Kybernetická bezpečnosť podnikových sietí

Bezpečnosť informačných či riadiacich systémov je nepochybne veľmi dôležitou súčasťou každého podniku. Zodpovední pracovníci si však nevedomosťou závažnosť tejto problematiky a nedostatočnými opatreniami vystavujú podnikové siete obrovskému nebezpečenstvu. Cieľom tohto článku nie je detailný rozbor tejto rozsiahlej témy, ale skôr základný náhľad na riziká a možnosti, ako im predchádzať.

Rizikové faktory

Rizikové faktory sa vo všeobecnosti rozdeľujú na vonkajšie, nezamestnať, vonkajšie a vnútorné. Klasický príklad je snaha zahraničnej prevádzať z vnútorného prostredia do firemnej siete a prísť tak o dôležité informácie.

Podľa štatistík však prichádza percentuálne k väčšinou počtu únosov z vnútra firmy vlastnými zamestnancami. A to je fakt, na ktorý sa veľkomyse zabúda. Zamestnanci väčšinou skúšajú, čo si môžu dovoliť. Ich snahy si často podporené softvérmi ľahko prekonajú bezpečnostné systémy. Ich motivácia môže byť rôzna, od nevinných hľadiu znalosť hackerských techník alebo pirátskeho softvéru a končiť spôsobením škody, ktorá sa bude počítať do milióna. Pre zamestnanca je situácia o to jednoduchšia, že so svojou zamestnať tým, ako sa prebrať cez bezpečnostné bariéry chránené prístup do siete z vnútorného prostredia. Má k dispozícii softvér, ani znalosti o fungovaní siete a to je prvý krok k úspešnému sabotážnemu. Základnými z vnútra firmy sa zaradiť do kategórie úmyselných útokov, to znamená, že pracovník si je dobre vedomý svojich nekalých zámerov.

K inému formám patrí neúmyselné zlúčkodcovstvo. Ide napríklad o prípad, keď administrátor pracuje na veľkom serveri omylom odstráni dôležitý súbor, ktorý vynaše poločica databázy. Riziko vzniknutia určitej spočíva tiež v omylu pracovníka dispozičného rozhodnutí prirovnávaní.

Ďalším rizikovým faktorom je hardvérová alebo softvérová porucha. Na tieto môže byť každý pripravený, ak používa kvalitné a overené komponenty. Pre hackera alebo softvéry však existujú rôzne spôsoby, ako využiť. Podobná situácia nastane aj vtedy, keď je zle nakonfigurovaná časť siete. Nesprávne nastavenie firewallu (nedbalosťou alebo nezmalosťou) spôsobuje dve samostatné pracujúce siete v rámci jedného podniku môže mať ľahšie dôsledky v prípade útoku hackera. Firewall je často používaný ochranný mechanizmus. Jeho funkcie je kontrola komunikácie na základe dopredu stanovených pravidiel, ktoré povoľuje alebo zakazuje prístup do siete.

N map

Ide o program využívaný hackermi na zistenie všetkých počítačových informácií o počítači vybranom na cieľ útoku. Zistí typ operačného systému, používané porty (ich otvorenosť či nepriepustnosť), softvér atď. Pôvodne bol koncipovaný ako unixový program, ale má aj windowsovskú verziu.

Program sa spúšťa na vzdialenom počítači hackera. Ak je však server správne chránený, sprostiť informácie nemožno získať. Dobre nakonfigurovaný firewall nie jeden z pravidiel, ktoré, ak je nastavené, zakazuje vybrané požiadavky prípojenia sa na firemný server z vonkajšieho prostredia. Firewall môže byť nainštalovaný priamo na unixovskom serveri alebo na inom počítači pred ním.

