Kapitola 4

Bezpečnost v síti Internet

Po prostudování kapitoly budete umět:

- orientovat se v pojmu bezpečnostní protokol;
- realizovat bezpečnou e-mailovou komunikaci;
- vysvětlit specifika bezdrátové komunikace
- popsat přístup k realizaci VPN

Klíčová slova:

Bezpečnostní protokoly, VPN, Wifi, e-mail.

4.1 Bezpečnostní protokoly

Internet obsahuje obrovské množství informací, z nichž většina je užitečná a vhodná pro všechny uživatele. Na druhou stranu se internet ukázal být účinným prostředkem pro šíření nevhodného obsahu (např. pornografie) i rozmanitých typů škodlivého SW – od jednoduchých virů až sofistikované „trojské koně“, nebo vyděračských programů typu ransomware. Nástroje filtrování obsahu mohou tyto informace filtrovat a zajistit, aby uživatelé k nim nemohli jednoduše přistupovat.

Dvě hlavní kategorie nástrojů zahrnují filtrování webových (internetových) a e-mailových adres. Filtrování Internetu lze použít k zablokování zobrazení určitých webových stránek, které obsahují nevhodný obsah. Filtry na Internetu se odkazují na databáze známých webových adres nebo adres URL s nevhodným obsahem. Webové filtry musí pravidelně aktualizovat databázové adresy URL, protože firmy, které spravují nevhodné weby, při eliminaci blokování svých webových adres, často mění adresy URL nebo název webu. Webové filtry také používají klíčová slova, která jsou považována za nevhodná, a blokují přístup k těmto stránkám a zprávám.

Spam je dnes obrovský problém a může v případě standardního podniku vytvářet až polovinu e-mailových přenosů. Filtrování e-mailů je podobné filtrování webových stránek a může zablokovat nevhodné a nevyžádané komerční e-maily.

Bohužel tyto nástroje jsou dnes reaktivní a spoléhají se na databáze známých webových stránek nebo e-mailových adres k filtrování obsahu. K dispozici jsou i sofistikovanější nástroje, které se také spoléhají na heuristiku, aby identifikovaly tyto zprávy a odstranily je. Stejně jako u jiných heuristických metod, které však ještě nejsou dost spolehlivé.

Před implementací nástrojů filtrování obsahu je třeba zvážit jak právní aspekty, tak i požadavky uživatelů. Kategorie, jako je pornografie, nenávist a hazard, jsou snadno filtrovány, ale jiné kategorie, jako je nakupování online, mohou vyžadovat mnohem větší analýzu nastaveného filtrování. Pokud se program filtrování stává příliš náročným, mohou např. uživatelé – zaměstnanci podniku pociťovat výrazné omezení, které zasahuje i do jejich pracovního procesu (vyhledávání obchodních příležitostí aj,).

Filtrování obsahu je důležitou složkou informační bezpečnosti kvůli značným dopadům produktivity spamu a používání (a zneužívání) webových stránek zaměstnanců při práci. Při vytváření strategie filtrování obsahu je nutné pečlivé zvážení právních a personálních otázek.

4.2 Bezpečná e-mailová komunikace

Autentizační systémy používají pro autentizaci protokoly pro vyhodnocování přenášených zpráv s určením, zda jsou oprávněné, nebo na druhé straně škodlivé či určené k neoprávněnému průniku do podnikového informačního systému. Protokoly vycházejí ze stanovených pravidel, kde je definováno, zda je zpráva v souladu se stanovenými parametry a může být považována za autentickou.

