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

Pravljica o vaši kreditni kartici

ali kako je hudobni volk požrl 40 milijonov digitalnih babic.

Imate Eurocard, Visa ali AmEx kartico? Ste jo v zadnjih par letih kaj peljali na shopping po ZDA? Pravite, da niste. Dobro. Kaj pa nakupi preko spleta, ste plačali kakšno letalsko karto ali knjigo? Aha, ste. Je praktično, ne? Pa vas z vaše banke niso obvestili, da so vam preklicali kartico in da vam bodo poslali novo? Ne. Poslali so vam sporočilo, da ste lahko prepričani, da vaša številka ni na seznamu ukradenih. No, potem je pa tako vse OK.

Če že nimamo vročega poletja, imamo vsaj primer res vročega vdora v informacijski sistem. Seveda govorim o nesrečnem procesnem centru kartičnih transakcij CardSystems Solution in ukradenih 40 milijonih številk kreditnih kartic, ki so zaradi »raziskovalnih« namenov ostale v njihovi bazi, čeprav jih tam že davno več ne bi smelo biti.

Teh 40 milijonov osebkov je postalo tako popularnih samo zato, ker imajo v Schwarzeneggerjevi deželi zakon, zaradi katerega mora podjetje, ki ima izpostavo v Kaliforniji ali zbira osebne podatke o Kalifornijčanih, obveščati morebitne žrtve digitalnih napadalcev o tem, da ima morda zlikovec v lasti njihove osebne podatke. Če bi se napad, četudi še obsežnejši, zgodil denimo v državi Mississippi, Veliki Britaniji ali sosedi Hrvaški, bi lahko vsi skupaj precej mirno spali, ker ne bi imeli pojma, da se sploh kaj dogaja. In samo posvečeni bi vedeli, da lahko ukradene podatke najdejo kje na novem »divjem vzhodu«, recimo na trgu Gorbushka v Moskvi.

Bodimo pošteni, CardSystems Solution so zelo privlačna tarča za raznolike napadalce. V informacijsko varnost so vložili zelo veliko denarja. Njihovi ključni partnerji so jim predpisali standarde in postopke, ki se jih morajo držati. Če niste ravno IT bančni strokovnjak ali računalniški sodelavec procesnega centra, za standarde CISP, SDP in PCI do dotičnega dogodka verjetno še niste slišali. Gre za paket precej znanih stvari: za zahteve po uporabi požarnih pregrad, protivirusne zaščite, šifriranja podatkov, nadzora in rednega preizkušanja varnosti omrežja, uporabe močnih seznamov dostopov in izvedba varnostne politike. Nič revolucionarnega.

A nekaj je v tej digitalni utrdbi šlo zelo narobe. Nekaj majhnega je pririnilo v veliki sistem, David je premagal Goljata. Trojanski konj je našel novo stalno pribežališče. Zelo verjetno mu je na stežaj odprl vrata uporabnik notranjega omrežja, ki je neumno klikal po napačnih linkih, zaganjal nedovoljene programe ali odpiral priponke s tazadnjimi šalami. Naj poudarim, da v tem primeru ni šlo za enega od avtomatiziranih načinov vdorov, kjer napadalec po metodi metanja ribiške mreže čaka, kaj se bo ujelo. David je bil prej strateg kot ribič, analitik s ciljem, znanjem, časom in idejami, kako bo uporabil plen. Protivirusna zaščita in protivohunsko programje ga nista spoznala, požarne zaščite se ni ustrašil, pametnim karticam se je znal izogniti. Verjetno je imel za vdor komercialne razloge.

Tisto, kar me pri vsej zadevi zelo skrbi, je dejstvo, s kakšno lahkoto vpleteni operirajo s podatki o potencialni škodi. 40 milijonov je ogromna številka, a kako vedo, da ni celo večja? Če ste kdaj naročili penetracijski preizkus in je white-hat heker uspel v vaše omrežje pritihotapiti zlonamerno kodo, veste, da zanj skorajda ni bilo več skrivnosti o vas. Zelo verjetno ga dalj časa nihče ni odkril, z malo sreče pa se je celo neopažen umaknil s svojim plenom. Če ste po nesreči gostili hekerja, ki si vas je izbral za žrtev, morda to razumete še bolj. Ni ga načina, da natančno odkrijete, po katerih diskih se je sprehajal, katere identitete je prevzemal, kateri podatki so šli z njim in v kakšni obliki. Morda si je nadel digitalno identiteto tajnice vašega direktorja in veselo nabiral strateške skrivnosti vašega podjetja. Verjetno je poskusil skočiti v čevlje administratorja in izkoristil njegove pravice dostopa do glavnega računalnika in podatkovne baze podjetja. Poskusil je pisati po vaši bazi. Pojma niste imeli, koliko časa ga oskrbujete z informacijami in kako jih je/bo izkoristil. In ne, v dnevnikih ga ne boste zasledili. Če niste popolnoma in sistematsko preinstalirali vseh sistemov, tako pomembnih kot nepomembnih, je zelo verjetno potuhnjeni slepi potnik še vedno v vašem sistemu.

Je za vse nas res tako dobro, da smo v varnost naših kreditnih kartic tako popolnoma prepričani? Vem, da se je včasih najboljše pred nevihto skriti v zaklon in počakati, da gre mimo. Verjeti javnim floskulam, vse je supervarno, nič se ni treba bati za vaše kreditne kartice, bo že zavarovalnica povrnila. Ne regairati na vsak oddaljeni pripetljaj. A vsaj 40 milijonov digitalnih babic je šlo v hudobni volkov trebuh. Za te vemo. Naslednjič se bo kdo seznanil z vašim transakcijskim računom. Še naslednjič bodo »ušle« zdravstvene kartoteke, nato morda digitalni zapisi biometričnih podatkov za potne liste. Nekdo se bo poigral s številkami v pokojninski bazi. Vse preveč preprosto je pritihotapiti se v omrežje, ker vse preveč ljudi misli, da to ni njihova stvar. Je vaša?

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