Návrh a ladenie bezpečnostných mechanizmov

Problematika nastavenia bezpečnostných mechanizmov v rámci podnikových sietí nie je otázkou hodín či dní, ale týždňov. Má svoju hierarchiu. Prvým krokom je analýza stavu siete. Na to existujú vyvinuté produkty, tzv. sniffery, ktorých úlohou je monitorovať celú komunikáciu v sieti (kto s kým, kedy, aké údaje sa prenášajú atď.). Na základe výsledkov monitoringov snifferov, informácií personálu zaoberajúceho sa celkovou koncepciou siete (majú detailné znalosti o jednotlivých subjektoch siete) a informácií z ďalších produktov, ktoré robia tzv. rizikovú analýzu (súbor otázok – desiatky až stovky, v závislosti od rozsiahlosti systému, na základe odpovedí na ne program vygeneruje odporúčania na zabezpečenie danej siete) možno navrhnúť príslušné zabezpečenie siete. Následné ladenie trvá v závislosti od jej rozmerov týždne až mesiace. Každopádne pri nastaveniach bezpečnostných prvkov treba zohľadniť aj používateľa. Sprísnenie bezpečnostných opatrení má zákonite negatívny vplyv na jeho komfort, pretože ho viac obmedzujú.

Používateľa možno takisto vybaviť bezpečnostnými prvkami, ktoré ho oprávňujú na vstup do podnikovej siete. Možností je neúrekom. Bežne používané a všeobecne známe je prihlasovanie heslom. Ďalšia z rozšírených alternatív je čipová karta. Tá sa vsunie do čítačky a po zadaní hesla je umožnený prístup do siete. V tomto prípade ide už o dvojstupňovú ochranu, pretože človek musí mať na prihlásenie fyzickú kartu (hardvérová ochrana) a musí vedieť heslo. Plejáda možností, ako zabezpečiť vstup len autorizovaným osobám, je skutočne bohatá. To, čo sa ešte nedávno mohlo zdať ako bujná fantázia hollywoodskych scenáristov, je dnes už skutočnosťou. A tak nie je nič výnimočné, keď je prístup realizovaný na základe odtlačku prstu, ruky, skenovaním očnej sietnice alebo kontrolou hlasu.

Komplexnejšou formou prihlásenia sú tzv. systémy single sign on (systémy jedného prihlásenia). Po zadaní prihlasovacieho hesla v kombinácii s kartou umožní systém používateľovi prístup do tých prostredí v sieti, do ktorých je autorizovaný bez osobitného prihlasovania.

Pri návrhu bezpečnostných mechanizmov sa nezabudlo ani na administrátorov. Podľa zaužívaných pravidiel by nemal byť administrátor systému ako takého tá istá osoba ako administrátor bezpečnosti. Dôvod je veľmi prozaický, aby aj administrátor systému podliehal kontrole. Rovnaká otázka sa vynára aj v súvislosti s administrátorom bezpečnosti. V prípade incidentu je štandardným riešením, že sa hlásenie o ňom neposiela len administrátorovi bezpečnosti, ale zväčša aj ďalším zodpovedajúcim osobám – priamym nadriadeným či pracovníkom vyššieho manažmentu. A to formou správy na pager, mobil alebo vykonaním inej akcie v závislosti od hardvérovej výbavy.

Druhy bezpečnostných produktov

Bezpečnostné produkty sa rozdeľujú do viacerých druhov. Za pasívne sa označujú také, ktoré zisťujú aktuálny stav systému (nainštalované softvéry, aktuálne záplaty na softvérové chyby, komponenty v konflikte s nastavenou bezpečnosťou,…). Aktívne zabraňujú, aby sa niečo stalo. Pomocou nich možno ošetriť aj prípad systémového administrátora, ktorý sa omylom môže dopustiť vážnej chyby. V ich réžii sú aj činnosti voči používateľom, ktorí sa úmyselne alebo neúmyselne pokúšajú o nepovolenú akciu. Alternatívy riešenia takýchto prípadov sú rôznorodé – odhlásenie páchateľa, poslanie sms, mailu, zablokovanie celej komunikácie, vypnutie služby, spustenie ďalšieho programu atď.

Produkty bezpečnosti zaznamenávajú každý incident a údaje o ňom ukladajú do vymedzeného priestoru zakódovaného prostredníctvom šifrovacieho kľúča. Navyše sú tieto produkty chránené voči neautorizovanému odstaveniu, resp. vypnutiu.

Ako doplnok k týmto aktívnym produktom je ešte prítomnosť ďalšieho počítača, ktorý všetky udalosti takéhoto charakteru ukladá do databázy a autorizovanej osobe v nej dovoľuje spätne listovať na základe zvolených kritérií (časových, lokalizačných, iných).

