OB ROBU

Najprej zlorabiš sam sebe, potem te še drugi

SIMONA ŠOLINIČ

Pred štirinajstimi dnevi smo pisali o podobnih, a manj nevarnih izsiljevalskih virusih, s katerimi so že v preteklem letu neznanci okužili tudi računalnike podjetij na Celjskem. Če kdaj, potem zdaj organi pregona jasno vidijo, da bi morali računalniški kriminaliteti posvetiti več pozornosti.

Isti preiskovalci, ki večkrat vodstvo policije sami opozarjajo, da delajo na stari in dotrajani računalniški opremi, naj bi preiskovali, kdo so »hekerji«, ki so sto svetlobnih let pred vsemi glede razmišljanja, znanja in opreme.

Petkov izsiljevalski virus je najbolj prizadel industrijo in zdravstvo v nekaterih državah. Gre za dve panogi, kjer se tehnologija razvija z astronomsko hitrostjo. Kjer se obračajo mastni denarji. Kjer je zaposlenih največ ljudi. Kjer se investira v robotizacijo sistema, delovnega procesa. Potem se zatakne pri stroških oziroma naložbi v informacijsko varnost?

Podjetja in organizacije imajo oboroženе varnostnike, da preprečujejo neželene prihode, vlome, tatvine, in potem jim jo zagode virus, ki pride po – elektronski pošti. Kdo nosi za to delno odgovornost?

Kup težav je. Tudi pri preiskavah. Storilce, ki počnejo takšna kazniva dejanja na spletu, je zelo težko izslediti, saj se zgodi, da imajo svojo »računalniško-hekersko bazo« tudi v tujini. Preden policija, če sploh, koga izsledi, naleti na birokracijske ovire med več državami in več tujimi organi pregona. Kako to izgleda? Za en podatek morajo slovenski policisti izpolniti kup dokumentov, jih poslati v tujino, celo prevajati, čakati. In medtem ko čakajo na odgovor, se kazniva dejanja prosto po Prešernu nadaljujejo.

Saj ne gre le za pošiljanje virusa, kot je bil petkov. Gre za številne goljufije, o katerih smo že pisali. Kraja identitete, goljufije z elektronskimi sporočili, goljufije pri preprodaji stvari na spletu, da ne omenjamo spletnih zlorab mladoletnih. Slednje so zgodba zase, posebej zaradi težje dokazljivosti, da je spletni pedofil virtualno napadel otroka. Takšnega storilca bi po slovenski zakonodaji težko kaznovali – razen če se z otrokom ne dobi v živo. A takrat je ponavadi že prepozno.

Spletna kazniva dejanja so kazniva dejanja prihodnosti. Nanje nismo dovolj pripravljeni. Ne organi pregona ne sodstvo – kjer nekateri sodniki še vedno, namesto da bi snemali sojenja, saj imajo tehnologijo, narekujejo zapisnikarjem med sodno obravnavo – ne ljudje. Ko bo imel sodnik pred sebaj »hekerja«, ki bo o njem na en mah s pomočjo spleta izvedel vse, še preden bo stopil v sodno dvorano, bo verjetno skrajni čas za razmislek o dodatnem izobraževanju o spletni kriminaliteti.

Lahkoverni smo. Najprej na spletu zlorabimo sami sebe, ko lahkoverno mislimo, da smo varni, potem pa nas zlorabijo še drugi.

Zanimivo je, da se tehnologija tako razvija, da spletne aplikacije danes že določajo, kje se gibamo. Po drugi strani se soočamo s primeri pogrešanih oseb, kjer nekaj časa – ta je pri iskanju izjemno pomemben – čakajo vsak nov podatek, kje je bil nazadnje kdo, pri čemer se do tega podatka na podlagi ravno tehnologije zelo težko pride. Ali ni to ironija? Ali bi morali zakonodaja, predpisi, splet in policija na kakršenkoli način stopiti skupaj in to informacijsko tehnologijo razviti za pomoč pri reševanju takšnih primerov?