Mezi tři základní protokoly, které se využívají pro autentizaci, patří protokoly Kerberos, RÁDIUS a 802.1x:

- Bezpečnostní systém Kerberos-A vyvinutý na MIT, který autentizuje pouze uživatele. Neuděluje povolení službám nebo databázím; zjišťuje identitu při přihlašování k použití během celé relace. Tento systém je využíván v prostředí jako jsou Novell NetWare a Microsoft Windows
- RÁDIUS (vzdálená autentizační volba uživatelské služby) - autentifikační protokol, který používá ověřovací metodu autentizaci vzdálených uživatelů. Využívá se pro zaměstnance, kteří vyžadují vzdálený přístup a je nutné identifikovat pracovní stanice, který používají, nestačí pouze uživatelské jméno a heslo, protože tento typ autentizace může být snadno zneužit a možnost neoprávněného přístupu je významná.
- Bezpečnostní protokol 802.1x-IEEE pro drátové sítě a bezdrátové místní sítě, které dodržují standard 802.11. Spoléhá na protokol Extensible Authentication Protocol (EAP) pro předávání zpráv některému z různých ověřovacích serverů, jako je například RÁDIUS nebo Kerberos.

4.3 Bezdrátové sítě

Bezdrátové sítě představují nové úkoly v zabezpečení informací. Bezdrátová technologie umožnila uživatelům se připojit přímo k jejich sítím místo toho, bez nutnosti využití síťových kabelů; tento trend bude v budoucnosti nadále růst. Vzhledem k tomu, že tato technologie byla nejprve vyvinuta pro jednotlivé uživatele pro osobní použití, a ne pro případy podnikových komunikací, byly vyšší priority kladeny na snadnost použití místo zabezpečení komunikovaných dat. Bezdrátová zařízení tedy nebyla navržena s cílem používat při přenosu dat šifrování, a dodatečně navrhované komunikační technologie často vykazovaly slabiny.

Ověřování nebo možnost určit, kdo se pokouší o přístup k systémům, je také omezeno bezdrátovou technologií a nemá měřítko na úrovni vstupů. Je také snadné, aby někdo připojil neoprávněné bezdrátové zařízení do firemní sítě, čímž dochází k možnosti neoprávněného přístupu do podnikového informačního prostředí, které může neoprávněný uživatel využít k získání přístupu k podnikovým zdrojům. Bezdrátový přístup (Wifi) a používání mobilních zařízení (smartphone), jakož i BYOD představují pro program zabezpečení informací nové úkoly.

4.4 Virtuální priváte sítě (VPN)

Nástroje VPN umožňují vytvořit bezpečné připojení mezi dvěma lokalitami pomocí veřejné sítě, jako je například Internet. VPN používá šifrování pro ochranu dat, a vytváří tak zabezpečený „tunel“ pro přenášená data, čím je chrání před neoprávněným přístupem nepovolaných osob. Připojení s využitím VPN vytváří zabezpečený spoj, který umožňuje propojit autorizované osoby, které chtějí vzdáleně přistupovat k podnikovému informačnímu prostředí, jako je například systém firemního e-mailu, nebo podnikovým serverům.

Pro vytvoření tohoto spojení VPN se používá kombinace hardwaru a softwaru. Jedná se nákladově efektivní způsob zabezpečeného rozšíření podnikového informačního systému ve srovnání s klasickou metodou využívající pronajaté linky.

Kapitola je orientovaná na realizaci bezpečnosti v nezabezpečeném komunikačním prostředí – Internetu. Jsou zde probrány základní charakteristiky bezpečné e-mailové komunikace. Jsou vysvětleny pojmy jako je VPN, Wifi.

1. Jaké jsou typy bezpečnostních protokolů, jaké jsou jejich charakteristiky?
2. Co znamená filtrování webových stránek?
3. Jak je řešena bezpečnost při komunikaci v prostředí Internetu?
4. Lze realizovat bezpečnost v prostředí Wifi?

Literatura k tématu:

[1] ŠENOVSKÝ, P. *Bezpečnostní informatika 1* [online]. 8. vydání. Ostrava: VŠB-TU Ostrava, 2017, 127 str. Dostupné z < http://homel.vsb.cz/~sen76/CMS/data/uploads/skripta/bi1_8ed_fin.pdf >.