IDS – Intrusion detection system

Profesionálny softvér pracujúci na báze sniffera, ale s privilégiom aktívneho zasahovania. V prípade zakázanej komunikácie sú tieto softvéry schopné prerušiť spojenie alebo inak zareagovať. Častým javom je aj zálohovanie podozrivej komunikácie a jej následná analýza.

Prístupové práva a manipulácia s konkrétnym koncovým zariadením

Prístup na konkrétne koncové zariadenie (napr. riadiaci systém, PLC) v sieti sa dá vyriešiť správnym nastavením pravidiel a právomocí. Na prácu sú vyčlenení autorizovaní používatelia, ktorým možno presnými nastaveniami prísne vymedziť pole pôsobnosti. Predstavme si hypotetickú situáciu, že sa zariadenie spúšťa špecifickým programom. Možno zadefinovať, v akom časovom rozmedzí sa smie spúšťať, akou osobou či prostredníctvom čipovej karty alebo prihlásením z konkrétneho počítača, resp. prostriedku. Ak nebudú splnené niektoré z kritérií, prístup je zablokovaný.

Medzi ďalší doplňujúci mechanizmus bezpečnosti patria šifrovacie kľúče. Spojenie sa nadviaže až po ich vzájomnej výmene.

Napriek tomu, že prihlasovacích fáz je niekoľko, stále hrozí potenciálne nebezpečenstvo, že nastane manipulácia v systéme subjektom, ktorý by bol schopný prevziať identitu autorizovanej osoby. Do úvahy prichádza napr. použitie snifferu záškodníkom. Aj na tento prípad tvorcovia bezpečnostných mechanizmov zohľadnili a vymysleli tzv. jednorazové heslá. Ide o malé elektronické zariadenie s displejom – token, ktoré je časovo synchronizované so serverom. V presne stanovených časových intervaloch (napr. každých 30 sekúnd) sa generuje iné šesťciferné číslo, ktoré plní úlohu hesla. A aj to možno zadefinovať ako jednorazové, t. j. vo vymedzenom čase platí iba na jedno použitie. Získanie prístupového hesla sa dá navyše podmieniť ešte prístupovým kódom PIN k tokenu. Aby toho nebolo dosť, všetko zastrešuje šifrovaná komunikácia medzi tokenom a serverom.

Virtual Private Network (VPN)

Doslovný preklad je virtuálna súkromná sieť. Ide o mechanizmus, keď sa medzi dvoma zariadeniami vytvorí šifrovaná komunikácia, ktorú nikto iný nedokáže dekódovať. Princíp nadviazania komunikácie je takýto. Obe zariadenia majú k dispozícii verejný aj vlastný kľúč. Verejný kľúč každého z nich sa nachádza v sieti v špecifickom sektore na to vyhradenom a je voľne dostupný. Zariadenie, ktoré chce nadviazať komunikáciu s partnerským prístrojom použije jeho verejný kľúč na zašifrovanie obsahu dátového balíka. Odkódovať ho vie len adresát so svojím privátnym kľúčom.

Predstavme si modelový prípad servera a klientskej stanice. Obaja majú k dispozícii verejné kľúče a vlastné privátne kľúče. Prvým krokom je prihlásenie sa do systému, ktoré môže prebehnúť pomocou niektorej zo spomínaných foriem (čipová karta, heslá). Následne nastáva výmena verejných kľúčov a bezprostredne potom komunikácia, ktorá však prebieha výhradne iba medzi serverom a stanicou, keďže žiadne iné zariadenie nie je schopné čítať zašifrovaný obsah.

Najnovšie šifrovacie kľúče sa vyznačujú vysokou kvalitou. Podľa aktuálnych informácií sa ešte nevyskytol jediný známy prípad rozlúštenia kódu vytvoreného pomocou šifrovacích kľúčov.

Vírusy

Úsilie hľadať slabé miesta informačných systémov sprevádza ich vývoj prakticky od samého začiatku. Najväčšiu „popularitu“ si v priebehu času vydobyli vírusy a dlhé roky udržujú v neustálom strehu všetkých administrátorov informačných systémov. Pri zlom nastavení bezpečnostnej ochrany sú v podnikových sieťach schopné napáchať veľké škody. Líšia sa štruktúrou, funkčnosťou či závažnosťou. Z hľadiska princípu činnosti sa rozdeľujú do niekoľkých skupín.