»Digitalna transformacija je prinesla mnogo pozitivnega. A kot vsaka stvar ima dve plati, tudi pri tem področju manj dobra stran. Mogoče je to treba gledati kot platformo, ki je prinesla polno pozitivnih stvari, ki jih je mogoče s pridom uporabiti. Mogoče je v tem vprašanju mogoče najti kakšno dobro idejo za nov slovenski start-up. Sam bi osebno takšno dobro idejo podprl, seveda pod pogojem, da bi bila aplikacija varna in da ne bi moje zasebnosti preveč zlorabljala.«

Organi pregona in sodstvo bodo morali bolj zagristi v izobraževanje o enem najnaprednejših področjih kriminala.

»Ni sistema, v katerega ne bi bilo mogoče vdreti«

Bi lahko bil petkov »hekerski« napad spodbuda slovenskim računalniškim zanesenjakom?

Približno tristo tisoč okuženih računalnikov, zastoj proizvodnje in dela v številnih industrijah in bolnišnicah po svetu. To je rezultat petkovega napada na Microsoftove operacijske sisteme z izsiljevalskim virusom, ki je blokiral delovanje računalnikov. Rešitev? Plačilo tristo evrov v virtualni valuti bitcoin za odblokado neznanim storilcem. Virus naj bi dosegel tudi Slovenijo. Po nekaterih podatkih naj bi bilo takšnih napadov osem. Med temi je najbolj znan iz podjetja Revoz v Novem mestu, kjer je bil rezultat okužbe z virusom štiristo vozil manj.

»Osebno se kraje identitete v Sloveniji ne bojim preveč. Za to obstaja preprost razlog – za veliko takšnih prevar smo premajhen narod. Če bi nas bilo vsaj desetkrat toliko, potem bi bilo lažje. Ker je Slovenija malo večja vas kakšnega velemesta ali države, je možnosti za to precej malo. Kar nas seveda ne odveže od odgovornosti, da moramo s svojimi podatki ravnati vestno. Nekateri primeri kraje identitete so že bili, vendar v zanemarljivem številu. Se je pa treba zavedati, da lahko takšna kraja marsikomu precej zagreni življenje.«

»Najšibkejši člen so uporabniki, torej ljudje. Če je tehnologija pravilno in ustrezno konfigurirana in je pod nadzorom, je na tem področju težje najti večjo ali kritično pomanjkljivost. Seveda je tehnologijo tudi upravljajo ljudje, kar v določenih primerih lahko pomeni precej visoko tveganje. V večini primerov danes napad začne sumljivo elektronsko sporočilo z okuženo priponko. Zato svetujem, da takšne elektronske sporočila dvakrat preverimo. Sam se izogibam recimo neznanim in sumljivim brezičnim omrežjem.«

Takšni »hekerski« napadi enostavno pomenijo, da ni sistema, v katerega ne bi bilo mogoče vdreti, meni **Milan Gabor iz podjetja Viris, kjer** skrbijo za varne informacijske sisteme. »Če incident malo bolj podrobno analiziramo, lahko vidimo, da so napadalci izkoristili varnostno pomanjkljivost, ki je bila javno objavljena pred dvema mesecema. Microsoft je sicer ponudil popravke, vendar kot smo videli, obstajajo sistemi, ki se jih v tem času ni posodobilo. Ta zadnji napad je tudi pokazal, na katerih področjih obstajajo vrzeli. Tako sta po tem napadu kar nekaj časa za okrevanje potrebovala zdravstvo in določen del industrije. Znano je, da sta ti panogi zelo konzervativni pri nameščanju popravkov, zato je imel virus v teh okoljih precej prosto pot.«

V zdravstvu in industriji o informacijski varnosti sicer že razmišljajo, vendar se velikokrat ustavi pri denarju. »V večini primerov je vlaganje v informacijsko varnost zanju čisti strošek, a se v napadih, kot smo jim bili priča zdaj, ta naložba v informacijsko varnost zelo hitro povrne.«

Ni meja

Za razliko od ostalih vrst kriminala je za računalniška kazniva dejanja značilno, da tu ni meja. In storilci so zviti. Napadejo tiste tarče, ki so zelo odvisne od informacijskih sistemov. Vedo, da se virus širi hitro. Torej dosežejo svoj namen. »Kot družba smo izredno ranljivi. Tudi zaradi precejšnje odvisnosti od informacijskih sistemov oziroma njihovega delovanja. Nekoč bi si težko predstavljali, da lahko zaradi računalniških sistemov ljudje umirajo, saj je bilo precej mehanskega sveta. Danes, v dobi digitalizacije, vidimo, da če se sistemi ustavijo, se nam lahko ustavi tudi življenje. Si lahko predstavljate, da bi Facebook prenehal delovati?« razmišlja Gabor.

