

Kako se obvarovati pred grožnjami, povezanimi z varnostjo naših zaposlenih?

Razvoj elektronskih komunikacij je omogočil sodobnemu poslovanju doslej nepredvidljive prednosti, ki se kažejo tako v hitrejši, enostavnejši in bolj pregledni izmenjavi vseh vrst storitev kakor tudi v zniževanju stroškov v primerjavi z že uveljavljenimi oblikami (spletno oglaševanje, trgovina, elektronske komunikacije in poizvedbe ...). Vse to zajema priljubljeni pojem Splet 2.0 (ang. Web 2.0). Nove možnosti poslovanja pa so žal spodbudile tudi nove oblike kriminala. Mehanizmi zaščite informacijskih virov in komunikacij, ki so jih podjetja uspešno uporabljala še pred nekaj leti, danes ne zadoščajo več.

Saj že imamo zaščito, mar ne?

Vsi poznamo uveljavljene metode zaščite elektronskega poslovanja – požarne pregrade preprečujejo

ne nepooblaščenim vstop v naše omrežje, protivirusni programi na strežnikih in delovnih postajah skrbijo za njihovo zdravje, morda celo higieno pred vohunskimi programi. Ponekod specializirani sistemi bdijo nad pretokom podatkov, spremljajo morebitna odstopanja od dogovorjenih pravil obnašanja, zaznavajo napade in ustrezno ukrepajo. Varnost pomeni nikoli zaključen krog, zato imajo bolj urejena okolja organizirana tudi redna izobraževanja zaposlenih na to tematiko. Vse to pa ni dovolj proti novim grožnjam!

Kaj nas ogroža?

Značilnost novodobnih nevarnosti je prepleteno delovanje. V navidez nedolžnih elektronskih sporočilih nas priložene povezave zavedejo na neželene okužbe ali spletne strani, kjer preži na nas zlonamer-

na koda. Pri deskanju po legalnih in priljubljenih straneh se lahko okužimo z vohunskimi programi, ki lahko zgolj spremljajo naše spletne aktivnosti ali pa kradejo naša gesla za dostop do zaščitene sistemov. Programi za trenutno sporočanje (MSN) ali spletno telefoniranje (Skype) so idealne poti za razširjanje škodljive kode, saj sistemi večinoma niso sposobni zaznati vsebine tovrstnih komunikacij. Podobno velja za ves kriptiran SSL promet, ki ga med drugim uporabljajo spletne trgovine in spletna pošta (Gmail, Hotmail ...) in predstavlja že skoraj polovico vsega spletnega prometa. Kaj pa naši spletni strežniki – ali so res zaščiteni pred podtikanji škodljive kode ali še hujšimi napadi?

Se sploh lahko zavarujemo?

Na srečo obstajajo tudi rešitve

pred vsemi omenjenimi zagatami. Celo zelo veliko jih je, vendar kako izbrati? Vsi proizvajalci trdijo, da je njihova najboljša in najbolj učinkovita, ali pa vsaj najlepša. Preizkus vseh je največkrat neizvedljiv, neodvisne recenzije je težko najti, poglobljanje v marketinške materiale je včasih zavajajoče, še bolj pogosto pa izguba časa. Zdi se, da pri izbiri še najbolj pomaga uveljavljeno mnenje velikih svetovalnih družb (Gartner, Forrester, IDC ...) ali pa subjektivno obarvano priporočilo kolegov in prijateljev.

Na kaj moramo paziti pri izbiri učinkovite rešitve?

V poplavi različnih ponudb nas lahko posamezna metoda neke rešitve hitro zapelje v nepremišljeno odločitev. Morda ne bodo odveč naslednje oporne točke:

- Edina učinkovita metoda so naprave za filtriranje, ki pregledno nadzorujejo promet med zaščitnim poslovnim omrežjem in Spletom.
- Različnih naprav za filtriranje prometa naj bo čim manj, idealno ena.
- Posodabljanje filtrirnih mehanizmov v napravah mora biti samodejno.
- Naprava mora znati proaktivno prepoznavati znano in še ne odkrito škodljivo kodo.
- Naprava mora imeti vpogled tudi v kriptirane oblike prometa (SSL).
- Prepoznavati mora zlonamerne spletne naslove in kategorizirati spletne strani.
- Po vpeljanih pravilnikih ali varnostnih politikah omogočiti ali preprečevati posameznim uporabnikom dostop do spletnih strani.

- Nadzor in spremljanje poročil o aktivnostih mora biti enostavno, hkrati pa informativno podrobno.
- Neželena elektronska sporočila (SPAM) mora prestreči že pred prihodom do poštnega strežnika.
- Zagotoviti mora možnost samodejne enkripcije in preverjanja vsebine pripetih dokumentov izhodne pošte za preprečevanje odtokanja zaupnih informacij.

Vsekakor pa je rešitev v ožjem izboru pametno testirati v lastnem okolju in sprejeti odločitev na podlagi rezultatov. Na tak način spoznate tudi izvajalca, kar je vsekakor prednost pri dolgoročnem upravljanju varnosti vašega poslovnega okolja in s tem poslovanja samega.

Andrej Vnuk, Sistemski inženir,
SIMT d.o.o.