a pravá ruka věděla, co dělá levá. O všech krocích, které by se týkaly změn na síti, se vzájemně informovali, a tudíž měla obě oddělení dobrý přehled o stavu sítě.

FYZICKÁ BEZPEČNOST ATD...

Věc, která dělala Brianovi potíže, byla fyzická bezpečnost budovy. Budova byla osm pater vysoká. Patřilo k ní rovněž několik menších budov, kde byly situovány sklady materiálu a vybavení. Pod budovou se nacházel rozsáhlý areál, kde byly umístěny laboratoře. Ostrahu budovy měla na starost najatá firma Security. Brian, který byl ze své vojenské kariéry o ostraze objektů velmi dobře informován, věděl, že tato ostraha nestojí za nic, a budova je tak otevřena každému, kdo má jen trochu snahy a nápaditosti. Rovněž nechápal, proč budovu nehlídají příslušníci ozbrojených sil. Toto vše však šlo mimo jeho kompetence. Ostraha byla rozdělena mezi tři skupiny hlídačů. Jedna skupina měla na starost vnitřek budovy, kde se nacházely kanceláře. Druhá skupina odpovídala za bezpečnost okolí budovy a třetí za bezpečnost podzemních laboratoří. Nejhorší bylo, že skupiny komunikovaly každá na jiné frekvenci a neměly jednotné velení. Pracovníci ostrahy, většinou vysloužilí policisté, byli, jak už to bývá, mizerně placení a nemotivováni. Všechny ty fajnové elektronické hračičky, jako jsou kamery, detektory pohybu či čipové karty, nebyly samospasitelné, pokud chyběl kvalitní lidský faktor. Brianovi se podařilo prosadit několik bezpečnostních opatření. Mezi ně patřilo důsledné prosazování bezpečnostní politiky. Přístup do areálu i počítačů byl řízen čipovými kartami. Tím odpadly problémy s používáním hesel. Horší to bylo s bezpečností těchto čipových karet. Brian se snažil prosadit opatření, kdy by každému zaměstnanci byla vydána karta při příchodu do budovy na základě kontroly totožnosti. To se však nepodařilo a zaměstnancům bylo umožněno nosit karty domů. Za jejich ztrátu či zcizení nehrozil žádný postih, což dělalo pracovníkům bezpečnostních oddělení nemalé starosti. Upozorňovali na to několikrát, ale veškerá snaha byla marná. Důvod, proč prý nemohli vydávat karty až při příchodu budovy na základě průkazu totožnosti, byl takový, že by to zaměstnance velmi zdržovalo a bylo by třeba najmout člověka, který by kontrolu prováděl. Jinými slovy zvítězila pohodlnost a lakota nad bezpečností. Na druhou stranu bylo toto opatření přijatelnější, než dovolit uživatelům používat vlastní hesla a riskovat tak, že by si vybírali slabá hesla a ohrozili tak bezpečnost celého systému, pokud jde o přístup zvenku. Brian spolu se svým týmem plánoval dobudoucna zavedení identifikačních zařízení, která budou pracovat na základě rozpoznávání otisků prstů a hlasu. To by mělo některé problémy vyřešit. Takové řešení je však velmi drahé, a zatím nemělo oporu u vedení. Dalším problematickým úsekem bylo umístění serverů. Brian by mnohem raději viděl všechny servery co nejblíže svému pracovišti a pod svým dohledem. Bohužel servery byly umístěny na druhém konci budovy a o pět pater níže. Přístup do místnosti se servery hlídala strážní služba. To byl další problém, jehož si byl Brian vědom. Okna v přízemí mívají obvykle silné mříže. Okna od první patra výše zpravidla již ne. Sídlo jejich firmy nebylo výjimkou. Stačil schopný člověk s lanem či žebříkem, a mohl se do místnosti se servery kdykoliv dostat. Architekti mu situaci ještě usnadnili, neboť hned vedle okna byl bleskosvod. Čidla pohybu v místnosti se servery samozřejmě byla, ale hlídala pohyb při příchodu dveřmi. Jeho předchůdce ve funkci manažera bezpečnosti zřejmě ve své genialitě na okno zapomněl nebo předpokládal, že oknem sem nikdo nepoleze. Brian ze své zkušenosti věděl, že předpokládat se nemá nikdy nic. Opravná opatření již byla navržena, ale byrokratické postupy dodávky potřebného vybavení velmi zdržely. Musel totiž vyplnit desítky formulářů, získat desítky souhlasů a čekat několik měsíců, než bylo vybavení dodáno. Marně se mnohokrát dožadoval zabezpečení místnosti se servery. Psal poplašné zprávy, přemlouval, loudil, ale vše marně. Nejčastěji dostal odpověď, že místnost je vybavena zařízením za desítky tisíc, a že není třeba vydávat na její ochranu další prostředky. Celková bezpečnostní situace tudíž nebyla nijak růžová. Ještě ke všemu se očekával útok na citlivá data. Briana vůbec nezajímalo, kde vedení tuto informaci získalo, pravděpodobně od bezpečnostní služby státu. Důležitá byla v tento moment opatření, která budou přijata. Brian se se svými pracovníky snažil vžít do role útočníka. Pokud půjde o profesionály, zjistí velmi brzo, že zvenku se do sítě snadno nedostanou. Bude pro ně snazší proniknout do objektu. V objektu se nacházelo mnoho systémů, na kterých bylo mnoho zajímavých informací. Pravý poklad byl však soustředěn na serverech. Proto se útočníci budou

