

Sigurnosna politika za priključak na internet

1.0 Svrha

Suvremeno poslovanje zahtjeva neprekidnu elektronsku komunikaciju s poslovnim partnerima (npr. kupci, dobavljači, razni ugovorni partneri,...). Pored toga da elektronska komunikacija putem međumreža donosi poslovne pogodnosti, svaki priključak našeg informacijskog sustava na međumrežu donosi opasnosti i rizike.

Svaki puta, kad upotrebimo internet ispostavljeni smo potencijalnom ugroženošću informacijskih sigurnosti a s tim i sigurnosti djelovanja poslovnih procesa i poslovanja. Zbog toga je potrebno posebno pažljivo kontrolirati sve aktivnosti, koje se tiču internetskih povezivanja s našom informacijskom okolinom. Potrebno je kontrolirati samo povezivanja, kao i brinuti se za aktualizaciju organizacijskih i tehničkih postupaka koji osiguravaju siguran pristup na svjetsku međumrežu.

U tehničkom pogledu potrebno je kontrolirati protok podataka i kod svake anomalije odgovarajuće postupati. Time osiguravamo konzistentnost podataka i evidentiramo moguće upade ili druge napadaje na naš sustav.

2.0 Cilj

Svrha te sigurnosne politike je standardizacija mjerila za povezivanje sustava poduzeća <> te Interneta. Ovime omogućavamo standardne kontrole i provjere sigurnosti veza našeg sustava sa svjetskim međumrežama.

3.0 Matrica internetnih veza sa informacijskim sustavima poduzeća <>

	DMZ	Požarni zid	Antivirusna zaštita	Enkripcija	LAN povezivanje
Samostalni sustavi	Ne	Ne	Da	Ne	Ne
Internetski pristup s namjerom izmjene javnih informacija (npr. informacije o proizvodima)	Da	Da	Da	Ne	Da
Informacijski pristup s namjerom izmjene povjerljivih informacija (npr. narudžbe)	Da	Da	Da	Da	Da

4.0 Osnovna pravila

Obvezno je izvoditi sve potrebne administrativne postupke, koje osiguravaju visok nivo sigurnosti informacijskih sustava. U tom slučaju je priključenje novog korisnika ili informacijskog sustava na internet brz, jednostavan i realiziran na standardan način.

U slučaju vanjskog upravljanja internetnim vezama (cjelovito upravljanje ili hosting), potrebno je s izvođačem potpisati ugovor, kojim se obvezuje osiguravati visoku razinu informacijske sigurnosti. Isto tako ugovor mora sadržavati mehanizme čuvanja i način spremanja zaštite od strane poduzeća <>. Jasno je potrebno dogovoriti odgovornost, aktivnosti i kriterije u slučaju upada ili drugačijeg sigurnosnog incidenta.

Sva povezivanja preko interneta moraju biti kontrolirana i spremljena s odgovarajućim mehanizmima. Jedina iznimka je povezivanje preko prividnih mreža (VPN), gdje je VPN uređaju omogućen direktan pristup do interneta.

Veze koje više nisu potrebne (IP adrese i/ili portali), moraju biti brisani i/ili blokirani u svim uređajima i aplikacijama gdje nastupaju.

Za uspostavu i održavanje internetskih veza odgovoran je odjel informatike.

5.0 Organizacijski postupci

Unaprijed je potrebno pripremiti plan eskalacije za slijedeće slučajeve:

- DDOS,
- sumnja upada u sustav,
- stvarni upad u sustav.

U slučaju događaja, postupa se prema eskalacijskom planu te se o svim aktivnostima kao i rezultatima vodi zapisnik. O rezultatima se obavještava uprava poduzeća, koja u pogledu razine problema poduzima odgovarajuće postupke.

Mehanizme pristupa do interneta i sigurnosne kontrole potrebno je provjeriti barem jedno godišnje. Pregled izvodi neovisan stručnjak. Prosudba mora uključivati pregled konfiguracije, sigurnost aplikacija i same mreže. Potrebno je i pregledati organizacijske postupke.

Svaki pregled mora biti dokumentiran, izvješće mora biti predano osobi zaduženoj za sigurnost i vodstvu poduzeća. Utvrđene manjkavosti moraju se ukloniti u što kraćem vremenu.

7.0 Povijest dokumenta