Bančni vestnik

REVIJA ZA DENARNIŠTVO IN BANČNIŠTVO

LJUBLJANA, LETNIK 72, ŠTEVILKA 9, SEPTEMBER 2023

KAZALO

Bančni vestnik

REVIJA ZA DENARNIŠTVO IN BANČNIŠTVO
THE JOURNAL FOR MONEY AND BANKING

ISSN 0005-4631

ZBS | Združenje bank Slovenije

Uredništvo in uprava Bančnega vestnika pri Združenju bank Slovenije / *The Bank Association of Slovenia*, Šubičeva 2, p.p. 261, 1001 Ljubljana, Slovenija, Telefon / *Phone*: +386 (0) 1 24 29 705, Telefax / *Fax:* +386 (0) 1 24 29 713, E-mail: bancni.vestnik@zbs-giz.si, www.zbs-giz.si, TRR / *Bank account*: SI56 0201 7001 4356 205.

Moramo biti še boljši

*Aleksandra Žibrat**

Združenje bank Slovenije je na pobudo članic pred letošnjimi poletnimi počitnicami v sodelovanju s strokovno delovno skupino in zunanjo oglaševalsko agencijo izvedlo prvo fazo obsežne kampanje ozaveščanja javnosti glede tveganj spletnih prevar. Kampanja je zajela večino aktualnih komunikacijskih poti; oglaševanje na TV, jumbo plakate po vsej Sloveniji, mestne svetlobne oglasne panoje, plačane članke, oglasne pasice na medijskih portalih, vzpostavitev spletnega mesta Pazi.se, opozorilne vizuale na spletnih medijih, oglaševanje SEM na Googlu in številne objave na socialnih omrežjih. Kampanjo so z objavami na svojih komunikacijskih kanalih podprle tudi vse banke in hranilnice. Vsebinsko jedro so predstavljala opozorila in napotki v zvezi z ribarjenjem za občutljivimi in osebnimi podatki oziroma tako imenovani phishing. Kampanja je naslovila tudi vse druge spletne prevare, s katerimi se v bankah in hranilnicah najpogosteje srečujejo.

S ciljem ugotoviti, kako so izvedbo kampanje ozaveščanja zaznali državljani, je ZBS naročilo javnomnenjsko raziskavo, ki je bila izvedena v obdobju od 17. do 21. Junija, in sicer na vzorcu 707 polnoletnih državljanov Slovenije.

Kaj je pokazala

Kampanjo ozaveščanja pred tveganji spletnih prevar je zaznalo tri petine (60,4 %) vprašanih. Med tistimi, ki so kampanjo opazili, je potek kampanje največ anketirancev zaznalo kot oglas na televiziji (41,9 %), sledijo objave na facebooku in instagramu (40,6 %), sporočila na jumbo plakatih (39,6 %) in oglasne pasice na različnih spletnih medijskih portalih (20,9 %). Sedem desetin anketirancev (70,3 %) je menilo, da so informacije, ki so jih pridobili s kampanjo ozaveščanja, koristne oz. zelo koristne, 37 odstotkov pa, da so srednje koristne. V primeru, da bi vprašani prejeli elektronsko sporočilo ali SMS neznanega pošiljatelja, bi 79,8 odstotkov dobro premislilo o vpisu svojih podatkov v spletne obrazce, 18,7 % vprašanih bi tako sporočilo preverilo na banki ali hranilnici, medtem ko bi 1,5 % vprašanih podatke vpisalo. Gesla za dostop do spletne in mobilne banke ter PIN plačilne kartice nikoli ne menja (kar!) 41,3 % anketiranih, 30,3 % menja gesla redkeje kot enkrat na leto, 11,1 % enkrat letno, 7,7 % vsake tri mesece, 7,2 % pa gesla menja na pol leta. Večina vprašanih ne bi prek telefona neznanemu klicatelju, ki bi se predstavil kot predstavnik banke ali tehnične pomoči, nikoli sporočilo svojih osebnih podatkov in gesel za dostop do elektronske banke, medtem ko bi sedem anketiranih to storilo nemudoma. Dobra osmina anketirancev je že bila žrtev spletne prevare, najpogosteje so anketiranci navedli, da so bili prevarani pri nakupu oz. prodaji v spletnih trgovinah, 16,2 odstotka je navedlo zlorabo plačilne kartice, 8,6 % vprašanih je nasedlo raznim plačljivim SMS-om in klicem, 8 % je bilo žrtev vdora v profil in 4,1 odstotka prevare s kripto valutami. Večina anketiranih (95,6 %) se je strinjala oz.

* prof. Aleksandra Žibrat, univ. dipl. fil. in soc., urednica ePublikacij in PR koordinatorka, Združenje bank Slovenije

popolnoma strinjala s trditvijo: „Zavedam se, da za svojo varnost lahko največ storim sam, zato na spletu ravnam v skladu z varnostnimi priporočili".
Glede na rezultate javnomnenjske raziskave in odzive nasploh lahko povzamemo, a) da je bila kampanja uspešna in tudi provokativna, saj so se nanjo odzvali tako FURS kot tudi policisti, ki so zaradi sporočil na jumbo plakatih in prijav občanov prišli na ZBS preverit, če gre za novo prevaro, b) da so bila televizija in socialna omrežja najuspešnejša po dosegu, c) da so opozorila glede ribarjenja (phishing) zalegla, saj bi kar 80 odstotkov poslej dobro premislilo o vpisu svojih podatkov v spletne obrazce, d) da je nadaljnje ozaveščanje nujno, saj, kar je zastrašujoče, slaba polovica vprašanih nikoli ne menja svojih gesel ali PIN-a in nekaj vprašanih bi še vedno sporočilo svoja identifikacijska sredstva neznanemu klicatelju, ter e) da je treba usmeriti pozornost tudi na prevare pri spletnih nakupih, ki so bili med vprašanimi najpogosteje navedene kot uspešne.

Anketo glede podpore skupni kampanji smo izvedli tudi med bankami in hranilnicami. Pokazala je, da so se banke in hranilnice odzvale ter kampanjo podprle z objavami na lastnih komunikacijskih kanalih, zagotovo pa je tu ostalo še nekaj prostora neizkoriščenega, ki bi lahko z aktivnejšo podporo uspešno prispeval k skupnemu cilju, tj. višji stopnji ozaveščenosti javnosti glede tveganj spletnih prevar.
Za konec naj navedemo, da so banke in hranilnice splošno uspešnost kampanje ocenile s povprečno oceno štiri, pri čemer pa so aktivnejše članice kampanji dale bistveno višjo oceno od tistih, ki so kampanjo podprle bolj skromno. Oktobra nadaljujemo z drugo fazo projekta in v upanju, da bodo tovrstne kampanje na delovnem programu vsaj enkrat letno ter da z vključitvijo preostalih deležnikov postanejo vseslovenska nacionalna aktivnost, zaključujemo še s posebno zahvalo delovni skupini v sestavi: Katja Butala, Mojca Strojan, Petra Shirley, Branka Dečman Terzič, Eva Rihtaršič in Lara Berlec, ki je kampanjo po vsebini izjemno učinkovito in strokovno pripravila ter vodila.

Dvigniti moramo raven kibernetske varnosti v celotni družbi

NA VPRAŠANJI O KIBERNETSKI VARNOSTI SO ODGOVORILI

Peter Grum, generalni direktor Finančne uprave Republike Slovenije, doc. dr. Tomaž Klobučar, vodja Laboratorija za odprte sisteme in mreže Instituta Jožef Stefan, dr. Emilija Stojmenova Duh, ministrica za digitalno preobrazbo, in dr. Uroš Svete, direktor Urada Vlade RS za informacijsko varnost

Zastavili smo jim dve enaki vprašanji, njihove odgovore pa navajamo po abecednem vrstnem redu.

Kako ocenjujete stopnjo ozaveščenosti javnosti o kibernetskih tveganjih, ki smo jim (vsi) izpostavljeni?

Peter Grum: Kolikor se vaše vprašanje nanaša na notranjo javnost, se pravi uslužbence Finančne uprave RS, smo ravno v letošnjem letu izvedli anketo med uslužbenci glede stanja informacijske varnosti ter vrednotenja resnosti problema spletnega ribarjenja v Finančni upravi RS, ki v zadnjih letih predstavlja največje in najhitreje rastoče tveganje na tem področju. Glede na rezultate ankete ugotavljamo, da je 97 % uslužbencev Finančne uprave RS seznanjenih s trendi na področju informacijske varnosti, od teh tretjina meni, da so dobro seznanjeni s trenutnim razvojem na tem področju. Tudi odgovorna ravnanja in ustrezno ter pravočasno reagiranje uslužbencev v zvezi s prijavljanjem sumljivih sporočil in neobstoj večjih incidentov na tem področju kažejo na zadovoljivo ozaveščenost uslužbencev.
Če me sprašujete na splošno, menim, da se je tudi pri naših zavezancih, zunanji javnosti, v zadnjih letih povečalo zavedanje o nevarnosti kibernetskih tveganj. K temu je pripomogla velika širitev uporabe novih tehnologij in digitalnih storitev med prebivalstvom, deloma tudi kot posledica pandemije covida-19, ko je uporaba digitalnih storitev predstavljala edino možnost delovanja posameznika v času protikoronskih ukrepov. Izkušnje z uporabo tehnologij v praksi so skupaj s programi računalniškega opismenjevanja pri ljudeh dvignili znanje in zavedanje o nevarnostih, ki jih novo okolje prinaša.

Seveda pa rast števila uporabnikov informacijske tehnologije in razvoj samih tehnologij močno vplivata tudi na rast števila kibernetskih napadov. V zadnjih letih se kaže jasen trend sporočil, ki želijo pod pretvezo "preverjanja podatkov", "potrjevanja transakcij" ipd. izvabiti avtentikacijske podatke. Tudi v lažnem imenu Finančne uprave RS so pod krinko vračila davka po elektronski pošti in sporočilih SMS potekali poskusi spletnih prevar in verjetno bo tega v prihodnjih letih vse več.
Finančna uprava RS v sodelovanju s pristojnimi organi, mediji in prek lastnih družbenih omrežij in aplikacij skrbi za sprotno obveščanje zunanje javnosti o vseh oblikah kibernetskih tveganj, ki jih zazna, in redno opozarja svoje uporabnike o splošnih nevarnostih in poskusih prevar, s čimer poskuša prispevati k dvigu ozaveščenosti zunanje in notranje javnosti glede kibernetskih tveganj.

Tomaž Klobučar: Vsakdanja praksa kaže, da ljudje še vedno izbirajo premalo varna gesla, svoja gesla in zasebne ključe za digitalno podpisovanje delijo z drugimi, obiskujejo nevarne spletne strani, mobilnim aplikacijam nevede dovoljujejo dostop do občutljivih zasebnih podatkov na svojem mobilnem telefonu, na računalniških napravah pa ne uporabljajo ustrezne varnostne zaščite. Stopnje ozaveščenosti javnosti o kibernetskih tveganjih zato žal ne moremo oceniti za visoko.
Za boljše zavedanje javnosti o tveganjih in posledicah, ki jih lahko prinese takšno neustrezno ravnanje, je potrebno dodatno prizadevanje vseh, ki smo kakor koli povezani s kibernetsko varnostjo. Samo zavedanje pa je le prvi korak. Ključno je, da ljudje to zavedanje o kibernetskih tveganjih prenesejo tudi v svoja dejanja.

Peter Grum, generalni direktor Finančne uprave Republike Slovenije

doc. dr. Tomaž Klobučar, vodja Laboratorija za odprte sisteme in mreže Instituta Jožef Stefan

Ni dovolj le spoznavati vedno nova tveganja, ampak moramo vsi aktivno sprejeti zaščitne ukrepe na vseh ravneh družbe, od varne rabe družbenih omrežij med mladimi in internetnih storitev med starejšimi do upoštevanja varnostnih standardov in izogibanja naprednim kibernetskim grožnjam med zaposlenimi.

Emilija Stojmenova Duh: Stopnja ozaveščenosti javnosti o kibernetskih tveganjih se je v zadnjih letih povečala, vendar je še vedno prostor za izboljšave. Splošna javnost se morda bolj zaveda nekaterih osnovnih kibernetskih groženj, ki so bile medijsko izpostavljene, kot so npr. kraje osebnih podatkov, izsiljevalski virusi in hekerski vdori. To je gotovo prispevalo k večji ozaveščenosti na tem področju.
Vendar pa se mnogi še vedno ne zavedajo vseh različnih kibernetskih tveganj, s katerimi se srečujemo v digitalnem okolju:

- **Socialni inženiring**: Veliko kibernetskih napadov se začne s prevarami, kjer napadalci uporabljajo prepričljive manipulacije in trike, da zvabijo žrtve v izdajo občutljivih informacij ali namestitev zlonamerne programske opreme.
- **Napadi z ribarjenjem**: To so poskusi prevar, pri katerih se napadalci pretvarjajo, da so zaupanja vredne organizacije ali posamezniki, in žrtvam pošiljajo lažna sporočila ali povezave, ki vodijo do nevarnih mest ali prenosov virusov oz. zlonamerne programske kode. V zadnjem času opažamo porast tovrstnih napadov, zato je ozaveščanje javnosti prek vseh možnih medijev izredno pomembno.
- **Napadi DDoS** (distribuirani napad z zavrnitvijo storitve): Ti napadi povzročijo nedostopnost spletnih mest ali storitev s preplavljanjem strežnikov z velikim številom zahtev, kar povzroči preobremenitev ali celo okvaro. Za podjetje lahko takšen napad pomeni ogromno gospodarsko škodo.
- **Nevarnosti v povezavi z napravami IoT**: Veliko ljudi se ne zaveda, kako lahko nezaščitene naprave IoT (internet stvari), kot so pametni hladilniki ali kamere, predstavljajo tveganje za njihovo zasebnost in varnost.

Za povečanje ozaveščenosti javnosti o kibernetskih grožnjah je treba pogosto izvajati izobraževalne kampanje. Ljudem se mora zagotoviti uporabne smernice za varno uporabo digitalne tehnologije, kot so nasveti za prepoznavanje napadov z ribarjenjem, pravilno uporabo dobrih gesel, uporabo dvofaktorske avtentikacije za večjo varnost, previdnost pri uporabi neznanih aplikacij in povezav itd. Le z ozaveščeno javnostjo lahko zmanjšamo tveganje za kibernetske napade in njihove posledice.

Uroš Svete: Spodbudno je, da se stopnja ozaveščenosti o kibernetskih tveganjih v Sloveniji izboljšuje. Vendar nas čaka še veliko dela, tudi pri mlajših generacijah. O kibernetski varnosti in njenem pomenu se več poroča v medijih, kar je posledica tudi nekaterih odmevnih varnostnih incidentov v preteklosti, pa tudi programov ozaveščanja. Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) financira na tem področju dva programa ozaveščanja, in sicer program Varni na internetu, ki ga že vrsto let izvaja nacionalni odzivni center za kibernetsko varnost SI-CERT (URSIV tudi v celoti financira delovanje centra prek svojega proračuna) in pa program Center za varnejši internet, ki ga izvaja konzorcij pod vodstvom fakultete za družbene vede. Prvi program je namenjen splošni populaciji ter malim in srednje velikim podjetjem (MSP), drugi pa je namenjen otrokom in mladostnikom ter njihovim staršem in učiteljem. Ker se zavedamo, da bi osnove kibernetske higiene moral poznati prav vsak državljan, si bomo prizadevali, da se teme s področja kibernetske varnosti vključijo v učne načrte v osnovnih in srednjih šolah. Ne smemo pa pozabiti tudi na

dr. Emilija Stojmenova Duh, ministrica za digitalno preobrazbo

dr. Uroš Svete, direktor Urada Vlade RS za informacijsko varnost

starejše, ki se digitalnih veščin in aplikacij tudi poslužujejo. Dvigniti moramo raven kibernetske varnosti v celotni družbi. Če dvignemo raven energije, časa in tehnične zahtevnost, ki jih kiber-kriminalci potrebujejo, da vdrejo v naše sisteme, jih s tem tudi odvrnemo od tega početja, saj bodo iskali lažje dosegljive tarče.
Z ozaveščanjem razbijemo njihov poslovni model ter povečamo lastno varnost ter varnost naše širše družbe – zasebnih in javnih entitet.
Na URSIV se zavedamo, da ostaja finančni sektor kljub močni regulaciji in dejstvu, da so določbe o kibernetski varnosti že vključene v več politik in zakonodaj EU, zaradi specifike področja in neposrednih finančnih koristi med primarnimi tarčami zlonamernih akterjev. To potrjujejo tudi podatki nacionalnega odzivnega centra za kibernetsko varnost SI-CERT. Zavedati se moramo, da se v digitalizirani družbi krepi pomen informacijske in komunikacijske tehnologije. Kompleksni in razvejani sistemi se danes uporabljajo za vsakdanje dejavnosti. URSIV pozdravlja dosedanja prizadevanja izvajalcev in regulatornih organov za izboljšanje kibernetske varnosti finančnih subjektov.

Katere aktivnosti na področju kibernetske varnosti načrtujete v prihodnje?

Peter Grum: Kot verjetno veste, so države članice EU v letošnjem letu sprejele direktivo (EU) 2022/2555, znano kot NIS2, ki je nadomestila prejšnjo direktivo in od držav članic zahteva močnejše varnostne zahteve, vključno z uskladitvijo ukrepov po vsej EU. Po implementaciji NIS2 v nacionalno zakonodajo (do oktobra 2024) bo tudi naš organ kot upravljavec kritične infrastrukture v prihodnjih letih dolžan uvesti napredne varnostne ukrepe, kot so sistemi zaznavanja vdorov, sistemi upravljanja varnostnih informacij in dogodkov (SIEM), ocene ranljivosti in druge, ki jih predvideva nova direktiva. Seveda bodo vsi ukrepi izvedeni v sodelovanju z ministrstvom za digitalno preobrazbo kot lastnikom in upravljavcem centralnega komunikacijskega omrežja državne uprave (HKOM), ki predstavlja hrbtenico, prek katere potekajo informacijski sistemi organov državne uprave.
V pogledu preventive bomo v prihodnosti še naprej skrbeli za izobraževanja in usposabljanja zaposlenih v zvezi z dobrimi praksami na področju kibernetske varnosti, prepoznave taktik in standardnih oblik poskusov prevar spletnih napadalcev ter pomembnosti odgovornega obnašanja glede neuporabe službenih računalnikov v zasebne namene, pomembnosti ne klikanja na sumljive povezave in odpiranja neznanih priponk ipd. Še naprej si bomo prizadevali ažurno obveščati zunanjo javnost oziroma zavezance o varnostnih tveganjih.

Tomaž Klobučar: Sodobni informacijski in komunikacijski sistemi so vse bolj kompleksni in potrebujejo proaktivno zaščito in hitro obnovo za preprečitev ali ublažitev posledic kibernetskih, fizičnih in kombiniranih napadov. Na tem področju bomo v Laboratoriju za odprte sisteme in mreže Instituta »Jožef Stefan« nadaljevali z raziskavami, razvojem in izvedbo najnovejših rešitev za zagotovitev kibernetske varnosti, predvsem varnostnih tehnologij na podlagi metod umetne inteligence in kvantnih omrežij za zaščito komunikacij.
Umetno inteligenco prištevamo med tehnologije, ki omogočajo učinkovitejše zagotavljanje kibernetske varnosti. Z njeno pomočjo lahko analiziramo in obdelamo večje število varnostno relevantnih dogodkov in hitreje in bolj učinkovito odkrijemo poskuse napadov in zlonamerne uporabnike. Uporabne so tudi pri analizi zlonamernih aktivnosti, modeliranju napadov, avtomatskem iskanju ranljivosti in ocenjevanju tveganj in njihovega vpliva.
Naše pretekle raziskave so pokazale, da Slovenija na tem področju zaostaja za razvitim svetom, tako pri razvoju no-

vih rešitev kot pri njihovi uporabi. Poleg raziskav in razvoja novih tehnologij je zato pomembna tudi pomoč slovenskim podjetjem pri uvajanju, uporabi in upravljanju teh varnostnih tehnologij in prilagoditvi obstoječih informacijskih sistemov. To še posebej velja za mikro, mala in srednje velika podjetja, ki si težje privoščijo strokovni kader v obsegu, ki bi omogočal ustrezno raven kibernetske varnosti.
K višji ravni varnosti komunikacij bodo v prihodnje pripomogla tudi kvantna omrežja za varno izmenjavo kriptografskih ključev in post-kvantna kriptografija. Institut »Jožef Stefan« je združil moči z nekaj slovenskimi organizacijami pri projektu SiQUID, ki vzpostavlja kvantno distribucijo ključev med več vladnimi vozlišči v Sloveniji in testno kvantno omrežje med raziskovalnimi ustanovami v Ljubljani. Aktivnosti predstavljajo pomemben mejnik pri razvoju kvantne komunikacije v Sloveniji.

Emilija Stojmenova Duh: Na področju kibernetske varnosti je ključno nenehno izboljševanje in prilagajanje, saj tudi kibernetske grožnje nenehno napredujejo. Ocenjujem, da so za boljšo kibernetsko varnost pomembne naslednje aktivnosti:

a. Izobraževanje in ozaveščanje: Treba je načrtovati in izvajati kampanje ter izobraževalne programe za različne ciljne skupine, vključno z javnostjo, podjetji in organizacijami. Osredotočiti se je treba na razlago tveganj, preventivne ukrepe in pravilno ravnanje ob incidentih.

b. Ocenjevanje tveganj in varnostne politike: Treba je izvajati redna ocenjevanja varnostnih tveganj in posodabljati politike ter postopke kibernetske varnosti v skladu z najnovejšimi grožnjami.

c. Krepitev infrastrukture: Nenehno je treba izboljševati varnostno infrastrukturo in tehnologijo, vključno z zanesljivimi požarnimi zidovi, varnostnimi rešitvami za odkrivanje groženj in varnostnimi posodobitvami programske opreme.

d. Sodelovanje z drugimi strokovnjaki: Kibernetska varnost je skupinsko prizadevanje. Sodelovanje z drugimi strokovnjaki in organizacijami je nujno za izmenjavo informacij o grožnjah in najboljših praksah.

e. Odzivanje na incidente: Načrtovanje in izvedba vaj postopkov za odzivanje na kibernetske incidente sta ključna za hitro ukrepanje ob morebitnih napadih. S tem lahko tudi učinkovito zmanjšamo nastalo škodo.

f. Spremljanje zakonodaje: Slediti je treba spremembam v zakonodaji o kibernetski varnosti in se prilagajati, da ostanemo skladni z veljavnimi predpisi.

Kibernetska varnost je dinamično področje, zato je ključno, da smo informirani o najnovejših grožnjah in razvijamo strategije, ki bodo zagotavljale varnost državne uprave, gospodarskih organizacij in širše družbe.