pravděpodobně snažit získat přístup k systému, který má neomezený přístup k datům na všech serverech. Takových systémů je v budově celkem pět. Další možností je, že se útočníci pokusí odnést disky ze serverů. To by pro ně bylo zřejmě nejsnazší. Obsah disků bohužel nebyl žádným způsobem šifrovaný, jak Brian při nástupu do funkce s hrůzou zjistil. K jejich zašifrování dosud neobdržel od vedení povolení. Bylo tedy třeba zajistit řádně místnost se servery.

NASTY

Tom Hartmann, v digitálním undergroundu známý pod přezdívkou Nasty, byl jedním z velmi schopných mladíků. Ve svých pětadvaceti letech toho o počítačových systémech, a zejména o jejich bezpečnosti věděl více než většina inženýrů a programátorů. Pronikal do systémů od svých patnácti let a za tu dobu jich měl na kontě již pěknou řádku. Byl posedlý novými technologiemi a řešeními, proto na sobě ustavičně pracoval a neustále se zdokonaloval. Nějakou undergroundovou etiku příliš neuznával. Jednal

tak, jak uznal za vhodné, čímž si ale získat velmi mnoho nepřátel. Nasty se s nimi potýkal poměrně často a to ať v situaci, kdy se setkali na nějakém nabouraném serveru, nebo na nějakém IRC kanálu. Nutno podotknout, že Nasty poměrně často vítězil, a to zejména díky své lstivosti a intelektu. To ostatní příslušníky digitálního undergroundu přivádělo k šílenství a skutečně ho nenáviděli a hledali možnost, jak se mu pomstít. To se jim jednoho dne povedlo a připravili na Nastyho léčku. Léčka byla opravdu důkladná a pracovalo na ní pouze omezené množství lidí, kvůli bezpečnosti celé akce. Nasty do léčky upadl, a výsledkem byl rok a půl v nápravném zařízení. Tom přísahal, že se pomstí. Nenáviděl celou společnost. Ve vězení získal kontakty na několik lidí, jejichž minulost byla pochybná. Po propuštění neměl peníze na obživu. Zaměstnat ho nikdo kvůli jeho minulosti nechtěl. Proto zavolal jednomu svému známému a zeptal se ho, zda o něčem neví. Jeho přítel, který moc dobře věděl o jeho znalostech a schopnostech, mu předal telefonní číslo, na které má zavolat. Po několika desítkách minut již Tom věděl, že má práci. Chvíli uvažoval, jestli má nabídku přijmout. Člověk na druhé straně telefonu nechtěl mluvit o podrobnostech. Práce byla velmi dobře placená a Tom potřeboval peníze velmi nutně. Rozhodl se, že nabídku přijme. Dal si s oním člověkem schůzku, na které si vyjasní podrobnosti.

