Kolumna (n)e-varnost
(razmišljanje o učinkoviti digitalni nevarnosti)

Ementalec ali parmezan?

Ali lov za izgubljenim tolarjem

Sedim ob računalniku in buljim v on-line stanje na mojem bančnem računu. Tragedija. Tristo kosmatih baferouverflovov, nekaj ključnega manjka! Praskam se po glavi, ki mi jo delovne utrujene ročice na večer že zelo težko podpirajo. Samo tega mi je treba. Le kam je izginil? Saj ni mogel kar tako izpuhteti? Sem morda na razprodajah pretiravala? Saj vem, da gre samo za en tolar, a tu se bije boj za osnovni koncept, za človekovo pravico do njegovega trdo prisluženega denarja in za ključno zaupanje v srčiko sistema. Tole smrdi. Smrdi kot luknja za kanalizacijo. Smrdi kot ... luknja? V varni programski opremi? Pa menda ja ne?

Programska oprema je dandanes luknjasta kot švicarski sir. Naj vas vse vesoljske varnostne tehnologije, ki jih imamo vgrajene v slovenske, pa tudi svetovne spletne aplikacije, in ki bi odgnale tudi najnevarnejše pošasti, ne zavedejo. V Sloveniji, ki še ni bila deležna svojega resnejšega paketa napadov, je morda lukenj še za odtenek več in so še precej bolj očitne. Ko poskušam razumeti, kaj mi razlagajo tisti, ki bi mi radi iz glave izbili idejo, da so bili pri mojem izhlapelem tolarju z bančnega računa na delu grdi hekerji ali mogoče celo plačani penetratorji, mi možgane razsvetli, kot da bi v enem požirku skonzumirala celi liter pangalaktičnega grloreza. Seveda. Hekerji so pravzaprav pravljične osebe. Izjemno čustveni, skrajno štorasti primerki z bolestno željo po večni osebni prepoznavnosti in stalnem zapisovanju svojih blodenj v sistemske in aplikacijske dnevnike svojih žrtev. So popolnoma izgubljeni luzerji v neskončni kompleksnosti še tako preprostih spletnih form, potrebni rešitve iz blodnjaka. Odvisniki od uporabe pametnih kartic ali bitja, ki namesto osebne izkaznice uporabljajo digitalno potrdilo. Osamljenci, ki namesto nočnega seksa že leta in leta raje razbijajo 32-bitno šifriranje in kam dlje še niso prišli. Primerki, katerih tiha, a nedosegljiva osebna ambicija je zgraditi TRANSLATR, kot ga je imela NSA v Digitalni trdnjavi. Pravzaprav precej neškodljivi specimenti in nesposobneži. Očitno so popolnoma precenjeni, z njimi pa si res ne rabim delati skrbi, ker so jih mojstri za varnost že davno popolnoma knockoutirali. Ja, verjetno sem res bila preveč aktivna na razprodajah.

A intelektualni črv v meni ne da miru. Punca, koliko razpok v varnih aplikacijah, velikih in očitnih kot Grand Canyon, si v zadnjih časih srečala? Koliko šolskih primerkov sql, html in še kakšnih vrivanj, prekoračitev vmesnikov, amaterskih doma skuhanih šifrirnih algoritmov se ti je režalo v ksiht? A res lahko kar tako preprosto pozabiš prefinjenost in lahkotnost, s katero se je dalo prevzemati identitete nič hudega slutečih dobrohotnih uporabnikov? Zaprašene in v kotu pozabljene funkcije tipa »izognimo_se_avtentikaciji« ali sejam, ki so kar prosile, da jih uporabi še kdo razen legitimnih uporabnikov? Prepotentne vnosne forme, ki svojim strežnikom pri nadzoru niso prepustile zadnje besede? Ljudi, ki so vse to zakuhali, pa tega sploh niso videli, ker so v duši predvsem graditelji, ki zidajo, in ne pikolovski, zlonamerni napadalci, ki iščejo samo in predvsem mesta, kjer so oni na drugi strani pogrnili?

Morda je to komu težko razumeti, a tisti, ki gradijo, ne morejo in ne smejo biti hkrati tudi tisti, ki preverjajo. Dober graditelj naredi dober načrt in ga dobro izvede. Vgradi protivlomna vrata. Na koncu preveri, če izdelek dobro dela. Dober napadalec dobro pogleda, katere malenkosti je graditelj spregledal in jih dobro izrabi. Ni kot hribolazec, ki želi osvajati najvišje vrhove. Išče najpreprostejše poti do ciljev. Če okno ne tesni, ga poskuša odpreti. Če je dimnik širok, se igra Božička v kamin. Če se da po okraskih ograje plezati, spleza čez. Izklopi kamere. Če ve, da sistem za odkrivanje plinov ne dela, vari. Velikokrat male nedoslednosti poveže tako, da ga ena luknjica pripelje do večje luknje. Naivno je pričakovati, da bo glasno razbijal protivlomna vrata, če pa ve, da je bistveno preprosteje iti skozi tiste male ljubke nedoslednosti v kodi, s katerimi se da zaobiti varnostne pasti. Žal je pri nas že tako, da si temeljitega in dovolj neodvisnega preizkusa resničnega stanja prodajalci programske opreme želijo približno toliko kot davčne inšpekcije in so zato aplikacije bolj podobne ementalcu kot parmezanu.

Zato ne razumem čisto, zakaj se me ne lotijo drugače. Zakaj mi ves čas razlagajo, da so vgradili vso tisto tehnično modrost, ki služi predvsem temu, da jo uporabljajo pridni, dobronamerni uporabniki in se ji tisti hudobni z lahkoto izognejo. Zakaj je dobra inženirska praksa nalezljiva približno toliko kot nosečnost? Zakaj mi ne povedo, da so se kvalitetno, po napadalsko lotili spreminjanja ementalca v parmezan? Da so ranljivosti bile in da jih je vsak dan manj. Da so stvar testirali varnostni analitiki, ki se že od prej lahko pohvalijo z obsežnim seznamom najdenih lukenj in vedo, kaj delajo. Da je krivulja prihajanja ranljivosti zanesljivo in brez statističnih mahinacij padla pod določeno mejo. Da so temeljito, pri napadalcih, izobrazili svoje razvijalce. Da bi zardeli od nohtov do las, če bi jih kdo dobil na kakšno res amatersko. Da so dobro in redno seznanjeni z najnovejšimi tipi napadov na spletne aplikacije in so sposobni iz glave stresti seznam. Pravi mojstri pridelave sira se stalno

trudijo, da nadzorujejo velikost in število lukenj v svojih sirih. Tudi pravi mojstri gradnje varnega softvera delajo tako.

In kje je ostal moj tolar? Nisem ga še našla. Verjetno je padel skozi kakšno luknjo v ementalcu. Prepričana sem le, da ni ostal na razprodaji. Morda mi ga povrne moja banka, saj sem ja zvesta stranka.

Stanka Šalamun
Objavljeno v reviji Sistemi (priloga revije Monitor), marec 2006