Uroš Svete: Na ravni Evropske unije je bila v letu 2022 sprejeta nova direktiva EU imenovana tudi NIS2. Zaradi tega je treba prilagoditi tudi slovensko zakonodajo na področju informacijske varnosti. URSIV zato že pripravlja prenovljen zakona o informacijski varnosti. Treba pa bo spremeniti tudi nekaj podzakonskih aktov, pripraviti prenovljen nacionalni načrt za odzivanje v primeru kibernetskih incidentov ter strategijo kibernetske varnosti.
URSIV želi za pridobivanje novih strokovnjakov na nacionalni ravni vzpostaviti mrežo srednjih šol, ki bodo v obliki dodatnega pouka zainteresiranim dijakom ponujale izobraževanje s področja kibernetske varnosti. V mrežo želimo vključiti šole iz celotne Slovenije in se povezati tudi s fakultetami, ki ponujajo oziroma bodo ponujale študijske programe s področja kibernetske varnosti, ter tudi z gospodarstvom.
V načrt za okrevanje in odpornost (NOO) smo uspešno umestili projekt za dvig ravni kibernetske varnosti, ki ga bomo izvajali skupaj z ministrstvom za digitalno preobrazbo. Pri tem bo URSIV izvajal aktivnosti za pripravo in vključitev tem s področja kibernetske varnosti v učne načrte v osnovnih in srednjih šolah, aktivnosti za pripravo vzorčne varnostne dokumentacije in vzorčnih varnostnih ukrepov za organizacije različnih velikosti, aktivnosti za vzpostavitev enotne platforme za priglasitev incidentov, aktivnosti za vzpostavitev centra za analizo in deljenje informacij (Information Sharing and Analysis Center, ISAC) ter aktivnosti za vzpostavitev sistema certificiranja kibernetske varnosti proizvodov, storitev in procesov.
V prihodnje bo pomembno vlogo s povezovanjem deležnikov v sistemu kibernetske varnosti in s pomočjo pri pridobivanju sredstev iz EU-programov, namenjenih področju kibernetske varnosti, odigral tudi nacionalni koordinacijski center za kibernetsko varnost NCC-SI, ki bo deloval na URSIV.
URSIV posveča posebno pozornost zavezancem po zakonu o informacijski varnosti (ZInfV) iz skupine izvajalcev bistvenih storitev na področjih energije, digitalne infrastrukture, oskrbe s pitno vodo in njene distribucije, zdravstva, prometa, bančništva, infrastrukture finančnega trga, preskrbe s hrano in varstva okolja, iz skupine ponudnikov digitalnih storitev in iz skupine organov državne uprave. Vsako leto urad organizira posvete z zavezanci, saj ocenjujemo, da je osebni kontakt dobra predispozicija za nadaljnje sodelovanje, izmenjavo izkušenj, dogodkov, dobrih praks, novosti. Omenjene aktivnosti bomo izvajali tudi v prihodnje. S tem želimo graditi in krepiti sodelovanje,

povezanost in izmenjavo informacij.
URSIV je v letu 2023 začel sodelovati z evropsko agencijo za kibernetsko varnost (ENISA) v pilotnem projektu hitre pomoči evropske komisije izvajalcem bistvenih storitev v državah članicah z namenom dviga ravni kibernetske varnosti. Pilotni projekt naslavlja pregledovanje sistemov oziroma preventivne ukrepe in odzivnost na morebitne incidente ter ponuja temu ustrezne storitve. Projekt se bo izvajal do leta 2025. Na URSIV smatramo, da so takšni projekti izjemno dobrodošli in jih zelo podpiramo.
Prav tako bomo nadaljevali in poglobili aktivnosti na mednarodnem področju. Prek bilateralnih partnerstev s podobno mislečimi državami bomo povečali izmenjavo informacij v realnem času. Implementirati bomo morali novo EU-direktivo NIS2 ter sooblikovali druge akte, kot na primer akt o kibernetski solidarnosti, ki bo povezal varnostno operativne centre v EU v t. i. kibernetski ščit. V zvezi NATO bo zaživela virtualna enota za primere kibernetskih napadov. Ne pozabljamo pa tudi na našo neposredno soseščino. Tako smo skupaj s Francijo ustanovili Center Kibernetskih Zmogljivosti v Podgorici, s katerim želimo prenesti dobre prakse in znanje v regijo Zahodnega Balkana.
Vsi ti ukrepi sledijo konceptu aktivne kibernetske zaščite, s katerim želimo zmanjšati število, impakt, in škodo nastalo kot posledica kibernetskih napadov, ter hkrati povečati odpornost naših sistemov in družbe na tovrstne napade.
V kibernetskem svetu moramo biti nenehno čuječi.

UDK 004.738.5:004.056

Od mene je odvisno vse

NACIONALNI PROGRAM OZAVEŠČANJA VARNI NA INTERNETU POSTAVLJA V SREDIŠČE KIBERNETSKE OBRAMBE POSAMEZNIKA

*Gorazd Božič**

IT'S MY CALL: USER-CENTRED NATIONAL CYBERSECURITY AWARENESS-RAISING PROGRAMME

This year marks 12 years since the launch of the Slovenian national information security awareness programme called Safe on the Internet. At the time we have filled the void in the education of adult users and small businesses with new content and communication approaches. Over a decade we at the National Computer Emergency Response Team SI-CERT have learnt important lessons that guide us in our further awareness-raising and education activities.

JEL K24 O33 O38

Letos mineva dvanajsto leto, odkar je zaživel nacionalni program ozaveščanja o informacijski varnosti Varni na internetu. Takratno praznino na področju izobraževanja odraslih uporabnikov in malih podjetij smo zapolnili z novimi vsebinami in komunikacijskimi modeli pod okriljem povsem novega projekta. V dobrem desetletju – kar je v svetu informacijske tehnologije, kjer še komaj lovimo vse spremembe, preboje in novosti, že precej dolgo obdobje, smo na Nacionalnem odzivnem centru za kibernetsko varnost SI-CERT izluščili pomembni lekciji, ki nas vodita pri nadaljnjih aktivnosti ozaveščanja in izobraževanja.

Prvo je dejstvo, da moramo v ospredje postaviti posameznika, uporabnika, ki je več kot zgolj floskula »najšibkejši člen v verigi kibernetske varnosti«. Po skoraj 30-ih letih delovanja centra SI-CERT in desetinah tisočev obdelanih incidentih še vedno trdimo, da so v samem vrhu napadi družbenega oz. socialnega inženiringa. V mislih imamo različne oblike spletnih goljufij in pa predvsem napadov z zvabljanjem (ang. phishing), ki so v zadnjih nekaj letih zabeležili globalen skok in so trenutno najpogostejša grožnja, ki preti povprečnemu spletnemu uporabniku. V preteklem letu smo v centru SI-CERT obravnavali 1432 incidentov z zvabljanjem, leta 2021 pa 950, kar pomeni, da je ravno v tej kategoriji ponovno zabeležena največja rast. V največ primerih je bil vektor napada elektronska pošta, velik skok pa je v porastu napadov z zvabljanjem z SMS-sporočili in prek aplikacij za hipno sporočanje. V zadnjih letih smo priče trendu, da se nevarnosti selijo na pametne telefone v obliki SMS-sporočil, ki želijo pod pretvezo "preverjanja podatkov", "potrjevanja transakcij" ipd. izvabiti avtentikacijske podatke za dostop do elektronske banke (t. i. smishing).

Gre za incidente, kjer napadalci izkoristijo naše ranljivosti, podobno kot bi poiskali in izkoristili napako v programski kodi. In v svetu kibernetske varnosti nas ravno lastnosti, ki so imanentno človeške, delajo tako ranljive – radovednost, strast, sočutje, strah, če naštejemo le nekatere. **Zaupanje v programske rešitve nas pred takšnimi zlorabami ne bo vedno obvarovalo, še vedno je glavna rešitev izobraževanje spletnih uporabnikov.** Ne zgolj s komunikacijskimi akcijami, ki naslavljajo posameznika v njegovem domačem okolju, ampak tudi s kontinuiranim, hkratnim izobraževanjem v poslovnem okolju. V SI-CERT že leta opozarjamo, da je še vedno (pre)pogosto prepriča-

* Gorazd Božič, vodja Nacionalnega odzivnega centra za kibernetsko varnost SI-CERT

nje, da manjša podjetja niso zanimiva za spletne napadalce, kar pa ne drži. Zaradi omejenih finančnih in kadrovskih virov so vlaganja v informacijska varnost tam velikokrat pomanjkljiva, zato so manjša podjetja lažje tarče. Tudi v večjih podjetjih in organizacijah, kjer je stopnja zavedanja o kibernetski varnosti mnogo višja, težavo še vedno predstavlja nezadostno izobraževanje zaposlenih. Vlaganje zgolj v programsko in omrežno opremo ne reši vseh težav, saj gre v večini primerov za tehnično nezahtevne napade, ki temeljijo na družbenem inženiringu. Če zaposleni nimajo ustreznih znanj in veščin, da bi prepoznali nevarnost, so napadalci pogosto uspešni. Vendar se tudi na tem področju v zadnjih letih dogajajo intenzivne spremembe.

Nove spletne platforme prinašajo nove priložnosti za napadalce

Če je zadnjih deset let poglavitni motiv napadalcev ostal enak – prepričati uporabnike v nakazilo denarja, pa so se močno spremenile komunikacijske poti, po katerih pridejo do svojih žrtev. Nove spletne storitve, nove oblike plačevanja na spletu, predvsem pa nove platforme družbenih omrežij so prinesle številne priložnosti za spletne goljufe. Ko smo zagnali naš program ozaveščanja Varni na internetu, smo opozarjali večinoma na spam oz. neželeno pošto, krajo Gmail-gesel in nekaj prevarantov na spletnih oglasnikih. **Desetletje kasneje pa obravnavamo povsem druge problematike, ki se kažejo v resni finančni in poslovni škodi.** Danes opozarjamo na vrivanje v poslovno komunikacijo, direktorske prevare, kraje z zvabljanjem (phishing) kreditnih kartic, številne prevare pri spletnem nakupovanju, izsiljevanje z intimnimi posnetki, lažne kredite, investicijske kripto prevare, ki se končajo z več deset tisoč evri škode. Pogosto so skupni imenovalec ravno družbena omrežja, kjer napadalci vzpostavijo prvi stik – postavijo lažno nagradno igro, oglas za lažno spletno trgovino ali lažni profil osamljenega marinca. Domišlija spletnih goljufov praktično ne pozna meja, kar pa zahteva **nove modele izobraževanja, torej kako nagovoriti spletne uporabnike, pritegniti njihovo pozornost in jim pojasniti, kje tiči nevarnost.**

Kibernetska varnost zadeva vse

Drugo pomembno zavedanje je, da kibernetska varnost ni neprijetna naloga enega oddelka znotraj podjetja ali ene organizacije znotraj države. Hkrati se kibernetske grožnje tudi ne ustavijo na nacionalnih mejah. Kibernetska varnost zadeva vse – *Cyber Security Is Everyone's Business,* in najti učinkovit odziv na kibernetske grožnje je globalni izziv naše dobe. Varnost in zaupanje sta prva pogoja, da uporabniki usvojimo vse spletne storitve, ki so nam na voljo. **Zato s programom ozaveščanja Varni na internetu aktivno sodelujemo tudi v širših pobudah in smo slovenski predstavnik oz. koordinator v kampanji Evropski mesec kibervarnosti**. Vseevropsko pobudo usklajujeta Agencija Evropske unije za kibernetsko varnost ENISA in Evropska komisija, ob podpori članic EU in prek 300 drugih partnerjev in podpornikov. Evropski mesec kibervarnosti se začne vsako leto oktobra in v mesecu dni intenzivnega dogajanja doseže milijone Evropejcev. Poglavitni cilj iniciative je okrepiti odpornost sistemov in storitev EU, opolnomočiti državljane ter narediti korak naprej k bolj kibernetsko varni in ozaveščeni družbi.
Leta 2012 je le osem članic EU, med njimi tudi že Slovenija z odzivnim centrom SI-CERT, prvič organiziralo kampanjo, ki je zdaj že stalnica. Lani smo obeležili pomembno prelomnico, saj je evropski mesec kibervarnosti obeležil deseto obletnico. Ob tej priložnosti so bile prvič

podeljene nagrade za najboljša gradiva, ki so nastala v teh letih. Naše aktivnosti niso bile neopažene, saj smo prejeli nagrado za najboljši video, s katerim opozarjamo na počitniške prevare. Podobno so države članice EU tudi letos izglasovale naš video, s katerim opozarjamo na pomen izobraževanja zaposlenih v podjetju kot primer dobrega ozaveščanja.

Ponosni smo na naše delo

Poglaviten namen ekipe, ki skrbi za razvoj strokovnih vsebin in program ozaveščanja, ostaja nespremenjen. Želimo pomagati. V dobrem desetletju smo oblikovali učinkovito in

dostopno platformo, ki je vsem državljanom v pomoč, da se opremijo z ažurnimi in relevantnimi napotki, kako zagotoviti učinkovito informacijsko varnost. **Pri tem je osrednjo vlogo prevzel portal www.varninainternetu.si, kjer je trenutno največja zbirka gradiv in nasvetov s področja informacijske varnosti ter opisov spletnih goljufij v Sloveniji.** Spletni uporabniki najdejo na portalu več kot 500 prispevkov, ki so lahko v pomoč pri varovanju spletne identitete, naprav in nenazadnje tudi bančnega računa, saj je ravno finančna korist najpogostejši motiv, ki stoji za varnostnimi incidenti.

V sklopu programa Varni na internetu smo pomagali več kot 3500 posameznikom, ki so prijavili goljufijo prek prijavne točke, posneli več kot 90 videov, hkrati pa držimo tempo skoraj vsakodnevne objave nasveta ali opozorila na kanalih družbenih omrežij. Trenutno smo v intenzivnem obdobju načrtovanja že dvanajste nacionalne kampanje v sklopu iniciative Evropski mesec kibervarnosti.

Naj izkoristimo priložnost in nagovorimo vse bralce, da tudi sami postanejo ambasadorji kibernetske varnosti v prihajajočem mesecu. Zaposlene v podjetjih pozivamo, naj se pridružijo pobudi in izvedejo vsaj eno aktivnost v podjetju. To je lahko spletni seminar, predavanje ali le elektronsko sporočilo zaposlenim z nekaj ključnimi nasveti. Gre za majhne korake, ki štejejo, saj je pomembno, da se zaposleni zavedajo, kako velik prispevek imajo pri zagotavljanju informacijske varnosti. Ne pozabimo tudi na najranljivejše, to so predvsem starejši uporabniki, naši starši in stari starši.

Gre za pogosto spregledano skupino uporabnikov, ki potrebuje prilagojena gradiva, kjer niso v središču zgolj programske rešitve, ampak razumljiva pojasnila, na kakšne načine delujejo spletni goljufi. Ravno njim bomo posvetili našo pozornost v letošnji kampanji in pripravili prilagojena izobraževalna gradiva za izvajalce računalniških usposabljanj za starejše uporabnike ter širšo komunikacijsko akcijo. Glavno sporočilo letošnje kampanje bo: **»Naj vas ne bo sram ali strah prositi za pomoč!«** Misel, ki nas lahko obvaruje marsikatere težave in hkrati deli odgovornost za zagotavljanje kibernetske varnosti med vse nas.

UDK 004.896:004.056

Dvostranski meč umetne inteligence: Kako UI oblikuje kibernetsko varnost?

*Matic Čaleta, Žiga Podgoršek in Denis Čaleta**

A DOUBLE-EDGED SWORD OF ARTIFICIAL INTELLIGENCE: HOW AI SHAPES CYBERSECURITY?
Artificial Intelligence (AI) has a significant influence on cybersecurity, introducing revolutionary methods for detecting and responding to digital threats. Despite its advantages in defense, AI can be exploited to conduct advanced and targeted cyber-attacks, presenting new challenges for security professionals.

JEL K24 O33

1. Uvod

V današnjem hitro spreminjajočem se digitalnem svetu sta umetna inteligenca (UI) in kibernetska varnost dve ključni področji, ki sta postali neločljivo povezani. Umetna inteligenca, ki posnema človeško sposobnost razmišljanja in učenja, je v zadnjem desetletju doživela eksploziven razvoj. Z napredkom v računalniški moči, algoritmih in dostopnosti podatkov so postali možni sistemi, ki lahko prepoznajo vzorce, analizirajo kompleksne nabore podatkov in celo ustvarjajo novo vsebino; od prepoznavanja obrazov in avtonomnih vozil pa vse do naprednih priporočilnih sistemov in virtualnih asistentov. UI je tako postala sestavni del našega vsakdana. Po drugi strani pa je s povečanjem digitalizacije prišlo tudi do povečanja kibernetskih groženj. Vsak dan se pojavljajo novi virusi, trojanski konji, ransomware in druge zlonamerne kode, ki ogrožajo naše digitalne naprave, podatke in zasebnost. V tem kontekstu je kibernetska varnost postala ključna za zaščito posameznikov, podjetij in vlad pred kibernetskimi napadi. Združevanje umetne inteligence in kibernetske varnosti je naravni korak v boju proti tem grožnjam. UI lahko pomaga pri prepoznavanju in preprečevanju kibernetskih napadov na načine, ki jih tradicionalne varnostne metode ne morejo. Na primer sistemi, ki temeljijo na umetni inteligenci, lahko v realnem času analizirajo milijone transakcij, da bi zaznali sumljive vzorce, ki bi lahko bili znak napada. Poleg tega lahko uporabljajo strojno učenje za prilagajanje in izboljšanje svojih detekcijskih algoritmov na podlagi novih groženj.

Vendar pa uporaba umetne inteligence v kibernetski varnosti prinaša tudi svoje izzive. Med njimi so vprašanja zasebnosti, etike in potencialne zlorabe tehnologij. Kljub temu je jasno, da bo vloga umetne inteligence v kibernetski varnosti še naprej rasla, saj se bomo soočali z vedno bolj sofisticiranimi in zapletenimi kibernetskimi grožnjami (Podgoršek, 2023:37).

2. Umetna inteligenca v detekciji groženj

V sodobnem digitalnem svetu, kjer se količina podatkov eksponentno povečuje, je postalo skoraj nemogoče ročno spremljati in analizirati vse potencialne grožnje v realnem času. Umetna inteligenca (UI) je postala ključna komponenta v boju proti kibernetskim grožnjam, saj omogoča avtomatizirano analizo velikih količin podatkov in prepoznavanje sumljivih vzorcev.

Kako UI pomaga pri prepoznavanju novih in neznanih groženj

Tradicionalne varnostne rešitve, kot so protivirusni programi, se pogosto zanašajo na podpisne baze, ki vsebujejo informacije o znanih grožnjah. Te baze se redno posodabljajo, vendar je njihova glavna pomanjkljivost v tem, da ne morejo prepoznati novih ali neznanih groženj, ki še niso bile dodane v bazo. Postopki UI, kot je strojno učenje, omogočajo sistemom, da se "učijo" iz preteklih podatkov in prepoznajo sumljive vzorce, ki se lahko

* Matic Čaleta, Certificirani etični heker, Institut za korporativne varnostne študije,
Žiga Podgoršek, Ceh (master), CPENT, OSCP, CHFI, ECIH, Institut za korporativne varnostne študije,
Izr. prof. dr. Denis Čaleta, predsednik Sveta, Institut za korporativne varnostne študije

razlikujejo od znanih groženj. Z uporabo algoritmov strojnega učenja lahko varnostni sistemi analizirajo obnašanje aplikacij, omrežnega prometa in uporabnikov ter prepoznajo nenavadne vzorce, ki lahko pomenijo potencialno grožnjo. Na primer, če se aplikacija nenadoma začne obnašati drugače kot običajno ali če se poveča količina omrežnega prometa iz določenega vira, lahko to kaže potencialni varnostni incident. Kot primer uspešne uporabe UI za detekcijo groženj lahko vzamemo podjetje Darktrace, ki uporablja tehnologijo umetne inteligence za prepoznavanje in odzivanje na kibernetske grožnje v realnem času. Njihov sistem se uči iz omrežnega prometa in je sposoben prepoznati nenavadne vzorce, ki lahko pomenijo potencialno grožnjo.

3. Umetna inteligenca v odzivanju na incidente

V svetu kibernetske varnosti je hitrost odziva ključnega pomena. Ko se pojavi varnostni incident, je vsaka sekunda dragocena. Zamuda pri odzivanju lahko povzroči večjo škodo, izgubo podatkov ali celo finančne izgube. Umetna inteligenca (UI) je v tem kontekstu postala nepogrešljivo orodje, saj omogoča avtomatizacijo odziva na incidente in s tem povečuje učinkovitost in hitrost varnostnih ekip.

Avtomatizacija odziva na varnostne incidente s pomočjo UI

Tradicionalno odzivanje na varnostne incidente pogosto zahteva ročno posredovanje varnostnih strokovnjakov. To lahko vključuje analizo datotek, preverjanje sistema za znake vdora ali izvajanje ukrepov za izolacijo in odpravo grožnje. Vendar pa je v velikih in kompleksnih omrežjih ročno odzivanje lahko počasno in neučinkovito. Z uporabo umetne inteligence je mogoče avtomatizirati številne korake v procesu odzivanja na incidente. Sistemi, ki temeljijo na UI, lahko samodejno zaznajo grožnjo, analizirajo njeno naravo, določijo ustrezne ukrepe in jih izvedejo brez človeškega posredovanja. Na primer, če sistem zazna sumljivo dejavnost, ki izhaja iz določenega IP naslova, lahko samodejno blokira ta naslov, da prepreči nadaljnje škodljive dejavnosti. Avtomatizacija odziva na incidente pa prinaša s pomočjo UI številne prednosti:

- Hitrost: UI omogoča skoraj takojšen odziv na grožnje, kar zmanjšuje čas, ki je na voljo napadalcu za povzročanje škode.
- Učinkovitost: Z avtomatizacijo rutinskih in ponavljajočih se nalog se osvobodi čas varnostnih strokovnjakov, ki se lahko osredotočijo na bolj kompleksne grožnje.
- Natančnost: Sistemi, ki temeljijo na UI, lahko analizirajo velike količine podatkov in zaznajo grožnje, ki bi jih človeški analitiki morda spregledali.
- Prilagodljivost: UI se lahko uči iz preteklih incidentov in se prilagaja novim grožnjam, kar s časom povečuje njeno učinkovitost. (Zhang, et all, 2022)

4. Umetna inteligenca v analizi ranljivosti

Kibernetska varnost je nenehna tekma med napadalci in potencialnimi žrtvami. Medtem ko si napadalci prizadevajo najti nove načine za izkoriščanje sistemov, si na drugi strani prizadevajo najti in odpraviti te ranljivosti, preden jih napadalci lahko izkoristijo. V tem nenehnem boju je umetna inteligenca (UI) postala ključno orodje za iskanje, analizo in ocenjevanje ranljivosti v digitalnih sistemih. Tradicionalne metode iskanja ranljivosti, kot so ročno testiranje ali uporaba standardnih orodij, so lahko časovno potratne in neučinkovite pri odkrivanju kompleksnih ali neznanih ranljivosti. UI, zlasti tehnike strojnega učenja, lahko avtomatizira in optimizira ta proces. Sistemi, ki temeljijo na umetni inteligenci, lahko analizirajo velike količine podatkov, kot so omrežni promet ali koda aplikacij, da bi našli nenavadne vzorce ali anomalije, ki lahko pomenijo ranljivost. Poleg tega se lahko ti sistemi "učijo" iz preteklih incidentov ali znanih ranljivosti, da bi bolje prepoznali in ocenili potencialne grožnje v prihodnosti.

Kako UI pomaga pri predvidevanju potencialnih točk napada

Ena izmed ključnih prednosti uporabe umetne inteligence v analizi ranljivosti je njena sposobnost predvidevanja. Namesto da bi se osredotočala samo na znane ranljivosti, lahko UI analizira sisteme in njihovo vedenje, da bi predvidela, kje se lahko pojavijo nove ranljivosti. Na primer, UI lahko analizira način, kako se različne komponente sistema medsebojno povezujejo, in prepozna potencialne točke napada, ki bi jih človeški analitik morda spregledal. Poleg tega lahko uporablja tehnike, kot sta simulacija ali modeliranje, da bi "testirala" sistem v varnem okolju in predvidela, kako bi se lahko odzval na različne vrste napadov.