NELEHKÝ ÚKOL

Když se dozvěděl podrobné informace, na chvíli znejistěl. Bylo před ním opravdu velké sousto. Nepůjde o průnik do lecjakého systému. Když se dozvěděl jméno úřadu, zarazilo ho to. Nejvíce ho však znervózňovala myšlenka, že se do budovy úřadu vloupe se skupinou několika profesionálních zlodějů. Uvnitř budovy pak zlodějům ukáže, která data jsou důležitá, případně jim pomůže získat přístup do nějakého systému. Pokud nebudou schopni data na místě získat, budou mít za úkol přinést pevné disky a další média, a z nich pak v klidu data získat. Tom věděl, že se pouští na tenký led, ale z jeho perspektivy jinou možnost neměl. Navíc prahl po pomstě celé společnosti, k čemuž měl teď jedinečnou příležitost. S nabídkou souhlasil. Člověk, se kterým měl schůzku, mu řekl, že se mu ozve, až nastane čas akce. Poté vylovil mobilní telefon a informoval Randyho, že může začít z průzkumem objektu. Byly dvě varianty útoku na budovu. Jednou byla možnost napadnout síť zvenku. Jelikož věděli, že síť je velmi dobře spravována, moc s touto možností nepočítali. Pravděpodobněji se pokusí do budovy vloupat a data ukrást organizaci přímo pod nosem. Přesto nebyla první možnost vyloučena. To byla práce pro Nastyho. Dostal k dispozici nejnovější laptop na trhu. Jako připojení si vybral mobilní telefon. Nejen že pevná linka se dá snadno identifikovat a stopovat, ale Nasty nepředpokládal, že bude nějaká data stahovat, potřeboval jen mobilní zařízení, které se nedá snadno vystopovat a umožní mu pokud možno nenápadně oťuknout síť a její správce. Předpokládal, že když se bude pokaždé připojovat jen na pár minut a z jiného místa, bude možnost jeho odhalení opravdu minimální, a to i v případě, že správce bude velmi schopný a zapojí do pátrání policii. O tom ale Nasty silně pochyboval, neboť kvůli nějakému skenování portů přece nebude nikdo dělat poplach. Rozjel se tedy vypůjčeným vozem na západní kraj města a připojil se do sítě. První, co bylo třeba udělat, je získat o síti informace. Dostal sice papír, kde byly uvedeny přidělené IP adresy a kontakty na správce sítě, o topologii a struktuře sítě tu však nestálo ani slovo. Nasty uvažoval. Pokud použije hromadného pingu, mohl by spustit alarm na některých hraničních firewallech a jejich IDS. Na druhou stranu není toto riziko tak velké. Sáhl tedy po nástroji fping a pustil jej na celou síť. Odpovědí mu bylo, že v provozu je osm systémů. Rozhodl se, že se na ně podívá blíže. Na to však přijde čas jindy a na jiném místě. Jeho předchozí akce totiž mohla vzbudit pozornost.

BUDOVU JE TŘEBA PROZKOUMAT

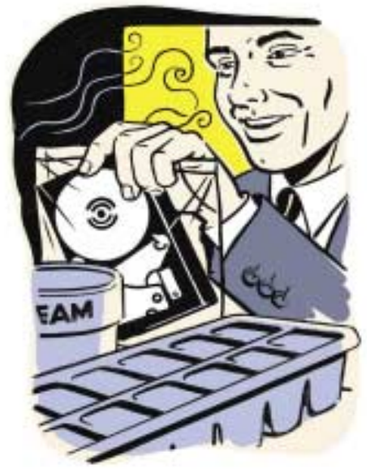
Skupina vedená Randym prováděla průzkum objektu. Randy jako bývalý zaměstnanec bezpečnostní firmy viděl většinu nedostatků v zabezpečení objektu na první pohled. Střecha budovy nebyla vůbec krytá a ze sousedního hotelu by nebyl takový problém, jak se na ni dostat. Rovněž všechna okna krom přízemí byla naprosto nezabezpečená. Kamery, které snímaly celý pozemek okolo budovy, byly statické a nebylo těžké najít mrtvé body. Strážní chodili ve dvojicích pravidelně každých patnáct minut na obhlídku, a nebude tudíž problém proklouznout v okamžiku, kdy se vzdálí. Rozvod elektřiny a telefonních kabelů byl rovněž mimo budovu a nebyl ani oplocený. I když má budova pravděpodobně záložní generátory, výpadek elektřiny by ji mohl na chvíli vyvést z míry a způsobit zmatek. Hlavní vchod nebyl zabezpečen vůbec. Byla zde malá vrátnice s jedním strážným. Ten navíc nekontroloval příchozí, pouze řešil problémy pokud se dožadoval do budovy vstupu někdo, kdo neměl čipovou kartu. Randymu už bylo jasné, že nebude absolutně žádný problém do objektu proniknout. Dokonce již věděl jak. Před vlastní akcí si však chtěl budovu prohlédnout zevnitř a zjistit, jak je to s bezpečností uvnitř budovy.

