dnevi slovenske informatike

"Nove razmere in priložnosti v informatiki kot posledica družbenih sprememb"

Kongresni center Grand hotel BernardinPortorož
Slovenija | 18. - 20. april 2011

18. konferenca
Dnevi slovenske informatike

KOMBINIRANE GROŽNJE INFORMACIJSKI VARNOSTI PRI RABI MOBILNIH NAPRAV

Blaž Markelj, Igor Bernik

18. 04. 2011

slovensko društvo informatika

UVOD

Globalizacija je povečala potrebe po hitrem dostopu do informacij. Informacije in dostop do njih danes pomenijo konkurenčno prednost.

Hiter razvoj tehnologije omogoča povezovanje v korporativni informacijski sistem in dostopanje do pomembnih informacij od koder koli.

Nevestno upravljanje z mobilnimi napravami in nepreudarno vključevanje v odprta omrežja, s pomočjo katerih uporabniki dostopajo do informacij znotraj korporativnega okolja, ogrožajo varnost celotne organizacije.

MOBILNE NAPRAVE

Hiter porast uporabe mobilnih naprav (prenosnikov, tabličnih računalnikov, pametnih telefonov, itd.) v poslovne namene.

Velika količina raznovrstne programske opreme, ki jo lahko uporabniki samodejno in brez preverjanja nameščajo na svoje mobilne naprave.

Možnost povezovanja v medmrežje od koder koli (UMTS, GPRS, javna omrežja WLAN).

Povezovanje v korporativni informacijski sistem in pregled podatkov, sinhronizacija pošte, koledarja itn. … s korporativnim informacijskim sistemom.

KOMBINIRANE GROŽNJE

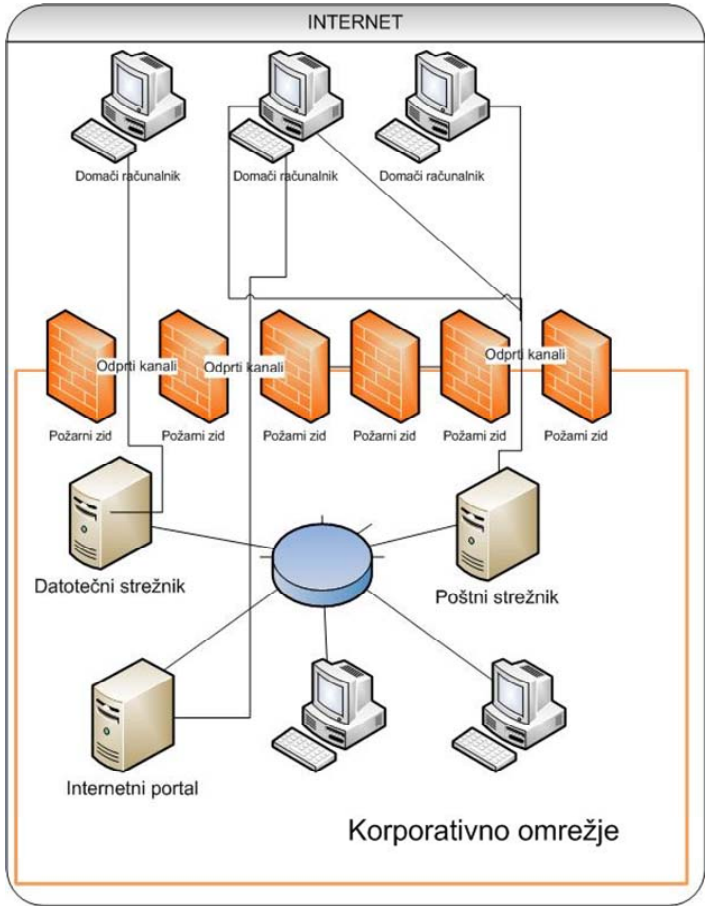
Mobilne naprave so tarča različnih groženj, včasih te delujejo sočasno ali kombinirano, zmeraj pa z namenom, da bi nekdo nepooblaščeno vstopil v informacijski sistem.

V preteklosti je zadoščalo varovanje korporativnega omrežja s požarnim zidom, saj komunikacija iz zunanjega dela ni prehajala v notranje omrežje brez dovoljenja na požarnem zidu. Hkrati pa ni bilo naprav, ki bi se nahajale zunaj korporativnega omrežja, se povezovale v korporativno omrežje in obenem komunicirale z zunanjim svetom preko drugih sistemov, kot npr. WiFi, UMTS, ...