Kadar poročamo o podobnih, sicer manjših okužbah računalnikov, zlorabah identitete in ostalih goljufijah na spletu, je treba priznati, da se redkokdaj zgodi, da storilec pristane za zapahi ali vsaj na sodišču.

Ali imamo v Sloveniji dovolj usposobljene kadre v policiji oziroma jih je sploh dovolj, da bi bili računalniškemu kriminalu kos? »Kolikor poznam situacijo, se organi pregona zavedajo, da jim primanjkuje znanja in da ne uspejo slediti vsem novostim na tem področju. Ampak ne zaradi tega, ker bi si želeli biti zadaj, ampak ker so te stvari povezane z več dejavniki. Prvi je nedvomno pomanjkanje denarja za nenehno izobraževanje in vlaganje v znanje kadrov. Naslednji dejavnik je plačni sistem, ki ni preveč stimulativen, zato se dobri kadri odločijo in poiščejo izzive kje drugje. Po drugi strani imajo kriminalci dobre finančne vire in tudi na črnem trgu se da marsikaj najti ali priskrbeti, zato jim ni treba spoštovati zakonodaje tako kot recimo organom pregona, kar lahko pomeni včasih precej veliko coklo pri preiskavi in pregonu takšnih dejanj,« meni Gabor.

Ob tem dovolj jasno izrazi tudi, da bi bilo smiselno o takšnih vrstah kaznivih dejanj izobraziti tudi sodstvo, saj imajo organi pregona včasih težave, ko morajo določene zadeve razložiti sodnikom.

Za denar ali le simbolni pomen?

In česa se lahko bojimo? Ne le izsiljevalskih virusov iz tujine, ampak tudi tistih virusov, ki so iz Slovenije! Zadnji petkov »hekerski« napad je namreč lahko »motivacija« za slovenske »hekerje«. Takšno skrb je izrazil tudi naš sogovornik.

»Slovenija premore poznavalce, ki bi lahko poustvarili podobne razsežnosti. Nekaj tednov nazaj smo bili priča napadu na zdravstvene domove, kjer so poskušali z okuženimi priponkami narediti podobno. Pri tem primeru je bilo zanimivo, da je bila slovenščina precej dobra, kar lahko posledično pomeni, da so bili v ekipi tudi slovensko govoreči člani. Ugibanje, ali bi jim lahko uspelo ali ne, je čista špekulacija.«

Se obeta računalniško-informacijski terorizem?

Slovensko zakonodajo je na tem področju država resda dopolnila, vendar samo zakonodaja ni dovolj, pravi Gabor, če organi pregona in sodstvo ne uspejo teh stvari tudi na sodišču uspešno pripeljati do konca. »Ravno zato je treba še toliko bolj investirati v izobraževanje teh organov.«

V sodobnem informacijskem sistemu je resda težko ugotoviti, od kod napad izvira, saj »hekerji« niso neumni in skrijejo svoje prave lokacije. »Poleg tega uporabljajo tudi ›pohekane‹ sisteme, ki jih je mogoče kupiti na črnem trgu. Tako da lahko sisteme napadajo računalniki iz naših krajev, napadalci so skriti nekje na drugem koncu sveta, vmes pa je še nekaj drugih sistemov. V večini primerov gre za denar, saj vemo, da se na digitalnem črnem trgu obračajo velike vsote, in to v različnih kripto valutah. Nekateri napadi imajo res bolj simbolni pomen – na primer za svobodo trgovanja – ali pa gre za druge aktivistične dejavnosti, vendar so te manj obsežne.«

Konec igre

Okužbe z virusi, ki zašifrirajo datoteke na računalnikih, nato storilci zahtevajo plačilo za odkodiranje, so med računalničarji znane kot »kripto napadi«. Sumljive priponke v elektronskih sporočilih so ljudje masovno v teh dneh dobivali tudi v Sloveniji.