BRIAN ČUCHÁ PODRAZ

Brian se ohlásil na pondělní ráno k vedoucímu úřadu. Při schůzce ho informoval, že pokud bude v nejbližších dnech podniknut útok na data společnosti, hrozí velké nebezpečí. Informoval ředitele, že co se týká průniku po síti, může zaručit bezpečnost dat. Pokud se týká fyzické bezpečnosti, nemůže za data ručit. Ředitel společnosti Brianovi poradil, ať se sejde se šéfem ochrany objektu a projedná celou záležitost s ním. On prý nemá čas, má zasedání jakési komise a během pěti minut musí jít. S těmito slovy doprovodil Briana ke dveřím. Na Brianovy námitky, že s ředitelem ostrahy není řeč, nebral ohled. Brian byl jednáním svého ředitele rozčarován. V tu chvíli mu začal hlasitě pípat pager. Podíval se na displej a zjistil, že ho volají lidé z jeho oddělení a že je to naléhavé. Vyběhl bleskově schody a vřítil se do společné pracovny. Mohl sice mít pracovnu vlastní, ale chtěl zůstat se svými lidmi. Proč by on měl mít polstrovanou židli, ledničku a květiny, když jeho lidé pracují úplně stejně jako on a takové právo nemají? Jeho kolega Peter mu oznámil, že někdo skenuje jejich síť. Na tom by nebyl ještě nic zvláštního. Skenů měli několik denně. Tento však byl něčím výjimečný. Přicházel z IP adresy, a tu identifikovali jako adresu jakéhosi providera připojení k internetu přes mobilní telefony. Přístup přes mobil mnoho firem nenabízelo a mnoho lidí nemělo, protože byl stále ještě poměrně drahý. Proč by si tedy někdo pořizoval drahý přístup k síti, a pak z něho podnikal takovou neužitečnou činnost jako je skenování systémů zrovna v jejich síti. Brianovy smysly zbystřely. Mobilní přístup k síti si pořizují většinou jen špičkoví manažeři, aby byli neustále v kontaktu, stahovali si poštu a komunikovali s klienty či nadřízenými. Tento přístup k síti nebyl příliš rozšířen ani mezi správci. Mohlo to znamenat, že jejich síť zkoumá někdo, kdo nechce být odhalen. Co bylo však divné, že se nepokusil ani proskenovat porty na systémech, které byly vidět zvenku. Hromadný ping a nic více. Někdo se snažit být velmi opatrný. Brian se přihlásil do svého systému a začal zkoumat záznamy. Ty mu ale nic důležitého stejně neřekly.

RANDY JDE NA PRŮZKUM...

Randy věděl, že nejlepším okamžikem pro vstup do budovy je pondělí ráno. Je zde nejvíce lidí a všichni mají po víkendu napilno. Vmísil se do skupiny zaměstnanců, kteří hromadně přijížděli linkovým autobusem. V autobuse se mu podařilo ukrást několik peněženek a spolu s nimi i dvě karty pro přístup do budovy. Karty opatrně vylovil a peněženky pak vrátil zpět do kapes jejich majitelů. Při příchodu do budovy si pak tito zaměstnanci budou myslet, že nechali kar-



tu doma, a buď se pro ni vrátí, nebo jim bude vystavena karta dočasná, poté, co se ověří jejich totožnost. Žádný rozruch tedy kvůli tomu nebude. Nikdo ze zaměstnanců, jak Randy věděl, nebude hlásit, že mu byla karta odcizena, raději se vymluví, že ji nechal doma nebo že mu ji poškodil domácí mazlíček. Lidé si totiž mysleli, že pokud nahlásí odcizení karty, budou mít problémy. Randy si počkal, až přijde k čipovému turniketu jeden z mužů, kterému odcizil kartu, a stoupl si za něj. Muž zalovil v kapse, vytáhl peněženku a začal hledat svou čipovou kartu. Když zjistil, že ji nemá, ohlásil strážnému, že kartu nechal pravděpodobně doma a požádal o vystavení karty dočasné. Vrátný si od něj vyžádal průkaz totožnosti a zavolal na bezpečnostní oddělení s žádostí o vystavení dočasné karty pro pana XY. Přesně jak Randy očekával, začala být řada lidí za ním nervózní a tlačila se ke vchodu. Randy zasunul svou kartu do turniketu, pokynul vrátnému a vešel do budovy. Vrátný, který stále ještě telefonoval s bezpečnostním oddělením, byl rád, že se fronta dala do pohybu a mávnul na Randyho rukou, ať pokračuje. Randy věděl, že nemůže chodit po budově jako turista a hledat cestu. Musí se tvářit jako že ví, kam jde. Jeho záměrem bylo prozkoumat celou budovu odshora dolů. Začne tedy dole, protože věděl, že vedení a vysoce postavené osoby mají kanceláře zpravidla v horních patrech budovy. Přízemím prošel bez problémů. Nic moc zajímavého zde nenašel, a proto se vydal do prvního patra. Zde nalezl to, co hledal. Dveře na konci dlouhé chodby. Na nich byl nápis IT-servery. Prohlédl si zabezpečení místnosti. Vstup řízen čipovou kartou. Podle drátů, které vedly do místnosti a z místnosti, usuzoval, že bude uvnitř nějaký detektor pohybu nebo kamera. V místnosti byla rovněž klimatizace a požární poplachové a hasicí zařízení na pěnu. Zapamatoval si číslo dveří a umístění místnosti, a pokračoval dále. Poté co prošel celou budovu již měl jasnou představu, jak budova zevnitř vypadá, kde jsou zajímavé kanceláře a kudy by se dalo do místnosti dostat. Z budovy se dostal bez nejmenších potíží.

