IT bezpečnosť automatizačných a SCADA systémov (3)

Základné sieťové architektúry na oddelenie technologickej siete

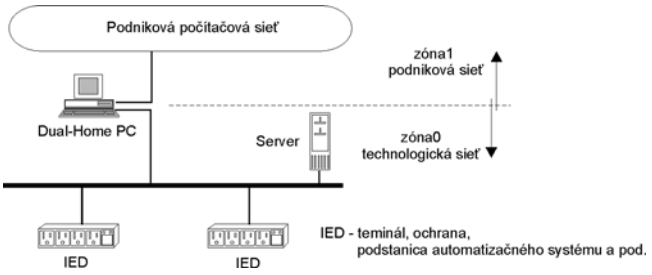
Z množstva architektúr používaných na vzájomné oddelenie sietí možno vybrať niekoľko základných typov, ktoré sú viac alebo menej vhodné pre oddelenie technologických informačných sietí pre automatizačné a SCADA systémy od podnikových informačných sietí. Opíšeme aj tie, ktoré sú menej vhodné, avšak paradoxne často navrhované, s cieľom upozorniť na riziká ich implementácie.

A. Oddelenie sietí pomocou zariadenia s dvoma sieťovými kartami

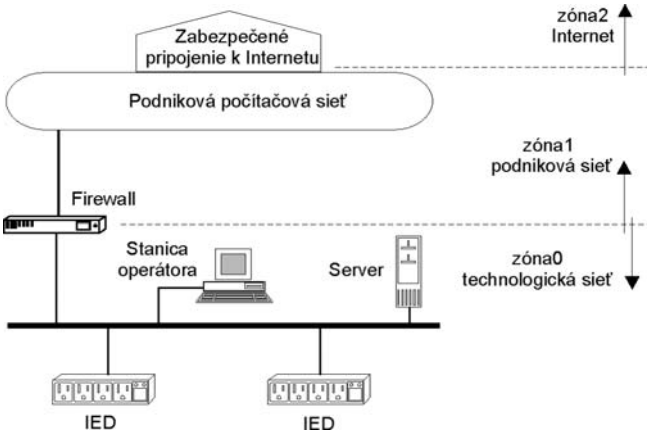
Táto sieťová architektúra nazývaná Dual-Home predstavuje najbežnejšie používané riešenie prepojenia dvoch sietí a je zložená na princípe použitia dvoch sieťových kariet v zariadení, ktoré vyžaduje prístup k podnikovej aj technologickej sieti (pracovná stanica, server a pod.) (obr. 2). Ponúka však minimálnu ochranu, pretože možno veľmi jednoducho upraviť sieťovú konfiguráciu tak, že cez dané zariadenie prechádzajú pakety bez obmedzenia, a naviac, ak dôjde k prelomeniu ochrany zariadenia s dvomi sieťovými kartami, ohrozené sú obidve siete. Alternatívou je doplnenie počítača dvoma sieťovými kartami o softvérový firewall, čo toto riešenie vylepšuje len zdanlivo. Od stupňa použitých pravidiel nastavených na firewall-e totiž závisí nielen stupeň zabezpečenia, ale aj dostupnosti technologickej siete. Väčšina firewall-ov tohto typu neobsahuje dokonalé nástroje na skúmanie paketov (stateful inspection), majú obmedzenú detekciu narušenia (IDS – intrusion detection system) a malý výkon. Navyše táto architektúra porušuje jedno zo základných pravidiel bezpečnosti – technologická sieť nesmie byť priamo prepojená s inou sieťou. Z týchto dôvodov je toto riešenie najmenej bezpečné a na prepojenie dvoch sietí, ktoré majú byť z hľadiska bezpečnosti izolované, by sa nemala používať.

