Vsak sistem, napravo in človeka **je mogoče zlorabiti**

Milan Gabor je etični heker, ki podjetjem in organizacijam pomaga dvigati raven informacijske varnosti. Pogosto opozarja tudi na pereče težave na področju varnosti, saj meni, da le izobraževanje in ozaveščanje ljudi lahko poskrbita za varnejšo družbo in delovanje podjetij. Kot opozarja sogovornik, varnost zgolj na papirju ne koristi nikomur.

Miran Varga

▶ Ste strokovnjak za računalniško varnost. Uporabniki se bojimo predvsem kriptovirusov, česa pa se bojite vi?

Na področju IT se bojim predvsem invazije v zasebnost, ki jo spretnim napadalcem omogoča tehnologija. Večkrat na kakšnih predavanjih ljudem pokažem, da se v pametnem in povezanem svetu zasebnost kaj hitro konča. In to ne nujno zunaj človeka, napadalec lahko pride celo do podatkov v nas. Na različne načine, npr. prek pametnih zapestnic, srčnega spodbujevalnika, zelo sveža tema so zlorabe brezžičnih vibratorjev. Danes je praktično vsak sistem in napravo mogoče zlorabiti, če napadalec oziroma napadalci le ima(jo) dovolj časa, denarja in motivacije.

▶ Omenili ste, da delujete tudi kot etični heker in podjetjem pomagate odkrivati varnostne ranljivosti. Kako ranljiva so po vaši oceni slovenska podjetja v povprečju?

Stanje varnosti IT v domačih podjetjih je zelo odvisno od panoge, v kateri delujejo. Bančni sektor je dobro varnostno urejen, izvaja tudi redne varnostne preglede, to mu navsezadnje narekuje regulativa, preostala podjetja pa sama presodijo, koliko bodo vlagala v varnost. Nekatera sploh ne vidijo potrebe po informacijski varnosti, temveč se jim zdi le nepotreben strošek. Verjamem, da se bodo stvari korenito spremenile s prenovljeno splošno uredbo o varstvu podatkov evropskih državljanov (GDPR), saj bodo podjetja kazensko odgovorna za zlorabe podatkov svojih strank in uporabnikov. Te kazni ne bodo majhne. Sicer se vprašanje nanaša na podjetja, a omeniti velja tudi državne ustanove, za katere menim, da se z vidika informacijske varnosti izboljšujejo. Država je sprejela Strategijo kibernetske varnosti, Svet za nacionalno varnost je prevzel general. Tudi na trgu opažam vedno več povpraševanja po varnostnih rešitvah in ozaveščanju ljudi. To pomeni, da se podjetja in organizacije bolj zavedajo digitalnih nevarnosti.

▶ Toda država je predvsem birokratski organ. Menite, da bo znala upravljati varnostne politike in pristope v lastno dobro in dobro vseh državljanov?

Slovenija se je začela varnostno prebujati. Že 15 let imamo Urad Vlade Republike Slovenije za varovanje tajnih podatkov, za katerega si želim, da bi bil predvsem operativni in ne birokratski organ. Informacijska varnost se dogaja predvsem na operativni ravni, varnosti zgolj na papirju pač ne potrebujemo.

▶ Kako zgovorno je ravnanje državnega organa AJPES, ki je svoje varnostne težave kljub opozorilom tehničnih skupnosti in medijev skušal le ignorirati in pomesti pod preprogo?

Varnostna problematika organa AJPES je lep zgled tega, kako določene stvari v Sloveniji niso urejene. Ena takih je vsekakor odgovorno razkritje, o katerem prej ni bilo javne razprave. Težava je tudi v odzivu na informacijo o ranljivosti – namesto, da bi čim prej odpravili ranljivost, so s prijavitelji, javnostjo in mediji raje polemizirali o njej. Na tem področju Slovenijo čaka še veliko dela, v bistvu sploh ni pripravljena na programe iskanja varnostnih pomanjkljivosti, kot jih pozna tuja praksa. Tam velika podjetja, varnostna podjetja pa tudi države razpišejo nagradni sklad za iskanje ranljivosti v programski opremi ali spletnih storitvah in povabijo javnost k iskanju vrzeli. Končni rezultat je bistveno varnejša aplikacija ali storitev. V Sloveniji bi morali to področje najprej pravno ustrezno urediti, šele potem sledita sprememba kulture in sama izvedba.