...A NASTY HNED PO NĚM

Nasty si po vydatném spánku a obrovské porci pizzy vzal klíčky od auta, přibalil svůj laptop a vydal se na cestu. Chtěl se podívat na jednotlivé systémy blíže. Měl v plánu systémy proskenovat a zjistit, zda by se nenašla nějaká skulinka do systému. Tentokrát se vydal na opačný konec města. Poté, co zastavil na jednom odlehlém parkovišti, spustil svůj notebook a přihlásil se do sítě. Sáhl po svém oblíbeném nmapu a pustil se do skenování. Pak provedl ještě revizi služeb pomocí netcatu. Věděl, že tento krok již zcela určitě vzbudí pozornost, pokud není správce úplně neschopný. Po deseti minutách již měl výsledky skenu uloženy, pro jistotu zašifrovány a byl na cestě domů. Neměl čas výsledky zkoumat, ale na první pohled jej příliš nepotěšily. Do podrobnější analýzy se pustí až doma v teple.

BRIANOVI SE TO NELÍBÍ

Brianovi se celá situace přestávala líbit. Byl unavený a vyčerpaný. Jeho instinkty rozpoznaly, že se blíží útok. Záhadné skeny portů z mobilního telefonu. Ráno byla podána žádost o vystavení dvou dočasných karet. Volal vrátný a nadiktoval jim jména dvou zaměstnanců, kteří neměli čipovou kartu. Oddělení bezpečnosti nezbývalo nic jiného, než vystavit kartu dočasnou. Pátrat po kartách nemohli. Neměli k tomu pravomoce. Brian věděl, že kdyby se chtěl dostat do budovy, pravděpodobně by si sehnal průkaz a prošel si celou budovu. Krádež je ideálním způsobem, jak si novou kartu opatřit. Musí se mít na pozoru, neboť pokud se nějaká data ztratí, bude to jeho zodpovědnost bez ohledu na to, jaká opatření navrhoval. Vylovil tedy telefonní záznamník s kontakty na svou soukromou bezpečnostní síť. Vytukal číslo přítele, který pracoval jako bezpečnostní manažer u jedné telekomunikační společnosti.

INFORMACE VEŠKERÉ ŽÁDNÉ

Záznamy nebyly příliš povzbudivé, jak Nasty zjistil. Systémy měly otevřeny jen ty porty, které potřebovaly, navíc všechny servery byly zřejmě součástí DMZ (demilitarizované zóny). Ve výpisu bylo také několik hardwarových firewallů,

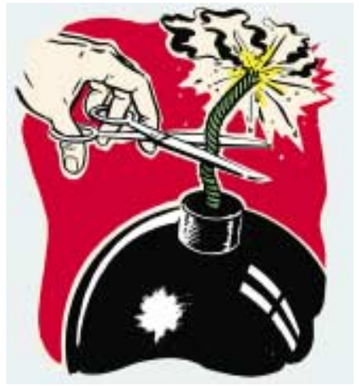
které byly nakonfigurovány velmi dobře a pravděpodobně jeho útok zaznamenaly, což Nastyho rozladilo ještě více. Přišel o moment překvapení. Nikde žádný zapomenutý systém, nikde žádné slabé heslo. Nasty uznal, že jednodušší bude proniknout do systému zevnitř. Čekal tedy, až bude akce připravena. Mezitím si připravil nástroje, které bude potřeboval. Hlavu si s tím, že nevedla do systému žádná cesta zvenku, nelámal, protože věděl, že s průnikem zvenčí se stejně nepočítalo. Bál se však zabezpečení systému. V porovnání se stovkami systémů, které se mu podařilo nabourat, byl tento zabezpečen velmi dobře. Schéma služeb a topologie sítě odpovídaly jeho představám o bezpečné síti, a sám by nepostupoval jinak. Možná by nějakou skulinku v zabezpečení našel, ale trvalo by to dlouho a bylo by to velmi namáhavé. Času mu však nebylo dopřáno a Nasty raději dělal věci jednoduše než složitě, a proniknout do budovy se mu zdálo jako snazší alternativa.