B. Oddelenie sietí pomocou firewall

V tejto architektúre sú vytvorené izolované sieťové domény pomocou firewall-u, ktorý je umiestnený na rozhraní podnikovej a technologickej siete (obr. 3). Ak je podniková sieť pripojená k ďalšej sieti, napr. internet, je nevyhnutné zabezpečiť izolovanie podnikovej siete od okolia vhodným spôsobom s dostatočnou úrovňou zabezpečenia. Konfigurácia firewall-u by mala umožniť prístup len k vybraným serverom a službám v zóne0 a opačne len vybrané zaradenia a služby zóny0 by mali mať povolenú komunikáciu so zónou1. Zo zóny0 nesmie byť povolený prístup do siete internet alebo prijímanie e-mailov. Ak firewall obsahuje funkciu podrobného skúmania paketov a detekciu narušenia a je agresívne konfigurovaný, potom toto riešenie zabezpečuje pomerne vysokú bezpečnosť, a preto býva často používané ako základné riešenie na ochranu siete. Slabinou tejto architektúry je však to, že v súbore pravidiel firewall-u treba nechať otvorené miesta na komunikáciu so servermi, čo možno využiť pri útoku, ktorý využíva napr. maskovanie dát (packet spoofing). Alternatívou tejto architektúry je zaradenie router pred firewall (obidva môžu byť aj súčasťou jedného zariadenia), čo síce nezvýši bezpečnosť, ale zlepšuje výkon celej sústavy. Router zabezpečuje základnú filtráciu paketov a odľahčuje za ním umiestnený firewall, ktorý zabezpečuje sofistikované služby.