Zaujímavosťou je, že veľká časť vírusov sa spolieha na hlúposť a naivitu používateľa. Typický príklad infiltrácie týchto programov je prostredníctvom elektronickej pošty. Súčasťou prichádzajúceho e-mailu je príloha, ktorá má lákavý názov, eventuálne je sprevádzaná textom, v ktorom používateľa navádza otvoriť prílohu tvrdením, že sa v nej nachádzajú pre neho nevyhnutné informácie. Úroveň vírusov je rôznorodá. Od jednoduchých a neškod-

Denial of service attack (DoS)

Technika spôsobujúca zahltenie servera nezmyselnými požiadavkami, vo väčšine prípadov vedúca k zrúteniu systému a jeho znefunkčneniu. Má takýto priebeh. Záškodník pošle na cieľový server napr. 50 000 žiadostí o službu za sekundu a napadnutému serveru zadá, aby odpoveď neposielal späť, ale na iné miesto (aj na identifikačnú adresu neexistujúceho zariadenia). Server po zodpovedajúcej reakcii čaká na odpoveď. Enormne stúpajúci počet požiadaviek napokon spôsobí, že napadnuté zariadenie je plne vyťažené čakaním a nereaguje na iné podnety. Záverečnou fázou je často pád systému. Tento mechanizmus sa nazýva synflood.

Cieľom hackera nie je v tomto prípade získanie údajov, ale znefunkčnenie zariadenia, ktoré, ak má priame spojenie s riadenou technológiou, môže viesť k fatálnym škodám.

Práčka vírusov, resp. mailov

ných, ktoré po aktivovaní zobrazia nejaké okno, obrázok či text a v skutočnosti nepredstavujú reálnu hrozbu. Oveľa rozšírenejšie sú vírusy vyznačujúce sa deštruktívnejším charakterom. Svoju dávku slávy si užili vírusy schopné fyzicky poškodiť počítač. Typickým príkladom sú tie, ktoré rozkmitajú hlavičky na harddisku vysokou frekvenciou a spôsobia ich odtrhnutie. V podobnom duchu je programovaná aj virtuálna pliaga, ktorá zníži otáčky ventilátora na procesore a spôsobí jeho prehriatie s následným poškodením.

Ďalšia odnož vírusov je už rafinovanejšia a prepracovanejšia. Vie monitorovať aktivity používateľa, zistiť softvérové, hardvérové vybavenie, prístupové heslá a odoslať ich na konkrétnu adresu po internete mailom alebo iným spôsobom.

Iný druh v prípade aktivácie na hostiteľskom počítači dokáže nadviazať spojenie s iným počítačom, ktorý následne nad ním získava plnú kontrolu. Ide o tzv. trójske kone. Tieto vírusy sú obzvlášť nebezpečné, pretože sú schopné obísť firewall, keďže nadväzujú spojenie z napadnutého počítača smerom von a navyše veľakrát cez komunikačné porty, ktoré slúžia na prístup k bežným webovým stránkam.

Ďalší typ sa dokáže aktualizovať z internetu na novšie verzie či seba samého morfovať podľa dopredu stanoveného algoritmu. Jednotlivé evolučné verzie sa zvyknú označovať príponou na konci mena, napr. Melissa.A, Melissa.B atď.

Najnovšie kolujú po svete mimoriadne zákerné druhy, tzv. trojan downloadery. Tie po aktivácii stiahnu na napadnutý počítač ďalších n vírusov, pričom číslo n je individuálne – môže byť aj niekoľko desiatok.

Mimoriadne náchylné na útoky vírusov sú predovšetkým produkty od firmy Microsoft. Živnou pôdou na jednoduché šírenie sa stal dobre známy Outlook, program slúžiaci na správu elektronickej pošty. V globálnom meradle je bez príslušnej ochrany najzraniteľnejší zrejme operačný systém Windows, ktorý ma sám o sebe veľký počet programových chýb. To sú hlavné dôvody, prečo väčšina strategických serverov vo firmách pracuje pod operačným systémom Unix, resp. Linux.