5. Umetna inteligenca pri naprednih napadih

Ko govorimo o umetni inteligenci (UI) v kontekstu kibernetske varnosti, pogosto razmišljamo o njeni vlogi pri obrambi pred grožnjami. Vendar pa je UI dvostranski meč, saj jo lahko uporabljajo tudi napadalci za izvedbo naprednih in sofisticiranih napadov. Z razvojem tehnologije so se tudi metode napadov razvijale, postajale bolj zapletene in težje zaznavne. Napadalci uporabljajo umetno inteligenco za avtomatizacijo in optimizacijo svojih napadov. Na primer, s pomočjo UI lahko ustvarijo napredne napade z ribarjenjem, kjer se sporočila prilagajajo posameznemu

uporabniku, da se poveča verjetnost uspešnega napada. UI lahko analizira pretekle komunikacije in ustvari prepričljivo lažno sporočilo, ki se zdi legitimno. Poleg tega se UI uporablja za avtomatizacijo napadov na več ciljev hkrati. Napadalci lahko uporabljajo algoritme, ki samodejno prepoznajo ranljive sisteme na spletu in jih napadejo brez človeškega posredovanja.
Za primer napada s pomočjo umetne inteligence lahko vzamemo napad na TaskRabbit: V aprilu 2018 je bilo s pomočjo UI podprtega napada na platformo TaskRabbit ogroženih 3,75 milijona uporabnikov, ki so izgubili svoje socialne varnostne številke in podatke o bančnih računih. Napadalci so uporabili obsežno botnet mrežo pod nadzorom UI za izvedbo razpršenega napada zanikanja storitve (DDoS) na strežnikih TaskRabbit, kar je privedlo do začasne ustavitve celotnega spletnega mesta. Medtem ko so bili strežniki nedosegljivi, je napad prizadel še 141 milijonov dodatnih uporabnikov.

Primeri, kako se lahko UI uporablja za odkrivanje anomalij in iskanje napak v kodi

Napadalci uporabljajo tehnike umetne inteligence za iskanje napak v kodi, ki jih lahko izkoristijo. S pomočjo strojnega učenja lahko analizirajo velike količine vrstic kode in prepoznajo vzorce, ki kažejo potencialne ranljivosti. Na primer, algoritmi lahko prepoznajo dele kode, ki se obnašajo nenavadno ali ne sledijo običajnim programerskim praksam, kar lahko pomeni ranljivost. Poleg tega se UI uporablja za odkrivanje anomalij v omrežnem prometu ali vedenju sistema. Napadalci lahko uporabljajo tehnike umetne inteligence za prepoznavanje nenavadnih vzorcev, ki kažejo varnostne pomanjkljivosti ali ranljive točke v sistemu.

6. Vpliv UI na varnost odprtokodnih programov

Odprtokodni programi so postali temelj sodobne tehnološke infrastrukture. Mnoge organizacije in posamezniki se zanašajo na odprtokodne rešitve zaradi njihove prilagodljivosti, transparentnosti in skupnostne podpore. Vendar pa prinaša odprta narava teh programov tudi svoje varnostne izzive. Umetna inteligenca (UI) ima ključno vlogo pri obravnavi teh izzivov, hkrati pa lahko tudi poveča tveganje za varnost kot že zgoraj omenjeno. (Atif, et all, 2023:4)
Umetna inteligenca lahko pomaga pri izboljšanju varnosti odprtokodnih programov na več načinov:

- Avtomatizirano testiranje: UI lahko avtomatizira proces testiranja kode, da bi našla in odpravila potencialne ranljivosti. S pomočjo strojnega učenja lahko sistemi "naučijo" prepoznati sumljive vzorce v kodi, ki lahko pomenijo varnostne pomanjkljivosti.
- Analiza obnašanja: UI lahko analizira, kako se odprtokodni programi obnašajo v realnem okolju, da bi prepoznala nenavadne ali sumljive aktivnosti, ki bi lahko bile znak napada ali zlorabe.
- Skupnostna analiza: Ker odprtokodne programe pogosto razvijjo s pomočjo skupnosti, lahko UI analizira komunikacijo in sodelovanje med razvijalci, da bi prepoznala potencialne grožnje ali sumljive dejavnosti.

Potencialne ranljivosti in izzivi pri zagotavljanju varnosti

Kljub prednostim, ki jih prinaša umetna inteligenca, obstajajo tudi izzivi in tveganja, povezana z varnostjo odprtokodnih programov:

- Transparentnost kode: Medtem ko je transparentnost odprtokodnih programov ena izmed njihovih glavnih prednosti, lahko to tudi poveča tveganje. Napadalci lahko preučujejo kodo, da bi našli in izkoristili ranljivosti, pri čemer jim UI lahko močno pomaga.
- Kompleksnost: Mnogi odprtokodni projekti so zelo obsežni in vključujejo prispevke številnih razvijalcev. To lahko oteži odkrivanje in odpravljanje ranljivosti.

7. Umetna inteligenca v spletnih prevarah

Spletne prevare so že dolgo del digitalnega sveta, vendar je z razvojem umetne inteligence (UI) postalo mogoče ustvariti bolj prepričljive in sofisticirane napade. Posebej zaskrbljujoče je, kako se UI uporablja za ustvarjanje ponarejenih glasov, posnetkov in drugih medijskih vsebin, ki jih je težko razlikovati od resničnih.

Uporaba UI za ustvarjanje ponarejenih glasov in posnetkov

Tehnologije, kot so "deepfakes", uporabljajo napredne algoritme strojnega učenja za ustvarjanje realističnih, a ponarejenih video posnetkov. Z uporabo velikih količin podatkov, kot so slike ali posnetki osebe, lahko ti algoritmi ustvarijo video, kjer ta oseba govori ali počne stvari, ki jih v resnici ni nikoli storila (Sarker, at all, 2021).
Podobno se UI uporablja tudi za ustvarjanje ponarejenih glasov. Z analizo vzorcev človeškega glasu lahko algoritmi ustvarijo glasovne posnetke, ki zvenijo skoraj identično kot resnični človeški glas. To se lahko uporabi za ustvarjanje lažnih telefonskih klicev ali sporočil.
Primeri spletnih prevar, ki temeljijo na tehnologiji UI:

- Prevare CEO: V tej prevari napadalci uporabljajo ponarejen glas direktorja ali druge visoke osebe v podjetju, da prevarajo zaposlene, da prenesejo denar ali razkrijejo zaupne informacije.

- Ponarejeni novinarski posnetki: Napadalci lahko ustvarijo ponarejene video posnetke znanih osebnosti ali novinarjev, ki poročajo o neresničnih dogodkih, da bi vplivali na javno mnenje ali tržne trende.
- Osebne izsiljevalske prevare: Z uporabo posnetkov ali slik žrtve lahko napadalci ustvarijo video posnetke in nato zahtevajo odkupnino v zameno, da jih ne objavijo.

8. Prihodnost umetne inteligence v kibernetski varnosti

Kot ena izmed najhitreje rastočih tehnologij v zadnjem desetletju je umetna inteligenca (UI) močno vplivala na številna področja, vključno s kibernetsko varnostjo. Njena sposobnost obdelave ogromnih količin podatkov in avtomatizacije kompleksnih nalog je prinesla revolucijo v načinu, kako se soočamo s kibernetskimi grožnjami.

Kaj lahko pričakujemo v prihodnosti

V prihodnosti kibernetske varnosti bomo priče revolucionarnim spremembam, ki jih bo prinesla umetna inteligenca (UI). Sistemi kibernetske varnosti bodo postali bolj avtonomni, z zmožnostjo samostojnega učenja in prilagajanja novim grožnjam, ne da bi moral posredovati človek. Namesto tradicionalne reaktivne obrambe se bo UI osredotočila na proaktivno iskanje in preprečevanje potencialnih napadov, še preden se zgodijo. Ta napredna tehnologija bo tesno integrirana z drugimi inovativnimi tehnologijami, kot so kvantni računalniki, blockchain in internet stvari (IoT), da bi skupaj zagotovile robustno in celovito varnostno rešitev. Poleg tega bo UI omogočila prilagajanje varnostnih rešitev specifičnim potrebam posameznih uporabnikov ali organizacij, kar bo zagotavljalo bolj ciljano in učinkovito zaščito v dinamičnem digitalnem okolju.

Potencialni izzivi in etična vprašanja

Z naraščajočo integracijo umetne inteligence (UI) v kibernetsko varnost se soočamo z dvojno naravo te tehnologije. Medtem ko UI prinaša izboljšane varnostne rešitve, jo lahko napadalci izkoristijo za izvedbo naprednih napadov, kar ustvarja zapleten boj med napadalci in zagovorniki varnosti. Poleg tega se z večjo uporabo UI v varnostnih sistemih pojavljajo pomisleki glede zasebnosti in nadzora. Ključno vprašanje, ki se postavlja, je, kako zagotoviti, da tehnologija ne krši zasebnosti uporabnikov, medtem ko še vedno učinkovito ščiti digitalne sisteme. (Podgoršek, 2023:37) Uporaba UI v kibernetski varnosti pa prinaša etična vprašanja, kot so: Kdo je odgovoren, če UI napačno identificira grožnjo? Ali je etično uporabljati UI za proaktivno iskanje potencialnih groženj, tudi če to pomeni nadzor nad uporabniki?

9. Sklepne misli

V sodobnem digitalnem svetu, kjer se količina podatkov in povezav med napravami eksponentno povečuje, je kibernetska varnost postala ena izmed najpomembnejših tem. Umetna inteligenca (UI) je v središču tega boja za varnost, saj prinaša revolucijo v načinu, kako se soočamo s kibernetskimi grožnjami.

Grožnje se nenehno spreminjajo in razvijajo, zato morajo tudi varnostne rešitve ostati korak pred njimi. Umetna inteligenca, s svojo sposobnostjo učenja in prilagajanja, je idealno orodje za to nalogo. (Modic, 2023:32)

Vendar pa je pomembno, da se ne zanašamo izključno na tehnologijo. Človeški dejavnik ostaja ključnega pomena, bodisi pri razvoju in izvajanju varnostnih strategij bodisi pri prepoznavanju in odzivanju na grožnje (Čaleta, 2023:17). Umetna inteligenca je močno orodje, vendar mora delovati v simbiozi s človeškimi strokovnjaki, da zagotovi najboljšo možno zaščito.

Ob koncu, umetna inteligenca je in bo še naprej imela ključno vlogo v kibernetski varnosti. Z nenehnim razvojem in prilagajanjem bomo lahko zagotovili, da bodo naši digitalni svetovi varni in zaščiteni pred grožnjami, ki jih prinaša prihodnost.

- Viri in literatura

- Atif Ali, Muhammad Arif Khan, Khushboo Farid, Syed Shehryar Akbar, Amna Ilyas Taher M. Ghazal, Hussam Al Hamadi. (2023): "The Effect of Artificial Intelligence on Cybersecurity," International Conference on Business Analytics for Technology and Security (ICBATS), Dubai, United Arab Emirates, 2023, pp. 1-7, doi: 10.1109/ICBATS57792.2023.10111151. https://ieeexplore.ieee.org/abstract/document/10111151
- Čaleta, Denis (2023): Je človek najšibkejši ali najmočnejši del varnostnega sistema? Revija korporativna varnost. Letnik 2023/3, str. 17-19. https://www.ics-institut.si/revija/32-%C5%A1tevilka
- Modic Jolanda (2023): Vodenje v dobi umetne inteligence: ravnovesje med tehnologijo in človekom. Revija korporativna varnost. Letnik 2023/2, str. 31-35. https://www.ics-institut.si/revija/31-%C5%A1tevilka
- Podgoršek Žiga (2023): Umetna inteligenca in Chat GPT. Revija Korporativna varnost, Letnik 2023/2, str. 37-39. https://www.ics-institut.si/revija/31-%C5%A1tevilka
- Rammanohar Das and Raghav Sandhane (2021): Artificial Intelligence in Cyber Security. J. Phys.: Conf. Ser. 1964 042072. https://iopscience.iop.org/article/10.1088/1742-6596/1964/4/042072/pdf
- Sarker, I.H., Furhad, M.H. & Nowrozy, R. (2021): AI-Driven Cybersecurity: An Overview, Security Intelligence Modeling and Research Directions. SN COMPUT. SCI. 2, 173 (2021). https://doi.org/10.1007/s42979-021-00557-0. https://link.springer.com/article/10.1007/s42979-021-00557-0
- Zhang, Z., Ning, H., Shi, F. et al. (2022): Artificial intelligence in cyber security: research advances, challenges, and opportunities. Artif Intell Rev 55, 1029–1053 (2022). https://doi.org/10.1007/s10462-021-09976-0. https://link.springer.com/article/10.1007/s10462-021-09976-0

UDK 657:004.738.5:004.056

Šest načinov za izboljšanje učinkovitosti notranje revizije kibernetske varnosti

*Matej Drašček in Sergeja Slapničar**

SIX WAYS FOR IMPROVING EFFICIENCY OF INTERNAL AUDIT OF CYBER RISK FACTORS

Cybersecurity is becoming an increasingly important focus for all organisations. The COVID-19 pandemic, global geopolitical tensions, etc., have only heightened the cyber risk for every type of business. The European Confederation of Institutes of Internal Auditing's (ECIIA) Risk inFocus 2023 report and the Institute of Internal Auditors' (IIA) OnRisk2022 report both ranked cyber as the top critical risk for the sixth time. Despite this, the report found that the most significant gap in internal audit capabilities relates to cybersecurity. This led to a research into how effectively internal auditors can provide assurance on cybersecurity risk management, and what internal auditors can do to improve cybersecurity risk management in banks.

JEL G21 K24 M42

Grožnje kibernetske varnosti za organizacije so notranjim revizorjem dobro znane in podrobno obdelane. Svetovni gospodarski forum (WEF) je v svojem letnem poročilu The Global Risk Report 2023[1] kibernetsko varnost uvrstil na osmo mesto najpomembnejših tveganj, le za raznimi tveganji podnebnih sprememb.

Tudi v Sloveniji grožnje kibernetske varnosti naraščajo. Od 1. januarja do 30. junija 2023 so na SI-CERT obravnavali 3.477 prijav, kar je povečanje za 4,57 % glede na enako obdobje lani[2]. Največji porast porast groženj je prav v bančništvu.[3]

Na drugi strani pa poročilo Risk in Focus 2023[4], ki ga je pripravil Evropska konfederacija Inštitutov notranjih revizorjev (ECIIA – European Confederation of Institutes of Internal Auditors), kaže, da notranji revizorji zaostajajo pri znanju in strokovnosti na področju kibernetske varnosti. Pri tem pa niso osamljeni. Zdi se, da se s temi tveganji spoprijemajo tudi nadzorni sveti, saj raziskava OnRisk 2022[5] Inštituta notranjih revizorjev (IIA – the Institute of Internal Auditors) kaže, da nadzorni sveti nimajo dovolj znanja za razumevanje tveganj kibernetske varnosti, kar lahko organizacije izpostavi nesprejemljivim tveganjem.

Kljub vsemu je raziskav o tem, kako celovito in učinkovito je revidiranje kibernetske varnosti, malo. V tem članku se sicer ne ukvarjamo s tem, kako izvajati notranjo revizijo na področju kibernetske varnosti, saj je to dobro opredeljeno v Praktičnih vodnikih IIA in drugih uveljavljenih okvirih (npr. COBIT, ISO, NIST itd.), temveč s tem, kateri so dejavniki, ki povečujejo učinkovitost notranje revizije pri obvladovanju tveganj kibernetske varnosti in tako zmanjšujejo izpostavljenost organizacij izgubam.

V izvedeni raziskavi[6] (Slapničar, Vuko, Čular in Drašček, 2022), ki je bila predstavljena različnim publikam, smo raziskovali, kateri dejavniki povečujejo raven zagotovil notranje revizije pri obvladovanju tveganj kibernetske varnosti. Raziskava je bila izvedena s pomočjo ankete, na katero je odgovarjalo 183 notranjih revizorjev in IT-revizorjev z vsega sveta. Analiza je pokazala, da notranja revizija kibernetskih tveganj pripomore k zrelosti upravljanja kibernetskih tveganj. Notranji revizorji lahko tudi z netehničnimi priporočili ter hitrimi rešitvami povečajo učinkovitost notranje revizije pri zagotavljanju kibernetske varnosti.

* Dr. Matej Drašček, Hranilnica Lon d.d. in izredna prof. dr. Sergeja Slapničar, University of Queensland

[1] World Economic Forum. The Global Risks Reports 2023. 18. izdaja. Dostopno: https://www3.weforum.org/docs/WEF_Global_Risks_Report_2023.pdf

[2] SI-CERT. Statistika SI-CERT za prvo polovica leta 2023. Dostopno: https://www.cert.si/statistika-si-cert-za-prvo-polovico-leta-2023/

[3] RTV. Banke opozarjajo na povečano število lažnih sporočil SMS in investicijskih prevar. Dostopno: https://www.rtvslo.si/crna-kronika/banke-opozarjajo-na-povecano-stevilo-laznih-sporocil-sms-in-investicijskih-prevar/677847

[4] ECIIA. Risk in Focus 2023. Dostopno: https://www.eciia.eu/wp-content/uploads/2022/09/Risk-in-Focus-2023.pdf

[5] IIA. Onrisk 2022. Dostopno: https://www.theiia.org/en/resources/research-and-reports/onrisk/

[6] Slapničar, S., Vuko, T., Čular, M., & Drašček, M. (2022). Effectiveness of cybersecurity audit. International Journal of Accounting Information Systems, 44, 100548.. Dostopno: https://www.sciencedirect.com/science/article/pii/S1467089521000506

Certifikati na področju notranje revizije so pomembni, še bolj pa so pomembni certifikati na področju notranje revizije informacijske ali kibernetske varnosti

Certifikati niso pomembni le za stroko notranje revizije kot tako, temveč tudi za kandidate, ki z opravljenimi izpiti pokažejo, da so dosegli raven obvladovanja za uspeh v stroki. IIA s CIA (Certified Internal Auditor)[7] je imela pomembno vlogo pri dvigu strokovnosti notranje revizije, vendar raziskave kažejo, da najpomembnejši dejavnik niso splošni certifikati notranje revizije, temveč certifikati notranje revizije informacijske tehnologije ali kibernetske varnosti. Zato je pomembno, da imajo banke v funkciji notranje revizije sodelavce s certifikati s področja informacijske tehnologije ali kibernetske varnosti, saj to vodi k višji ravni zagotovil na področju kibernetske varnosti.

Kaj naj stori vodja notranje revizije

Standard 1210[8] zahteva, da morajo imeti notranji revizorji znanje, spretnosti in druge kompetence, potrebne za opravljanje svojih nalog. Matrika kompetenc/sposobnosti je standardno kadrovsko orodje, v katerem je opredeljeno pomanjkanje določenih kompetenc, zato jo vodje notranje revizije običajno uporabljajo za ugotavljanje pomanjkanja kompetenc. Vodja notranje revizije mora načrtovati razvoj sposobnosti IT in kibernetske varnosti tako, da se usposabljanje ali izobraževanje notranjih revizorjev konča z mednarodnim certifikatom s področja IT ali kibernetske varnosti. Ker je strokovni razvoj v vsakem notranjerevizijskem DNK, identifikacija pripravljenih kandidatov ne bi smela biti problematična.

Novi model treh linij pravi: Sodelovanje med pooblaščencem za informacijsko varnost in vodjo notranje revizije je ključnega pomena

Novi posodobljeni model treh linij IIA[9] se ponovno osredotoča na pomen sodelovanja druge in tretje linije ter njegovo vlogo pri dodajanju vrednosti organizaciji. Kartiranje dajanja zagotovil (ang. assurance mapping) ali celovito dajanje zagotovil itd., so le nekatera od orodij, ki so v notranjerevizijski stroki postala obvezna. Naša in nekatere druge mednarodne raziskave pa kažejo, da sodelovanje med pooblaščencem za informacijsko varnost in vodjo notranje revizije vodi do boljšega obvladovanja tveganj kibernetske varnosti, predvsem zaradi komplementarnih kompetenc, ki jih imata.

Kaj naj stori vodja notranje revizije

Če ima služba notranje revizije strokovnjaka za notranjo revizijo kibernetske varnosti, potem naj ima vsaj nekdo v ekipi osnovno znanje žargona kibernetske varnosti in lahko vzpostavi dober stik s pooblaščencem za informacijsko varnost. Pooblaščenca za informacijsko varnost je treba obravnavati kot osebo, s katero mora imeti notranjerevizijska služba tesen odnos, zlasti v okoliščinah, ko je zaradi razmer (npr. geopolitične razmere) povečano tveganje na področju kibernetske varnosti. Služba notranje revizije bi lahko organizirala ne le redne letne sestanke s pooblaščencem za informacijsko varnost, na katerih bi razpravljali o tveganjih in karti zagotovil, temveč tudi redne mesečne sestanke med celotno notranjerevizijsko službo in pooblaščencem za informacijsko varnost s poudarkom na novih in nastajajočih tveganjih na področju kibernetske varnosti. To bi bilo treba obravnavati tudi kot priložnost za usposabljanje celotne notranjerevizijske službe, da izboljša svoje kompetence na področju kibernetske varnosti. Ker s tem nastaja tveganje domačnosti, mora notranji revizor pri pregledovanju področja upravljanja kibernetskih tveganj paziti, da ohrani svojo neodvisnost.

Sodelovanje in zunanje izvajanje (outsourcing) sta znamenje moči in ne slabosti

Soizvajanje (cousourcing) ali zunanje izvajanje (outsourcing) bi lahko pomagalo bankam, v katerih primanjkuje strokovnjakov za kibernetsko varnost in kjer tudi notranjerevizijska služba nima ustreznih veščin za revidiranje kibernetske varnosti. To ni le v skladu s standardom 1210, temveč bi ga bilo treba obravnavati tudi kot takojšnjo rešitev problema kibernetske varnosti, pa tudi kot možnost usposabljanja za celotno notranjerevizijsko službo. Izvedena raziskava je pokazala, da večina organizacij in še posebej majhnih notranjerevizijskih skupin pri zagotavljanju kibernetske varnosti uporablja soizvajanje in zunanje izvajanje. Zunanji izvajalec ima na voljo primerjalne podatke o napadih, ranljivostih, zrelosti sistema upravljanja kibernetskih tveganj iz drugih bank v Sloveniji in tujini, ki jih notranji izvajalec težko dobi. Prav tako se s sodelovanjem in zunanjim izvajanjem povečuje učinkovitost notranje revizije. To je situacija, v kateri zmagajo vsi, ne le notranjerevizijska služba, temveč tudi celotna banka.

Kaj naj stori vodja notranje revizije

Kadar primanjkuje notranjih kompetenc o kibernetski varnosti, bi moral vodja notranje revizije nadzornemu svetu ne le predstaviti pomen kibernetske varnosti, temveč tudi poudariti, da lahko pomanjkanje kompetenc v notranjerevizijski službi izpostavi banko tveganjem kibernetske

[7] IIA. Certified Internal Auditor. Dostopno: https://www.theiia.org/en/certifications/cia/

[8] IIA. What Are The Standards. Dostopno: https://www.theiia.org/en/standards/what-are-the-standards/

[9] IIA. The IIA's three lines model. Dostopno: https://www.theiia.org/globalassets/documents/resources/the-iias-three-lines-model-an-update-of-the-three-lines-of-defense-july-2020/three-lines-model-updated-english.pdf

varnosti in da je rešitev v obliki skupnega ali zunanjega izvajanja koristna za celotno banko. Za vodjo notranje revizije je pomembno, da je v pogodbo o skupnem ali zunanjem izvajanju vključena komponenta usposabljanja, saj lahko z njo notranjerevizijska služba sodeluje pri notranji reviziji in se iz nje uči. Ker je lahko soizvajanje ali zunanje izvajanje za banke z omejenimi viri precej drago, je pragmatična in zaželena rešitev večletna pogodba z zunanjim izvajalcem, kjer se lahko na podlagi ocene tveganja razvije model revizije kibernetske varnosti po korakih, pri čemer se potrebna finančna sredstva razporedijo na več let.

