Kapitola 5

Bezpečnost koncových zařízení

Po prostudování kapitoly budete znát:

- základní principy při stanovení bezpečnostní politiky;
- nezbytné bezpečnostní požadavky, které je nutné při řešení bezpečnosti v koncových zařízeních dodržet;
- pojmy firewall, antivirový SW, IPS, IDS;
- způsoby správy zranitelností informačního systému;
- specifika při zajištění bezpečnosti mobilních zařízení.

Klíčová slova:

Antivirová ochrana, IPS, IDS, správa zranitelnosti, SCADA.

5.1 Bezpečnostní koncepce, bezpečnostní politiky, bezpečnostní opatření

Informační technologie přináší do programu informační bezpečnosti řadu aktuálních otázek. Kromě toho rychlý rozvoj informačních technologií má zásadní vliv na efektivnost realizovaného bezpečnostního programu. Většina nastolených otázek vychází z důležitého faktu – že samotná technologie tyto požadavky a problémy nevyřeší, navíc stávající bezpečnostní opatření mohou být u nových informačních technologií neúčinná. Na druhé straně při přecenění možností technologií (deklarovaných v bezpečnostních parametrech daného produktu) se snadno přijme nesprávné rozhodnutí, které často přivede podnik do situace, kdy musí hledat opatření proti zbytečně vzniklým rizikům.

Ze systémového pohledu plyne nutnost řešit na úrovni technologií zejména následné požadavky:

- autentizace, autorizace, správa uživatelských účtů;
- firewall; VPN;
- antivirová ochrana;
- správa rizik;
- správa detekce narušení systému;
- filtrování obsahu dat;
- šifrování.

5.1.1 Firewally

Firewally tvoří "elektronický" obvod kolem podnikového počítačového prostředí. Brány firewall mají filtry, které umožňují přivádět pouze určité typy síťové komunikace do sítě podniku a zabránit přístupu jakýchkoli dalších dat, které nesplňují kritéria bezpečnosti, autenticity apod. Tímto způsobem vytvářejí firewally základní bezpečnostní propust na přístupu do podnikového informačního systému.

Při návrhu nasazení firewallů do podnikového prostředí je třeba uvažovat s kompromisem mezi rychlostí a úrovní zabezpečení. Firewally lze kategorizovat takto:

- filtrování paketů firewally;
- stavové firewally;
- ochranné metody na aplikační vrstvě nebo proxy serveru.

Metody ochrany v firewallech využívající filtrování paketů ověřují záhlaví, resp. informaci o adrese, paketu nebo zprávy pro identifikaci potenciálních problémů, na základě nastavených pravidel je buď příchozí paket blokován nebo propuštěn.

Stavové firewally sledují stav transakce, aby ověřily, že cíl příchozího paketu odpovídá zdroji a předchozímu odchozímu požadavku. Firewall kontroluje souvislost příchozích paketů proti předchozím odchozím paketům, aby byla určena jejich legitimitu. Firewall využívá korelaci s tabulkou stavových připojení a oproti paketovému firewallu zkoumá kontext datových paketů, tj. zdrojové a cílové adresy zprávy, spíše než jejich filtrování.

Nejbezpečnější firewall, jsou firewally na aplikační vrstvě nebo firewally na proxy serveru. Firewall analyzuje obsah příchozích paketů podle výsledků analýzy rozhoduje, zda budou do sítě propuštěny pouze platné zprávy. Jedná se o nejbezpečnější způsob filtrování, neboť je obtížné napsat do datové části paketů nevhodný obsah. Nevýhodou je, že tento proces snižuje významně propustnost. Existuje několik variant těchto řešení firewallu, kdy před aplikační firewall je předřazen paketový firewall, aby byla zátěž aplikačního firewallu, který zpracovává jen filtrované pakety. Představitelem aplikačních firewallů je proxy firewall, zde všechna data prochází vždy přes proxy server, který je podle nastavených podmínek filtruje. U tohoto typu aplikačního firewallu je výhodou, že jsou skryty zdrojové adresy uživatele, neboť je za něj je uvedena aplikační brána.

5.1.2 Antivirový software

Stejně jako u lidí i v elektronickém prostředí je nezbytné se chránit proti virům. Antivirový software pomáhá zabránit infikování počítačů škodlivým SW (počítačovými viry, červy, trojskými koni apod.). Souhrnně lze vymezit jako ochranu proti malware. Vzhledem k tomu, že každý den přibývají stovky nových typů škodlivého SW, je nezbytné a povinné aktualizovat antivirový software pravidelně s novými definicemi virů.

