

Daljinski pristup sa aspekta sigurnosti

Današnja preduzeća se sve češće susreću sa potrebom da svojim mobilnim prodajnim timovima, saradnicima u maloprodaji, strateškim partnerima i ostalim korisnicima od poverenja, omoguće daljinski pristup informacijama na svojim korporativnim mrežama.

Prema informacijama sa globalne mreže, grubo, oko 80% velikih kompanija u svetu u ovom trenutku ima u upotrebi VPN sisteme (Virtual Private Network), što je porast od gotovo 40% u odnosu na samo par godina u nazad. Ovakav bum, za sobom neminovno donosi, probleme u pogledu sigurnosti, neusaglašenosti standarda, tehnologija pristupa i sl. Glavninu zastupljenih sigurnosnih tehnologija za daljinski pristup čine IPsec, Secure Sockets Layer (SSL) i Multiprotocol Label Switching (MLS), obezbeđujući jeftin način povezivanja sa udaljenog mesta.

IPsec je u suštini set ekstenzija razvijenih od strane Internet Engineering Task Force, kako bi se obezbedila sigurnost komunikacije preko Internet Protokola (IP), i ne samo to nego i bilo kog drugog protokola koji funkcioniše na vrhu IP, npr. TCP, UDP i ICMP. IPsec standard obezbeđuje autentifikaciju, integritet, kontrolu i poverljivost pristupa, i na taj način pruža kriptovanu i sigurnu razmenu informacija.

Međutim, tehnologija ima i svojih mana. IPsec od korisnika, ili njihovih sistem administratora, zahteva da prethodno instaliraju i podese sigurnosni softver na svakom sistemu koji je uključen u ovakav vid VPN komunikacije. Kao paralelu možemo posmatrati SSL model, koji ne zahteva od korisnika koji pristupaju daljinskim putem, bilo kakvo prethodno konfigurisanje jer je ugrađen u skoro sve internet pregledače i Web servere. To znači da se jednostavnim instaliranjem digitalnog sertifikata, ili identifikacije na serveru, omogućava SSL konekcija.

U svakom slučaju, i kada je konekcija sa udaljenog mesta samo aktivirana ili posebno implementirana, proces sam po sebi uključuje i izvesne rizike. Bez odgovarajućih dodatnih mera zaštite preduzeća rizikuju odliv informacija, krađu identiteta, zloupotrebu mreže, probleme poznate pod terminom *denial-of-service* kao i druge vidove "digitalnih" pretnji.

Opcije

Kako bi smanjili navedene rizike, lica odgovorna za sigurnost informacija u preduzećima, sve češće uvode opisane sisteme zaštite saobraćaja. Međutim, time se rešava samo deo izazova koje sa sobom nosi problem sigurnosti. Preporuka je da se postave i drugi sistemi bezbednosti kao što su zaštitni zid (Firewall), Adware filter, sistem za kontrolu upada, kako na stacionarnim tako i na mobilnim uređajima. Za sisteme koji sadrže kritične informacije po funkcionisanje preduzeća, treba razmotriti uvođenje i neke vrste lokalno razvijenog softvera za enkripciju, ako za to postoje uslovi. Bez ovih sigurnosnih mera VPN sistemi su ranjivi na upade i infiltracije raznih vrsta.

Saveti pre nego što postanete "mobilni"

1. Pre kupovine uređaja i softvera, proverite na koji način proizvođač testira svoj proizvod sa stanovišta sigurnosti.
2. Testirajte softver/hardver i njegove karakteristike po pitanju sigurnosti.
3. Uspostavite proceduru za kontrolu ranjivosti sistema.
4. Instalirajte najnovije zakrpe, ali prethodno se informišite na specijalizovanim News grupama i forumima na Internetu, o postojanju eventualnih anomalija u tim zakrpama.
5. Nakon instalacije novog hardvera i softvera uvek instalirajte i najnovije zakrpe ako su dostupne.
6. Koristite specijalizovane alate za proveru ranjivosti uređaja u mreži.
7. Razdvojte funkcije servera na više fizičkih mašina.
8. Postavite zaštitni zid unutar mreže.
9. Postavite sistem za kontrolu upada na svim segmentima mreže ako postoje.
10. Koristite jednokratne lozinke, jer iako budu otkrivene, neće moći da se koriste u budućim sesijama za pristup.

Autor: Velibor Simikić