RANDY JE SPOKOJEN

Randy byl s obhlídkou spokojený. Budova byla otevřena dokořán. S jeho týmem nebude problém se do budovy dostat. Trápilo ho, že s sebou budou muset tahat ještě nějakého mladého počítačového experta – ty Randy neuznával a pohrdal jimi. To by mohlo celou akci ohrozit. Rovněž bylo třeba vyřešit otázku, kdy útok provedou. Pokud by jej chtěli provést přes den, budou sice ve výhodě a nebudou tolik nápadní při průniku do budovy, na druhou stranu budou mít uvnitř omezený pohyb. Akce večer bude náročnější na průnik do budovy, ale budou se moci pohybovat jak se jim zachce. Jelikož bylo třeba najít terminály, ze kterých je neomezený přístup ke všem databázím, rozhodl se pro variantu v noci. Začátek akce stanovil na 3.30 v neděli. Tou dobou je pozornost hlídačů nejmenší, a pokud některý z nich ve službě usne, bude mít nejsilnější spánek. Podle plánu by celá akce neměla trval déle než 45 minut. Nákupem vybavení již Randy pověřil jednoho člena svého týmu. Moc toho ostatně s sebou brát nebudou.

PŘÍPRAVA NA AKCI

Sraz měla skupina, která měla proniknout do budovy, v pátek brzy ráno. Bylo třeba projednat všechny bezpečnostní otázky, taktiku průniku do budovy i činnost uvnitř. Randyho úkolem bylo provést skupinu do objektu a zajistit pohyb po budově tak, aniž by si toho někdo všiml. Nastyho úkolem bude vyhledat vhodné terminály a získat potřebná data. Pokud se to nepodaří, vezmou všechny disky s sebou, a Nasty se poté pokusí jejich obsah dekódovat. Plán byl velmi jednoduchý, a proto také bude fungovat. Čím je plán jednodušší, tím méně věcí se může pokazit. Průnik byl naplánován následujícím způsobem: celá skupina se přesune v pronajaté dodávce do blízkosti budovy. Jelikož hlídka chodí po pravidelné trase vždy po 15 minutách, proběhnou přes trávník před budovou ve 3.32. Doběhnou k bleskosvodu a po něm vyšplhá jedna skupina do místnosti se servery, druhá do druhého patra do jedné z kanceláří nižších úředníků. Problém bude s Nastym, který zřejmě po bleskosvodu vyšplhat nedokáže. Proto Randy spolu s jedním ze svých lidí vezmou lano, jež hodí Nastymu, ten si jej



uváže kolem pasu a oba ho pak do místnosti vytáhnou. Zde vyřadí z provozu detektory pohybu a nechají Nastyho dělat jeho práci v kanceláři ředitele. Druhá skupina pronikne do místnosti se servery a tuto místnost zabezpečí. Pokud se Nastymu nepodaří získat přístup k serveru z počítače ředitele, půjdou do místnosti se servery, odkud to zkusí znovu. Pokud ani zde nebude úspěšný, odnesou si pevné disky s sebou. Celá akce se bude odehrávat beze zbraní a ve vší tichosti. Randy si ještě pro případ problémů připravil několik dýmovnic a velké kleště. Ty nechá spolu s jedním členem svého týmu v autě a v případě, že by vznikly nějaké potíže, dýmovnice zapálí a kleštěmi přestřihne telefonní spojení a přívod elektřiny. To by mělo způsobit dost zmatku na to, aby se jim podařilo bezpečně zmizet i se svým nákladem.