Navíc útoky jsou v průběhu let mnohem propracovanější a v dnešní době je mnohem snazší, aby malware infikoval vaše počítače, než tomu bylo v minulosti, neboť nový škodlivý SW, využívá současně několik různých zranitelností systému a vytváří nové formy pro své rozšiřování. Tyto hrozby vedly bezpečnostní průmysl k vývoji nástrojů, které pravidelně automaticky vybírají definice virů, často jednou za den, aby rychle a efektivně zabránily nákazám. V případě, že škodlivý kód infikuje počítač, dodavatelé zabezpečení nabízejí nástroje, které odstraňují infekce z počítače a pokoušejí se vyčistit jakékoli poškození způsobené virem.

Antivirový software je požadovanou součástí programu zabezpečení informací kvůli rostoucímu počtu virů. Pouze s implementovaným antivirovým software (doporučuje se od několika výrobců) lze přistoupit k bezpečnému využívání Internetu. Antiwirový software musí poskytovat komplexní

ochranu proti všem typům hrozeb v prostředí sítě Internet. Proto výrobci bezpečnostního softwaru dodávají „balíky“ antivirového programu, pokrývajícího známé spektrum škodlivého SW.

5.1.3 Vulnerability management – správa zranitelnosti

Řízení chyb zabezpečení je způsob, jak aktivně odstranit nedostatky z programu zabezpečení informací. Efektivní bezpečnostní program využívá nástroje pro automatickou správu chyb zranitelnosti pro identifikaci možných zranitelností v podnikovém informačním systému. Nástroje pro správu zranitelnosti porovnávají prostředí s databází známých zranitelností a kontrolují, jaká zranitelná místa obsahuje podnikové informační prostředí.

Existují dva typy nástrojů správy zranitelnosti: síťové a hostitelské. Pomocí nástrojů založených na síti můžete naskenovat síťovou komunikaci, abyste zjistili známá zranitelná místa a nástroje hostitele pro skenování fyzických zařízení, například počítačových serverů.

Vzhledem k narůstajícímu počtu zranitelných míst je třeba zajistit aktuální záplatování (patching) informačních programů. Jedná se o složitý úkol, neboť záplaty musí být před jejich aplikací testovány, což v případě velkých podniků, s rozsáhlým informačním prostředím (velký počet aplikací, serverů a uživatelů) vyžaduje systematický přístup, který musí být zakomponován do business procesů podniku.

Pravidelný a řízený program skenování zranitelných míst informačního prostředí a systém řešení potřebných oprav musí být součástí zajištění odpovídající úrovně bezpečnosti daného podniku. Z tohoto důvodu se do informačního prostředí začleňuje SIEM. Technologie správy chyb je tedy důležitou součástí systému řízení bezpečnosti informací. Tyto nástroje vám umožňují proaktivně identifikovat zranitelná místa a provést potřebná proaktivní bezpečnostní opatření.

5.1.4 IDS – Detekce narušení

Systémy detekce narušení (IDS) monitorují provoz a události v síti a v podnikových informačních systémech kde zjišťují příznaky možného útoku, či informace o útocích, které byly provedeny. Stejně jako v případě řízení zranitelnosti, nástroje pro detekci narušení lze zajistit ve dvou režimech, tj. v síťovém nebo hostitelském prostředí,

Nástroje založené na síti aktivně vyhledávají provoz na klíčových částech vaší sítě a hledají možné útoky.

Nástroje hostitele pracují na serverech a kontrolují informace o auditu nebo záznamu, aby detekovaly možné útoky. Protože vyhodnocování datového protokolu může být náročné na zdroje, mohou tyto nástroje negativně ovlivnit výkon serverů. V daném případě nutné průběžně sledovat „propustnost“ informačního systému, ale při jejím snížení nelze řešit danou situaci vypnutím nástrojů detekujících narušení.

Tyto nástroje se opírají o dvě metody identifikace narušení: rozpoznávání založené na popisu a detekci anomálií.

Rozpoznání založené na popisu porovnává určité vzorce činností s neznámými scénáři útoku.

Nástroje detekce narušení založené na popisu rozpoznávají vzorky nebo příznaky nestandardní činnosti. Zde detekce nestandardní situace závisí na určení vzorků pro normální chování a poté na zjištění chování, které se liší od normy.

