

## Digitalno promiskuitetni

**Neverjetno, a resnično: jedrska elektrarna varno daleč stran od nas, dežela vzhajočega sonca. Fuzija tehnološko zapletenega z radioaktivnimi naravnimi elementi, smrtonosna mešanica. Zunanji izvajalec opravi fizični varnostni pregled in vstopi v IT oddelek. Dovolijo mu, da priklopi svoj prenosni računalnik na omrežje. Dobi dostop do projektnih podatkov in še česa. Nihče ne ve, niti on, kako se je vse lahko zgodilo. Le naključje, trenutek nepazljivosti? Skrivnosti jedrske elektrarne so od njega le tiho spolzele po neskončnih P2P navezavah do milijonov anonimnih spletnih uporabnikov in tako za zmeraj in legendarno postale od vseh in razvpito javne.**

Ah, lepote in dobrote današnjega računalniškega sveta, vse ste mi na dlani! Vročica? Oddaljena en klik. Dobra šala? Seveda, v elektronski pošti Janeza Novaka (le kdo je Janez Novak?). Severinin novi video? Ona ljubka igrice, ki se je končno lahko grem, ko otroci sprostijo računalnik? Oba varno pospravljena na službenem prenosniku, domači računalnik je že malo ... khm ... podhranjen. Nobelovo nagrado dam tistemu, ki je izumil dolvleko (download). In kje je že program za tisti fantastični ohranjevalnik zaslona? Že kje, jutri v službi malo pobrskam po Netu, morda najdem še kaj boljšega. Prijatelj Google morda tudi ve za par odpuljenih digitalnih voščilnic. Še prej preverim messenger, da vidim, kdo od znancev je v službi in razpošljem filmček z zadnjega žura - joj, smo ga sekali.

In ob tem privlačnem, znanja polnem, brezmejno zabavnem svetu veselo odmislim, da sem pri varovanju skrivnosti jaz, človek, najpomembnejši element svete trojice (ljudje, tehnologija, procesi). Ključen, a najbolj ranljiv in zelo na udaru. Družba mi je brez velikih besed dopustila, da mešam službeno in neslužbeno. V zameno za to, da tudi izven delovnega časa veliko razmišljam o delu, smem s službenimi viri občasno in po zdravi pameti opraviti tudi kaj zase: plačati položnico v spletni banki, pogledati novice, zavrteti melodijo ali se malo sprostiti ob dobrem vicu. Saj vsi to počno, tudi zunanji izvajalci jedrskih elektrarn, zakaj pa ne. Na srečo so za vedno mimo časi, ko je bil greh privatno uporabiti službeni telefon ali za stalno izposoditi kulico. Tako sem, kot verjetno tudi ti, moj bralec, postala digitalno promiskuitetna.

V tako svobodnjaškem okolju se skoraj nihče ne želi vprašati, kakšne so lahko posledice enega samega izgubljenega prenosnika, napačnega klika ali okuženega programa. Tako se tudi ne zdi vredno, da bi se morali spraševati, kaj je pravo in kaj napačno uporabniško obnašanje. Zato so ribiški in drugi hekerski napadi tako učinkoviti, saj uporabniki nismo priučeni in motivirani, da bi znali ločiti podtaknjene spletne strani od pravih. Lažne varnostne indikatorje prepoznamo kot legitimne, bogati grafični elementi v naših očeh dvigujejo varnostno kredibilnost strani, ne znamo preveriti SSL potrdil ali si razložiti njihove vsebine. Če smo že poučeni, pa morda nismo vedno pozorni in odpremo elektronsko pošto od kolega Ivana, misleč, da je od Ivana. Umovati, da bi si nam kdo v imenu direktorja (razen tajnice, seveda) upal poslati e-pošto, je pa sploh znanstvena fantastika - je bilo že prvič dobro kaznovano. Kako veste, da vašega računalnika ne nadzoruje veliki brat onega malega tečnega pop-up okna, ki se pojavlja od enega samega osamljenega ukradenega XXX trenutka radovednosti izpred nekaj tednov? Če mislite, da izjava ne velja za vas, se preizkusite: je [www.ecpedia.com](http://www.ecpedia.com) prava ali podtaknjena? In če vam tat ukrade računalnik, vas bo kaj skrbelo, da bi iz diska prebral vaše skrivnosti in jih prodal?

Pravijo, da so najboljše stvari v življenju gratis. Kup malih, preprostih opravil, kot umivanje zob, vpeljanih v vsakdan, lahko po varnostnih učinkih močno preseže investicije v drage varnostne mehanizme in zapletene procese. Tega potenciala še sploh nismo začeli izkoriščati. Najprej se namesto kot administrator vsakodnevno prijavljajmo na računalnik kot nepriviligiran uporabnik, saj bomo s tem zelo omejili tudi napadalce. Nato končno pričnimo uporabljati šifrirano elektronsko pošto, saj so nekatera digitalna potrdila že dolgo brezplačna. Saj veste, da je nešifrirana elektronska pošta 'varna' kot dopisnica. Osebni požarni zidovi so tudi del operacijskih sistemov, le vključiti in konfigurirati jih je treba. In ne, niso več tako neprijetno zapleteni za uporabo, kot so bili včasih. Manj je več - zato na računalnike nič nepotrebne programske opreme za čim več varnosti. P2P programje, zabavne ActiveX kontrole ali java skripte so vse prevečkrat vstopno mesto v varovana omrežja. Pomembni diski pa morajo biti šifrirani, sploh, če se skupaj z uporabniki odpravljajo na službene poti ali vsakodnevno migrirajo med domom in službo. Čim manj klikanja po neznanih linkih ali odpiranja elektronske pošte od oseb, ki jih ne poznamo, sploh pa čim več vaje v ločevanju legitimnih internetnih virov od podtaknjenih.

Ja, vem, vabim vas, da se zavestno odrečete prijetni digitalni promiskuiteti. Najprej zato, da prihranimo kar nekaj denarcev, ker sicer izničimo druge investicije v digitalno varnost. Nato zato, ker ste kot ITjevec zelo verjetno tudi vi nekomu zunanji ali notranji izvajalec, človeške napake pa se dogajajo, tudi pri nas. In tudi, ker smo nevarno blizu jedrske elektrarne, električnega omrežja, plinovodov in kemičnih laboratorijev. Na koncu, ker nas je, ljudi, še vedno vse prelahko ujeli na finte.

Stanka Šalamun, Sistem, okt. 2006