Regulativo je treba obravnavati kot minimum

Čeprav regulativa nikoli ne velja za dobro prakso, izvedena raziskava kaže, da strožja regulativa vodi k boljši reviziji kibernetske varnosti. Tu lahko potegnemo vzporednico z okoljsko ureditvijo, kjer so raziskave bolj številne in kažejo, da lahko le regulativa (in ne moč trga) pripelje do uspeha pri spopadanju s podnebnimi spremembami. Izvedena raziskava kaže, da je ne glede na geografsko območje največja učinkovitost revizije kibernetske varnosti v organizacijah, kjer obstaja stroga regulativa, ne le na področju IT, temveč tudi kibernetske varnosti (npr. bančništvo, kritične panoge itd.). Sedanje zahteve v regulativi pa vendarle niso tako poglobljene in stroge, da bi jih lahko jemali kot dobro prakso, ampak zgolj kot minimum. Ali jih bo banka samo dosegala ali presegala, je odvisno od velikosti banke, virov, ki jih ima na voljo, nagnjenosti k tveganju in izpostavljenosti.

Kaj naj stori vodja notranje revizije

Vodja notranje revizije bi moral na regulativo gledati kot na sodilo, ki jo je treba uporabiti pri dajanju zagotovil kibernetske varnosti. V bančništvu naj notranja revizija še naprej sledi zahtevam predpisov in naj jih banka tudi presega. Prav tako je smiselno, da so banke v svoji panogi vodilne in si prizadevajo za predpise v vseh panogah, s katerimi so v stiku, saj bo to koristilo vsem akterjem v panogi. Panoga kot celota je tako močna, kot je močan njen najšibkejši člen (tudi dobavitelj ali kupec).

Ton z vrha naj bo zlati standard

Če ni podpore z vrha, to je s strani uprave in nadzornega sveta, upravljanje s kibernetskimi tveganji in notranja revizija tega področja nista dobro razviti, kaže naša raziskava in tuje sorodne raziskave. Ton z vrha smo merili s pogostnostjo poročanja nadzornemu svetu, s strokovnim znanjem in z vključenostjo nadzornega sveta v upravljanje kibernetskih tveganj ter s proračunom namenjenim zanje.

Tudi tehnične kompetence uprav, ki so tudi po naši raziskavi pomanjkljive, neposredno vplivajo na raven zrelosti kibernetske varnosti v organizaciji. Če ne razumejo poročil, ne morejo sprejemati odločitev o kibernetski varnosti.

Kaj naj stori vodja notranje revizije

Odnos med vodjo notranje revizije in nadzornim svetom ni pomemben le pri kibernetski varnosti, temveč pri vsem, kar notranja revizija počne v banki. Vodja notranje revizije mora biti politično spreten, ko se obrača na nadzorni svet glede pomanjkanja znanja in spretnosti na področju kibernetske varnosti. Ko poroča o reviziji kibernetske varnosti, naj komunicira z nadzornim svetom tako, da bodo poročila članom razumljiva in se bodo lahko nanje odzvali. Nadzorni svet in upravo zanima, kakšnemu tveganju je banka izpostavljena, kakšne posledice lahko utrpi in ali je banka učinkovita pri upravljanju tveganj. Pogosto pa poročila zanje ne vsebujejo odgovorov na ta vprašanja, pač pa kopico tehničnih ukrepov, s katerimi je težko odgovoriti nanje. Vendar pa je tudi res, da bi v času digitalnega poslovanja tudi kompetence nadzornikov morale pokrivati tehnološka znanja. Pri izvajanju notranje revizije pri upravljanju banke bi morala notranjerevizijska služba preveriti tehnične sposobnosti članov nadzornega sveta na področju kibernetske varnosti. To nikoli ni lahko, vendar
bi morala biti to prednostna naloga vodje notranje revizije, saj se tveganja kibernetske varnosti, kot že omenjeno, zdaj dotikajo vseh in ni več izjem.

Dajanje zagotovil nadzornemu svetu samo po temeljitem pregledu

Tudi pri notranji reviziji ni vse dobro in prav. Največja pomanjkljivost, ki jo je pokazala izvedena raziskava, je, da so nekateri notranji revizorji dosegli nizke rezultate pri globini načrtovanja in ravni ustreznih dokazov in postopkov v izvajanju, kar pa jih ni ustavilo, da ne bi nadzornemu svetu poročali o utemeljenem zagotovilu in mnenju glede zrelosti kibernetske varnosti banke. To ni le neskladje s standardi, ampak lahko povzroči tudi veliko škodo banki.

Kaj naj stori vodja notranje revizije

Standardi zagotavljanja kibernetske varnosti vključujejo veliko tehničnih podrobnosti ter zahtevajo za izvedbo potrebna posebna tehnična znanja, a treba jih je upoštevati. Vodja notranje revizije bi moral biti v tem primeru zelo strog in spodbujati ekipo, naj spregovori, če se ne počuti kompetentno pri izvajanju revizije kibernetske varnosti.

Čas za začetek je zdaj

Kibernetska varnost med notranje revizorje še vedno vnaša nelagodja zaradi svoje tehnične zahtevnosti. Toda tveganja kibernetske varnosti se ne zmanjšujejo in vsaka banka jim je izpostavljena. Ker je poslanstvo notranje revizije zaščititi in dodati vrednost organizacijam, je zato tudi za notranje revizorje nujno, da so pri vsaki notranji reviziji pozorni na ta tveganja. Članek prikazuje nekaj taktik, kako izboljšati splošno učinkovitost dajanja zagotovil na področju kibernetske varnosti, in vsaka notranjerevizijska služba bi morala vključiti vsaj nekatere od njih, saj ne zahtevajo obilice virov. To bo privedlo do boljše revizije in na koncu tudi pomagalo notranjerevizijski službi izpolniti njen namen: zaščititi in dodati vrednost banki.

UDK 004.056:343.9

Kibernetska varnost in spletne goljufije skozi oči goljufov

*David Gracer**

CYBERSECURITY AND INTERNET FRAUD SEEN THROUGH FRAUDSTERS' EYES

The article talks about cyber security in connection with online fraud in Slovenia, which has been on the rise in the last few years. The content describes the various methods of online fraud service and how online fraudsters operate and the reasons for their success. The reasons are different, and the success depends on the different characteristics of the Internet users or the victims, as well as the extraordinary ingenuity of online fraudsters and the advanced technologies they use.

JEL K14 K24

Dobro znano je, da je obseg obravnavanih spletnih goljufij v obdobju zadnjih nekaj let v velikem porastu. To sicer ne pomeni, da je kibernetska varnost v Sloveniji vedno slabša, saj se število incidentov povečuje zaradi različnih drugih dejavnikov, kot npr. večjega števila novih neveščih uporabnikov spleta, ki imajo najrazličnejše lastnosti, nekateri so preveč radovedni, naivni, želijo hitro zaslužiti, iščejo ljubezen, enostavno niso dovolj pozorni in nasedejo goljufijam, o katerih je na spletu nešteto opozoril policije, bank in drugih institucij. Vsekakor pa je treba izpostaviti tudi ekstremno iznajdljivost spletnih goljufov, ki poleg vedno novejših oblik spretno prilagajajo načine storitve glede na njihove izkušnje »s terena«.

Spletni goljufi so aktivni že vrsto let, vendar so se v zadnjih letih prav zaradi uspešnosti in enormnih dobičkov še bolj namnožili. K temu je nedvomno pripomogla epidemija, saj so nepričakovano dobili milijone novih »tarč«, tj. uporabnikov, ki spleta pred epidemijo sploh niso uporabljali in jim je v obdobju, ko so imeli več časa, predstavljal samo lažji način za komunikacijo s sorodniki, spletno nakupovanje ali samo krajšanje časa. Spletni goljufi so to pridoma izkoristili in sistemsko na različne načine pristopili k večji množici spletnih uporabnikov, kar se je zelo hitro obrestovalo.

Dejstvo je, da velike večine spletnih goljufij ne izvršujejo posamezniki, ampak zelo dobro organizirane kriminalne združbe, ki delujejo v obliki klicnih centrov, najbolj razširjenih v Indiji, v zadnjem obdobju pa tudi v Ukrajini. Prav zaradi izjemnega učinka pa se je število klicnih centrov povečalo, tako da imamo v tem trenutku občutek, da jih lahko na spletu srečamo na vsakem koraku, skoraj vsak pa je že prejel njihovo elektronsko pošto, kratko sms-sporočilo ali telefonski klic. Sicer je e-pošta eden najbolj uporabljenih komunikacijskih kanalov po vsem svetu. Po podatkih s spleta je v letu 2023 dnevno poslanih okrog 347,3 milijarde e-poštnih sporočil, od tega je okrog polovice sporočil t. i. nezaželene pošte (»spam«). Raziskave so pokazale, da pošiljatelji neželene pošte prejmejo en odgovor na vsakih 12,5 milijona poslanih neželenih sporočil. Navedeno pomeni, da spletni goljufi dnevno prejmejo skoraj 30 tisoč odzivov in s tem potencialnih oškodovancev.

Prav ta način delovanja z ogromnimi množicami jim prinaša uspeh, saj spletni goljufi v klicnih centrih delujejo po vnaprej predvidenih scenarijih in uporabljajo pripravljene skripte za interakcijo s tistimi, s katerimi so vzpostavili kontakt. Ena izmed najstarejših oblik je nigerijska prevara, ki v največjem obsegu poteka prek elektronske pošte, v nekaterih primerih pa so lahko pisma poslana tudi po navadni pošti. Pošiljatelji se najpogosteje predstavljajo kot bankirji, direktorji, zdravniki, bolniki, vojaki, loterije...ipd. Zgodbo imajo vnaprej pripravljeno in jo rahlo prilagajajo glede na to, od kod prihaja potencialna žrtev. Običajno je vsebina pošte napisana v slabi angleščini ali pa je s pomočjo spletnih prevajalnikov prevedena v slovenščino. V začetni pošti je ponavadi omenjen mamljiv obljubljeni

* David Gracer, mag., višji kriminalistični inšpektor, Sektor za gospodarsko kriminaliteto, Generalna policijska uprava

znesek več sto tisoč ali milijonov v različnih valutah (najpogosteje evri, funti, dolarji,..). Pri tem pa pošiljatelj zahteva zgolj malo podatkov prejemnika, npr. ime, priimek, telefonsko številko ali elektronski naslov. S tovrstnimi podatki si goljuf seveda ne more pomagati, po prejemu odgovora s podatki pa ugotovi, da prejemnik morda lahko postane njegova žrtev.

Po prvem odgovoru prejemnika sledi navezovanje stikov, ponavadi prek elektronske pošte, lahko pa tudi prek telefonskih klicev. Goljufi ponujajo velike količine denarja, ki pa ga seveda ni mogoče takoj dobiti. Da bi bila zadeva videti resna, žrtvam pošiljajo kopije ponarejenih dokumentov, bančne dokumentacije, nakazil, zapuščinskih pisem, ipd. Največkrat oškodovanci nasedejo ponarejenemu potrdilu o nakazilu na žrtvin transakcijski račun, do katerega seveda nikoli ne pride, saj pred tem vedno prihaja do določenih zapletov, plačil dajatev, davkov, odvetniških storitev, carine, poštnine..ipd, ki jih mora žrtev poravnati pred nakazilom. Zneski so sprva praviloma nižji, če pa žrtev nakaže denar, se večajo. Spletni goljufi so namreč ugotovili, da večanje zneskov pri oškodovancih psihološko običajno deluje tako, da ne želijo izgubiti tistega, kar so že nakazali, zato bodo tvegali in nakazali še več, nekako po pregovoru »Kamor je šel bik, naj gre še štrik«.

Med zelo priljubljenimi metodami je tudi t. i. romantična prevara, ki sicer deluje po principu nigerijskih prevar. Gre namreč za preslepitev žrtve z vplivanjem na njena čustva, vse pa se ponovno dogaja po vnaprej predpisanem scenariju, ki je glede na tisoče predhodnih uspešnih goljufij pripravljen v skripti in ga izvrši spletni goljuf, ki deluje v klicnem centru. Zelo verjetno žrtve romantičnih goljufij nevede komunicirajo z veliko različnimi osebami, saj je za njih značilno, da komunikacija po začetni vzpostavitvi stika goljufa z žrtvijo traja dlje časa, mesece ali celo več let. Namen pa je pridobiti popolno zaupanje in naklonjenost žrtve. Če žrtev spravijo v fazo, ko verjame, da je na drugi strani nekdo, ki jo ima rad in je sicer v zelo dobri finančni situaciji, vendar zaradi trenutnih okoliščin potrebuje samo začasno pomoč zaradi npr. nakupa letalske karte, plačila rojstnodnevnega darila za otroka, se tudi višina nakazil, ki jih v nadaljevanju zahteva goljuf, običajno stopnjuje. Izjemno veliki zneski pa so običajno nakazani zaradi dragocenega paketa, ki je na poti v Slovenijo in je zanj treba plačati različne davke, carino, odvetniške stroške ipd. Zelo dobro se vidi prilagajanje spletnih goljufov glede na reakcije žrtev pri t. i investicijskih goljufijah, s čimer poskušajo pridobiti čas potreben za izvršitev in število žrtev. V preteklih letih je bila namreč daleč najbolj aktualna zgodba z velikim dobičkom pri vlaganju sredstev v kripto valute. Nekateri posamezniki so v želji po hitrem zaslužku postali relativno lahka tarča goljufov, ki na svoje žrtve prežijo s privlačnimi obljubami o možnosti visokih zaslužkov ob minimalnem tveganju. V preteklosti je bilo zelo učinkovito, da so vzpostavili lepo urejeno spletno stran s ponudbo glede vlaganja sredstev v različne naložbene produkte z nerealno visokimi stopnjami donosa. Po registraciji je bilo treba začeti investirati, vendar to ne gre brez osebnega asistenta, saj so s podatki o vložkih ter dobičkih manipulirali spletni goljufi. Da goljufi pridejo do denarja s tovrstno goljufijo, jim v vsakem primeru vzame veliko časa, da bi vse skupaj pohitrili, pa osebni asistent naveže (običajno telefonski) stik z oškodovancem ter predlaga namestitev programov za oddaljeni dostop. Tako lahko v nadaljevanju upravljajo z računalnikom vlagatelja, v njegovem imenu izkazujejo odpiranje trgovalnih računov, profilov, v primerih uporabe virtualne valute tudi odpirajo elektronske denarnice. Najpomembnejši razlog za uspešnost tovrstnih goljufij so podatki, ki jih spletni goljufi vnesejo v osebni trgovalni račun, kjer lažnivo prikazujejo dobičke. Vlagatelji pa se velikokrat zaradi lažno prikazanega visokega dobička odločijo za dodatna vlaganja. V resnici goljufi vlagateljevega denarja ne oplemenitijo z vlaganjem v kakršne koli naložbe, ampak ga ukradejo, saj imajo dostop do elektronskih denarnic, ki so jih odprli v imenu žrtev. To storijo s prenakazili na druge denarnice, v enem izmed korakov v manjšem deležu tudi na denarnice drugih vlagateljev, ki jih imajo prav tako pod nadzorom. Ta nakazila oškodovancem prikažejo kot donos oziroma izplačilo dobička in jih s tem prepričajo v resničnost poslov. Seveda je tako kot pri drugih oblikah spletnih goljufij glavni namen storilcev od vlagateljev pridobiti čim več denarja, za katerim se zaradi pretvorbe v kripto valute, uporabe različnih orodij (npr. mikserjev), izvedenih prenakazil in dvigov v tretjih državah lahko izgubi sled, predvsem pa zaradi hitrosti delovanja sistema kripto transakcij izgubi možnost povrnitve sredstev, saj vse skupaj poteče v nekaj minutah, pri čemer pa oškodovani subjekti ugotovijo, da so bili ogoljufani šele, ko jim je onemogočena povrnitev finančnega vložka, ki so ga namenili za izbrano investicijo, kar pa lahko traja tudi več mesecev ali celo let.

V zadnjem obdobju so navedeni način storitve goljufij z investicijo v kripto valute nekoliko spremenili, saj jim očitno prihrani čas in/ali uspejo prepričati več vlagateljev. Goljufi namreč iz klicnih centrov kličejo na naključne telefonske številke in se lažno predstavljajo kot uslužbenci znanih menjalnic kripto valut. Ljudje so že nekako navajeni, da se na telefonske številke, ki prihajajo iz oddaljenih držav, ne javljajo, zato vedno bolj uporabljajo modificirane slovenske telefonske številke (t. i. spoofing). Tako skušajo pri prejemnikih klicev vzbuditi zaupanje, saj se bodo na takšen klic ja-

vili prej kot na klic s tuje telefonske številke. Oškodovancem običajno v polomljeni slovenščini zagotavljajo, da jih na virtualni denarnici čakajo sredstva v višini nekaj tisoč evrov. Lahko da imajo seznam s kontaktnimi podatki tistih, ki so v preteklosti že bili oškodovani iz naslova investicijske goljufije, lahko pa imajo enostavno srečo in se pogovarjajo z nekom, ki je v preteklosti dejansko sredstva investiral v kripto valute, v nekaterih primerih pa ljudje sploh nikoli niso investirali v kripto valute in kljub temu verjamejo, da jih nekje čakajo sredstva. Seveda imajo goljufi drugačen načrt, saj je zahtevani pogoj za izplačilo teh sredstev namestitev programa za oddaljeni dostop (anydesk) na računalnik in/ali mobilni aparat. V nadaljevanju storilci upravljajo z računalnikom in telefonom. To pomeni, da lahko odprejo spletno banko, s pomočjo uporabniških podatkov, ki jim jih sporoči oškodovanec, vstopijo v spletno banko in odtujijo vsa sredstva, ki so na voljo na računu.

Navedeno programsko orodje je, kolikor je uporabljeno za legalne namene, v bistvu zelo dobra aplikacija, ki zagotavlja oddaljeni dostop do osebnih računalnikov in drugih naprav ter ponuja daljinsko upravljanje, prenos datotek in funkcionalnost VPN. Ima pa eno opcijo, ki jo spletni goljufi pridoma koristijo, in sicer se imenuje »ugasni zaslone«. Opcija je uporabna v vseh primerih, kjer spletnim goljufom uspe vstop v spletno banko oškodovanca, največkrat v opisanem primeru lažnega dobička pri investiciji v kripto valute, običajno pa tudi pri goljufijah z lažno tehnično pomočjo Microsofta. Tovrstne goljufije se najpogosteje izvršujejo iz klicnih centrov nastanjenih v Indiji, tudi klicatelji po navadi govorijo angleško z indijskim naglasom. Tistega, ki se na klic zglasi, poskušajo prepričati, da kličejo iz tehnične pomoči Microsofta zaradi napake na računalniku. Če prejemnik klica goljufiji nasede, je naslednji korak, da zažene računalnik, namesti navedeno programsko opremo in z upravljanjem računalnika prikaže nekatere napake ter navaja, da je računalnik okužen z virusi, ki jih je nujno treba odstraniti. Za plačilo storitve običajno zahtevajo majhen znesek v višini nekaj evrov, njihov cilj pa je pridobitev podatkov o plačilni kartici ali še huje, uporabniških podatkov za dostop do spletne banke. Če jim uspe slednje, bodo v naslednjem koraku z omenjeno opcijo ugasnili zaslone, dejali, da je nekaj narobe in je treba počakati, medtem pa izpraznili bančni račun.

Še ena izmed zvijač spletnih goljufov, ki je v zadnjem obdobju zelo razširjena, pri tem pa so tudi izjemno učinkoviti, je lažno predstavljanje finančnih institucij. Ponovno gre za množična sporočila po elektronski pošti ali SMS-sporočila, kjer gre za ribarjenje podatkov. Prejeta sporočila namreč delujejo, kot da so jih poslale banke ali davčna uprava in vsebujejo lažno opozorilo (običajno o posodobitvi podatkov) ter obvezno povezavo, na katero je treba klikniti. Ob kliku se odpre spletna stran, ki od uporabnika zahteva vnos podatkov, običajno davčne številke, telefonske številke ter v nadaljevanju enkratnega gesla za dostop do spletne banke. Spletni goljufi v nadaljevanju te podatke uporabijo, vstopijo v spletno banko in ukradejo sredstva, ki jih najpogosteje nakažejo na transakcije račune odprte v tujini, v nekaterih primerih tudi na račune v Sloveniji.

Največje tveganje predstavlja spletnim goljufom prenos denarja, saj so ob pogoju, da je bila prijava s strani oškodovanca izvedena hitro po transakciji, ki je bila izvedena na bančni račun denarne mule, policija, banke, uradi za preprečevanje pranja denarja in druge institucije relativno uspešni pri sami zamrznitvi sredstev. Zato se spletnim goljufom dogaja, da kljub temu, da so vložili veliko časa in ukradli veliko denarja, niso uspešni oziroma ne morejo priti do sredstev, ki so jih sicer že uspešno prenesli. Prav zaradi tega se vedno bolj poslužujejo odpiranja virtualnih denarnic v imenu oškodovanca. Težava pa je, da tudi slednje zahteva nekaj časa, pri tem pa morajo poleg nadzora virtualne denarnice oškodovanca imeti tudi dostop do njegove spletne banke. V tem primeru je prenos sredstev bistveno hitrejši, saj lahko denarna sredstva prenesejo z bančnih računov drugih oškodovancev, ki jih imajo pod nadzorom, na bančni račun oškodovanca, v imenu katerega nadzorujejo tudi virtualno denarnico. Prav zato gre običajno za prenos denarja z računov več oškodovancev na račun, s katerega lahko opravijo nakup virtualnih valut, le-te pa v nekaj minutah usmerijo v druge virtualne denarnice, mikserje ipd. ter pred organi pregona poskušajo zakriti sled za denarjem.

Dokler bodo spletni goljufi uspešni, bodo seveda z goljufijami nadaljevali ter svojo dejavnost širili, tako da jih bo vse več in izvrševali bodo lahko še številnejše različne spletne goljufije, tako starejših kot novejših oblik. Zato bo v prihodnosti ključnega pomena dobra ozaveščenost uporabnikov spleta, spletnih bank, plačilnih kartic in drugih oblik porabe denarnih sredstev na spletu, saj lahko vsak uporabnik za lastno varnost naredi največ sam, tako da se pred kakršnim koli poslom dodobra prepriča v njegovo legitimnost. Velikokrat pride do finančnih posledic kljub temu, da so ljudje do odgovora na vsa vprašanja oddaljeni le nekaj klikov, ki pa jih niso opravili ali pa so jih takrat, ko je bilo že prepozno.

UDK 366.5:343.72:004.056

Pravična prihodnost za žrtve spletnih zlorab

*Alina Meško**

A FAIR FUTURE FOR VICTIMS OF INTERNET FRAUD

Online fraud is increasing, consumers are exposed to various risks in the digital environment, especially when using modern payment methods. Digital literacy and strategies for fraud prevention are crucial. However, we must also take care of the victims of online scams, provide them with the support they need, and share the responsibility and consequences.

JEL D18 K14 K24

Na Zvezi potrošnikov Slovenije (ZPS) mesečno prejmemo več pritožb potrošnikov, ki so bili žrtev spletne prevare. Poleg očitne težave – kraje njihovega denarja – dodatno razočaranje neredko povzroči stališče banke, da je odgovornost za nastalo škodo izključno na strani uporabnika. Seveda, do nas pridejo le primeri, ko izid za potrošnika ni ugoden. Morda je tistih drugih bistveno več, a tega na ZPS ne vemo. Tudi zato si želimo več transparentnosti na področju spletnih zlorab, več sodelovanja in deljeno odgovornosti tistih, ki spletne prevare lahko preprečijo.