Obě tyto metody musí reagovat na vysoký stupni variability kontrolovaného prostředí a určit co jsou standardní situace a čím může útočník disponovat.

5.1.5 IPS – prevence narušení

Typické podnikové sítě bývají připojeny k několika vnějším sítím. Vzdálené pobočky lze k centrální síti připojit pomocí různých technologií (pevné linky, DSL, různé typy VPN…), čímž vznikne rozlehlá síť. Vzhledem k různorodosti možných útoků není možné řešit bezpečnostní perimetr podniku pouze s využitím firewallů, ale je nezbytné navrhnout bezpečnostní zóny, které bezpečnostní nástroje strukturují s oddělením na jednotlivé oblasti – Internet, DMZ (demilitarizovaná zóna, Intranet aj.). Musí být nastavena pravidla pro přenos dat, přičemž základní pravidla jsou nastavena na firewallu. Na přenos a kontrolu kritických dat jsou určeny systémy detekce a prevence narušení (IDS/IPS systémy.

IPS systémy, stejně jako IDS systémy se dělí na síťové a hostitelské. Pro obě kategorie je společné sledování systému, schopnost upozornit administrátora na případný útok a provést bezpečnostní záznam (logu).

Hostitelské systémy se nasazují přímo na jednotlivé stanice nebo servery. Jedná se o softwarové produkty a jsou tudíž omezeny podporou pro OS na dané stanici. Monitorují systémová volání, logy a podobně. Chrání před útoky na OS a aplikace. Síťové systémy jsou specializovaná zařízení pro monitorování dění na síti.

Systém prevence narušení (IPS) je schopný útoky zároveň detekovat a reagovat na ně (tj. zabránit útoku nebo ho přerušit). Jsou zde nastaveny 2 druhy monitoringu“:

- útok na aplikace škodlivým SW;
- útok z Internetu – DoS, DDoS útoky.

Porovnání IPS a IDS

IPS, díky možnosti připravovat reakci na útoky, umožňují spolehlivější způsob ochrany. Tato reakce však může mít i negativní dopad. Jedná se o tzv. plané poplachy. V souvislosti s tím může odpojit oprávněného uživatele nebo zcela zablokovat síťový provoz na daném síťovém segmentu.

Některé IDS systémy dokáží, za spolupráce s firewallem, který dynamicky mění svoji politiku tak, aby zamezil komunikaci vyhodnocenou jako útok, také reagovat na útok.

Systémy detekce a prevence narušení jsou realizovány jako specializovaná zařízení, která jsou spravována z centrálního řídicího systému.

5.2 Vynucování bezpečnostních opatření na aplikační úrovni

Nejčastějšími útoky na aplikační vrstvě jsou útoky na webové služby a elektronickou poštu. Proti útokům na web se lze bránit jeho audit detekcí průniků, řízením přístupu, autentizací, elektronickými podpisy (včetně DBP) a šifrováním. Elektronickou poštu je třeba chránit šifrováním a elektronickými podpisy.

Na aplikační úrovni jsou útoky založeny zejména na přepisování webových stránek, odcizení a falšování pošty, využití phishingu apod. Jsou tak využívány nedostatky v navržených bezpečnostních opatřeních – příliš obecná bezpečnostní politika a s tím spojené nesprávná správa hesel, nedostatečně nastavené bezpečnostní komponenty nebo i nezodpovědní uživatelé.

Na aplikační úrovni se jedná zejména o útoky odmítnutí služby typu DoS (Denial of Service) a DDoS (Distributed Denial of Service). Termín DoS označuje útok, jehož cílem je zabránit oprávněným uživatelům v přístupu ke službám výpočetního systému, anebo alespoň tento přístup zpozdit. Termín DDoS označuje útok na internetovou službu či webovou stránku, jehož cílem je zahltit servery obrovským množstvím požadavků, a způsobit nedostupnost tohoto serveru i pro oprávněné uživatele.

Některé typy těchto útoků:

Ping-of-Death (smrtící ping) - použití paketů delších než 65 535 bajtů povolených IP specifikací, přičemž při jejich přijetí dojde k přetečení vyhrazené paměti.

Teardrop – využití IP fragmentů. V případě, že počítač útočníka generuje fragmenty, jejichž délka neodpovídala údaji v záhlaví, operační systémy neumí nesprávný fragment zpracovat.

Smurf attack – útočník vyšle záplavu pingů, které následně směrovač rozhlásí v cílové síti. Pokud ještě útočník uvede v IP záhlaví pingu adresu cizího odesilatele, zaplaví se odpověďmi ještě další síť.