Če nas nedelovanje podjetja stane milijon evrov na dan, lahko za varnost namenimo do milijon evrov sredstev.

▶ Za informacijsko varnost pogosto slišimo, da je vedno kompromis. Kako velik kompromis pa naj bo, da bomo vendarle mirno spali?

Odvisno od področja – čim več denarja imamo na voljo za informacijsko varnost, tem lažje je. Znesek bi vsekakor moral biti večji od minimalnega. V informacijsko varnost moramo vlagati premo sorazmerno s kritičnostjo naših podatkov. Sistemi kritične infrastrukture in banke bodo torej vlagali veliko, posamezniki pa manj. Vsak podjetnik in podjetje bi si morala izračunati, koliko ju stane, če en dan ne delata. To je hiter izračun in dober pokazatelj tega, koliko bi morali biti pripravljeni vlagati v varnost. Potem je tu še odnos do tveganja. Če nas nedelovanje podjetja stane milijon evrov na dan, lahko za varnost namenimo do milijon evrov sredstev. Metrike so različne, a velika podjetja, ki nekaj dajo na varnost svojih podatkov, vlagajo vanjo okoli dva ali tri odstotke letnega prometa.

▶ Če izvzamemo banke in podobna podjetja, ki načrtno zaposlujejo tudi strokovnjake za informacijsko varnost, kako lahka tarča s(m)o vsi drugi?

V celotnem ekosistemu varnosti IT je človek najšibkejši člen, predvsem zaradi pomanjkanja ozaveščenosti in izobraževanja. Tudi precej lažje ga je napasti kot korporacijo. V bistvu danes napadalcu sploh ni treba iti v banko, temveč »zlorabi« njenega uslužbenca. Ta bo naslednji dan v službi odprl prenosni računalnik z našo zlonamerno priponko in nam omogočil dostop v omrežje banke. Tako preprosto je. Včasih v šali rečem, da so ljudje najšibkejši člen prav zato, ker ne posodabljajo svoje strojne programske kode (angl. firmware). Če naj posameznik ne bo več zgolj tarča in žrtev, se mora izobraziti o nevarnostih, ki mu pretijo. Pomagajo le varnostni treningi, pa tudi medijska pozornost – čim več se piše in govori o varnostnih incidentih, tem prej bodo ljudje ugotovili, da kaj takega lahko doleti tudi njih.

▶ Kaj pa ponudniki storitev IT iz oblaka – različni sistemski integratorji, telekomunikacijski operaterji in drugi, kako varna so njihova okolja in podatkovni centri, če začnete vanje vrtati vi s svojo ekipo? Mar svoje podatke zaupate oblaku?

Lahko rečem, da zaradi same narave dela podatkov ne hranim v javnih oblakih, temveč v lastnem oblaku. Kar pa zadeva informacijsko varnost ponudnikov oblačnih storitev, ne morem dati neke pavšalne ocene – brez preverjanja jo namreč težko ocenim. Žal so primeri, ko se je že pokazalo, da napadalci lahko dostopajo tudi do podatkov v oblaku. V bistvu v povezavi informacijske varnosti in oblaka vidim drugo težavo. Ste se kdaj vprašali, kaj se zgodi, ko oblak neha delovati? Mar takrat ostanemo brez vsega? Bomo sploh lahko ugotovili, kdo je kradel in kaj je ukradel? Kako naj ga ulovimo? Če nimamo strežnikov v oblaku, bomo težko iskali digitalne sledi napadalca. Prav zato sem skeptičen glede rabe oblaka. Za preproste in manj občutljive aplikacije in storitve se mi sicer zdi primerna rešitev, za hrambo za poslovanje kritičnih in zaupnih tajnih podatkov pa nikakor.

▶ Torej za vas oblak ne pride v poštev?

Redko. Tudi moje stranke se ne bi strinjale s tem, da se njihovi podatki oziroma njihove vrzeli v sistemu varnosti hranijo nekje v oblaku. Na to ne bi nikoli pristale in bi se mi le zahvalile za sodelovanje. Toda to ne pomeni, da nimamo svojega oblaka, kjer so ti podatki varno spravljeni.