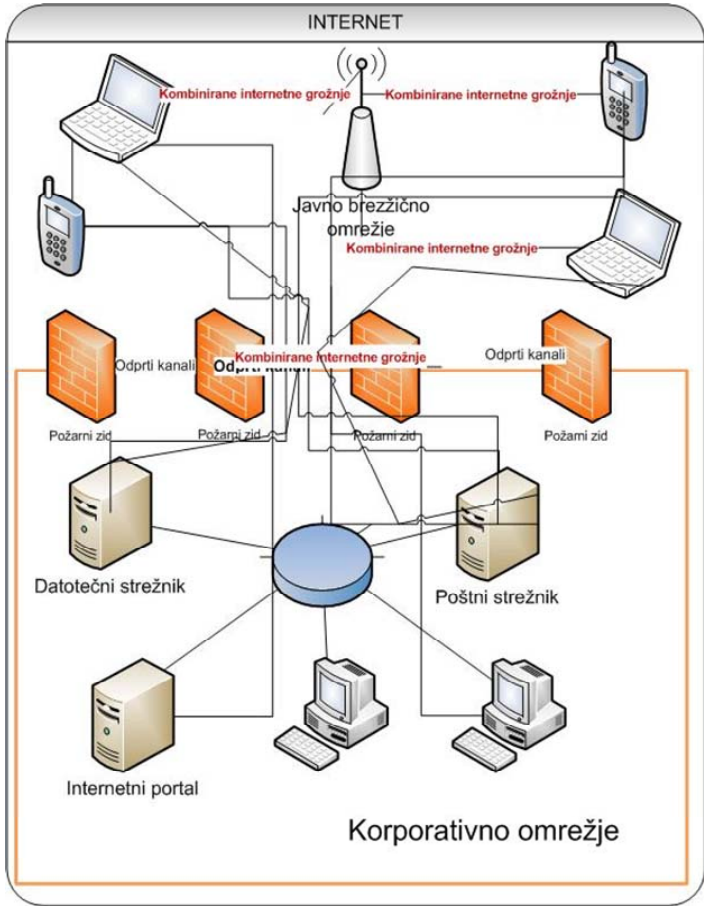
Danes pa veliko mobilnih naprav dostopa v korporativno omrežje mimo požarnega zida in hkrati komunicira z zunanjim svetom.

Pomanjkanje pravilnikov o varni rabi izročenih sredstev in splošno slabo poznavanje problematike.

SHEMATSKI PRIHAZ KOMBINIRANIH GROŽENJ



Slika 1: Komunikacija centralnega informacijskega sistema z internetom preko požarnega zidu (v preteklosti).



Slika 2: Komunikacija centralnega sistema z mobilnimi napravami in komunikacija mobilnih naprav z internetom.

MOŽNOSTI ZAŠČITE

Nadzorovanje spletnega prometa s pomočjo :

- požarnega zida in
- naprav, ki preprečujejo nepooblaščene vdore v sistem.

Napredna varnostna programska oprema, ki hkrati skrbi za varnost korporativnega sistema in mobilnih naprav.

Programska oprema, ki določa varnostno politiko na vseh napravah znotraj korporativnega omrežja.

Organizacije v postopku pridobivanja certifikata naredijo pravilnike o varni uporabi izročenih sredstev (mobilnih naprav, programske opreme …).

PRIPOROČILA

Uporaba standardizirane oz. s strani organizacije odobrene programske opreme na mobilnih napravah.

Protokoli varnega povezovanja v korporativni sistem, tudi iz javnih omrežij.

Obvezno izobraževanje o pravilni uporabi izročenih sredstev in o splošni informacijski varnosti.

Standardi avtentikacije v sistem ter inkripcija podatkov na mobilnih napravah.

Posledice kršenja določil pravilnika.

ZAKLJUČEK

Poznavanje pravilne in varne uporabe mobilnih naprav lahko razumemo tudi kot konkurenčno prednost v tekmi za prevlado v gospodarskem in znanstvenem svetu.

Z zmanjševanjem možnosti za vdor v informacijski sistem, odtujitev in zlorabo informacij se krepi zaupanje v procese in informacije, s katerimi operiramo v določenem okolju, zato je nujno vzpostaviti varen dostop do korporativnega sistema.

Hvala za vašo pozornost.

blaz.markelj@fvv.uni-mb.si, igor.bernik@fvv.uni-mb.si