Najbolj pogosto ribarjenje za podatki

Največ primerov spletnih prevar se nanaša na ribarjenje za podatki, ko potrošniki prek elektronske pošte ali sporočila SMS prejmejo vsebino, ki jih poziva k obisku lažne spletne strani in vnosu osebnih podatkov, kot so davčna številka, telefonska številka, koda PIN plačilne kartice in podobno. Lažne spletne strani so zelo podobne izvirnim in uporabljajo logotipe bank, pogosto uporabnike nagovarjajo celo z opozarjanjem pred spletnimi prevarami – z vpisom podatkov naj bi poskrbeli za večjo varnost svojega denarja. V zadnjem času opažamo tudi zlorabe prek mobilnih denarnic, ki jih v preteklosti ni bilo. V večini primerov gre za zlorabe v višini nekaj sto ali nekaj tisoč evrov, a dobimo tudi primere, ko potrošnikom spletni kriminalci ukradejo življenjske prihranke v vrednosti več deset tisoč evrov.

Spletne prevare postajajo vedno bolj prefinjene, žrtve so ne le finančno, temveč tudi psihično zelo prizadete. Pogovori z njimi razkrivajo stisko – počutijo se osramočene, izgubijo zaupanje v sodobne načine plačevanja, pogosto imajo občutek, da so v težkem položaju ostale same, brez ustrezne podpore in razumevanja. Številni prizadeti so starejši potrošniki, teža zlorabe je zanje še toliko večja, saj imajo občutek, da ne zmorejo več sodelovati v – sodobnem digitalnem – svetu.

Deljena odgovornost in huda malomarnost

Digitalna preobrazba je hitra in prinaša uporabnikom številne prednosti, vse od nižjih stroškov, manj porabljenega časa za ista opravila, poenostavljene postopke, možnost, da si življenje urejamo kar od doma. A koristi imajo tudi ponudniki spletnih storitev, kot so telekomunikacijski operaterji, spletni iskalniki, družabna omrežja in spletne trgovine ter ponudniki plačilnih storitev. Na ZPS smo prepričani, da moramo proti spletnemu kriminalu nastopiti skupaj, odgovornost pa ne sme biti le na strani žrtev, temveč deljena med tistimi, ki lahko zmanjšajo število spletnih zlorab. Popolnoma preprečiti jih ne moremo. Za boj proti spletnim zlorabam potrebujemo okolje, v katerem vsi vpleteni prevzemamo odgovornost in finančne posledice.

* Alina Meško, Zveza potrošnikov Slovenije

Uporabnike v primeru spletnih zlorab ščiti zakon o plačilnih storitvah, storitvah izdajanja elektronskega denarja in plačilnih sistemih (ZPlaSSIED). Če je do neodobrene plačilne transakcije prišlo zaradi ukradenega ali izgubljenega plačilnega instrumenta ali z zlorabo, uporabnik krije izgubo do največ 50 evrov. Celotno izgubo pa krije v primeru uporabnikove prevare ali goljufije ter kadar naklepno ali zaradi hude malomarnosti ni izpolnil ene ali več obveznosti v zvezi z uporabo plačilnih instrumentov. A kaj je huda malomarnost?

Pregledali smo mnenja IRPS (izvensodno reševanje potrošniških sporov), kamor se potrošniki obrnejo, kadar menijo, da njihova pritožba na banki ni ustrezno razrešena. Huda malomarnost, so zapisali, je nedoločen pravni pojem, ki ga je opredelila sodna praksa. Pomeni, da je oseba ravnala z manjšo skrbnostjo od skrbnosti, ki se v posameznem primeru lahko pričakuje od povprečno skrbnega človeka. Vrhovno sodišče je v enem od postopkov pojem hude malomarnosti razložilo kot ravnanje, ki ne upošteva niti tistega, kar bi v danem položaju upošteval vsakdo, torej ne samo skrben, ampak tudi manj skrben uporabnik. Tako v nekaterih primerih žrtve prevar niso ravnale hudo malomarno – šlo je za okoliščine, ki lahko zapeljejo povprečnega manj skrbnega (malomarnega) uporabnika. Manj skrbni ali malomarni uporabniki torej niso hudo malomarni, upoštevati je treba tudi osebne okoliščine in ločeno obravnavati ranljive uporabnike.

Sodna praksa nemških sodišč kaže, da se pošiljanje podatkov na lažne spletne strani večinoma ne šteje za hudo malomarnost, še celo tedaj ne, ko je uporabnik posredoval več osebnih varovalnih elementov. Slovenska sodna praksa se še ni izrekla, kakšna skrbnost se zahteva od potrošnika pri ravnanju s plačilnimi karticami in podatki, ki predstavljajo varnostne elemente. Obstaja pa sodba Višjega sodišča v Ljubljani, ki je v konkretnem primeru izreklo, da zgolj vpisovanja podatkov na lažno spletno stran ni mogoče šteti za hudo malomarnost. Za hudo malomarnost bi lahko šlo kvečjemu, če bi bila lažna stran opazno drugačna od prave.

Primer dobre prakse in pogled v – za potrošnike bolj pravično – prihodnost

Poznan nam je primer angleške banke TSB, ki zagotavlja garancijo vračil pri spletnih goljufijah, saj se zavedajo, da lahko žrtve izgubijo ne le svoje življenjske prihranke, temveč tudi zaupanje v banke in plačilne sisteme. Strah, da se bodo zaradi garancije uporabniki vedli bolj tvegano, se v TSB ni uresničil. Odkar so leta 2019 uvedli garancije vračil v primeru spletnih zlorab, so sredstva povrnili 97 odstotkom žrtev.

Na ZPS si želimo, da bi njihovemu zgledu sledile tudi banke v Sloveniji. Sami vlagamo veliko truda v izobraževanje potrošnikov na področju spletnih zlorab, objavljamo nasvete in primere zlorab na spletnih mestih in v reviji ZPStest, izvajamo delavnice in svetujemo potrošnikom, kako ukrepati, če so žrtev zlorabe. Odgovornost seveda nosijo tudi uporabniki, ki morajo skrbeti za digitalno pismenost, se redno izobraževati, če želijo (varno) uporabljati spletne storitve, biti pozorni na morebitne zlorabe ter se vesti odgovorno.

A veliko lahko naredijo tudi podjetja, ki digitalno okolje uporabljajo pri svojem poslovanju. Na ravni EU se pojavljajo predlogi in ponekod tudi že izvajajo ukrepi, ki odgovornost porazdeljujejo med vse, ki imajo moč vplivati na spletne zlorabe. Uporabnik mora biti v svetu, ki digitalno postavlja na prvo mesto, ustrezno zaščiten. Predlogi ukrepov, ki bi poskrbeli za bolj varno in pravično digitalno prihodnost:

- **Sistematična povračila** – Na ravni EU je za 68 odstotkov prevar ugotovljena uporabnikova huda malomarnost. Taki primeri so po našem mnenju izjemni in naj ne bi presegali 10 odstotkov. Izkušnje kažejo, da povračila škode potrošnikov ne spodbujajo k neodgovornemu ravnanju.
- **Transparentnost** – Javno objavljeno število zlorab ter delež povračil s strani ponudnikov plačilnih storitev. Tako lahko uporabniki presodijo, kje je varnost najboljša in katerim podjetjem lahko zaupajo upravljanje svojega denarja ter jim s tem omogočajo poslovanje.
- **Takojšnje povračilo** – Žrtev bi morala škodo dobiti nemudoma povrnjeno, nato se ugotavlja njena morebitna odgovornost.
- **Dokazovanje** – Dokazovanje, da je naredil vse, da bi prevaro preprečil, naj bo na strani ponudnika plačilnih storitev.
- **Definicija hude malomarnosti** – Potrebujemo definicijo hude malomarnosti, ki je trenutno preveč odprta za interpretacijo.
- **Deljena odgovornost med obema ponudnikoma plačilnih storitev** – Tako podjetje, ki izvede plačilo, kot podjetje, ki prejemniku omogoči prevzem sredstev, bi morala prevzemati odgovornost.
- **Sklad** – Vanj bi sredstva za povračilo škod žrtvam vplačevali ponudniki plačilnih storitev, višina vplačil bi bila odvisna od njihovega vlaganja v preprečevanje prevar in števila zlorab.
- **Nadzor, blokade transakcij** – Potrebne so hitre blokade sumljivih nakazil, omejitev števila transakcij in opozorila v primeru nenavadnih transakcij s strani ponudnika plačilnih storitev.

Žrtev spletne prevare lahko danes postane kdorkoli. Tudi tisti, ki digitalne finančne storitve poznamo, jih dnevno uporabljamo, se na tem področju izobražujemo in skrbimo za spletno varnost. Poskrbeti moramo za kontinuirano izobraževanje in ozaveščanje potrošnikov – veliko lahko naredimo s sodelovanjem in usklajenimi akcijami. Razmisliti pa bi morali tudi o pravični porazdelitvi odgovornosti, tako moralne kot finančne. Žrtvam spletnih zlorab, ki pri uporabi digitalnih storitev niso bile hudo malomarne, moramo ponuditi ustrezno podporo in zagotovilo, da v težkih razmerah ne bodo ostale same. Ter da finančno breme ne bo le na njihovih ramenih.

UDK 336.71:004.056

Smernice upravljanja kibernetske varnosti v finančnem sektorju

*Grega Prešeren**

GUIDELINES FOR CYBERSECURITY MANAGEMENT IN THE FINANCIAL SECTOR

The article will address the current cybersecurity issues in the banking and financial sectors. We will focus on the most common attack vectors, vulnerabilities, and techniques for improving an organization's cybersecurity posture. Security testing and user awareness will be discussed in detail. Cybersecurity management has become integral to various regulatory frameworks, leveraging its importance, and moving it closer to management. Cybersecurity management will be discussed in terms of NIS2 directive, DORA regulation, NIST cybersecurity framework, and ISO 27001 standard.

JEL G21 K24 O38

Uvod

Kibernetska varnost je v zadnjih letih zagotovo postala ena ključnih prioritet bančnega in širšega finančnega sektorja. Velike baze uporabnikov, ogromne količine občutljivih podatkov in finančna sredstva, ki so povezana s temi podatki, postavljajo finančne institucije v posebej ranljiv položaj. Od napadov na bančne sisteme in uporabnike imajo organizirane hekerske skupine direktno finančno korist, kar je največkrat tudi njihov končni cilj. Kot odgovor na vedno naprednejše oblike napadov vpeljujejo odgovorni za kibernetsko varnost strateške načine upravljanja kibernetske varnosti. V pričujočem članku bomo naslovili najpogostejše ranljivosti in vektorje napadov ter predstavili dobre prakse upravljanja kibernetske varnosti, ki med drugim vključujejo redno testiranje sistemov in ozaveščanje uporabnikov.

1. Najpogostejši vektorji napadov

Finančne institucije se soočajo s plejado potencialnih kibernetskih groženj, od napadov z ribarjenjem (*ang. phishing*), izsiljevalske kode (*ang. ransomware*) in kampanj s škodljivo kodo (*ang. malware*). V nadaljevanju opisujemo uspešne vektorje napadov, ki jih najpogosteje zasledimo pri testiranju finančnih institucij.

Napadi s socialnim inženiringom

Napadalci uporabljajo metode socialnega inženiringa, da posameznike pregovorijo v razkrivanje zaupnih informacij ali posredovanje poverilnic za dostop do zaščitenega omrežja. Socialni inženiring se izvaja v različnih oblikah. Najpogosteje se srečujemo z napadi z ribarjenjem po elektronski pošti, ne smemo pa zanemariti niti poskusov napadov prek SMS-sporočil ali celo osebnega pristopa na lokacijah. Tovrstni napadi so zelo učinkoviti, ker smo ljudje pogosto preveč radovedni ali ustrežljivi. Že klik na škodljivo povezavo ali odprtje škodljive priponke lahko hekerjem odpre vrata v vaš informacijski sistem.

Napadi s škodljivo in izsiljevalsko kodo

Napadalci uporabljajo škodljivo programsko opremo, ki lahko resno poškoduje IT-sistem ali podatke organizacije. Zlasti nevarni so napadi z izsiljevalsko kodo, ki zakleni (zašifrira) podatke, napadalci pa za povrnitev podatkov ali preprečitev njihove javne objave zahtevajo visoke odškodnine. Res je sicer, da s pogajanji višino odškodnine lahko deloma znižate, v vsakem primeru pa je ob takšnem dogodku na udaru ugled podjetja, ogroženi so podatki komitentov, poleg tega pa pride tudi do slabše uporabniške izkušnje, saj so storitve običajno vsaj nekaj časa onemogočene. Današnje zaščite pred škodljivo programsko kodo so deloma učinkovite, tipično pa ne preprečijo najbolj naprednih napadov. Zato so potrebni dodatni tehnični ukrepi.

* Grega Prešeren, univ. dipl. ing. el., CTO, gpreseren@carbonsec.com, Carbonsec d.o.o.

Napadi z onemogočanjem storitev
Napadi z onemogočanjem storitev (DDoS) tipično temelijijo na pošiljanju velike količine prometa proti strežnikom organizacije, kar v prvi fazi upočasni delovanje omrežja in spletnih strani, v drugi fazi pa pride do odpovedi delovanja sistema.

Napadi po dobavni verigi
Napadi po dobavni verigi so eden novejših vektorjev napadov in vključujejo več deležnikov. Uporabljajo se zlasti takrat, ko želijo napadalci dostopati do omrežja velikega podjetja, ki ima dobro kibernetsko zaščito, prek interneta pa se povezuje z manjšimi podjetji oz. od njih dobavlja strojno ali programsko opremo. Napadalci izberejo enega teh manjših podjetij, ki običajno slabše skrbijo za kibernetsko varnost, in se po dobavni verigi pomikajo do končne tarče. Tako s hekerskimi tehnikami, ki morda niso učinkovite v ciljnem podjetju, po drugi poti, t. i. poti z najmanjšim odporom, vdrejo v ciljno podjetje.
Finančne institucije morajo strategije upravljanja kibernetske varnosti oblikovati z mislijo na najpogostejše vektorje napada in krepitev odpornosti še intenzivneje graditi na teh področjih. Pri tem se moramo zavedati, da ni pomembna le namestitev varnostnih naprav, temveč njihova pravilna umestitev v posamezno okolje, prilagoditev nastavitev posameznemu okolju ter spremljanje delovanja v življenjskem ciklu IT-okolja. Različne nadgradnje in druge spremembe lahko pomembno vplivajo na pravilno prepoznavanje škodljivih vsebin in poskusov napadov.

2. Najpogostejše ranljivosti

Eden od razlogov, zakaj so finančne institucije tako ranljive in posledično privlačne za kibernetske kriminalce, je njihova usmerjenost k uporabnikom ter obsežnost in kompleksnost informacijskega sistema. V nadaljevanju bomo opisali pri testiranjih najpogosteje zaznane ranljivosti v finančnem in bančnem sektorju.

Nezavarovana omrežja in zastarela programska oprema
Dobro zaščiteno omrežje in posodobljena programska oprema sta dve osnovni predpostavki za zagotavljanje varnosti v informacijskem sistemu. Z varnostnimi napravami na perimetru omrežja in v zadnjem času tudi v samem omrežju nadzorujemo promet in zaznavamo morebitne deviacije. Odsotnost varnostnih naprav, njihova neustrezna umestitev in pomanjkljivo spremljanje dogajanja na omrežju so pogost vzrok uspešnih napadov.

Pomanjkljivo izobraženi zaposleni
Zaposleni, ki ne znajo prepoznati potencialne kibernetske grožnje in se nanjo odzvati, lahko za organizacijo predstavljajo veliko ranljivost. Po drugi strani je to ranljivost, ki jo lahko z izobraževalnimi programi za uporabnike precej enostavno rešujemo, dovzetnost za napade s socialnim inženiringom pa se že v nekaj mesecih bistveno zmanjša. Ozaveščanje uporabnikov bomo podrobneje naslovili v nadaljevanju.

Šibki varnostni mehanizmi za prijavo v sisteme
Napadalci lahko pridobijo dostop v poslovno omrežje z ukradenimi ali šibkimi gesli, zato je vpeljava politike močnih gesel nujna za zagotavljanje varnosti. Za dostop do javnih in ključnih sistemov in aplikacij je zelo priporočljiva uporaba večfaktorske avtentikacije (*ang. multi-factor authentication*) s sistemom enkratnih gesel, avtentikatorjev na mobilnem telefonu, ali tehnologije FIDO.
Odpravljanja ranljivosti se je smiselno lotevati celostno in strateško. Ad-hoc načini reševanja kibernetskih tveganj niso zaželeni, saj lahko sicer kratkoročno rešijo težavo, pogosto pa ne prispevajo k splošnemu izboljšanju kibernetskovarnostne drže.

3. Testiranje kibernetske varnosti

Testiranje kibernetske varnosti je ena najpomembnejših komponent učinkovite varnostne strategije. Organizacijam pomaga prepoznavati šibke točke na sistemih, da lahko ukrepajo, preden ranljivosti izrabijo napadalci. Bančni sektor je na področju izvajanja varnostnih testov po naših izkušnjah v slovenskem prostoru eden najbolj naprednih, saj večina bank že leta vestno skrbi za kibernetsko varnost s testiranjem, ozaveščanjem uporabnikov in implementiranjem različnih varnostnih rešitev. Kljub temu se pri varnostnem testiranju pogosto izkaže, da so občutljivi podatki odloženi na lahko dostopnih mestih, na primer v datotekah v skupni rabi, v katerih so zapisana administratorska gesla različnih sistemov. Avtomatski testi takšno ranljivost tipično označijo kot nizko ali info, dejanski vpliv izrabe ranljivosti na poslovanje in ugled banke pa je lahko ogromen. Takšni anomaliji se lahko izognemo z ročnim penetracijskim oz. vdornim testom ali z uporabo avtomatiziranih rešitev, ki poskušajo odkrite ranljivosti v danem sistemu tudi izrabiti. Ob ustreznih vhodnih podatkih (npr. specificiranju, kateri podatki so za nas kritični) bo izbrana rešitev takšno ranljivost rangirala z višjo stopnjo kritičnosti.
Testiranja kibernetske varnosti potekajo na različnih ravneh in na različni infrastrukturi. Kljub vsemu pa lahko klasični varnostni test razdelimo na tri osnovne faze: popis ranljivo-

sti, penetracijsko testiranje in ocena tveganja. Nekoliko drugačen potek pa je pri kibernetski vaji Red Teaming, ki jo bomo v nadaljevanju tudi natančneje opisali.

Popis ranljivosti

S popisom ranljivosti identificiramo potencialne ranljivosti v poslovnem sistemu in jih razvrstimo po pomembnosti. To je prvi korak pri testiranju varnosti sistema, ki se mora nujno nadaljevati z natančnim pregledom in preizkusom izrabe odkritih ranljivosti (penetracijski test). Pri tem se ne smemo osredotočiti le na ranljivosti, ki so v popisu označene za kritične ali visoke, temveč moramo pregledati tudi tiste z oznako info ali nizko, saj se med njimi pogosto skrivajo ranljivosti, ki na prvi pogled neposredno ne predstavljajo večje grožnje, lahko pa vsebujejo podatke, ki napadalcem omogočijo izvajanje nadaljnjih napadov prek drugih virov.

Penetracijsko testiranje

Cilj penetracijskega testa je na podlagi simulacije hekerskega napada preveriti, kako varen je informacijski sistem organizacije. Penetracijski test lahko izvajamo na zunanjem ali notranjem omrežju, na celotnem omrežju ali le na vnaprej določenem segmentu, več segmentih, na aplikacijah ali programskih vmesnikih, t. i. API-jih. Priporočljivo je, da se varnostno testiranje izvaja ciklično, saj se zaradi velike dinamike informacijskih okolij neprestano pojavljajo nove ranljivosti in grožnje. Smiselno je, da organizacije razmislijo o uporabi avtomatiziranih orodij, ki omogočajo redno in učinkovito izvajanje standardiziranih testov, na daljše časovno obdobje (npr. enkrat letno) pa se izvede obsežnejši penetracijski test. Pri izbiri avtomatiziranega orodja je dobro, da to ne le popiše ranljivosti in jih razvrsti po objavljeni stopnji kritičnosti (CVE), temveč jih tudi oceni glede na to, ali je ranljivost v vašem sistemu dejansko mogoče izrabiti in predlaga postopek odprave.

Ocena tveganja

Na podlagi izsledkov popisa ranljivosti in penetracijskega testa se izdela ocena tveganja, ki poleg tehničnega dela vključuje tudi poslovni vpliv. V oceni tveganja povežemo ranljivosti s potencialnimi posledicami njihove izrabe in se na podlagi rezultatov odločimo, katere je smiselno najprej reševati ter predlagamo ustrezne ukrepe za zmanjšanje ali odpravo tveganj.

Red Teaming

Posebna vrsta varnostnega testiranja je t. i. kibernetska vaja oz. Red Teaming, ki je simulacija dejanskega hekerskega napada na organizacijo. Če pri penetracijskem testiranju velja, da naročnik definira obseg testa (npr. segmente omrežja, aplikacijo ipd.) in se izvajalci držijo dogovorjenega obsega, se pri vaji Red Teaming test izvaja na organizaciji kot celoti, uporablja pa se najbolj aktualne hekerske taktike in tehnike. Cilj takšne vaje je preveriti, kako dobra sta zaznava in odziv organizacije na kibernetski napad. Na strani naročnika je tipično ena kontaktna oseba, ki z izvajalcem koordinira potek testa, drugi uporabniki o vaji niso obveščeni. Prav zato je pri takšnem testu pomembno, da se interno vnaprej dobro pojasni, zakaj ima organizacija v določenem letu ali polletju namen izvesti kibernetsko vajo in kaj je cilj takšnega testa.
Red Teaming je edini varnostni test, s katerim ne preverite le varnosti omrežja, temveč dejansko odpornost organizacije na kibernetski napad. Čeprav se morda sliši vabljivo, kibernetska vaja ni primerna za vsako organizacijo. Smiselno je, da podjetje prej že doseže določeno zrelostno raven kibernetske varnosti, kar pomeni, da ima izkušnje z izvajanjem penetracijskih testov, morda tudi z ozaveščanjem uporabnikov in skrbjo za skladnost. Eden od ciljev kibernetske vaje je lahko tudi trening ekipe za odziv. Na podlagi izsledkov vaje ekipa izvajalca (Red Team) poda priporočila ekipi za odziv (Blue Team), ki lahko z njimi izboljša prepoznavanje potencialnih napadov in s tem varnostno držo organizacije. Naprednejša oblika urjenja ekipe za odziv pa je t. i. Purple Teaming, kjer s premišljenimi tehnikami napadov organizacija testira zaznavo napada in glede na reakcijo ekipe za odziv uvede nadaljnje izpopolnjevanje veščin.