V současné době jsou vedeny útoky typu Distributed Denial of Service (DDoS), které využívají útoků spuštěních z mnoha navíc cizích zdrojů, což neumožňuje lokalizovat útočníka.

5.3 Bezpečnost mobilních zařízení – zabezpečení a autentizace

Bezpečnostní problémy vzniknou vždy, když k datovým zdrojům získají přístup neoprávněné osoby, nebo když uživatelé překročí úroveň jim definovaného přístupu k daným systémům.

V rámci Informačních technologií lze využít metod pro kontrolu přístupu do informačních a komunikačních systémů k regulování přístupů uživatelů tak, aby se chovali ve shodě s jejich potřebami a ve vymezených oblastech. Důležité je, aby při realizaci bezpečnostního programu byla u této problematiky dána do souladu bezpečnostní opatření s hodnotou chráněných informací.

5.4 BYOD, IoT – kontrola a monitoring

V současné době dochází k významnému problému zabezpečení tzv. koncových bodů. Počítačová infrastruktura podniků bývá často zabezpečená, její slabá místa však představují vypalovací zařízení, tiskárny, média USB, laptopy uživatelů či chytré mobilní telefony. Slabými místy jsou také „chytré“ produkty, kdy důvodem jejich nasazení je automatizace rutinních činností, ať u v domácnostech (ledničky, pračky, topení), ale v podnikové struktuře, řízená vzdáleným přístupem přes Internet, který

sebou přináší nové bezpečnostní hrozby. Jedná se o nový fenomém IoT (Internet věcí) A v neposlední řadě rychle se rozšiřující BYOD, tedy využívání zařízení uživatele v podnikové síti, přičemž v tomto zařízení není instalována podniková „image“.

5.5 Bezpečnost průmyslových systémů (SCADA, PLC)

Údaje získané ze senzorů monitorujících bezpečnostní údaje je třeba zpracovávat nebo připravit k revizi určenému operátorovi. Data ze senzorů je lze zobrazit při sejmutí v jejich formátu, tj. v tabulce jako sled měření s časovou značkou. Údaje v takové formě však jsou odpovědnou osobou obtížně interpretovatelné, proto jsou tyto údaje před jejich zobrazením převedeny do jednodušší formy umožňujícími jejich vizualizaci.

K tomuto účelu jsou využívány tzv. systémy SCADA (Supervisory Control and Data Acquisition). SCADA systémy tvoří další vrstvu v logice průmyslové automatizace. Nejnižší vrstvu tvoří PLC automaty regulující proces v reálném čase. Systém SCADA, jelikož údaje musí, načíst (obvykle po síti), zpracovat a zobrazit, pracuje ve „skoro“ reálném čase. Je důležité si uvědomit, že SCADA systém informace nezískává přímo ze senzorů (prostřednictvím PLC), ale z definovaného místa, zejména z výkonného databázového serveru. Tyto servery jsou označovány jako real-timové databáze. Lze uvažovat i o přímém propojení SCADA – PLC přitom je však nutné uvažovat s tím, že PLC je přizpůsobeno regulaci, ale není schopna poskytovat informace v podobě srovnatelné s relační databází. Výhodou však je, že je jednoduché nastavit, aby PLC použil jako úložiště dat nějaký databázový server (spojení PLC – databáze) a propojit tento server se systémem SCADA (databáze – SCADA).

Kapitola pojednává o základních principech při stanovení bezpečnostní politiky a bezpečnostní strategie. Studenti jsou seznámeni s nezbytnými bezpečnostními požadavky, které je nutné při řešení bezpečnosti v koncových zařízeních dodržet. Jsou probírány bezpečnostní komponenty a metody jako je firewall, antivirový SW, IPS, IDS. Je probírána otázka správy zranitelností informačního systému. A na druhé straně jsou zde uvedeny základní vlastnosti systému SCADA.

1. Co znamená pojem IDS a jaký je rozdíl mezi IDS a IPS?
2. Vysvětlete princip SCADA.
3. Co znamená antivirová ochrana, jak lze charakterizovat škodlivý SW?
4. Co znamená správa zranitelnosti?

Literatura k tématu:

[1] ., SMEJKAL, V., Rais, K. *Řízení rizik ve firmách a jiných organizacích.* 4., aktualizované a rozšířené vydání. Praha: GRADA, 2013, 488 str., ISBN 978-80-247-4644-9