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

O božanju, prodiranju, vdiranju.

Kdaj ste nazadnje učinkovito penetrirali?

Danes bom zelo poredna. Prav nič damsko, ob nagajivem plahutanjem trepalnic, vas bom spraševala: kolikokrat ste? Kdaj nazadnje? Kako globoko? Je bilo dobro? Je šlo vse do srca in skozi možgane? Bi morda še enkrat?

Verjamem, da ste za svoje notranje omrežje in najbolj ključne podatke nabavili kup digitalnih prezervativov. Notranje omrežje ste oblekli v požarno zaščitno obleko, nabavili ste neprebojna protivlomna vrata, postavili stroge vratarje v obliki najmodernejših varnostnih naprav, ki vas pogledajo globoko v oči ali zahtevajo, da jim izdate kakšno samo vam znano skrivnost. Namestili ste digitalne kamere v obliki sistemskih dnevnikov, kjer se zapisuje vse. Največje skrivnosti šifrirate v žlobudravščino, ki jo razumejo le posvečeni. Vsakega digitalnega virusnega bolnika ali prenadležnega prodajalca vržete skozi vrata. Vse samo zato, da ostanejo vaši kronski dragulji na varnem in samo vaši.

A kako veste, da vsi ti super mehanizmi delujejo in da niste varnostno neplodni? Da vam kdo drug ne skače čez plot? Da ni podkupil vratarja? Da ne gostite skrite staje konj, ki komaj čakajo, da se napojijo z informacijami, ključnimi podatki, dostopi do vaših podatkovnih baz, prebiranjem poslovnih strategij ali naslajanjem nad ceno v ključni ponudbi za javni razpis, ki ga oddajate naslednji teden? Ja, vem - veste, da delujejo. So vam proizvajalci garantirali, da je to tako. So rekli, da so zadevo namestili na (sami izberite številko) mestih in da deluje. Tudi visoka cena, ki ste jo plačali za rešitev, pravi, da stvar mora delovati. Da to uporabljajo vsi. Da če kupite njihovo rešitev, boste lahko strošek zagotovo dobro upravičili pri šefu. Da ima ta sistem vaša konkurenca, torej ga morate imeti tudi vi. Da še nihče ni uspel v realnem času in dovolj tiho zvrtati niti luknje v protivlomna vrata, kaj šele priti skozi... Vse to je popolnoma res.

A vse te rešitve temeljijo na dejstvu, da jih bodo vedno nujno uporabili prav vsi (kar je iluzorno) in zato delujejo predvsem na poštenjakih, ki tako ali tako ne bi iskali drugih poti. Naj vam povem štorijo o bogatašu, ki je za svojo novo hišo kupil odlična protivlomna vrata. Prijateljem je razlagal o fantastičnih neprebojnih lastnostih teh vrat in prav vsi prijatelji so rekli, da se je odlično zavaroval. Medtem je, zaklenjenim novim vratom v posmeh, lopov lezel v njegovo hišo skozi odprto okno v pritličju. Vratom ni bilo kaj očitati, dragulji pa so šli.

Zato veste, kako lahko ali težko je priti v vaš sistem le, če stvar res temeljito preizkusite. In ker sistemi po načelu entropije sami težijo k neredu, je stvar težja: preverjati boste morali periodično. Da pa se kompleksnost problema ne konča, vam vaš vzgojeni uporabnik ali najboljši razvijalec pri testu ne bo mogel koristiti, saj pač ne razmišlja na dovolj sprevržen način in njegovo mnenje ne šteje. Ne borite se, namreč, proti njemu in škoda je graditi varnostne mehanizme za njih, kajne? Borite se proti resnemu napadalcu!

Kako pa si vseeno lahko pomagate? Viager za varnostno neplodnost je veliko, nekatere med njimi so izrazito poceni, a to je tako pomembna tema, da jo v celoti pustimo za kdaj drugič. Kot je za vsak dober odnos ključnega pomena, je treba pri dejanski varnosti pogledati resnici globoko v oči in se včasih sprijazniti s tem, da imajo drugi pač boljše orodje. No, na srečo so tehnika, iznajdljivost in pozornost tisti, ki so na področju varnosti res pomembni, zato še ni vse izgubljeno. Načinov je veliko. Lahko uporabite programe, ki vam redno skenirajo omrežje od zunaj in znotraj ter avtomatično odkrijejo najbolj znane varnostne luknje, viruse ali vohune. Temu bi rekla božanje. Uporabite orodja, ki nad vašimi na kožo napisanimi spletnimi aplikacijami poskusijo izvesti preprostejša sql vrivanja ali kakšne druge tipizirane vrste vdorov, razbijajte uporabniška gesla in iščite mape v skupni rabi, pa boste že bližje prodiranju. A najbolj učinkovito bo, če se prepustite belemu hekerju, polnemu trikov in najnovejših varnostnih trendov, na katere se sami niti pod razno ne bi spomnili, da za vas poišče vaše šibke točke in metode, kako vam od zunaj priti do srca.

Naj še enkrat uporabim poceni trik z začetka pisanja. Če ste vztrajali do sem, si domišljam, da ste mi ga oprostili in vzeli za dobro. Prosim vas, pustite se božati, po vseh najbolj izpostavljenih mestih ter povsod, kjer vam lahko pridejo blizu. Poskusite prodirati, čim globlje, kadarkoli je le možno. Bolje, da to naročite vi, nadzorovano, brez škode. Spremljajte, kateri vgrajeni mehanizmi so se pravočasno vklopili ter popravite tiste, ki se niso. Ker če tega redno ne počnete, boste kot noj z glavo v pesku čakali, da vas kdo od zadaj. To pa bo zares bolelo.

Stanka Šalamun
Objavljeno v reviji Sistemi (priloga revije Monitor), oktober 2005