4. Ozaveščanje uporabnikov

Poleg testiranja kibernetske varnosti je izredno pomembno tudi neprestano izobraževanje in ozaveščanje uporabnikov. Po statistikah in izkušnjah iz prakse so uporabniki še vedno zelo ranljiv del informacijskega sistema. Z dobro pripravljenim lažnim sporočilom velik delež uporabnikov napadalcem neposredno ali posredno posreduje svoje poverilnice. Sodobni napadi so temeljito premišljeni, pogosto usmerjeni v pridobivanje podatkov o točno določeni osebi ali profilu v organizaciji. Napadalci informacije poiščejo na družabnih omrežjih in spletu ter tudi s pomočjo umetne inteligence pripravijo usmerjena lažna sporočila (*ang. spear phishing*), ki nimajo slovničnih napak, na podlagi katerih jih je bilo mogoče enostavno prepoznati v preteklosti.
Organizacije naj svoje zaposlene izobražujejo o najboljših praksah na področju kibernetske varnosti, kot so močna gesla, varno shranjevanje zasebnih podatkov in zaščita pred napadi z ribarjenjem. V tem kontekstu je priporočljivo, da organizacije spodbujajo zaposlene, naj poročajo o

kakršnem koli sumljivem dogajanju, ki ga opazijo na omrežju ali v elektronski pošti.
Drugi zelo pomemben del ozaveščanja pa je praktični trening prepoznavanja kibernetskih napadov s socialnim inženiringom. V ta namen obstajajo rešitve, ki ponujajo različen obseg vsebin, raznovrstne učne materiale, ki so lahko razvrščeni tudi po težavnosti in tako spodbujajo vedno višjo stopnjo ozaveščenosti in sposobnosti prepoznavanja napadov. Ključni del treninga ozaveščanja je povratna informacija o uspešno ali neuspešno opravljeni vaji. Uporabnike, ki vaje niso uspešno opravili, seznanimo z mesti, ki bi jih v vaji morali prepoznati kot škodljiva (*ang. red flags*), ponudimo jim dodatna izobraževalna gradiva in po določenem času ponovno pošljemo podobno vajo. Skrbnikom programa ozaveščanja je na voljo statistika klikov, s katero lahko merijo trend izboljšanja in uspešno prepoznavajo, kateri oddelki ali skupine uporabnikov bolje napredujejo in jim lahko ponudijo težja gradiva, in kateri potrebujejo dodatne vaje na nižji ravni.
Smiselno je, da organizacije vpeljejo politiko upravljanja z varnostnimi incidenti in določijo postopke, ki jih je treba upoštevati pri poročanju o incidentu. Tako se bodo zaposleni zavedali svoje odgovornosti pri poročanju o incidentih ter se bodo nanje odzvali hitreje in bolj učinkovito. V varnostnih politikah oz. internih pravilnikih naj organizacije določijo pravice in odgovornosti glede na različne uporabniške vloge, hkrati naj po vlogah tudi prilagodijo vrsto in zahtevnost izobraževanja.
Dokumentacija naj bo shranjena na mestu, kjer je dostopna vsem zaposlenim s ciljem, da jo uporabljajo kot smernice pri vsakdanjem delu.
Bančne institucije se pogosto srečujejo tudi s posledicami kibernetskih napadov na komitente. V tem pogledu opažamo vedno večjo angažiranost bank, da z različnimi sredstvi obveščanja komitente opozarjajo na poskuse napadov in jih ozaveščajo o ustreznem ravnanju in prepoznavanju pasti. S takšnimi akcijami banke bistveno pripomorejo k izboljšanju ozaveščenosti o kibernetskih napadih v širšem družbenem kontekstu.
Pri ozaveščanju o kibernetski varnosti je pomembno tudi, da organizacije redno pregledujejo svoje varnostne politike in ustrezno obravnavajo najnovejše kibernetske grožnje. K temu zavezujejo organizacije v finančnem in bančnem sektorju tudi različni standardi in direktive, ki spodbujajo učinkovito upravljanje kibernetske varnosti.

5. Direktiva NIS2 in uredba DORA

Konec leta 2022 je Evropska unija sprejela dva pomembna dokumenta, ki bistveno spreminjata položaj kibernetske varnosti v velikem delu gospodarstva in javne uprave. Direktiva NIS2 določa ukrepe za skupno visoko raven kibernetske varnosti v Evropski uniji, ki jih morajo države članice v lokalno zakonodajo implementirati do sredine oktobra 2024. Med drugim direktiva širi nabor zavezancev, ti pa bodo morali po novem spremljati tudi kibernetska tveganja svojih dobaviteljev. S tem direktiva naslavlja vedno bolj pereč problem napadov prek dobavne verige.
Uredba DORA pa je specializirana za digitalno operativno odpornost finančnega sektorja in je kot taka zavezujoč pravni akt v vseh državah članicah EU. V praksi bo začela veljati 17. januarja 2025 in do takrat se morajo vse institucije, ki jih uredba zavezuje, nanjo ustrezno pripraviti. Obe regulativi sta pomembni za zagotavljanje ustreznih ukrepov, s katerimi se bodo organizacije zaščitile pred potencialnimi kibernetskimi grožnjami in krepile kibernetsko odpornost. Ti ukrepi vključujejo vpeljavo varnostnih pregledov in testiranj, krepitev ozaveščenosti uporabnikov, zaznavanje škodljivih aktivnosti na omrežjih in ustrezen odziv. V primeru kibernetskih incidentov se morajo organizacije odzvati hitro, a koordinirano, odločitve morajo biti preudarne in vsi postopki dokumentirani.
NIS2 in DORA ponujata organizacijam ogrodje, s katerim si lahko pomagajo pri sistematični krepitvi varnostne drže.

6. NIST Cybersecurity Framework

Pri učinkovitem upravljanju kibernetske varnosti se lahko organizacije oprejo tudi na NIST Cybersecurity Framework, ogrodje za upravljanje kibernetske varnosti, ki ga je razvil ameriški nacionalni inštitut za standardizacijo in tehnologijo (NIST). Ogrodje podaja smernice, kako prepoznavati potencialna tveganja in ranljivosti, razviti politike in postopke, da jih lahko obravnavamo,, in razviti načrt odzivanja na incidente. Poleg tega je ogrodje v pomoč tudi pri ocenjevanju zrelosti organizacije na področju kibernetske varnosti ter izpostavljenosti organizacije tveganjem.
Trenutna verzija ogrodja NIST vsebuje petstopenjski krog upravljanja kibernetske varnosti: identifikacija – zaščita – zaznava – odziv – obnova (*ang. identify – protect – detect – respond – recover*). Glavni cilj je cikličnost postopka, s čimer so poudarili, da je kibernetska varnost neprestano razvijajoče se področje, ki zahteva nenehno spremljanje in izboljšave.
V začetku leta 2024 pričakujemo novo verzijo ogrodja NIST, ki uvaja novo kategorijo »upravljanje« (*ang. governance*) in jo postavlja nad vseh pet stopenj kroga. S tem so avtorji ogrodja poudarili pomen obvladovanja kibernetskih tveganj in upravljanje kibernetske varnosti pomaknili bližje vodstvu in odločevalcem.

Če se v okviru tako prepoznanega ogrodja, kot je NIST Cybersecurity Framework, uveljavlja pojem upravljanja, naj si tudi odgovorni za kibernetsko varnost v organizacijah prizadevajo, da sprememb na tem področju vodstvu in upravam ne bodo predstavljali v obliki podatkov o številu novo odkritih ranljivosti ali novo nameščenih varnostnih napravah. Večji poudarek naj bo na vsebini, kot je spremenjeno področje napada, različne oblike groženj in tveganj, in šele nato, kako bodo te izzive naslovili znotraj ekipe in organizacije. Pomembno je prepoznavati kibernetsko varnost kot enega od temeljev za uspešno poslovanje podjetja in tudi varuha ugleda, saj zlasti v ustanovah, kjer se obdeluje veliko osebnih in občutljivih podatkov, vsak vdor in razkritje zelo verjetno pomenita tudi veliko negativno publiciteto. Organizacije, ki so vpeljale standard ISO 27001, so že dokazale, da vodstvo prepoznava informacijsko varnost kot vodilo pri poslovanju, nova verzija standarda iz leta 2022 pa dodatno vpeljuje nekatere kontrole, ki so bolj tehnološko naravnane.

7. Sklepne misli

Če se torej NIST Cybersecurity Framework z dodajanjem elementa upravljanja približuje poslovodstvu, se ISO 27001 v verziji 2022 s tehničnimi kontrolami približuje področju kibernetske varnosti. Ugotovitev je v obeh primerih podobna: kibernetska in informacijska varnost sta področji, ki ju obravnavamo tako s tehnološkega kot poslovodnega vidika in prispevata k uspešnemu delovanju organizacij. Doseganje višje ravni kibernetske varnosti v organizacijah je cikličen postopek, ki zahteva stalno spremljanje, odzivanje na aktualne razmere in izboljševanje. Temelj za izboljšave je jasna slika o stanju kibernetske varnosti, ki jo prikažejo rezultati varnostnih testov in priporočila, osnovana na podlagi teh rezultatov.

Viri

ISO/IEC, 2022: Standard ISO 27001:2022
NIST, 2018: Cybersecurity Framework V1.1
Uradni list Evropske unije, 2022: Direktiva EU 2022/2555
Uradni list Evropske unije, 2022: Uredba EU 2022/2554

UDK 004.738.5:004.056

Kibernetska varnost

*Gaja Šilak, Simona Sternad Zabukovšek in Samo Bobek**

CYBERSECURITY

Information technology security protects computer networks, systems and stored data from unauthorized access or misuse. Its purpose is to ensure the integrity, confidentiality and accessibility of relevant information and resources. In addition, it prevents unauthorized access to sensitive data or infrastructure. The main goal of cyber security is to minimize the probability of successful attacks on information systems and networks and to limit the negative consequences of potential security incidents. Cyber attacks can take many forms, such as using malware, social engineering, or hacking techniques to access systems, steal information, or disrupt business operations. The scope of cyber threats is constantly increasing, and cyber threats have increasing dimensions, from cybercrime to cyber attacks and cyber terrorism. As part of their security policy, organizations must continuously monitor, on the one hand, the development of threats and the characteristics of new threats and be familiar with the latest information technologies and solutions for defence against threats. Many cyber-attacks are based not only on the technology the attackers use to attack but also on the human dimension, and various social engineering methods are used for this purpose

JEL K14 K24 O33

1. Uvod

Razvoj informacijskih tehnologij in njihova pogosta uporaba pri vsakdanjih opravilih, tako doma kot v poslovnem svetu, prinašata številne prednosti. Vendar pa se s tem povečuje tudi tveganje za zlorabo in krajo podatkov, kar zahteva, da jih upravljavci ustrezno zaščitijo. Zaradi širjenja količine podatkov, ki jih je treba zaščititi, postaja nujno zagotoviti čim bolj učinkovito varovanje na tem področju.

S stalnimi spremembami v kibernetskem prostoru se število groženj nenehno povečuje, obstoječe grožnje se spreminjajo in dobivajo novo obliko, pojavlja pa se tudi mnogo novih groženj. Zaradi tega je ključno, da smo o tem seznanjeni in da grožnje poznamo in da jih razumemo ter da vemo, kako se pred njimi ubranimo. Poleg vsakega posameznika, ki je lahko tarča hekerjev, pa je treba varnostno zaščititi tudi informacijske sisteme, omrežje in programe. Posebno pozorni moramo biti pri programih, ki so namenjeni dostopanju, spreminjanju ali uničenju občutljivih informacij. Učinkovito izvajanje ukrepov kibernetske varnosti predstavlja velik izziv, saj je število naprav večje od števila ljudi, napadalci pa postajajo vse bolj iznajdljivi (Šilak, 2023).

Pojem kibernetske varnosti se nenehno širi in spreminja in kar je bilo pomembno še pred nekaj leti, danes ni več v središču pozornosti. Sodobno pojmovanje kibernetske varnosti zahteva vsestransko razumevanje. Gre za naslednje dimenzije kibernetske varnosti: kibernetske grožnje, tehnologije in rešitve za zagotavljanje kibernetske varnosti, klasifikacija kibernetskih napadov in načinov obrambe pred njimi ter t. i. mehke grožnje, kamor uvrščamo socialni inženiring. Vsem tem dimenzijam je treba posvetiti pozornost, hkrati pa se zavedati, da so dimenzije med seboj povezane in se dopolnjujejo. Prav tako zahtevajo posamezne grožnje primerno uporabo tehnologij in rešitev za zagotavljanje kibernetske varnosti, zlasti pa uporabo najsodobnejših tehnologij in rešitev. Popolne varnosti sicer ni, s sledenjem razvoju in prilagajanjem varnostnih postopkov pa lahko posamezniki in finančne institucije dvignejo kibernetsko varnost na višjo, bolj zadovoljivo in primerno raven ter s tem zmanjšajo tveganja.

* Gaja Šilak, Samo Bobek, Simona Sternad Zabukovšek, Univerza v Mariboru, Ekonomsko – poslovna fakulteta Maribor

Pričujoči članek poskuša predstaviti in analizirati trende na področju kibernetske varnosti, zlasti tehnologije in rešitve ter njihovo uporabo pri posameznih novejših kibernetskih napadih.

2. Dimenzije kibernetske varnosti

Kibernetska varnost se nanaša na različne ukrepe za zaščito računalniških sistemov in podatkov pred napadi, ki bi lahko omogočili nepooblaščen dostop. Vključuje številne dimenzije, od poslovnega do mobilnega računalništva, in obsega kategorije, ki vključujejo varnost omrežij, varnost aplikacij, varnost v oblaku, varnost interneta stvari (angl. Internet of Things; IoT), kibernetsko varnost kritične infrastrukture, operativno varnost, obnovo po nesrečah in neprekinjeno poslovanje, izobraževanje uporabnikov ter informacijsko varnost (Kaspersky, 2022; Governance, 2022).

Za zagotovitev **varnosti omrežij** je treba vzpostaviti požarni zid, ki preprečuje nepooblaščen dostop do omrežja. Za šifriranje komunikacije med napravami in preprečevanje prestrezanja podatkov je treba uporabljati ustrezne varnostne protokole. Za odpravljanje ranljivosti in ohranjanje varnosti omrežja so potrebne redne posodobitve programske in strojne opreme.

Varnost aplikacij se ukvarja z zaščito programske opreme in naprav pred različnimi grožnjami. Če je aplikacija ogrožena, lahko to omogoči dostop do podatkov, ki jih aplikacija sicer varuje. Varnost aplikacij se povečuje z vsako novo verzijo, kajti razvijalci sproti odstranjujejo ugotovljene ranljivosti, ki so nastale ob oblikovanju, razvoju in objavi aplikacije.

Varnost v oblaku zajema varovanje podatkov, aplikacij in infrastrukture, ki so shranjeni v oblaku.

Varnost interneta stvari vključuje varovanje omrežnih naprav, ki sestavljajo IoT-ekosistem. Te naprave so pogosto ranljive za kibernetske napade zaradi omejene procesorske moči, šibkih mehanizmov avtentikacije in zastarele programske opreme.

Kibernetska varnost kritične infrastrukture se nanaša na varovanje infrastrukture, ki je ključna za delovanje družbe, saj so takšni sistemi bolj izpostavljeni napadom kot drugi.

Operativna varnost se nanaša na ukrepe, ki jih organizacije sprejmejo za zaščito svojih operativnih sistemov in storitev pred kibernetskimi grožnjami. To vključuje zagotavljanje zanesljivega delovanja informacijskih sistemov, ohranjanje integritete in zaupnosti podatkov ter zaščito pred nepooblaščenim dostopom, krajo podatkov, vdori in drugimi oblikami kibernetskih napadov.

Obnova po nesreči in **neprekinjeno poslovanje** vključujeta postopke, kako se organizacija odzove na incident, ki povzroči izgubo podatkov. Politike obnove po nesreči določajo postopke, ki jih organizacija izvede za ponovno vzpostavitev svojega delovanja in podatkov po dogodku. Neprekinjeno poslovanje pa je načrt, ki ga organizacija uporablja za delovanje brez določenih virov.

Izobraževanje uporabnikov se nanaša na ljudi, ki so najbolj nepredvidljiv dejavnik kibernetske varnosti. Poučevanje uporabnikov o kibernetski varnosti je ključnega pomena za varnost vsake organizacije.

Informacijska varnost se osredotoča na zaščito celovitosti in zasebnosti podatkov, bodisi pri shranjevanju ali prenosu.

Skupni cilj kibernetske varnosti je zagotoviti, da so računalniški sistemi in podatki varni pred grožnjami in nepooblaščenimi dostopi.

3. Zaščita pred kibernetskimi grožnjami

Na področju kibernetske varnosti lahko definiramo tri vrste groženj (Kaspersky, 2022a):

1. Kibernetska kriminaliteta, ki vključuje posamezne napadalce ali skupine, ki si prizadevajo za finančno korist ali motnje v delovanju sistemov.
2. Kibernetski napadi, ki pogosto vključujejo politično motivirano zbiranje informacij.
3. Kibernetski terorizem, katerega namen je destabilizacija elektronskih sistemov, da bi povzročili paniko ali strah.

Kibernetski kriminal postaja za države vse večji izziv, saj je zelo kompleksen in ga je težko nadzorovati. Kljub temu, da se vsako leto nameni veliko denarja za odkrivanje in preprečevanje kibernetskih napadov, pa ostaja upanje, da jih bo mogoče omejiti, majhno. To je zato, ker so finančne koristi takšnih kaznivih dejanj pogosto večje od njihovih posledic. Da se ubranimo pred kibernetskimi napadi, je treba poznati naslednje tehnologije in metode za zagotavljanje varnosti in zasebnosti v računalniških sistemih organizacij: požarni zid, šifriranje podatkov, biometrija, antivirusni programi, demilitarizirana območja, upravljanje gesel in teste CAPTCHA, ki jih v nadaljevanju poglavja pojasnujemo.

Požarni zid

Požarni zid (angl. firewall) je program ali naprava, ki nadzira vhodni in izhodni omrežni promet in se odloča, ali naj dovoli ali blokira promet na podlagi določenih varnostnih pravil. Uporablja se za zaščito varnejšega omrežja pred manj varnim omrežjem. Na splošno se požarni zidovi uporabljajo za zaščito notranjega/zasebnega omrežja pred internetom. Požarni zid, ki deluje na omrežni ravni, lahko na primer blokira promet na podlagi izvornega ali ciljnega naslova IP, medtem ko lahko požarni zid, ki deluje

na aplikacijski ravni, pregleda vsebino prometa in odkrije določene vrste napadov, kot na primer vbrizgavanje poizvedb strukturiranega povpraševalnega jezika (angl. Structured Query Language – SQL) ali križno skriptiranje spletnega mesta. Požarni zid ve, kaj prihaja in kaj odhaja ter vse to spremlja. Če je torej podatkovni paket poskušal priti, vendar ni bil zahtevan, požarni zid to ve in ga zavrže. Požarni zidovi so pomemben sestavni del varnosti omrežja, saj pomagajo preprečevati nepooblaščen dostop do občutljivih podatkov ali virov, kot so finančni podatki ali informacije o strankah. Prav tako lahko pomagajo preprečevati širjenje zlonamerne programske opreme z blokiranjem prometa iz znanih zlonamernih virov (Liu in Gouda, 2008).
Požarni zid za spletne aplikacije (angl. Web Application Firewall – WAF) je, kot pove že sam izraz, požarni zid, ki je posrednik med spletnimi aplikacijami v spletnem strežniku in internetom. WAF opravlja dve glavni funkciji: preprečuje zlonamerni promet do spletnih aplikacij, ki gostujejo v strežniku, in preprečuje, da bi nepooblaščeni podatki zapustili spletni strežnik. V sedemnivojskem modelu OSI deluje WAF na aplikacijski ravni, ki je sedma in najvišja raven. WAF torej spremlja in pregleduje vsak podatkovni paket, ki vstopa v spletni strežnik in izstopa iz njega, ter tako zagotavlja, da so podatkovni paketi varni in s tem preprečuje napade na spletne aplikacije (bunny.net, 2023a). Požarni zid je ključna komponenta v mnogih omrežnih varnostnih rešitvah.

Šifriranje podatkov

Šifriranje podatkov je postopek pretvarjanja podatkov v šifrirano besedilo, tako da jih nepooblaščeni uporabniki, ki nimajo šifrirnega ključa, ne morejo prebrati. Zagotavlja zaupnost, celovitost in pristnost podatkov, saj nepooblaščenim osebam ali hekerjem otežuje ali onemogoča branje ali spreminjanje občutljivih informacij (Kaspersky, 2022b).
Metode šifriranja podatkov (Kaspersky, 2022b):

- Šifriranje s simetričnim ključem, kjer se za šifriranje in dešifriranje podatkov uporablja isti ključ.
- Šifriranje z asimetričnim ključem, kjer se za šifriranje podatkov uporablja javni ključ za šifiranje in zasebni ključ za njihovo dešifriranje. Torej ta metoda uporablja dva različna ključa.
- Šifriranje s pomočjo »hasha« je metoda, kjer se za vsak vhodni podatek ustvari unikaten izhodni podatek, imenovan »hash«.

Pri šifriranju s simetričnim ključem se za šifriranje in dešifriranje podatkov uporablja isti ključ. Ključ je tajen in se uporablja za šifriranje in dešifriranje podatkov. Ta metoda je razmeroma hitra in učinkovita, vendar je varnost šifriranih podatkov tako močna, kot je močna tajnost ključa. Šifriranje s simetričnim ključem se običajno uporablja v primerih, ko morajo iste podatke šifrirati in dešifrirati iste stranke, na primer pri prenosu podatkov prek varne omrežne povezave.
Šifriranje z asimetričnim ključem je način šifriranja, ki za šifriranje in dešifriranje uporablja dva različna ključa, javni in zasebni ključ. Javni ključ je lahko prosto dostopen vsakomur in se uporablja za šifriranje podatkov, zasebni ključ pa je tajen in se uporablja za dešifriranje podatkov. To omogoča varno komunikacijo med strankami, ki se nikoli niso srečale ali si izmenjale ključev, saj lahko podatke dešifrira le predvideni prejemnik z zasebnim ključem. Šifriranje z asimetričnim ključem se pogosto uporablja v varnih komunikacijskih protokolih in v algoritmih za digitalno podpisovanje. Glavna prednost šifriranja z asimetričnim ključem pred šifriranjem s simetričnim ključem je v tem, da med strankami ni treba deliti tajnega ključa, zato je varnejše za komunikacijo med strankami, ki se še nikoli niso srečale. Vendar je šifriranje z asimetričnim ključem običajno časovno bolj potratno od šifriranja s simetričnim ključem.
Šifriranje s pomočjo »hasha«, je šifriranje, ki vhodni podatek (pogosto imenovan »sporočilo«) pretvori v niz znakov, znan kot »hash«. Ta je edinstven za sporočilo, zato že majhna sprememba vhodnega podatka povzroči popolnoma drugačen »hash«. Ta metoda se pogosto uporablja za preverjanje celovitosti podatkov, na primer pri shranjevanju gesel in preverjanju datotek. Računsko je neizvedljivo ustvariti isti »hash« za dva različna vhoda ali ustvariti izvirni vhod iz obstoječega »hasha«.

Biometrija

Biometrija je statistično in matematično merjenje edinstvenih fizičnih ali bioloških značilnosti za namene identifikacije. V kibernetski varnosti se opredelitev biometrije nanaša na uporabo edinstvenih bioloških značilnosti za digitalno preverjanje pristnosti in nadzor dostopa. Biometrično preverjanje pristnosti zagotavlja višjo raven varnosti kot tradicionalne metode preverjanja pristnosti, kot so gesla ali žetoni, saj je biometrične podatke težko ponarediti ali ukrasti. Biometrija se pogosto uporablja v različnih panogah, kot so finance, zdravstvo in vlada, za zaščito občutljivih podatkov in preprečevanje goljufij. Vendar uporaba biometričnih podatkov sproža tudi pomisleke glede zasebnosti, zato morajo organizacije zagotoviti, da zbirajo, hranijo in uporabljajo biometrične podatke v skladu z ustreznimi zakoni in predpisi (Molinaro, 2022).

Antivirusni program

Antivirusni program je programska aplikacija, namenjena odkrivanju, preprečevanju in odstranjevanju zlonamerne programske opreme iz računalniškega sistema. Protivirusna programska oprema običajno pregleduje računalniški sistem v realnem času ali po rednem urniku ter išče sumljivo vedenje in skuša preprečiti delovanje zlonamerne programske opreme v napravah. Če odkrije virus ali drugo zlonamerno programsko opremo, protivirusna programska oprema okuženo datoteko postavi v karanteno ali jo izbriše (NCSC, 2021).

Za zagotovitev celovite zaščite pred kibernetskimi grožnjami je pomembno, da se antivirusni programi posodabljajo in dopolnjujejo z drugimi varnostnimi ukrepi, ker se nenehno pojavljajo nove grožnje zlonamerne programske opreme.