▶ Ste že bili tarča hekerjev?

V moje podjetje poskušajo vdreti vsako leto, a niso bili napadalci nikoli uspešni. Bolj me čudijo druge vrste »napadov«. Občasno namreč v podjetje prejmemo t. i. nespodobne ponudbe, vprašanja, ali bi lahko »pohekali« nekega človeka, podjetje, aplikacijo ali storitev. Tega se seveda ne gremo, hekamo le okolja IT podjetij, ki to od nas naročijo in so stvari pogodbeno urejene. Etični heker ima za razliko

od klasičnega hekerja jasno postavljene meje.

▶ Ob vsesplošni digitalizaciji postajajo bolj povezani in hkrati izpostavljeni tudi veliki sistemi, denimo energetika, oskrba z vodo, nafto, plinom ... Kako dobro je zaščitena kritična infrastruktura naše države?

Veseli me že to, da nam je uspelo definirati, kaj kritična infrastruktura države sploh je. Glede na uredbo o kibernetski varnosti je jasno, da gredo stvari naprej. Država se torej zaveda, da padec telekomunikacijskih storitev ali pa zlorabe semaforjev ali pa prometa na železniških tirih lahko povzročijo znatno motnjo v delovanju države in naših vsakdanjih življenj. Torej morajo imeti ti sistemi višjo stopnjo varnostnega tveganja. Težava je v tem, da gre skoraj povsod za sisteme, ki so stari več let ali celo desetletij. Dokler niso bili povezani v internet, je bilo tveganje manjše. V intranetu nihče ni skrbel za varnost, niti je ni potreboval. Danes so ti sistemi dostopni prek splet a predvsem zaradi udobja sistemskih skrbnikov, to pa ni najboljša praksa. Odpiranje navzven je z varnostnega stališča nevarno, tudi če gre za nadzirano odpiranje.

▶ Kakšen bi sicer bil vaš grob nasvet za posameznika in podjetje - kako se vsaj približno ustrezno zavarovati, da ne bo(mo) prav najlažja tarča?

Osnove so napreden požarni zid, ki omogoča vpogled v napade od zunaj in znotraj, sistemi odkrivanja in preprečevanja vdorov ter predvsem ljudje, ki z varnostnimi rešitvami upravljajo in nadzorujejo področje informacijske varnosti. V podjetjih je prav človeški dejavnik največkrat šibki člen, opremo podjetje še kupi, na ljudi in njihovo izobraževanje pa prepogosto pozabi. Tako nastane težava v tem, da varnostne rešitve niso dobro konfigurirane, vse deluje na privzetih nastavitvah itd. Krivda je tudi na strani podjetja, ki je v vlogi naročnika opreme in storitve – od izvajalcev bi moralo zahtevati preprosto več. Tako pa velikokrat ob varnostnih pregledih naletimo na požarne zidove s privzetimi gesli, kar pomeni, da pridemo v zaledne sisteme praktično brez truda. Tudi kriptiranje prenosnih naprav, ki naj bi bilo osnova, da ne pride vsak napadalec do podatkov v njih, je v domači praksi prej izjema kot pravilo.

▶ V filmih, ki so bolj ali manj natančen približek realnega stanja, vidimo, da imajo tudi vojske posameznih držav posebne oddelke za kibernetsko vojskovanje. Mar imamo kaj takega tudi pri nas? Se branimo ali napadamo?

Slovenija ne more prevzeti nobene vloge, ki jo opisujete. Še najboljši opis trenutnega stanja je to, da smo v Sloveniji gasilci varnostnih incidentov, ki se nam dogajajo. Uredba o kibernetski varnosti je sicer dober zametek, da se nekaj premakne naprej. Slovenija ne bo nikoli kibernetska velesila na področju vojskovanja. Že zaradi svoje velikosti – je bistveno premajhna. Strokovnjake in znanje posameznikov sicer imamo, nimamo pa nekaj deset tisoč hekerjev, da bi bili na področju vojskovanja ali zaščite res lahko konkurenčni svetovnim velesilam.