Vírusy sú schopné napadnúť počítače zapojené v kancelárskej sieti podnikovej štruktúry, ale len ťažko preniknú do prevádzkových sietí. Treba si uvedomiť, že takýto zákerný programátorský výtvor by musel mať v sebe zakomponovanú rozsiahlu bázu znalostí. Musel by poznať štruktúru siete, komunikáciu medzi jej súčasťami, heslá a množstvo ďalších podstatných položiek. Na prevádzkovej úrovni je skôr pravdepodobnejšie znemožnenie poskytovania služby, častejšie označované v anglickej jazykovej mutácii ako Denial of service attack (DoS).

Tradičná štruktúra pripojenia na internet autorizovanými používateľmi v podniku je presne stanovená. Ako ochranný prostriedok okrem firewallu sa používa aj tzv. práčka vírusov, resp. mailov. Kontroluje aktivity na internete, mailovú komunikáciu a program ftp (File transfer protocol), slúžiaci na výmenu súborov. Celá komunikácia teda najskôr prechádza firewallom, ktorý ju v prípade potreby presmeruje ďalej do práčky a až potom pokračuje k používateľovi.

Honeypots – hrnčeky s medom

Rafinovanosť nie je len výsadou sabotérov. V oblasti kybernetickej bezpečnosti sa takisto vynašiel prefíkaný spôsob, ktorý značne pribrzdí, resp. úplne eliminuje nekalé aktivity votrelca. Ide o mechanizmus, ktorý hackera odkloní do virtuálnej podnikovej siete vytvorenej na jednom výkonnom počítači. Ten simuluje prítomnosť všetkých prostriedkov bežných v sieti – od pracovných staníc cez servery až po tlačiarne. Je to vlastne návnada, ktorá oklame potenciálneho votrelca a po celý čas ho utvrdzuje v presvedčení, že sa mu podarilo preniknúť do podnikového systému. Za ten čas sa môže bezpečnostný administrátor venovať úplnému zablokovaniu útočníka, prípadne jeho vystopovaniu.

Honeypots môžu byť nainštalované v rámci štruktúry siete na rôznych miestach, prevádzkovú úroveň nevynímajúc a v podstate v ľubovoľnom počte, kde môžu simulovať prácu konkrétneho systému.

Zoskupovanie firewallov

V záujme zvyšovania úrovne bezpečnosti sa zvyknú firewally zoskupovať do väčších celkov. Zriedkavým javom nie je ani zapojenie štyroch firewallov v sérii (každý od iného výrobcu) na vstupe komunikačnej linky zabezpečujúcej spojenie podniku s okolitým svetom. Inou alternatívou je paralelné zapojenie firewallov, ktoré sú medzi sebou synchronizované.

Cisco router

V podstate inteligentný firewall (hardvérový), ale funkčne menej komplexný ako softvérový. Dokáže sa sám učiť a rozširovať vlastnú bázu znalostí. Vo firmách, kde sa pripojenie realizuje pomocou dial-up, pôsobí Cisco router ako prvý styčný bod. Vykonáva overenie používateľa (kódy PIN, kartičky atď) a iniciuje spojenie smerom do vnútra. Využíva sa hlavne pri neštandardných alebo zriedka využívaných riešeniach, keď sa linky pripájajú priamo do firewallu.

O jeho kvalite svedčí aj fakt, že doteraz nebol zaznamenaný jediný známy prípad narušenia jeho integrity hackermi s následnou zmenou konfigurácie.

Bežným riešením je v porovnaní s Cisco routerom obyčajný modem.

Konkrétny príklad zabezpečenia podnikovej siete

Spoločnosti uvedomujúce si závažnosť problematiky ochrany informačných systémov a údajov nešetria na financiách vkladaných do bezpečnostných mechanizmov. Uvedieme konkrétny, ale predsa len trochu extrémny príklad riešenia najdôležitejších sekcií podnikových sietí, ktoré sú vo svete pomerne bežným javom najmä v spoločnostiach disponujúcich citlivými a cennými údajmi.