»Honey Pot« in demilitarizirano območje

»Honey Pot« je lažni računalniški sistem, ki simulira resnični sistem, pri čemer se zdi, da je legitimni del omrežja, vendar je v resnici izoliran in pozorno nadzorovan za lovljenje hekerjev ali novih metod vdora, ki so nato blokirane in ujete. Glavni namen je torej zaznavanje napadov in učenje iz njih ter nadaljnja uporaba informacij za izboljšanje varnosti (Chipkin, 2018).

Na drugi strani je demilitarizirano območje (angl. demilitarized zone – DMZ) omrežni segment, ki je izoliran od notranjega omrežja organizacije in interneta, vendar je še vedno dostopen iz obeh. DMZ je zasnovan tako, da zagotavlja dodatno raven varnosti z ločevanjem strežnikov organizacije, ki so namenjeni javnosti, od njenega notranjega omrežja, ki vsebuje občutljive informacije. DMZ je običajno skrbno nadzorovan in zanj velja strog nadzor dostopa, da se prepreči nepooblaščen dostop (BasuMallick, 2022).

Upravljanje gesel

Na področju informatike in informacijske varnosti se upravljanje gesel nanaša na možnost upravljanja uporabniških gesel za celotno organizacijo z enega samega centraliziranega mesta v omrežju. Močna gesla sama po sebi niso dovolj za preprečitev kršitve varnosti podatkov. Kibernetski napadi so vse bolj izpopolnjeni, saj se za krajo prijavnih podatkov uporabljajo metode, kot so napadi z grobo silo in socialni inženiring (Kinzer, 2022).

Naloge programa za upravljanje gesel so (Kinzer, 2022):

- Ustvarjanje močnih gesel: močno geslo je mešanica velikih in malih črk, številk in posebnih znakov.
- Izvrševanje zahtev: upravitelj gesel zagotavlja, da se vse zahteve izvajajo v celotnem omrežju in da se upošteva osnovna raven moči gesla.
- Zagotavljanje rotacije gesel: pogosto menjavanje gesel pomaga zmanjšati ranljivost za napade, ki temeljijo na geslih.
- Sinhronizacija med napravami in operacijskimi sistemi: ker je sodobna organizacija okolje z več napravami, morajo imeti uporabniki možnost deliti gesla med vsemi napravami, ki jih uporabljajo – tako ni treba ročno vnašati gesla na vsaki napravi.

Večfaktorsko preverjanje pristnosti (angl. Multi Factor Authentication Methods – MFA) je varnostni mehanizem, ki od uporabnikov zahteva, da za dostop do sistema ali aplikacije predložijo dve ali več oblik identifikacije. MFA je zasnovana tako, da z uporabo dejavnikov preverjanja doda dodatno raven zaščite sistemov, omrežij in občutljivih podatkov. Pri MFA se uporablja več vrst dejavnikov avtentikacije (Davidson, 2022):

- Nekaj, kar uporabnik pozna: vključuje geslo, kodo PIN ali druge tajne informacije, ki jih pozna samo uporabnik.
- Nekaj, kar uporabnik ima: vključuje fizični žeton, na primer pametno kartico, žeton USB ali mobilno napravo, ki jo ima uporabnik.
- Nekaj, kar uporabnik je: vključuje biometrično značilnost, kot so prstni odtis, prepoznavanje obraza ali skeniranje šarenice, ki edinstveno identificira uporabnika.
- Kje se uporabnik nahaja: vključuje preverjanje lokacije, na primer GPS ali naslov IP, ki preverja lokacijo uporabnika.

MFA se lahko izvaja na različne načine, odvisno od zahtevane ravni varnosti in posebnih potreb organizacije. Nekatere rešitve MFA na primer od uporabnikov zahtevajo vnos gesla, ki mu sledi koda, poslana v mobilno napravo, druge pa lahko uporabljajo biometrično preverjanje pristnosti v kombinaciji s fizičnim žetonom. MFA se pogosto uporablja v različnih panogah, kot so finance, zdravstvo in vlada, za zaščito občutljivih podatkov in preprečevanje nepooblaščenega dostopa.

Test CAPTCHA

Spletni obrazci »Prijava« in »Kontaktirajte nas« so velikokrat tarča avtomatiziranih računalniških programov, t. i. botov, ki želijo izkoriščati nezavarovane in nezaščitene obrazce oziroma sisteme. Prek teh pošiljajo razne poizvedbe in druge programske kode za onemogočanja storitev in pridobivanja nepooblaščenega dostopa, zato je na spletnih mestih potrebna potrditev človeške identitete. Popolnoma avtomatiziran javni Turingov test (angl. Completely Automated Public Turing – CAPTCHA) je test

z izzivom in odgovorom (angl. challenge-response), ki deluje kot mehanizem za preverjanje pristnosti na spletnih mestih, v iskalnikih in spletnih aplikacijah ter zagotavlja, da so uporabniki ljudje in ne avtomatizirani roboti, ki poskušajo napasti sistem in sprožiti kibernetski napad (BasuMallick, 2023).
Test CAPTCHA je sestavljen iz dveh preprostih delov: naključno ustvarjenega zaporedja črk in/ali številk, ki se prikažejo kot popačena slika, in besedilnega polja. Če želimo uspešno opraviti test in dokazati svojo človeško identiteto, v besedilno polje preprosto vnesemo znake, ki jih vidimo na sliki (Gossweiler, Kamvar, in Baluja, 2009). Ko je na strani prikazan izziv (izzivi so lahko različni, od izbire niza slik, vnosa težko berljivega besedila ali celo zvočnega izziva za slabovidne uporabnike), mora uporabnik vnesti ustrezno rešitev in zahteva bo nato poslana logiki obdelave vnosa. Če je izziv rešen pravilno, uporabnik prejme pozitivno povratno informacijo (bunny.net, 2023b).

4. Vrste kibernetskih napadov

4.1 Zlonamerna programska oprema

Zlonamerna programska oprema (angl. malware) je ena izmed najbolj razširjenih groženj na področju kibernetske varnosti. Gre za programsko opremo, ki jo ustvarijo kibernetski kriminalci ali hekerji s ciljem poškodovati ali onemogočiti računalnik uporabnika. Kriminalci lahko z uporabo zlonamerne programske opreme, ki se pogosto širi prek priponk v elektronski pošti ali pod krinko legitimnih prenosov, izvajajo napade za dosego finančnega dobička ali iz političnih motivov (Kaspersky, 2022a).
Zlonamerna programska oprema in datoteke so lahko izredno nevarne za računalniške sisteme, saj lahko povzročijo različne težave. Med najpogostejšimi težavami so onemogočanje dostopa do kritičnih komponent omrežja, pridobivanje podatkov s trdega diska, onemogočanje delovanja sistema ali celo njegova popolna onesposobitev.
Vrste zlonamerne programske opreme (Kaspersky, 2022a; Governance, 2022; CISCO, 2023):

- Virus je program, ki se lahko širi med računalniškimi sistemi prek okuženih datotek. Ko se virus enkrat namesti na računalniški sistem, se lahko samodejno kopira in širi na druge računalniške sisteme.
- Trojanski konji so vrsta zlonamerne programske opreme, ki se skriva kot legitimni program ali datoteka, vendar pa ima škodljive namene. Ko se trojanski konj namesti na računalnik, lahko dostop omogoči tudi drugi zlonamerni programski opremi.
- Vohunska programska oprema je program, ki se namesti na računalnik brez uporabnikovega dovoljenja in zbira podatke o uporabnikih, kot so zgodovina brskanja po spletu, gesla, kreditne kartice in druge osebne podatke. Te podatke nato pošiljajo zlonamernemu uporabniku, ki jih lahko uporabi za različne namene.
- Ransomware je zlonamerna programska oprema, ki šifrira datoteke na računalniku in zahteva odkupnino, da se datoteke dešifrira. Ransomware je lahko izjemno nevaren in lahko povzroči nepopravljive posledice, kot so izguba pomembnih podatkov.
- Botneti so omrežja računalnikov, ki jih nadzirajo zlonamerni uporabniki in jih uporabljajo za izvajanje nalog na spletu brez dovoljenja uporabnika. Botneti običajno delujejo skrito, zato jih je težko zaznati in ustaviti.

4.2 Vbrizgavanje SQL-poizvedbe

Vbrizgavanje SQL- poizvedb je ranljivost, ki temelji na programski kodi in napadalcu omogoča branje in dostop do občutljivih podatkov iz podatkovne zbirke. Napadalci lahko zaobidejo varnostne ukrepe aplikacij in z zlonamernimi poizvedbami SQL spreminjajo, dodajajo, posodabljajo ali brišejo zapise v zbirki podatkov. Uspešen napad z vbrizgavanjem SQL lahko slabo vpliva na spletna mesta ali spletne aplikacije, ki uporabljajo relacijske zbirke podatkov, kot so MySQL, Oracle ali SQL Server (Shruti, 2023).
Napadalec lahko z vpisom prave poizvedbe v spletni obrazec pridobi iz podatkovne baze podatke, do katerih ni pooblaščen. V izogib temu programska koda ne sme nikoli neposredno uporabljati vhodnih podatkov, kar pomeni, da vnesenega podatka nikoli ne smemo direktno prenesti kot poizvedbo v podatkovno bazo. Koda razvijalca mora preveriti vse vhodne podatke, ne le vhodnih podatkov spletnih obrazcev.

4.3 Napad »mož sredi poti«

Pri tem napadu napadalec prestreže dvosmerno komunikacijo ter se vključi v njo, pri čemer lahko podatke ukrade ali z njimi manipulira. Ta vrsta napada običajno izkorišča varnostne ranljivosti v omrežju, kot je nezaščiteno javno omrežje WiFi, da se med napravo uporabnika in omrežjem vstavi napadalec. Glavna težava te vrste napada je, da ga je zelo težko zaznati, saj žrtev misli, da se informacije pošiljajo na legitimni naslov. Za izvedbo napada "mož sredi poti" (angl. Man-in-the-middle attack – MitM) se pogosto uporabljajo napadi z ribarjenjem ali zlonamerno programsko opremo (Fichtner, 2022).
Pri MitM na ravni omrežja napadalec prestreže promet med ciljem in internetom, na ravni aplikacije prestreže

komunikacijo med aplikacijo in njenim strežnikom, na fizični ravni pa prestreže komunikacijo na javni lokaciji (npr. WiFi). Cilj napada MitM je kraja občutljivih informacij, manipulacija komunikacije ali prekinitev običajnega pretoka informacij med dvema strankama.

4.4 Napad DDoS

Napad za zavrnitev storitve (angl. Denial of Service – DoS) je vrsta napada, ki preobremeni sisteme, strežnike in/ali omrežja z veliko količino prometa, kar vodi do izčrpanja virov in pasovne širine. Posledično sistem ne more obdelati in izpolniti zahtev. Poleg napadov DoS obstajajo tudi porazdeljeni napadi na zavrnitev storitve (angl. Distributed Denial of Service – DDoS), ki se izvajajo iz več okuženih gostiteljskih računalnikov. Ti napadi imajo cilj preprečiti dostop do storitev in izklopiti celoten sistem, kar omogoči izvajanje drugih napadov v omrežju (Fichtner, 2022).
Napad DDoS se izvede tako, da veliko število botov hkrati pošlje veliko število zahtevkov na cilj, s čimer preobremeni njegove strežnike in povzroči zavrnitev storitve. Napade DDoS pogosto izvajajo kriminalci, ki želijo od tarče izsiliti odkupnino, ali politično motivirani posamezniki, ki želijo onemogočiti delovanje spletnega mesta ali omrežja.

4.5 Napad BGP

Prevzem mejnega usmerjevalnega protokola (angl. Border Gateway Protocol Hijacking) je napad, pri katerem napadalec prevzame nadzor nad mejnim usmerjevalnikom, ki uporablja mejni usmerjevalni protokol (angl. Border Gateway Protocol – BGP), in objavi neveljavne usmerjevalne informacije, ki motijo delovanje omrežja.
Ta vrsta napada lahko omogoči napadalcu, da prestreže, preusmeri ali blokira promet, ki teče med dvema omrežjema. BGP je torej protokol, ki se uporablja za usmerjanje prometa med avtonomnimi sistemi. Medtem ko je usmerjanje znotraj posameznega avtonomnega sistema odvisno le od politike tega sistema, se usmerjanje med avtonomnimi sistemi vedno izvaja s protokolom mejnega prehoda. Protokol izvajajo usmerjevalniki, ki se nahajajo na mejah avtonomnih sistemov in predstavljajo njihove izhodne in vstopne točke (bunny.net, 2023c).

4.6 Skriptiranje med spletnimi mesti

Skriptiranje med spletnimi mesti (angl. Cross Site Scripting – XSS) je oblika napada, katerega cilj je, da se v drugih odjemalcih zažene nepooblaščen JavaScript. Če je spletno mesto izpostavljeno napadu XSS, to pomeni, da lahko napadalec v strežnik pošlje delček kode, ki se nato izvede v drugih brskalnikih odjemalcev (bunny.net, 2023d). Uporabniki lahko nenamerno izvedejo skripte, ki so jih napisali napadalci, ko sledijo povezavam v prikritih ali neznanih virih, bodisi v spletnih straneh, e-poštnih sporočilih, objavah v novičarskih skupinah ali različnih drugih medijih. Ker zlonamerne skripte uporabljajo ciljno spletno mesto za skrivanje svojega izvora, ima napadalec popoln dostop do spletne strani in lahko podatke, ki jih oseba vsebuje na stran, pošlje nazaj v svoj strežnik. Na primer zlonamerna skripta lahko prebere polja v obrazcu, ki ga zagotovi pravi strežnik, in nato te podatke (na primer podatke za prijavo) pošlje v napadalčev strežnik (Spett, 2005).

4.7 Napad na gesla

Gesla predstavljajo najbolj pogosto uporabljen način za preverjanje pristnosti dostopa, kar jih naredi za privlačno tarčo kibernetskih napadov. Če napadalec pridobi geslo, lahko s tem pridobi nepooblaščen dostop do podatkov ali sistemov, pri čemer lahko nato z njimi manipulira in jih nadzira (Fichtner, 2022).

4.8 Napad na internet stvari (IoT)

Vedno večja povezljivost skoraj vseh naprav z internetom omogoča uporabnikom udobje in preprostost, vendar hkrati predstavlja tudi številne točke dostopa, ki pomenijo ranljivosti in jih lahko kibernetski napadalci izkoristijo za povzročanje škode. Zaradi medsebojne povezanosti lahko napadalec izkoristi le eno ranljivost na le eni izmed povezanih naprav in tako pridobi dostop do vseh preostalih v povezanem IoT.
Napad na IoT je vrsta kibernetskega napada, ki je lahko usmerjen v (Chang and Li, 2019):

1. Dele naprave, iz katerih lahko izvirajo ranljivosti – pomnilnik, vdelana programska oprema, fizični vmesnik, spletni vmesnik in omrežne storitve. Napadalci lahko med drugim izkoristijo tudi nezanesljive privzete nastavitve, zastarele komponente in nezanesljive mehanizme posodabljanja.
2. Komunikacijske kanale, ki med seboj povezujejo komponente IoT. Protokoli, ki se uporabljajo v sistemih IoT, imajo lahko varnostne težave, ki lahko vplivajo na celotne sisteme. Sistemi IoT so dovzetni tudi za znane omrežne napade, kot sta DoS in DDoS.
3. Aplikacije in programsko opremo – ranljivosti v spletnih aplikacijah in povezani programski opremi za naprave IoT lahko privedejo do ogrožanja sistemov. Spletne aplikacije je na primer mogoče izkoristiti za krajo uporabniških poverilnic ali posredovanje zlonamernih posodobitev strojne programske opreme.

5. Socialni inženiring

Izraz socialni inženiring se nanaša na raznolike zlonamerne dejavnosti, ki se izvajajo prek medčloveških interakcij, in vključuje uporabo psiholoških manipulacij, da bi žrtve zavedli v razkritje občutljivih informacij (Imperva, 2022). Napadi socialnega inženiringa se lahko izvajajo v enem ali več korakih. Napadalec najprej preuči svojo ciljno žrtev in zbere informacije o potencialnih možnostih vdora. Z žrtvijo skuša napadalec vzpostaviti čim večje zaupanje, ki nato vodi do razkritja občutljivih informacij in pridobivanja dostopa do kritičnih virov (Imperva, 2022).
Čeprav so takšne oblike prevare obstajale že od nekdaj, so se z razvojem informacijsko-komunikacijskih tehnologij močno razvile in pomnožile. V tem kontekstu lahko na IT-tehnike socialnega inženiringa gledamo na dva različna načina (Enisa, 2022):

- uporaba psihološke manipulacije za pridobitev nepooblaščenega dostopa do IT- sistema ali podatkov,
- obstoječa informacijska tehnologija omogoča podporo psihološkim manipulacijam pri pridobivanju nepooblaščenih dostopov zunaj področja IT.

Socialni inženiring postaja vse pogostejši zaradi vse višje ravni varnosti samih sistemov, po drugi strani pa ljudje kot uporabniki še vedno predstavljajo največjo ranljivost, ki jo lahko napadalci izkoristijo z manj truda.
Čeprav se napadi socialnega inženiringa med seboj razlikujejo, imajo skupen vzorec s podobnimi fazami. Skupni vzorec vključuje naslednje štiri faze (Salahdine in Kaabouch, 2019):

1. zbiranje informacij o tarči,
2. vzpostavitev odnosa s ciljem,
3. izkoriščanje razpoložljivih informacij in izvedba napada ter
4. odhod brez sledi.

V fazi raziskovanja, imenovani tudi zbiranje informacij, napadalec izbere žrtev na podlagi nekaterih zahtev. V drugi fazi začne napadalec pridobivati zaupanje žrtve z neposrednim stikom ali komuniciranjem po elektronski pošti. V fazi izkoriščanja in napada napadalec čustveno vpliva na žrtev, da mu posreduje občutljive informacije ali izvede napad na varnostne pomanjkljivosti. V fazi odhoda napadalec odide, ne da bi pustil kakršen koli dokaz (Salahdine in Kaabouch, 2019).
Napad s socialnim inženiringom se začne z raziskovanjem tarče, da bi napadalec ugotovil njene ranljivosti, nato pa te informacije uporabi za pripravo načrta. Ustvari pretvezo ali lažno identiteto, da pridobi zaupanje tarče in z njo manipulira, da razkrije občutljive informacije ali izvede dejanja, ki jih lahko napadalec izkoristi. Življenjski cikel napada s socialnim inženiringom torej vključuje faze: zbiranje informacij, načrtovanje, pridobivanje zaupanja, manipuliranje s ciljem, izkoriščanje informacij, zakrivanje sledi in spremljanje posledic, da bi ohranili nadzor in se izognili odkritju.
Različne vrste napadov socialnega inženiringa lahko razvrstimo v več kategorij. Na primer lahko jih razdelimo glede na subjekt, ki je vključen: človek ali programska oprema. Lahko jih tudi razvrstimo glede na način izvedbe napada na socialne, tehnične ali fizične.
Obstajata tudi dve glavni kategoriji napadov socialnega inženiringa, to sta neposredni in posredni napad. Napadi, ki spadajo v prvo kategorijo, uporabljajo neposredni stik med napadalcem in žrtvijo, na primer fizični stik, očesni stik ali glasovno interakcijo. Za izvedbo napada je lahko potrebna tudi prisotnost napadalca na delovnem območju žrtve. Primeri teh napadov so: fizični dostop, napad z opazovanjem, brskanje po smeteh, telefonski socialni inženiring, pretvarjanje, izdajanje za pomoč uporabnikom in kraja pomembnih dokumentov.
Po drugi strani pa se napadi, ki spadajo v kategorijo posrednih napadov, izvajajo na daljavo s pomočjo zlonamerne programske opreme, ki se prenaša prek elektronske pošte ali sporočil SMS (Salahdine in Kaabouch, 2019).

Napad z vabo

Napadi z vabo (angl. baiting) uporabljajo lažne obljube, da bi sprožili pohlep ali radovednost žrtve, in s tem napadalci svoje žrtve zvabijo v past. Cilj napadov z vabo je prevarati žrtev, da posreduje občutljive informacije ali izvede zlonamerno kodo, ki lahko ogrozi varnost njenega računalnika ali omrežja (Enisa, 2022).
Ena izmed vrst napada z vabo vključuje tudi USB-ključke, pri čemer napadalci pustijo ključek, ki je okužen z zlonamerno programsko opremo na vidnem mestu. Vaba ima privlačen in realen videz in nalepko, kjer je zapisana vsebina – plače zaposlenih 2023, odpuščanje 2023 ... Žrtev ključek vstavi v svoj računalnik, kar povzroči samodejno namestitev zlonamerne programske opreme v sistem (Imperva, 2022).
Napade z vabo je težko odkriti, saj pogosto temeljijo na človeškem vedenju in ne na tehničnih ranljivostih. Pomembno je, da smo previdni pri nerealnih ponudbah ali darilih in da za prenos ali dostop do datotek uporabljamo le zaupanja vredne vire.
Takšne vrste napadov lahko napadalci izvajajo tudi na spletu, ključni del pa so vabljivi oglasi, ki vodijo na zlonamerna spletna mesta ali pa uporabnike spodbujajo k

prenosu aplikacije, ki je okužena z zlonamerno programsko opremo (Imperva, 2022).

Nekaj za nekaj

Quid pro quo, kar v latinščini pomeni "nekaj za nekaj", je napad, pri katerem napadalec žrtvi v zameno za občutljive informacije ali dostop ponudi nekaj vrednega. Napadalec se lahko predstavlja kot zaupanja vreden posameznik, na primer tehnik IT ali predstavnik službe za pomoč strankam, in žrtvi v zameno za njene prijavne podatke ali druge zaupne informacije ponudi pomoč pri reševanju težav. Napadalec lahko na primer ponudi, da bo odpravil računalniško težavo v zameno za geslo žrtve, ali ponudi, da bo žrtvi dal brezplačno darilno kartico v zameno za njene podatke o kreditni kartici. Napadi quid pro quo so lahko zelo učinkoviti, saj žrtev navdajajo z lažnim občutkom zaupanja, zaradi česar je bolj verjetno, da bo razkrila občutljive podatke (Enisa, 2022).

Pretihotapljanje

Pretihotapljanje (angl. tailgating) je varnostni napad, pri katerem napadalec pridobi nepooblaščen dostop do območja ali stavbe, tako da sledi osebi, ki ima varnostno dovoljenje za dostop do tega prostora. Napadalci prosijo žrtev, naj drži odprta vrata, ker so pozabili službeno izkaznico. Napadalci lahko napad izvedejo tudi prek izposojenega računalnika ali mobilnega telefona, kjer izvajajo razne zlonamerne dejavnosti, kot je npr. nameščanje zlonamerne programske opreme (Salahdine in Kaabouch, 2019).

Ribarjenje

Ribarjenje (angl. phishing) je oblika kibernetskega napada, pri kateri se napadalec izdaja za legitimno osebo ali organizacijo, da bi pridobil občutljive podatke. Napadi ribarjenja običajno vključujejo pošiljanje lažnih e-poštnih sporočil, ki posnemajo uradne spletne strani in prejemnike pozivajo, naj kliknejo na povezavo ali prenesejo priponko, ki jih nato pripelje na lažno prijavno stran ali spletno mesto, okuženo z zlonamerno programsko opremo. Cilj je pridobiti občutljive podatke, kot so številke kreditnih kartic in prijavni podatki. Uporabniki se lahko pred takšno vrsto napada zavarujejo sami, če so s tem dovolj seznanjeni, lahko pa se pred ribarjenjem zavarujejo tudi z uporabo tehnološke rešitve, ki filtrira zlonamerna e-poštna sporočila (CISCO, 2023).