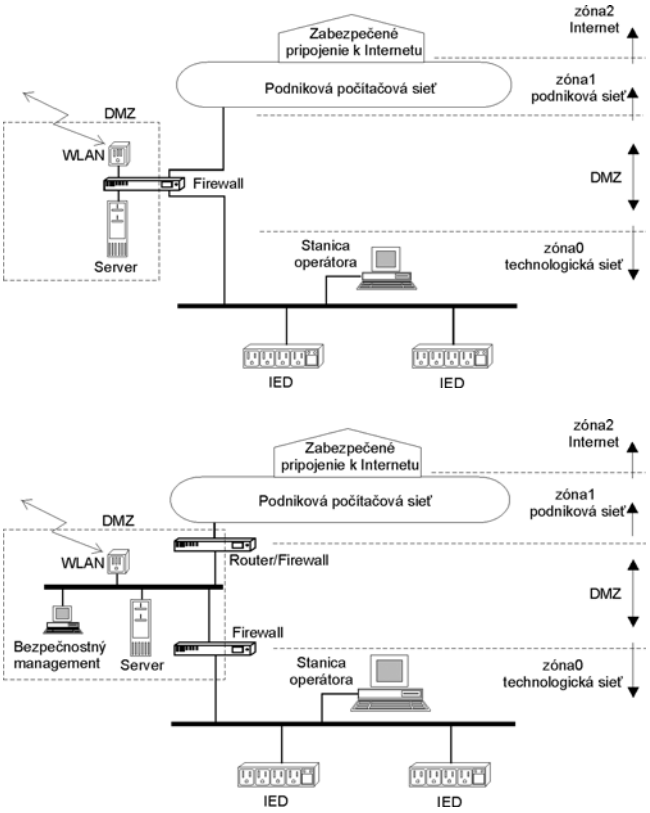
Obr.2 Sieťová architektúra Dual-Home



Obr.3 Oddelenie sietí pomocou firewall

C. Oddelenie sietí pomocou DMZ

Vytvorenie demilitarizovanej zóny (DMZ) na rozhraní podnikovej siete a siete automatizačného systému podstatne zvyšuje úroveň zabezpečenia zóny0. V demilitarizovanej zóne sú umiestnené všetky kritické komponenty, napr. servery, ale aj prístupový bod do bezdrôtovej siete, diaľkový prístup tretích subjektov do siete a pod. DMZ možno vytvoriť použitím firewall-u s viacerými portmi (min. 3 porty), použitím dvoch firewall-ov na rozhraniach obidvoch sietí a DMZ alebo kombináciou firewall na rozhraní technologická sieť – DMZ a router na rozhraní podniková sieť – DMZ (obr. 4). V podstate až architektúra s DMZ vyhovuje bezpečnostnej zásade, že sieť SCADA nesmie byť priamo prepojená s inou sieťou. Každá komunikácia s podnikovou sieťou končí v DMZ a firewall na základe vopred určených pravidiel rozhoduje, aký typ dát môže byť vymenený medzi oboma sieťami, pričom priama komunikácia medzi podnikovou sieťou a sieťou SCADA môže byť zakázaná. Z podnikovej siete, resp. prostredníctvom nej je tak veľmi náročné uskutočniť útok. Slabinou tejto architektúry sú však zariadenia umiestnené v DMZ – ak dôjde k prelomeniu ich ochrany, potom môžu byť jednoducho použité na útok, pretože sa predpokladá, že prevádzka medzi DMZ a zónou0 je dôveryhodná. Aj tu však existuje riešenie, napr. možno nastaviť pravidlá tak, aby pri podstatnom náraste požiadaviek na komunikáciu do siete zóny0 došlo k zablokovaniu komunikácie s DMZ, alebo aby všetky spojenia s DMZ boli iniciované zo siete zóny0 a pod. Pretože však nemožno vždy takto nastaviť pravidlá (závisí to to od konkrétnej aplikácie), treba považovať zariadenia v DMZ za slabé miesto a posilniť ich zabezpečenie iným spôsobom. To, čo môže odradiť podniky od implementácie tejto architektúry, je zložitosť a potreba vy-

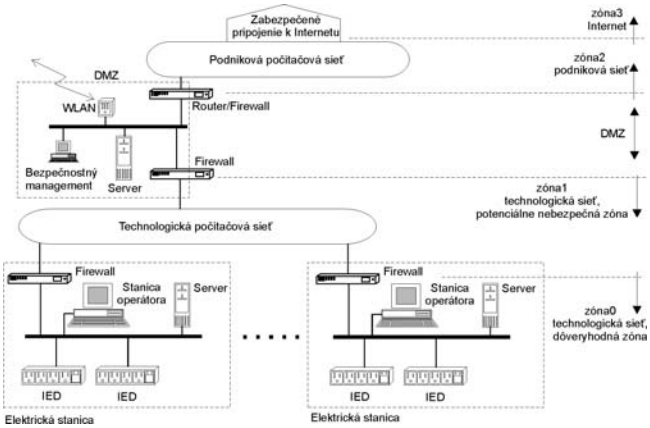


Obr.4 Oddelenie sietí pomocou DMZ

sokokvalifikovaného personálu, čo zvyšuje náklady na bezpečnostný systém.

D. Virtuálne siete (VLAN) na procesnej úrovni

Alternatíva VLAN je použiteľná v prípadoch, keď existujú funkčné celky, medzi ktorými nie je potrebná priama komunikácia. Platí to predovšetkým na procesnej úrovni (napr. terminál 22 kV poľa nemusí priamo komunikovať s terminálom 110 kV poľa), ale tento princíp možno za určitých podmienok rozšíriť aj na vyššie úrovne siete automatizačných a SCADA systémov – staničnú a dispečerskú (napr. stanica A nemusí komunikovať so stanicou B a pod.). Takéto rozdelenie umožňuje vytvoriť virtuálne siete pre dané celky, v rámci ktorých je komunikácia považovaná za dôveryhodnú a komunikáciu s ostatnou sieťou možno riadiť prostredníctvom router-ov alebo L3 switch-ov s filtráciou paketov. Takéto riešenie sa vyznačuje pomerne vysokou bezpečnosťou v rámci celej siete, avšak nízkou bezpečnosťou v rámci danej virtuálnej siete, to znamená, že eventuálny útok znefunkční danú časť siete, avšak nemôže sa rozšíriť na celú sieť. V kombinácii s predchádzajúcimi architektúrami môže vzniknúť veľmi silné bezpečnostné riešenie, no za cenu zložitého manažmentu, takže obvykle je výhodnejšie fyzicky oddeliť technologickú informačnú sieť.