Zakaj jih napadalci največkrat usmerjajo v podjetja? »Iz čisto preprostega razloga. Ljudje ostajajo še vedno najšibkejši člen v celotni verigi. Sistemski administratorji lahko poskrbijo za tehnične rešitve, vendar če uporabnik klikne na neko zelo ›sofisticirano‹ priponko, ki je posledica načrtovanega napada, je skoraj vedno konec igre. Zato je v takšnih primerih treba dvakrat preveriti, ali je pošiljatelj res pravi ali se samo izdaja za pravega. Ali res pričakujemo takšno sporočilo in ali ni malo čudno, da si je pošiljatelj izbral ravno nas kot srečnega dobitnika različnih nagrad,« svari Gabor.

Zato ljudem svetuje, naj se pred odpiranjem priponk ali pri sledenju povezavam vprašajo, ali je sporočilo res pristno in namenjeno resnično njim. Poleg tega poudarja, da sta redno posodobljen operacijski sistem in telefon danes skoraj že nuja.

Toda ljudje smo pogosto lahkoverni. Premalo vemo, kako smo lahko oškodovani že zaradi nedolžnega brskanja po spletu. »Razgalimo svoj navade, svojo lokacijo, svoje sisteme, ki jih uporabljamo. Takšne digitalne sledi puščamo vsepovsod, a se jih premalokrat zavedamo. Zato je pomembno tudi osveščanje uporabnikov na tem področju, saj se jih večina niti ne zaveda, da je lahko nedolžno sporočilo na družbenem omrežju povod za rop ali drugo dejanje. In tega osveščanja je premalo. Za vožnjo avta potrebujemo izpit in dokazilo, da to znamo. Če malo posplošim, za vožnjo po internetu ne potrebujemo ničesar,« še dodaja računalniški strokovnjak.

Gabor kot računalniški strokovnjak preverja varnost informacijskih sistemov na javnem in zasebnem področju. Imajo veliko lukenj? »O tem zaradi različnih pogodb o nerazkritju podatkov ne morem govoriti, vendar lahko rečem, da obstajajo podjetja, ki se te tematike dobro zavedajo, pri čemer so velikokrat omejena ali zaradi finančnih sredstev ali zaradi pomanjkanja drugih virov. Lahko pa rečem, da sem videl marsikaj in da me skoraj nič več ne more presenetiti.«

Varni Facebook, banke in spletni nakupi ...

Danes skoraj vsi uporabljamo Facebook in druga socialna omrežja, kjer anonimnosti skorajda ni, čeprav se marsikdo trudi zanjo. Toda ne gre. Večina ljudi živi v lažnem prepričanju, da lahko na družbena omrežja dajo dobesedno vse, kar jim v določenem trenutku pade na pamet.

»Če bi te stvari morali povedati v živo pred množico ljudi, bi najbrž ravnali drugače. To je pač past informacijske dobe, kjer digitalni svet nekateri dojemajo drugače kot realnega. Zato svetujem, da preden kdo karkoli objavi, to prebere in se vpraša, ali res želi to objaviti. Verjamem, da bo marsikdo zbrisal kakšno stvar pred objavo, če se bo kdaj spomnil tega majhnega testa. Dejstvo je, da vse ni za objavo na družbenih omrežjih,« dodaja Gabor.

Kljub različnim svarilom nas banke, ustanove prepričujejo, da se je varno naročiti po elektronski poti na pregled, plačevati položnice, račune za izdelke. Vse se prenaša na splet. Je to res vse tako zelo varno? Gabor trdi, da so takšni sistemi predmet rednih pregledov, saj se te ustanove zavedajo pomembnosti varovanja informacij.

»Je pa res, da je trajalo, da so uspele priti do tega. Seveda so si tudi izračunale, da je ceneje investirati v varnost sistemov kot potem gasiti požare in plačevati za povzročeno škodo. Bonke imajo na primer predpisano, da morajo enkrat letno izvesti zunanji varnostni pregled sistemov, in brez tega v bančnem svetu žal ne gre. Seveda se morajo tudi uporabniki zavedati, da so lahko najšibkejši člen, in morajo z gesli ali drugimi varnostnimi napravami skrbno ravnati.«

SIMONA ŠOLINIČ
Foto: Osebni arhiv MG

Sočasni preiskavi pokazali na dve kaznivi dejanji

Osumljenca ostala v priporu

Celjski kriminalisti so zaradi domnevnega sprejemanja podkupnine ovadili moškega, ki je bil zaposlen v podjetju, ki se ukvarja z opravljanjem tehničnih pregledov. Pri preiskavi so ugotovili, da naj bi 59-letnik z območja Celja sprejel denar in v zameno izpolnil zapisnik o tehnično brezhibnem vozilu, čeprav to ni bilo res.