Servery sú rozdelené do niekoľkých zón. Strategické servery sú fyzicky oddelené od ostatných častí firemnej siete a lokalizované v osobitnej miestnosti. Serverovňa a chodby vedúce do nej sú nepretržite monitorované priemyselnou kamerou. Vstup do miestnosti je možný len cez pancierové dvere. Priestor miestnosti je obohnaný hrubými a masívnymi múrmi. Vstup je možný, samozrejme, len autorizovaným osobám prostredníctvom bezkontaktnej karty. Vchádza sa do dverí v tvare valca, ktoré sa po vstupe zatvoria. Potom prebieha kontrola hmotnosti, aby sa v priestore náhodou nenachádzali dve osoby. Po splnení všetkých kritérií sa umožní vstup do serverovne. Niektoré spoločnosti považujú svoje údaje za príliš cenné, a preto si zriaďujú tzv. paralelné alebo záložné pracoviská, ktoré sú identickou kópiou riadiaceho, prípadne informačného centra. Všetky údaje sa duplicitne ukladajú v jednom aj druhom systéme. Obe pracoviská môžu byť vzdialené od seba na desiatky či stovky kilometrov. Táto forma zálohovania sa využíva ako preventívne opatrenie v prípade živelnej katastrofy, teroristického útoku či inej udalosti, ktorá by mohla spôsobiť nezvratnú stratu údajov.

Hardvérové firewally

Jeden z najkvalitnejších a najuznávanejších na svete je od firmy Nokia. Fínsky gigant vyrába viac typov v závislosti od náročnosti, vybavenia, požadovanej priepustnosti. Je to forma čiernej skrinky, ktorú inštalujú na mieste určenia autorizovaní pracovníci. Pracuje pod operačným systémom Linux, čo je prvý predpoklad odolnosti voči útokom. Nainštalovaným komponentom je softvérový firewall. Ide vlastne o jednoúčelové zariadenie, ktoré vykonáva iba požadovanú činnosť. Ak má plniť funkciu firewallu, žiadne iné aktivity nevykonáva. Má modulárnu štruktúru so základným vybavením, ktoré sa voliteľne dopĺňa podľa požiadaviek. Šifrovanie je realizované hardvérovo, keďže je vždy rýchlejšie ako softvérové, pretože nezaťažuje procesor. V minulosti uskutočnil jeden z renomovaných svetových časopisov priamo v laboratóriách spoločnosti Nokia test spoľahlivosti najvyššieho radu tohto zariadenia, ktorého cieľom bolo jeho znefunkčnenie. Firewall sa napokon nepodarilo znefunkčniť ani pri extrémnom zaťažení.

Ochrana pracovných staníc

Pracovnú stanicu možno zabezpečiť podobným spôsobom ako server. Prihlásenie na ňu sa dá realizovať takisto hardvérovým prostriedkom (token, čipová karta). Po nainštalovaní operačného systému sa stanici pridelia príslušné právomoci a vykoná sa tzv. slap shot. To znamená, že z každého nainštalovaného softvéru sa vygeneruje na základe algoritmu jedinečný číselný identifikátor (hash), ktorý je nositeľom informácie aj o povolení využívať konkrétny program. V prípade napadnutia vírusom a zmeny programov v takej miere, že sa modifikuje aj hash, zaniká povolenie na spustenie programu.

Vo svete je činných niekoľko spoločností, ktoré vystavali svoju výbornú povesť na produktoch zabezpečujúcich ochranu počítačov a podnikových sietí. Okrem už spomenutých Cisco či Nokia patria medzi renomované firmy Symantec (www.symantec.com), Computer Associates (www.ca.com) alebo Internet Security Systems (www.iss.com).

Problematika kybernetickej bezpečnosti je veľmi rozsiahla a vďaka snaživosti sabotérov neustále aktuálna. Priestor niekoľkých strán článku ju zďaleka dostatočne neosvetľuje, ale to nebolo ani naším zámerom. Vzhľadom na svoju závažnosť si zaslúži veľkú pozornosť, pretože akékoľvek zanedbanie bezpečnostných opatrení vedie väčšinou k nepríjemným finančným stratám. O nespornom význame tejto problematiky svedčí aj skutočnosť, že v bežnej praxi sa jej venujú niekoľkotýždňové školenia.

Branislav Bložon