AKCE – NEDĚLE 3.15 V NOCI

Celá skupina dorazila před budovu právě v okamžiku, kdy před ní procházela dvojice hlídačů. Apatická chůze svědčila o jejich pozornosti. Jedině dobře, pomyslel si Randy. Hlídači šli pravidelným krokem, nerozhlíželi se a ani je nenapadlo kouknout do oken budovy. Skupina se připravila na průnik. Přesně ve 3.30 prošla dvojice hlídačů znovu. Tentokrát byli ještě více apatičtí a unavení. Tou dobou již obě skupiny ležely v křoví na svých výchozích stanovištích. Skupina, ve které byli Randy a Nasty, vyrazila dříve. Bleskově přeběhli prostor před budovou a pokračovali k bleskosvodu. Jako první lezl Randy. Překonat dvě patra pro něj bylo otázkou několika vteřin. Po něm i druhý člen skupiny. Poté, co se oba ocitli v místnosti a ujistili se, že je všude klid, hodili připravené lano Nastymu. Ten si je uvázal k bezpečnostním popruhům. Zvládl to celkem rychle, neboť podobnou akci předtím nacvičovali. Randy nechtěl nic ponechat náhodě a nechtěl aby celá akce zkrachovala na tom, že si nebude Nasty umět přivázat lano nebo že se rozbije o zeď, až jej budou vytahovat. Poté co se Nasty ocitl v místnosti a odvázal si bezpečnostní popruh, se celá skupina vydala na cestu do kanceláře ředitele. Vnitřek budovy byl chráněn kamerovým systémem a detektory pohybu. Tyto překážky však dokázali velmi snadno překonat. Kamery měly mnoho mrtvých úhlů a vzájemně se nepokrývaly. Pokud se tedy budou držet u zdi a šikovně kličkovat, nemají strážní u monitorů šanci je vidět. A i kdyby se náhodou dostali do prostoru, odkud by mohli být viděni, pochybovali, že strážní budou pečlivě sledovat monitory celou noc. Stejné to bylo i s detektory pohybu. Jejich buňky byly velmi snadno odhalitelné a překročit je nebyl žádný problém. Konečně se dostali do kanceláře ředitele. Vstup do kanceláře jim umožnila padělaná čipová karta, kterou si Randy „vypůjčil“ od uklízečů při své první návštěvě. Randyho ale trápila jiná věc. Vše probíhalo až příliš snadno. To bylo podezřelé. Soustředil se však na svou práci. Po vniknutí do místnosti provedl zběžnou kontrolu a dal pomocí vysílačky signál druhé skupině, že jsou na místě. Rovněž od druhé skupiny se dozvěděl, že je na svém místě a má situaci pod kontrolou. Nasty zasednul k systému a spustil jej. Objevila se výzva k vložení čipové karty. Nasty byl s těmito technikami zabezpečení velmi dobře obeznámen, a proto pro něj bylo otázkou několika minut, než zařízení odpojil a spustil počítač znovu, tentokrát již bez požadavku na vložení karty. Spustil program pro připojení k databázi. Až dosud šlo vše velmi snadno. Získal plný přístup k databázi. Žádné požadavky na heslo. Bylo to způsobeno tím, že veškerá bezpečnost byla postavena na principu čipových karet. Nasty vyťukal několik příkazů, ale zjistil, že data z databáze se mu exportovat nepodaří, protože na to neměl dostatečná práva. Mohl sice číst libovolná data, ale způsob, jak je dostat na svůj systém, neexistoval. To ho velmi rozlítilo. Jeho ješitnost a škodolibost mu však nezabránily v provedení několika změn. Do mechaniky vložil vlastní datový disk, který si s sebou přinesl, a spustil několik vlastních programků. Tyto programy měly za cíl způsobit po své aktivaci na síti chaos. Šlo o několik trojských koňů, červů a flooderů. Až se pokusí ředitel některý z nich spustit, o čemž Nasty nepochyboval, spustí tak, jak doufal, zkázu. Nasty oznámil Randymu, že neexistuje způsob, jak data získat po síti a že musí do místnosti se servery. Vydali se tedy do prvního patra. Přesun proběhl opět bez nejmenších problémů. Nasty zasedl k hlavnímu serveru, o němž již věděl, že je na něm umístěna databáze s daty, která chtějí. Zde však žádná ochrana čipovou kartou nebyla. To všechny členy skupiny zarazilo. Proč není používán systém zde, a v celé budově ano? Zřejmě proto, že správce nebyl žádný hlupák a spoléhal na staré dobré metody. Nasty přemýšlel, co bude dělat. Prolamování hesla by trvalo nepřiměřeně dlouho. A i kdyby se mu podařilo získat data, nemá jak si je odnést. Navrhl tedy Randymu, že bude nejschůdnější řešení data odnést i s pevnými disky a podívat se na ně v klidu někde jinde. Neměl s sebou jiný systém, kam by mohl disk připojit a alespoň prozkoumat jeho obsah. Až tuto možnost mít bude, nebude problém se k datům dostat. Randy souhlasil a řekl Nastymu, ať disky ze systému vyjme. To trvalo Nastymu několik minut, protože byl server zajištěn. Nakonec pomohl jeden šroubovák a trochu fyzické síly. Disky naházeli do připraveného pytle a chystali se k odchodu. Cestu zpátky měli naplánovanou opět přes okno. Randy věděl, že ústup je nejhorší částí každé operace. Počkali si tedy, až projde hlídka, a začali opatrně lézt dolů. Randy s Nastym poté nastoupili do připraveného auta a chystali se odjet. Zbytek týmu se nahrnul do dodávky. Vyrazili na předem sjednané místo. Všichni už se začínali tiše usmívat nad podařeným lupem. Proto jen nechápavě přihlíželi, když jim cestu zablokovala dodávka, ze které se vyhrnulo pět maskovaných postav se samopaly. Dalších deset můžů se náhle objevilo po obou stranách auta, a podle jejich výrazu bylo jasné, že není čas na žerty. Řidič se ještě pokusil zařadit zpátečku, ale i vzadu za autem se z ničehonic objevilo auto plné ozbrojenců.