▶ Bo tretja svetovna vojna res zgolj v spletu? Se že dogaja?

Spletne vojne se že dogajajo. Prva je bila med Rusijo in Ukrajino, ko so ruski napadalci prevzeli nadzor nad delom energetskega omrežja sosednje države in četrtino njenega energetskega sistema ugasnili za več dni. Menim, da bo spletno vojskovanje nepogrešljiv del sodobnega vojskovanja, lahko celo odločilen. Če bi nam, denimo, sovražnika uspelo s kibernetskimi napadi onesposobiti, denimo, da bi mu preprečili, da bi vojsko poslal v zrak, po morju ali kopnem, mu onemogočil komunikacijo z vojaki, bi bili v veliki prednosti. Če ugasneš stolp na letališču, letala težko vzletijo ali pristanejo.

▶ Danes je ranljiva skoraj vsaka tehnologija, kje pa vi opažate največ varnostnih pomanjkljivosti? So to žična ali brezžična omrežja, mobilne naprave, stari sistemi, kaj drugega?

Naša praksa kaže, da so daleč najbolj ranljive spletne aplikacije. V požarne zidove in brezžična omrežja je bistveno težje vdreti, če nekdo nastavi dobro in dolgo geslo. Penetracijski testi so uspešni predvsem na aplikacijski ravni. Razvijalci aplikacij imajo žal še vedno precej šibko zavedanje glede varnosti IT, dejal bi, da so celo drugi najšibkejši člen, takoj za zaposlenimi. Večkrat nevede napačno programirajo aplikacije in puščajo obilo možnosti za vdore.

▶ Zelo učinkovita metoda napada so tudi tehnike socialnega inženirstva. Smo ljudje res najšibkejši člen varnostne verige?

Definitivno. Pa še na slabše nam gre. Ljudje se sploh ne zavedajo, da so podatki, ki jih vehementno objavljajo v družabnih in drugih omrežjih, v napačnih rokah zelo koristni. Še pred desetletjem in pol je bilo težko zbrati uporabne podatke o posamezniku, če niste bili ravno obveščevalna služba, policija ali kriminalisti. Danes pa na Facebooku najdete vse in še več, lahko si preberete, kaj imajo ljudje radi in česa ne, kaj jedo, počno in kdaj. Ime in priimek ali pa telefonska številka so dovolj, da o posamezniku izvemo vse. Če napadalec te podatke kombinira s psihologijo, je praktično vedno uspešen – vsak pade. Žalostno je predvsem to, da se ljudje sploh ne zavedajo nevarnosti, ki jim preti. Če greš na dopust, tega podatka ni dobro objaviti na Facebooku, ker te lahko ob vrnitvi pričaka prazno stanovanje.

▶ Kaj bi morali storiti, da uporabniki tehnologije vendarle ne bi bili najšibkejši člen?

Če hočemo voziti avto, moramo narediti izpit. Drugače je iluzorno pričakovati, da bi delali izpit za uporabo interneta, a izobraževanje in ozaveščanje morata biti prisotna. Ljudem je treba razložiti, kaj je nevarno. Mediji lahko veliko naredite za ozaveščanje uporabnikov vseh vrst tehnologije. Ljudje se morajo začeti zavedati, da svojega pametnega doma ne smejo objavljati v internetu, drugače kar sami kličejo nepovabljene goste.

Spletni uporabniki so Microsoftovega klepetalnega robota na Twitterju v dveh dneh spremenili v nacista.

▶ Eden izmed glavnih razlogov, zakaj internet stvari še ni dosegel na desetine milijard naprav, kot mu sicer prerokujejo, je prav varnost oziroma pomanjkanje varnosti. Kako bi ga vi »popravili«?