Obstaja več vrst napadov ribarjenja (Fichtner, 2022):

- Usmerjeno ribarjenje (angl. spear phishing) – je vrsta ribarjenja, kjer je napad ciljno usmerjen na določena podjetja ali posameznike.
- Kitolov (angl. whaling) – je vrsta ribarjenja, kjer je napad usmerjen na vodje oddelkov, direktorje in višje vodstvene delavce.
- Lažno usmerjanje (anlg. pharming) – je vrsta ribarjenja, kjer napadalec prestreže promet, ki prihaja z določenega spletnega mesta, tako da ga preusmeri na drugo lažno spletno mesto, da bi pridobil prenesene informacije. Ta napad deluje tako, da napadalec vdre v strežnik sistema domenskih imen in izkoristi morebitne ranljivosti.

Zastraševanje

Zastraševanje (angl. scareware) je prevara, s katero hekerji prestrašijo ljudi, da prenesejo zlonamerno programsko opremo, kliknejo na nevarne povezave ali obiščejo okužena spletna mesta. Zastrašujoča programska oprema je lahko razmeroma neškodljiva in preprosto moti spletno brskanje. Lahko pa povzroči okužbo z zlonamerno programsko opremo in resnično škoduje napravi (Buxton, 2022).

Oglasne pasice, ki se uporabniku prikazujejo med brskanjem v brskalniku z besedami »Vaš računalnik je napadel trojanski konj!«, so pogost primer napada »scareware«. Ponujajo namestitev orodja z namenom, da bi zaščitili računalnik, vendar ravno s to namestitvijo na računalnik namestimo zlonamerno programsko opremo. V primeru, da pasica ne ponuja »varnostnega programa«, pa uporabnika usmeri na zlonamerno spletno mesto, kjer se računalnik okuži in tako napadalec pridobi nepooblaščen dostop (Imperva, 2022).

Predstavljanje lažne identitete

Predstavljanje lažne identitete (angl. pretexting) je vrsta socialnega inženiringa, pri katerem napadalec pridobi občutljive informacije od žrtve s pretvarjanjem, da je nekdo drug, ali s ponarejenimi identitetami.

Napadi s pretvezo so sestavljeni iz izmišljanja lažnih in prepričljivih scenarijev, da bi žrtvi ukradli osebne podatke, in se izvedejo prek telefonskih klicev, elektronske pošte ali fizičnih medijev. Napadalci uporabljajo objavljene informacije na telefonskih imenikih, javnih spletnih straneh ali konferencah (Salahdine in Kaabouch, 2019).

Običajno poskuša napadalec pridobiti zaupanje žrtve z izdajanjem za sodelavca, policista, bančnega uslužbenca, za davčni urad ali druge osebe, ki imajo pravico dostopati do zaupnih informacij. S pridobljenim zaupanjem lahko napadalec od žrtve pridobi pomembne informacije, ki jih kasneje izkoristi v njeno škodo (Imperva, 2022).

Drugi napadi

Obstajajo še številne druge vrste napadov, nekatere so naštete spodaj (Salahdine in Kaabouch, 2019):

- Napadi službe za pomoč uporabnikom: napadalec se pretvarja, da je pooblaščena oseba ali zaposleni v podjetju, in pokliče službo za pomoč uporabnikom ter zahteva informacije ali storitve.
- Napadi z iskanjem v smeteh (angl. dumpster diving), kjer napadalec pride do podatkov s pomočjo zbiranja občutljivih dokumentov iz smeti podjetja ali zavržene opreme, kot so stari računalniški materiali, diski, CD-ji in DVD-ji.
- Napadi s preusmeritvijo in krajo: gre za napačno usmerjanje prevoznega podjetja, da dostavi kurirja ali paket na želeno lokacijo.
- Opazovanje prek ramen (angl. shoulder surfing): gre za opazovanje žrtve med vnašanjem gesel ali občutljivih informacij.
- Napadi s krajo pomembnih dokumentov: gre za krajo datotek s pisalne mize zaradi osebnih interesov.

6. Sklep

Ugotovimo lahko, da se kibernetska varnost nanaša na širok nabor različnih ukrepov za zaščito pred napadi, ki bi lahko omogočili nepooblaščen dostop do računalnikov, informacijskih rešitev in informacij. Zaradi kompleksnosti vključuje danes številne dimenzije, od poslovnega do mobilnega računalništva, in obsega kategorije, ki vključujejo varnost omrežij, varnost aplikacij, varnost v oblaku, varnost IoT, kibernetsko varnost kritične infrastrukture, operativno varnost, obnovo po nesrečah in neprekinjeno poslovanje, izobraževanje uporabnikov ter informacijsko varnost.

Obseg kibernetskih groženj nenehno narašča in kibernetske grožnje imajo vse večje razsežnosti: od kibernetskega kriminala, ki vključuje posamezne napadalce ali skupine, ki si prizadevajo za finančno korist ali motnje v delovanju sistemov, kibernetskih napadov, ki pogosto vključujejo gospodarske interese in so v nekaterih primerih politično motivirani, do kibernetskega terorizma, katerega namen je destabilizacija elektronskih sistemov, da bi povzročili paniko ali strah.

V okviru svoje varnostne politike morajo organizacije neprestano spremljati po eni strani razvoj groženj in značilnosti novih oblik groženj ter biti seznanjene z najnovejšimi tehnologijami in rešitvami za obrambo pred grožnjami. Delovati morajo aktivno in vnaprej analizirati scenarije kibernetskih napadov in obrambe pred njimi, saj bodo le tako pripravljene, če se res kakšen kibernetski napad zgodi. Mnogi kibernetski napadi ne temeljijo le na tehnologiji, ki jo napadalci uporabijo za napad, temveč na človeškem vidiku ranljivosti organizacij. V ta namen se uporabljajo različne metode socialnega inženiringa, ki se ga organizacije lahko obranijo le s kombinacijo varnostnih tehnologij, ustreznih organizacijskih rešitev za njihovo uporabo in s seznanjanjem zaposlenih o teh načinih kibernetskega kriminala.

Literatura in viri:

NCSC. (2021). Antivirus and other security software. Pridobljeno 3. 4 2023 iz National Cyber Security Centre: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/antivirus-and-other-security-software

BasuMallick, C. (2022). What Is a Demilitarized Zone (DMZ)? Definition, Examples, Working, and Importance in 2022. Pridobljeno 3. 4 2023 iz https://www.spiceworks.com/it-security/network-security/articles/what-is-demilitarized-zone/

BasuMallick, C. (2023). What Is CAPTCHA? Meaning, Working, Features, and Threats. Pridobljeno 3. 4 2023 iz https://www.spiceworks.com/it-security/network-security/articles/what-is-captcha/

bunny.net. (2023d). What are Cross Site Scripting (XSS) attacks? Pridobljeno 28. 2 2023 iz https://bunny.net/academy/security/what-are-cross-site-scripting-xss-attacks/

bunny.net. (2023c). What is BGP (Border Gateway Protocol) hijacking? Pridobljeno 28. 2 2023 iz https://bunny.net/academy/security/what-is-BGP-border-gateway-protocol-hijacking/

bunny.net. (2023b). What is CAPTCHA? How does it work and is it effective? Pridobljeno 28. 2 2023 iz https://bunny.net/academy/security/what-is-captcha-completely-automated-public-turing-tests-and-how-does-it-work/

bunny.net. (2023a). What is Web Application Firewall (WAF) and How is it Used to Protect Your Website? Pridobljeno 28. 2 2023 iz https://bunny.net/academy/security/what-is-web-application-firewall-WAF-and-how-it-works/

Buxton, O. (2022). What is Scareware? Detection, Prevention, and Removal. Pridobljeno 3. 4 2023 iz https://www.avast.com/c-scareware#topic-6

Chang, Z., in Li, S. (2019). The IoT Attack Surface: Threats and Security Solutions. Pridobljeno 3. 4 2023 iz https://www.trendmicro.com/vinfo/mx/security/news/internet-of-things/the-iot-attack-surface-threats-and-security-solutions

Chipkin, P. (2018). Honeypots. Pridobljeno 3. 4 2023 iz http://automatedbuildings.com/news/aug18/articles/chipkin/180717102101chipkin.html

CISCO. (2023). What Is Cybersecurity? Pridobljeno 8. 12 2022 iz https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html#~types-of-threats

Davidson, M. (2022). What is Multi-factor Authentication (MFA) and How Can it Protect Your Company Assets? Pridobljeno 3. 4 2023 iz https://www.globalsign.com/en/blog/what-is-multi-factor-authentication

Enisa. (2022). What is "Social Engineering"? European Union: Glossary. Pridobljeno 7. 12 2022 iz https://www.enisa.europa.eu/topics/incident-response/glossary/what-is-social-engineering

Fichtner, E. (2022). What are the common types of cyber security attacks? Datto, Inc. Pridobljeno 7. 12 2022 iz https://www.datto.com/blog/common-types-of-cyber-security-attacks

Gossweiler, R., Kamvar, M., in Baluja, S. (2009). What's up

CAPTCHA? A CAPTCHA based on image orientation. Proceedings of the 18th international conference on World wide web, 841-850. Pridobljeno 28. 2 2023 iz https://storage.googleapis.com/pub-tools-public-publication-data/pdf/35157.pdf

Governance, I. (2022). What is Cyber Security? Definition and Best Practices. Pridobljeno 7. 12 2022 iz https://www.itgovernance.co.uk/what-is-cybersecurity

Imperva. (2022). Social Engineering. Pridobljeno 8. 12 2022 iz https://www.imperva.com/learn/application-security/social-engineering-attack/

Kaspersky. (2022a). What is Cybersecurity? Pridobljeno 7. 12 2022 iz https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security

Kaspersky. (2022b). What is Data Encription? Pridobljeno 30. 12 2022 iz https://www.kaspersky.com/resource-center/definitions/encryption

Kinzer, K. (2022). What Is Password Management? Pridobljeno 3. 4 2023 iz https://jumpcloud.com/blog/what-is-password-management

Liu, A. X., in Gouda, M. G. (2008). Diverse firewall design. IEEE Transactions on Parallel and Distributed Systems 19.9, 1237-1251. Pridobljeno 3. 4 2023 iz https://www.cs.utexas.edu/~gouda/papers/journal/Diversity_TPDS.pdf

Molinaro, D. (2022). What is Biometrics and How Secure is Biometric Data? Pridobljeno 3. 4 2023 iz Avast: https://www.avast.com/c-what-is-biometric-data#topic-1

Salahdine, F., in Kaabouch, N. (2019). Social Engineering Attacks: A Survey. University of North Dakota: School of Electrical Engineering and Computer Science. Pridobljeno 3. 4 2023 iz https://pdfs.semanticscholar.org/8220/aa685354d53868899a08ca97c74c669f7c4a.pdf?_gl=1*otf5l3*_ga*MTcwNzY1NTI1OS4xNjcyNDI4ODgz*_ga_H7P4ZT52H5*MTY4MDUyNDMzMS4yLjAuMTY4MDUyNDMzMi4wLjAuMA..

Shruti, M. (2023). What is SQL Injection & How to Prevent SQL Injection. Pridobljeno 3. 4 2023 iz https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-sql-injection

Spett, K. (2005). Cross-site scripting. SPI Labs 1.1, 20.

UDK 004.738.5:004.056:

Izzivi generativnih vnaprej usposobljenih transformatorjev (GPT) na področju informacijske varnosti

*Boris Vardjan**

CHALLENGES OF GENERATIVE PRETRAINED TRANSFORMERS (GPTs) IN THE FIELD OF INFORMATION SECURITY

Generative Pretrained Transformers (GPT) are a key technology that enables this growth, attracting the attention of researchers, experts, and industries worldwide. GPTs are a fundamental tool for automated natural language generation, laying the foundation for various applications. However, with all its complexity and innovation, GPT technology also brings significant challenges, particularly in terms of information security. To use this technology safely, we must be very careful.

JEL K24 O33

1 UVOD

Po ocenah[1] bo trg generiranja naravnega jezika do leta 2026 dosegel 26,4 milijarde ameriških dolarjev, kar kaže na njegov velik potencial in vpliv. Med tehnologijami, ki omogočajo to rast, so generativni vnaprej usposobljeni transformatorji (GPT), ki so pritegnili pozornost raziskovalcev, strokovnjakov in industrij po vsem svetu. GPT predstavljajo ključno orodje za avtomatizirano generiranje naravnega jezika, kar postavlja temelje za različne aplikacije. Vendar pa z vso svojo kompleksnostjo in inovativnostjo prinaša tehnologija GPT tudi pomembne izzive, predvsem v pogledu informacijske varnosti.

2 Teoretično ozadje in praktična uporaba

Generativni vnaprej usposobljeni transformatorji (GPT) so temeljni modeli globokega učenja, ki temeljijo na nevronskih omrežjih.

OpenAI ChatGPT, Google Bard, Microsoft Bing AI in Claude 2.0 podjetja Anthropic [2]so vsi veliki jezikovni modeli, ki ponujajo različne zmogljivosti za izboljšanje uporabniške izkušnje in produktivnosti. ChatGPT je znan po svoji sposobnosti usmerjanja pogovorov, Bing AI pa je najboljši za pridobivanje informacij s spleta. Bard in Claude 2.0 sta oba v razvoju, vendar obetavna pri generiranju besedila in ustvarjanju ustvarjalne vsebine. Konkurenca med temi modeli se bo verjetno še povečala, kar bo privedlo do še bolj naprednih in prijaznih pogovornih programov prihodnosti.

Njihova sposobnost generiranja naravnega jezika iz podanih vhodnih podatkov je impresivna in ima širok nabor aplikacij:

- **Avtonomna povzetja besedil**
  GPT lahko iz obsežnih besedil generira kratek povzetek, ki ohrani bistveno vsebino. Lahko npr. povzame besedilo strokovnega članka ali pa določenega zakona ali akta.

* Boris Vardjan, Vodja tima informacijske varnosti (CISO) Nova KBM d.d.

[1] The Worldwide Natural Language Processing Industry is (globenewswire.com)

[2] ChatGPT vs Bing vs Bard vs Claude comparison - Geeky Gadgets (geeky-gadgets.com)

- **Odgovarjanje na vprašanja**
  Z razumevanjem konteksta lahko GPT ponudi relevantne odgovore na postavljena vprašanja.
- **Avtomatsko dopolnjevanje besedil**
  Pisateljem omogoča, da avtomatsko dokončajo začete stavke ali odstavke.
- **Pogovorni sistemi**
  Uporabljajo se za razvoj chatbotov, ki so sposobni voditi smiselne in kontekstualno bogate pogovore.
- **Analiza čustvenega stanja besedil**
  GPT zmore razpoznati čustveno stanje v besedilih, kar je koristno za analizo sentimenta.
- **Prepoznavanje entitet**
  Identificira imena, lokacije, datume itd. v besedilu, kar je ključno za razumevanje vsebine.

Vendar pa s takšnimi izjemnimi sposobnostmi prihajajo tudi izzivi, ki jih je treba obravnavati z vidika informacijske varnosti.

3 Informacijska varnost – tveganja in priložnosti

Kljub svoji uporabnosti predstavlja tehnologija GPT pomembne varnostne izzive:

- **Generiranje lažnih vsebin**
  Napadalci lahko zlorabijo GPT za ustvarjanje verodostojnih, a popolnoma lažnih vsebin, kot so lažne novice, lažni pregledi ali lažni profili, kar vodi v razširjanje dezinformacij.
- **Phishing in socialni Inženiring**
  Z uporabo GPT lahko kibernetski napadalci ustvarjajo prepričljive phishing e-pošte in sporočila, ki poskušajo pridobiti osebne ali finančne podatke od žrtev.
- **Razširjanje zavajajočih Informacij**
  Hitro širjenje zavajajočih informacij postaja še bolj problematično zaradi sposobnosti GPT za generiranje verodostojnih besedil.

Na letošnji varnostni konferenci DEF CON 2023[3] so hekerji preizkušali varnost modelov GPT, kot so ChatGPT, Bard in drugi AI jezikovni modeli. Namen tega izziva je bil odkriti ranljivosti teh sistemov in preveriti, ali proizvajajo škodljive informacije in dezinformacije. Hekerji so uporabljali besede namesto kode in strojne opreme, da bi vdrli v te sisteme umetne inteligence. Med izzivom je več kot 2000 ljudi v treh dneh na konferenci DEF CON tekmovalo proti osmim vodilnim AI klepetalnicam podjetij, kot so Google, Meta (matično podjetje Facebooka) in OpenAI (proizvajalec ChatGPT).

[3] https://www.axios.com/2023/08/12/defcon-redteam-generative-ai

Pri tem so imeli kar nekaj uspeha na naslednjih področjih:

- **Ustvarjanje lažnih vsebin**[4]
  Napadalci so uporabili posebne ukaze, imenovane »prompt injections«, da bi prisilili ChatGPT, da generira lažne novice, oglase, ocene, zgodbe in druge vsebine, ki bi lahko vplivale na javno mnenje ali zavajale potencialne stranke
- **Zavajanje uporabnikov**[5]
  Napadalci so izkoristili sposobnost ChatGPT za prilagajanje slogu in jeziku uporabnika, tako so se pretvarjali, da so resnične osebe, kot so prijatelji, znanci, slavne osebnosti ali uradni predstavniki. Tako so poskušali pridobiti zaupne informacije, denar ali dostop do računov uporabnikov.
- **Prevzemanje nadzora nad pogovorom**[6]
  Napadalci so izvedli »session hijacking« napade, pri katerih so prekinili obstoječo sejo med uporabnikom in ChatGPT in prevzeli nadzor nad pogovorom. S tem so lahko spremenili cilj ali namen pogovora, vnesli škodljivo kodo ali preusmerili uporabnika na zlonamerne spletne strani.

Glavni povzetki s konference DEF CON so bili[7]:

- **Sodelovanje**
  Za doseganje zaupanja v umetno inteligenco je potrebno sodelovanje med podjetji, ki se ukvarjajo z umetno inteligenco.
- **Napake pri prevajanju so varnostne napake**
  Celoviti zaščitni ukrepi zahtevajo regulativno, človeško in tehnološko usklajevanje ter prevajanje za ustvarjanje kontrol, ki zagotavljajo pokritost in redundanco.
- **Dobro je stvari odpreti in pogledati, kaj je v njih**
  Medtem ko potekajo zdrave razprave o tem, v kolikšnem obsegu bi morali biti modeli odprtokodni, je jasno, da so sistemi umetne inteligence varnejši, če so ranljivosti odkrito objavljene.
- **Uporabi metode upravljanja kibernetskih tveganj tudi pri umetni inteligenci**
  Uporabiti je treba podobne metode, kot se že uporabljajo pri obravnavi tveganj zunanjih izvajalcev.

Vendar pa ima tehnologija GPT tudi potencial za izboljšanje informacijske varnosti:

- **Odkrivanje in preprečevanje groženj**
  Z implementacijo GPT v varnostne sisteme se lahko povečata zaznavanje in preprečevanje lažnih vsebin,

4 The Security Hole at the Heart of ChatGPT and Bing | WIRED
5 The Most Fearsome Hackers Just Went Ham on ChatGPT (futurism.com)
6 OPWNAI : Cybercriminals Starting to Use ChatGPT - Check Point Research
7 https://www.credo.ai/blog/the-hacker-mindset-4-lessons-for-ai-from-def-con-31

poskusov ribarjenja (phishinga) in drugih kibernetskih napadov. Na primer, nekateri raziskovalci so razvili metode za odkrivanje in odstranjevanje pristranskih, neprimernih ali zavajajočih podatkov iz naborov podatkov. Drugi so uporabili GPT za generiranje protiprimerov, ki lahko razkrijejo slabosti ali napake v drugih modelih globokega učenja.

- **Izboljšanje kvalitete vsebine**
  GPT lahko prispeva k ustvarjanju kakovostnih varnostnih smernic, politik in izobraževalnih vsebin za dvig ozaveščenosti o informacijski varnosti.

4 Etika in pravne implikacije

Obenem z informacijsko varnostjo se postavljajo tudi etična in pravna vprašanja. Skrb zbujajo zlasti vprašanja glede zasebnosti, saj temelji tehnologije GPT na obsežnih naborih podatkov, ki lahko vsebujejo osebne ali občutljive informacije. Poleg tega je treba upoštevati vprašanja o odgovornosti, saj avtomatizirani sistemi lahko proizvajajo vsebine z obsežnim vplivom, ki lahko povzročijo škodo ali kršijo pravice. Vprašanje glede upravljanja z intelektualno lastnino pri uporabi že usposobljenih modelov je dodaten izziv. Na primer, nedavna tožba OpenAI[8] glede uporabe podatkov za trening modela GPT-3 odpira vprašanja o lastništvu, licenciranju in odgovornosti za generirane vsebine.

5 Zagotavljanje informacijske varnosti in zaupanja v GPT

Da bi se spopadli s tveganji in zagotovili zaupanje v tehnologijo GPT, je ključna celostna obravnava[9]:

- **Razvijte jasne politike uporabe**
  Vzpostavite organizacijske smernice in politike, ki opisujejo sprejemljivo uporabo ChatGPT in drugih orodij AI. Zagotovite, da so zaposleni seznanjeni s temi politikami in zagotovite usposabljanje o najboljših praksah za varno in odgovorno uporabo.
- **Izvedite nadzor dostopa**
  Omejite dostop do ChatGPT in drugih sistemov AI na pooblaščene osebe. Uporabite metode močne avtentikacije, kot je večfaktorska avtentikacija, za zmanjšanje tveganja nepooblaščenega dostopa.
- **Varni komunikacijski kanali**
  Zagotovite, da je vsa komunikacija med uporabniki in ChatGPT šifrirana za zaščito pred morebitnimi zlorabami.
- **Spremljajte in nadzirajte uporabo**
  Redno pregledujte in spremljajte uporabo orodja ChatGPT ter izvajajte ustrezne ukrepe za preprečevanje srednjih napadov in drugih varnostnih groženj.
- **Preverjanje izvora podatkov**
  Temeljito preverjanje avtentičnosti in kakovosti izobraževalnih podatkov je ključno za zmanjšanje možnosti za zlorabo. Na primer, nekateri raziskovalci so razvili metode za odkrivanje in odstranjevanje pristranskih, neprimernih ali zavajajočih podatkov iz naborov podatkov.
- **Smernice za odgovorno uporabo**
  Razvoj smernic in standardov za etično in odgovorno uporabo tehnologije GPT za preprečevanje neetične uporabe. Na primer, OpenAI je objavil svojo politiko o varni uporabi modela GPT-3, ki vključuje načela o spoštovanju človekovih pravic, transparentnosti, poštenosti, zanesljivosti in skladnosti.
- **Izobraževanje uporabnikov in ozaveščanje**
  Sistematično izobraževanje uporabnikov in javnosti o prednostih in tveganjih tehnologije GPT za povečanje njihove digitalne pismenosti in kritičnega mišljenja. Na primer, nekatere organizacije so organizirale delavnice, tekmovanja ali kampanje za spodbujanje ustvarjalne in varne uporabe tehnologije GPT.

6 Sklep

Tehnologija GPT je ena najbolj naprednih in vplivnih tehnologij na področju generiranja naravnega jezika. Njene aplikacije so številne in raznolike, kar odpira nove možnosti za izboljšanje komunikacije, izobraževanja, zabave in drugih področij. Vendar pa tehnologija GPT ni brez izzivov, še posebej na področju informacijske varnosti. Da bi se spopadli s temi izzivi in zagotovili zaupanje v tehnologijo GPT, je potrebna celostna obravnava, ki vključuje preverjanje izvora podatkov, robustno avtentikacijo in šifriranje, smernice za odgovorno uporabo, izobraževanje uporabnikov in ozaveščanje. Le tako lahko izkoristimo polni potencial tehnologije GPT za dobrobit človeštva.

[8] ChatGPT maker OpenAI faces class action lawsuit over data to train AI - The Washington Post

[9] https://cloudsecurityalliance.org/artifacts/security-implications-of-chatgpt/