BRIAN DOSTAL RANDYHO A SPOL.

Brian se usmíval. Věděl, že vyhrál, a přelstil velmi profesionální skupinu zlodějů. Poté, co zavolal svému kamarádovi z telekomunikační společnosti, zjistil, komu mobilní telefon patří. Byl registrován na jednu soukromou firmu. Brian požádal svého kamaráda, zdali by nemohl sledovat pohyb tohoto telefonu. To nebyl za použití moderních technologií žádný problém. Dostával tak výpisy, kam bylo z čísla voláno, kde se majitel pohyboval. Časy, kdy docházelo ke skenování sítě, přesně odpovídaly časům, kdy se majitel telefonu pokoušel připojovat k síti. Další výpis nebyl nijak zajímavý. Několik telefonátů na místní rozvoz pizzy, několik na erotickou linku. Brian rovněž zanesl do mapy souřadnice a věděl, že útočník se snažil být velmi opatrný. Sken prováděl vždy jen minimálně dlouho, a navíc pokaždé z jiného místa. To upoutalo Brianovu pozornost natolik, že se rozhodl toto číslo zkoumat. Svého dalšího kamaráda, který pracoval pro jednu bezpečnostní složku státu, požádal, zda by nemohl v jejich databázi zkontrolovat jistou firmu. Když se dozvěděl, že firma je již delší dobu sledována bezpečnostní službou a že obchoduje zejména s východní Evropou, v hlavě se mu rozsvítilo. Jde o pokus o špionáž. Proto zalarmoval svou soukromou síť kontaktů a podařilo se mu přimět několik známých ve vlivných funkcích, aby firmu sledovali. Dostával tak pravidelně velmi přesné údaje o tom, kde se lidé spojení s firmou nachází, co dělají, kupují, jedí, pijí. Zkrátka vše. Proto Brian o chystaném útoku věděl ještě dříve, než se uskutečnil. Mohl samozřejmě oznámit celou záležitost a nechat členy přepadového týmu zatknout, ale chtěl mít v ruce nezvratné důkazy a zjistit, po jakých datech vlastně jdou. Věděl, že neomezený přístup k informací má jen několik lidí. Proto všechny tyto systémy upravil tak, aby se tvářily, že poskytují důležitá data, ale zároveň chtěl vetřelce zahnat do místnosti se servery a donutit je ke krádeži dat. To se mu nakonec skutečně podařilo. Disky, které se jim podařilo ukrást, však nebyly ty, na kterých by bylo něco důležitého. To Brian riskovat opravdu nechtěl. Vyměnil celý systém a do databáze nahrál neškodná data. Poté již stačilo jen čekat, až past sklapne.

PONAUČENÍ NAKONEC

Brian a jeho pracovníci si rovněž odnesli mnohá ponaučení z toho případu, a získali tak velmi silné argumenty při prosazování bezpečnostních opatření. Od nynějška se budou kontrolovat všichni příchozí pomocí otisků prstů a detekce hlasu. Okna v celé budově budou vybavena bezpečnostními detektory. Kamerový systém bude přebudován a detektory pohybu budou ukryty. Celý prostor před budovou bude oplocen a v noci osvětlen. Rovněž bude třeba zabezpečit telefonní a elektrické rozvody. Zaměstnanci budou pravidelně školeni v otázkách bezpečnosti. Ostraha objektu dostane nové taktické pokyny. Čipové karty budou vydávány při příchodu do budovy a odebírány při odchodu. Zpětně si Brian uvědomil, že i zabezpečení sítě není ideální, a rozhodl se provést několik dílčích změn. První z nich bude instalace několika honeypotů, což jsou systémy, které slouží jako návnada. Přiláká to tak mnoho útočníků a umožní sledovat jejich kroky. Je to lepší řešení, než se snažit zabezpečit celou síť nedobytně. Kdyby došlo k nějakému prolomení, byla by situace mnohem horší. Největší ponaučení, které si však Brian z akce odnesl, bylo, že fyzická bezpečnost je minimálně stejně důležitá jako bezpečnost programová. 3 0372/FEL ❑