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

Nevidni dotiki

Koliko je vredna vaša poslovna strategija v rokah konkurence?

V moji garaži me čaka prelep rdečečrn Bugatti Veyron. Tisoč konjičkov je ubogljivo pospravljenih pod oblinami pokrova motorja in komaj čakajo, da se strumno dvignejo v pozor za dirko, da obrnem ključ in jih povabim na dogodivščino. Spolirani boki se svetijo, v žaru hitrosti me zapečejo pogledi poželjivih oči, ki jih puščam za sabo. Občutek, vreden zelenih milijon in pol.

Nato zazvoni budilka. Saj menda niste zares verjeli, da je besedilo iz uvoda v mojem primeru resnično? A za trenutek se pretvarjajmo še naprej in poglejmo črno stran te sicer tako bleščeče trofeje. Nekega jutra odprem garažna vrata in ugotovim, da je moj lepotec šel po svojih poteh, z nekom drugim. Film se zavrti hitreje. Policisti, zavarovalnica, vprašanja, avtobusi. Nato ima lahko zgodba več koncev, poglejmo si dva najbolj verjetna: rdeče-črnega močerada najdejo (o njegovi takratni kondiciji raje ne razmišljam) ali zavarovalnica povrne odškodnino in si pri novem bodočem transportnem sredstvu lahko premislim glede vrste, barve in opreme. Zgodba se tako konča.

Kaj pa, če bi ta članek lahko že kak mesec pred izidom Sistemov ujeli kje na spletu in jaz ne bi o tem vedela nič? Ali če bi naslednja uspešnica Dana Browna nenadzorovano in seveda brez privoljenja njega ali njegovega založnika ušla z domačega računalnika v javnost? Če že avto v tej ali oni obliki dobite nazaj, Danu Brownu nič ne bi moglo povrniti prihodka od izgubljenih bodočih kupcev njegove knjige, četudi najdejo in javno linčajo capina, ki mu je naredil škodo.

Obvladovanje informacij je danes krasen biznis, prodaja skrivnosti pa še bolj. Na ilegalnih črnih trgih nastaja nov poslovni model, po katerem se da odlično zaslužiti, a ima eno posebnost: pomembno je, da se tistemu, ki mu jemljejo, sploh ne sanja, da se je kaj zgodilo. Najpopolnejši nevidni dotiki so najbolj cenjeni in najdlje prinašajo denarce, zato je nastalo kup pripomočkov, ki skrbijo, da so dotiki res čim dlje nevidni. Samo zaganjanje protivirusne zaščite, redno nalaganje popravkov, požarna pregrada ter občasno upoštevanje varnostne politike vam bodo proti njim pomagali približno toliko kot kamilice proti gripi.

Zdaj pa iskreno: ste si pri pripravi prijave na pomemben razpis ali večje ponudbe stranki kdaj potiho zaželeli, da bi kot muhica pribrenčali okrog konkurentovega monitorja in tako izvedeli vsebino njegove ponudbe, skupaj s ceno? Sploh, če so vas že nekajkrat zaporedoma premagali in zelo težko čakate na novi posel? Če ste rekli ne, upate pihniti v pojočo travico? Ali če obrnemo ploščo, kdaj ste nazadnje pripravljali pomembno ponudbo za še bolj pomembno stranko, pa vam je nekdo za nekaj malega razlike v ceni posel speljal pred nosom? Ste vprašali: le kako so vedeli? Ko se podjetja borijo za moč ali obstoj, je linija med poslovno še sprejemljivim in nelegalnim precej zamegljena. Če je dovoljeno in v nekaterih delih sveta celo nekaj zelo običajnega, da si poslovni partnerji pri dogovarjanju za posel pomagajo z alkoholom, denarjem in drugimi opojnostmi, tudi izkušnja, ki je pred časom odmevala pod imenom »izraelski trojanski škandal«, ni prav nič nepričakovana. Nenavadno je le to, da so jo odkrili, a če ne bi bilo zraven naključja, še danes ne bi nič vedeli o njej. Začelo se je, ko je pisateljski par iz Izraela slučajno odkril delčke svoje nove, še ne povsem dokončane knjige, na spletu. Po prijavi policiji so ugotovili, da je užaljeni bivši zet izdelal nanoprogramček z zlobnimi nameni in ga namestil na računalnik. Tako je prišel do dokumenta, ki ga je objavil. Nato je uporabil nov poslovni model: trojanca je prodal domačim detektivom. Za njih je to samo še ena od napravic, ki jih rabijo vsak dan in ki jim je zelo olajšala delo pri pridobivanju »competitive intelligence« podatkov. Naročila so jih velika in uspešna podjetja, med njimi nekatera pomembna mednarodna, mobilni operaterji ter članice newyorške borze. Industrijska špijonaža se je preselila v digitalni svet, kjer je vse bistveno bolj preprosto od tradicionalnih metod. Dokler niso trojanca začeli iskati policisti, ni nihče nič opazil. Popoln nevidni dotik.

Vedno znova sem presenečena nad lahkotnostjo, s katero pomembni ljudje v podjetjih ravnajo s svojimi najbolj zaupnimi digitalnimi podatki. Če so že pozorni pri osebnem stiku, internem PR in prav nadležni s skrivanjem notranjih podatkov pred zaposlenimi, so pri ukvarjanju z digitalno obliko podatkov precej površni. Na kraj pameti jim ne pade, da bi skrivnosti pošiljali na dopisnici ali jih obesili na oglasno desko, zelo malo pa jih šifrira komunikacijo ali pospravlja pomembne skrivnosti na šifrirane dele diska. Velikokrat za svoje potrebe zahtevajo dostop do več informacij ali odpiranje vrat na požarnih pregradah. Ko zaposlenim dovoljujejo, da v omrežje z nelegalnimi programi prinašajo sovražno kodo in varnostne luknje, izpostavljajo svoje podjetje, svoj posel, poslovne rezultate, lastnike in zaposlene. Ker s prenosnimi računalniki velikokrat gostujejo v drugih omrežjih in jih odnašajo domov, kjer je praviloma manj varno okolje, so še bolj zanimiva tarča. Več ponudb ko pripravijo, o

višjih številkah govorijo, z bolj pomembnimi strankami se lahko pohvalijo, bolj so na udaru. Če je podjetje na borzi ali nekje med enim in drugim lastnikom, če gradi sisteme za vojsko, državne finance ali banke, je vsaka poslovna informacija lahko vredna tudi toliko kot moj sanjski Bugatti ali še več. Ko odpirate digitalne čestitke in prejemate lepe želje, imejte v mislih, da je praznični čas rajsko obdobje za hekerje. Upam, da bo med njimi malo tistih z nevidnim dotikom.

Zato naj vam v novem letu zaželim čim manj izgubljenih poslov, ki bi jih lahko dobili, če le vdiralci v vaš sistem ne bi vedeli zanje.

Stanka Šalamun
Objavljeno v reviji Sistemi (priloga revje Monitor), januar 2005