

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

Nesrečna smrt ene srečne iluzije

Juhu, pomembni smo!

Nekako se ne morem upreti razmišljanju o prav filmskem ropu, ki se je pred kratkim zgodil v eni od slovenskih institucij. Saj veste, o čem govorim. Razlogov, zakaj se mi zdi, da vlom v bančne sefe vsaj malo spada tudi v kolumno o učinkoviti digitalni nevarnosti, je več. Prvi je v dejstvu, da napadena organizacija v glavah uporabnikov, državljanov ter po zakonu spada v skupino »tistih bolj varovanih v državi«, »tistih, ki najskrbneje varujejo naše osebne podatke, denar, diamantne orglice in vrednostne papirje«, »tistih, ki že vedo, kaj delajo«. Večina denarja je danes v digitalni obliki, na računalnikih taistih institucij. Še ena pomembna podrobnost postavi predrzne, garaške varilce ob bok tihim, a odločnim tatovom bitov informacij (torej zlobnim hekerjem): niti pod razno se nam ne more sanjati, katere dragotine so odnesli. Hakerji so se sposobni skrivati v zaprtih delih računalniških omrežij včasih tudi mesece, preden jih odkrijejo, in ne le borih sedem ur. V primeru kraje digitalnih informacij je stvar še bolj zapletena, saj tudi po pretepanju hekerja ne moremo vzeti nazaj vseh skrivnosti, ki jih ve in jih je verjetno prodal naprej. Tudi to bi morali vedeti iz filmov.

Nekaj dobrega pa je vseeno prišlo iz te nesrečne situacije: končno smo si dokazali, da smo tudi v tej mali lepi deželici postali očitno pomembni in zanimivi in se tako postavili ob bok največjim. Kaže, da imamo denar in zlatnino, ki druge zanima tako zelo, da so nam jo pripravljene ukrasti. V teminah naših sefov ležijo izjemne informacije, označene skoraj kot vojaške skrivnosti, zgodovinski okostnjaki, vsemogočne črne liste ter kupi vrednostnih papirjev. Nekaj posameznikov je bilo pripravljenih vso noč variti, da bi prišli tja, kamor se baje ne da. Ker gre pri fizičnih vdorih za precej tradicionalni pristop, ki ga v večjih državah že počasi, a zanesljivo izrivajo bolj oddaljeni, anonimni ter digitalni napadi, se ne moremo delati, da sporočila nismo slišali.

Slovenci iskreno verjamemo, da so naši najintimnejši podatki odlično pospravljeni. Očitno se nam zdi dovolj varno, če organizacije občasno zaganjajo protivirusno zaščito in nalagajo popravke, kupijo požarno pregrado, izvedejo neke vrste on-line overjanje (če se le da z digitalnim podpisom) ter uporabijo nekaj malega kriptografije, karkoli že to je. Ja, pa nič ne škodi, če povedo, da so usklajene z varnostnimi standardi, ki morajo biti v skladu z direktivami EU. Nič o tem, če to sploh kaj deluje, če so standardi primerni za nas in če se jih sploh kdo drži. Vsak učinkovit vdor in sistem je kot v posmeh, da smo počeli napačne stvari in da nam je morda zmanjkalo časa ali volje za vključitev najpomembnejše varnostne funkcije - zdrave pameti. Ta bi nam povedala, da se največ varnostnih problemov zgodi, ker zatajijo malenkosti.

In zdaj tisto, kar res lahko boli. Morda ste med tistimi, v čigar sef so vdrl. Morda imate sef pri kateri drugi banki, v katero pač še niso vdrl, zelo verjetno pa imate pri kateri od bank vsaj transakcijski račun. Če obvladate računalnik in dostop do interneta, verjetno uporabljate spletno bančništvo. Zagotovo pa imate EMŠO številko in davčno številko, ki ju lahko izve prav vsak, ki bi ga to lahko zanimalo. Imate kreditne kartice, zdravstveno kartoteko z vsemi vašimi boleznimi, vsakoletno davčno napoved, z malo sreče vrednostne papirje, premičnine in nepremičnine, zdravstvena in druga zavarovanja, morda ste se po naključju ali z razlogom znašli v policijski ali sodni evidenci. Vse to je zapisano nekje globoko v digitalnih nedrjih naših najbolj varovanih finančnih, državnih in drugih institucij.

In v nekatere od teh organizacij vdrejo, mar ne? Takrat se pokaže, kdo je tisti, ki bo plačal za neučinkovito varnost. Če vam bo z bančnega računa zmanjkalo kaj denarja in bo zgledalo, kot da je heker za to izrabil vaš računalnik, vam bodo povedali, da ste bili obveščeni, da morate skrbeti za varnost svojega računalnika. Ko boste zavrnil tisto čudno transakcijo, razvidno z mesečnega izpiska bančne kartice, bodo rekli, da bi morali javiti prej in zakaj niste bili pri plačevanju bolj previdni. Ženi boste po objavi medicinskih kartotek na spletu morali razlagati, od kot v mladosti tista spolno prenosljiva bolezen. Sosedje se bodo hahljali nad seznamom vaših prometnih prekrškov. Ker so na drugem koncu sveta vdrl v pomembno bančno institucijo, so preklicali kup potencialno napadenih kartic, med njimi tudi vašo, in tako se boste osramotili pred pomembnimi poslovnimi partnerji na večerji, ki je ne boste mogli plačati. Seveda pa boste morali plačati tisti ogromni telefonski račun, ki so ga iz vašega računalnika pridelali nevidni »dialerji«. In ja, ostali boste brez tiste zlatnine, milijonov in skrivnosti, ki ste jih baje imeli varno pospravljeni v bančnem sefu, zavarovanje in pogodba gor ali dol. Razlagati boste morali, kaj vse imate v njih, nato kako ste do tega prišli in zakaj ste upravičeni do tega. Vso zgodbo boste nekajkrat ponovili: policiji, kakšni komisiji, zavarovalnicam, na sodišču. Ogromno dela pri zaježitvi škode boste opravili sami. Veliko vašega časa bo šlo za to. Dosti živcev in denarja. Veliko korakov od enega birokratskega okenca do drugega. Največjo škodo boste zase plačali sami, zato morate tudi sami začeti razmišljati zase. Ne glede na to, kaj vam govorijo, tiste srečne iluzije, da bo nekdo drug poskrbel vašo varnost, ni več.

Zato že končno začnimo na glas govoriti, da hočemo več resničnega varovanja. Manj izgovorov. Ogromne kazni za tiste, ki ne spoštujejo standardov, kot je čisto normalno v drugih panogah. Več nadzora nad igranjem z našimi podatki in lastnino. Odvzem licenc podjetjem in posameznikom, ki nas izpostavijo. Manj marketinške megle, več preverjanja varnosti. Če bo pravi čas zelo bolelo njih, bo kasneje manj bolelo nas. Če pa se najhujše že zgodi, po ameriškem zgledu zahtevajmo odškodnino.

Stanka Šalamun

Objavljeno v reviji Sistemi (priloga revije Monitor), november 2005