Obr.5 Príklad fyzického oddelenia technologickej siete

E. Fyzicky oddelená technologická komunikačná sieť

Fyzické oddelenie technologickej siete od podnikovej počítačovej siete poskytuje vysokú úroveň bezpečnosti pre automatizačný a SCADA systém. Technologická WAN je vybudovaná na báze samostatných sieťových zariadení, ktorých komunikácia môže prebiehať po samostatnej komunikačnej sieti (optickej, SDH, chrbticový ethernet a pod.). Takúto konfiguráciu si, samozrejme, môže dovoliť len organizácia, ktorá vlastní privátnu prenosovú sieť. Treba počítať s vyššími nákladmi na vybudovanie takejto siete, avšak jej prevádzka môže byť lacnejšia, nakoľko architektúra technologickej siete môže byť jednoduchšia, založená na iných princípoch ako podniková počítačová sieť. Na obr. 5 je uvedený príklad takéhoto riešenia, pričom rozdelenie zón možno upraviť v závislosti od konkrétneho použitia. Vo všeobecnosti sa však neodporúča definovať ako zónu0 celú technologickú sieť, pretože takéto riešenie je veľmi rizikové z hľadiska útokov iniciovaných zvnútra technologickej siete. Preto ak vnímame technologickú sieť ako samostatné informačné prostredie, odporúča sa realizovať samostatne jej internú ochranu a prepojenie s vonkajším svetom (inými sieťami) takisto samostatne, niektorým už z uvedených spôsobov. Uvedený príklad je len jednou alternatívou – konečné riešenie vždy závisí od rozhodnutia a možností danej organizácie.

Na záver kapitoly jedna dobre známa, avšak často málo dodržiavaná zásada:

Akákoľvek silná sieťová architektúra bude v konečnom dôsledku málo efektívna, ak nie je definovaný a uplatňovaný proces, ktorý zaistí, že používatelia si budú vedomí nielen svojich práv, ale aj zodpovednosti za správanie v sieti.

Záver

Dosiahnuť stav stopercentnej bezpečnosti v zmiešanom prostredí podnikových a technologických počítačových sietí prakticky nemožno. Rozdiely medzi štandardnými počítačovými systémami a automatizačnými systémami sú také veľké, že nie vždy sa dajú priamo aplikovať známe a osvedčené bezpečnostné postupy (pozri príklady uvedené v kapitole o heslách). Na druhej strane však nemožno absolútne zavrhnúť všetky bezpečnostné praktiky IT sveta, ale niektoré z nich rozumne využiť, doplniť ich novými a zamerať sa predovšetkým na vzťah BEZPEČNOSŤ verzus DOSTUPNOSŤ systému. Ak v dôsledku kybernetického útoku zlyhá komunikačná infraštruktúra alebo automatizačný systém, môže nastať situácia s nepredvídateľnými následkami, a to paradoxne aj napriek bezchybne fungujúcej infraštruktúre na prenos elektriny.

Literatúra

[1] When SCADA Systems Are Attacked!, Dick Lord, The Steadfast Group, August 2005

[2] Industrial information system security, Dzung D., Naedele M., ABB Review, 2/2005

[3] Concerns about intrusions into remotely accessibile substation controllers and SCADA systems, Paul Oman, Edmund O. Schweitzer, Deborah Frincke, III Schweitzer Engineering Laboratories Inc., University of Idaho, SEL 2000

Ing. Július Tomčík, PhD.

Východoslovenska energetika, a. s., Košice
e-mail: tomcik_julius@vse.sk

Ing. Iveta Tomčíková, CSc.

Technická univerzita Košice
e-mail: iveta.tomcikova@tuke.sk