Internet stvari je iz dneva v dan bolj zanimiv za vse, tudi za napadalce. Milijarde povezanih naprav so izjemna priložnost. Danes je internet stvari nekakšen divji zahod, v njem najdemo na milijone naprav z aplikacijami, skoraj vse je ranljivo, ker je na hitro napisano v želji po čim hitrejšem lansiranju izdelka/storitve na trg, nihče pravzaprav ne ve, kje vse so razpoke, ki jih lahko izkoristijo napadalci. Kamera v sobi lahko snema aktivnost/spanje dojenčka ali pa napadalcu omogoči kukanje v spalnico nekoga ... Zloraba večjega številna naprav interneta stvari lahko vodi tudi do izjemnih napadov DDoS na kakršnokoli tarčo. Menim, da bo treba v prihodnje tudi v internetu stvari uvesti segmentiranje, podobno kot to danes počno podjetja na ravni omrežja. Imeli bomo ločeno omrežje za domače naprave, ki predstavljajo visoko tveganje, in drugo za poslovne naprave. Univerzalnega recepta in smernic, kako enostavno zaščititi internet stvari in ga narediti varnega, še ni. A verjamem, da bo varnost v internetu stvari stvar evolucije, podobno kot smo v brezžičnih omrežjih dobivali vedno boljše metode enkripcije podatkov (WEP, WPA, WPA2).

▶ Kriptovirus WanaCry je maja samo v enem vikendu pokazal svetu, kako ranljivi so pravzaprav starejši sistemi. Kako ste njegovo širjenje in sam napad doživljali vi?

Virus WannaCry je tudi nam spremenil načrte tisti vikend. Dogajanje smo aktivno spremljali, se igrali z virusom in bili v pripravljenosti, če bi katera izmed naših strank potrebovala pomoč. Pozneje se je sicer izkazalo, da je bila morebiti napoved glede nastanka novih variant in mutacij virusa tega, vendar preveč previdnosti ne škodi. Smo bili pa presenečeni nad hitrostjo izdaje popravka s strani Microsofta, saj je čez konec tedna izdal popravek za sisteme, na katere je že uradno pozabil. Glede na to, kako so ustavili širjenje virusa, bi lahko rekli, da smo v tem konkretnem primeru imeli srečo. Te sreče morda naslednjič ne bo.

▶ Menite, da bi lahko umetna inteligenca pomagala pri reševanju informacijskih varnostnih izzivov? Kako?

Vidimo, da nekateri ponudniki varnostnih rešitev tehnologiji umetne inteligence in t. i. globokega učenja že uporabljajo za analiziranje anomalij, prepoznavanje vzorcev, odkrivanje netipičnih napadov v omrežju. Takšna tehnologija lahko pomaga k dvigu varnosti, saj vidi več stvari in prej kot ljudje. Smo pa priča tudi ponesrečenim poskusom umetne inteligence. Spletni uporabniki so Microsoftovega klepetalnega robota na Twitterju v dveh dneh spremenili v nacista. Tudi poskusi, da bi umetna inteligenca sama pisala programsko kodo, se doslej niso obnesli. Videli bomo, ali bo umetna inteligenca v prihodnje poleg zaznavanja napadov lahko uporabljena tudi za preprečevanje napadov. Zaenkrat tako daleč vendarle še nismo.

▶ Mar posameznikom varnostni ukrepi nekaterih držav, ki »vohunijo« za nami, nas digitalno »spremljajo«, že škodijo? Ali je varnostnih mehanizmov in politik kdaj celo preveč?

Zavedati se moramo dveh svetov. Sveta velikih in malih. Prvi si nekako prilašča pravico, da nadzoruje (več od) drugega. Pomembno je, da se na to opozarja in nasploh govori o tem. Vohuni se že od nekdaj, v tehnološko obarvanih časih so drugačne le metode. Tehnologija in sistemi omogočajo zbiranje velikanskih količin podatkov. Bolj nas mora skrbeti, kaj nato počno z njimi. Jih le analizirajo v imenu naše varnosti, prodajajo tretjim osebam? S tem se ne smemo sprijazniti. Na tej točki ljudem večkrat rečem, naj zmaga zdrava kmečka pamet. Treba se je ustaviti in premisliti. Treba je kdaj reči ne in kaj zadržati zase. Tudi v podjetju ima direktor informatike, tako kot vsak posameznik, možnost, da neke aplikacije ali storitve z »nemogočimi« pogoji ne uporablja. A je zato prikrajšan za uporabniško izkušnjo. V svetu »brezplačnih« aplikacij in storitev se je namreč že velikokrat pokazalo, da če uporabnik za neko storitev ne plačuje, je »plačilo« on sam oziroma njegovi podatki. ◀