Policisti so zaznali tudi primere, ko je oseba izpolnila zapisnik o opravljenem tehničnem pregledu in brezhibnosti vozila, čeprav avtomobila na tehničnem pregledu sploh ni bilo. Podjetje o početju zaposlenega ni vedelo, policija je namreč ovadila samo 59-letnika. Preiskava je trajala več mesecev, v njej pa so kriminalisti uporabljali tudi prikrite preiskovalne ukrepe.

Vzporedno je policija preiskovala še kazniva dejanja tihotapljenja tobačnih izdelkov, kjer sta se kot osumljeni pojavljali isti osebi, ki sta dajali podkupnine pri tehničnih pregledih. Zaradi sočasne preiskave tihotapljenja so bile pretekli teden hišne preiskave v Celju in Mariboru, od koder izvirata tudi osumljenca. Pri hišnih preiskavah so zasegli več kot pet tisoč zavojčkov cigaret in ugotovili, da sta osumljena doslej preprodala za najmanj 37 tisoč evrov cigaret. Gre za 60-letnika iz Celja in 48-letnega Mariborčana. Kriminalisti so ju v teh dneh pripeljali na zaslišanje k preiskovalnem sodniku, ki je za oba odredil pripor.

Foto: PU Celje

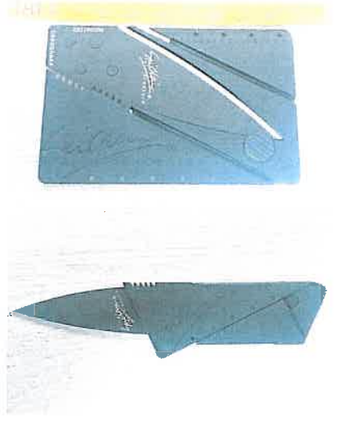
Za kaznivo dejanje tihotapstva je zagrožena zaporna kazen od enega do kar desetih let zapora.

Nož v kartici

Celjski prometni policisti so med nadzorom prometa vozniku zasegli nož v posebej prirejeni kartici. 22-letnega voznika osebnega vozila iz Braslovč so ustavili v nedeljo popoldne na območju Žalca.

Pri varnostnem pregledu so pri 22-letniku našli hladno orožje, prirejeno za napad. Šlo je za prikrit nož v obliki plastične bančne kartice, v kateri je bilo zloženo kovinsko rezilo, dolgo sedem centimetrov, ki se sestavi v nož. Med postopkom pregleda so pri vozniku odkrili in zasegli še dva mlinčka z ostanki rastlinske snovi, najverjetneje konoplje, in dve epruveti, prav tako najverjetneje napolnjeni s konopljo. Če bo potrjeno, da je šlo za prepovedano drogo, bo zoper 22-letnika uveden prekrškovni postopek zaradi posedovanja prepovedane droge in hladnega orožja, prirejenega za napad.

Foto: PU Celje



Padel in se hudo poškodoval

V Šentjurju se je v preteklih dneh zgodila huda prometna nesreča. 17-letni voznik motornega kolesa je med vožnjo po Cesti Kozjanskega odreda zaradi spuščene stranske kovinske opore za parkiranje izgubil nadzor nad vozilom. Pri tem ga je zaneslo čez bankino v varovalno ograjo. V trčenju se je hudo telesno poškodoval.

Spravil se je na hmelj

Policisti bodo ovadili 76-letnega domačina, ki ga je pretekli teden pri kaznivem dejanju zalotila detektivka. Moški je namreč povzročal škodo na bližnjem hmeljišču, tako da je izpulil več sadik hmelja. Policijo je na to opozoril lastnik nasada in podal predlog za pregon kaznivega dejanja.

Popravek

V prejšnji številki smo v prispevku z naslovom Za večjo varnost v križišču napačno navedli, da je na križišču v Medlogu postavljena opozorilna tabla, ki naj bi jo postavila Mestna občina Celje v sodelovanju s podjetjem Aktivna signalizacija Korun in z Zavarovalnico Maribor. To ne drži. Tablo je financirala Zavarovalnica Triglav. Za napako se opravičujemo.

Uredništvo