Sieťová bezpečnosť

Komunikačná infraštruktúra musí zabezpečiť dostupnosť a integritu prenášaných údajov. Vzhľadom na predpokladaný prenos osobných údajov v LAN aj WAN, musí byť zabezpečená ich dôvernosť. Vnútorné prostredie komunikačnej infraštruktúry musí byť chránené pred prienikom neželaného kódu a pred výskytom ďalších bezpečnostných incidentov. Preto komponenty komunikačnej infraštruktúry musia byť schopné takéto incidenty identifikovať a chrániť vnútorné prostredie organizácie.

Riešením týchto požiadaviek je vytvorenie vhodnej sieťovej architektúry, kde sa vo vnútornom prostredí zabezpečí možnosť oddelenia citlivých segmentov LAN minimálne na úrovni riadenia smerovania tak, aby sa pre citlivé procesy, alebo komponenty zabezpečila dostatočná úroveň dôvernosti a integrity. Dôležité je aj dôveryhodné zabezpečenie správy prostredia, vrátane vhodného systému identifikácie a autentizácie, riadenia prístupu a ochrany prenášaných údajov. Odporúčame, aby bol každý komponent vo WAN identifikovaný. V prípade, že sa využíva na vytvorenie šifrovaného spojenia, je potrebné aplikovať aj jeden zo spôsobov autentizácie. Okrem toho je potrebné navrhnúť dôležité časti komunikačnej infraštruktúry tak, aby umožnili vytvorenie záložného (redundantného) spojenia. Centralizovanie všetkých externých prístupov na jeden zabezpečený prístupový bod internej siete patrí k ďalším prvkom ochrany komunikačnej infraštruktúry. Taktiež všetky komunikačné rozvody – t. j. počítačové a telekomunikačné siete musia byť chránené pred zničením, poškodením alebo zneužitím.
Citlivé údaje prenášané elektronicky je potrebné chrániť v súlade s definovanými požiadavkami pre ochranu citlivých údajov.

Na zabezpečenie uvedených požiadaviek Vám ponúkame:

- Návrh bezpečnej sieťovej infraštruktúry
- Implementáciu bezpečnostného protokolu IPSec – samostatne, alebo vo väzbe na projekt JIS
- Implementáciu demilitarizovanej zóny (DMZ) alebo firewalov
- Implementáciu pripojenia organizácie k Internetu
- Implementáciu riešenia pre bezpečnú elektronickú poštu
- Implementáciu riešenia na vytvorenie bezpečnej komunikácie pre vzdialených používateľov

Využívané technológie:

- Komponenty Cisco, Cisco PIX
- Check Point
- Phion, Barracuda
- Symantec Network Access Control

Využitie:

- Ochrana prenášaných údajov
- Ochrana integrity sieťovej infraštruktúry
- Dynamické riadenie bezpečnosti komunikačných kanálov
- Ochrana citlivých údajov

EMM®

EMM, spol. s r.o., Sekurisova 16, 841 02, Bratislava 42, Slovensko
tel: +421 (2) 60 254 111, fax: +421 (2) 60 254 901
www.emm.sk