Bančni vestnik

REVIJA ZA DENARNIŠTVO IN BANČNIŠTVO

LJUBLJANA, LETNIK 73, ŠTEVILKA 10, OKTOBER 2024

KAZALO

Bančni vestnik

REVIJA ZA DENARNIŠTVO IN BANČNIŠTVO
THE JOURNAL FOR MONEY AND BANKING

ISSN 0005-4631

ZBS | Združenje bank Slovenije

Uredniški odbor: dr. Primož Dolenc (predsednik), dr. Damjan Kozamernik (namestnik predsednika), mag. Andrej Krajner, Boštjan Leskovar, univ. dipl. ekon., dr. Vasja Rant, dr. Igor Stubelj, dr. Marko Košak, Bojan Ivanc, univ. dipl. ekon, CFA, dr. Marko Simoneti, ddr. Timotej Jagrič, dr. Matej Drašček, Mateja Lah Novosel, univ. dipl. ped., **odgovorna urednica:** Mateja Lah Novosel, univ. dipl. ped., **strokovna sodelavka:** Azra Beganović, **lektorica:** Alenka Regally, **AD in oblikovanje:** Edi Berk/ KROG, **oblikovanje znaka ZBS:** Edi Berk/ KROG, **fotografija/ilustracija na naslovnici:** Kreb Ide, **prelom:** Pasadena, **tisk:** Roboplast, **naklada:** 45 izvodov. Izhaja enkrat mesečno, letna naročnina 80 EUR, za študente 40 EUR. Razmnoževanje publikacije v celoti ali deloma ni dovoljeno. Uporaba in objava podatkov in delov besedila je dovoljena le z navedbo vira. Rokopisov ne vračamo. Poštnina je plačana pri pošti 1102 Ljubljana. Revijo subvencionira Banka Slovenije.
Revija je indeksirana v mednarodni bibliografski bazi ekonomskih revij EconLit.

Editorial Board: Primož Dolenc (Chairman), Damjan Kozamernik (Deputy Chairman), Andrej Krajner, Boštjan Leskovar, Vasja Rant, Igor Stubelj, Marko Košak, Bojan Ivanc, Marko Simoneti, Timotej Jagrič, Matej Drašček, Mateja Lah Novosel, **Editor-in-Chief:** Mateja Lah Novosel, **Business Associate:** Azra Beganović, **English-language editing:** Vesna Mršič; **Cover design and ZBS logo:** Edi Berk/KROG; **Cover photography/ illustration:** Kreb Ide; **Graphic pre-press:** Pasadena; **Printed by:** Roboplast; **Number of copies:** 45. Bančni vestnik is published monthly. Annual subscriptions: EUR 80; for students: EUR 40. Reproduction of this publication in whole or in part is prohibited. The use and publication of parts of the texts is only allowed if the source is credited. Manuscripts will not be returned to the author. Postage paid at the 1102 Ljubljana Post Office. This journal is co-financed by the Bank of Slovenia.
The journal has been indexed and abstracted in the international bibliography of economic literature EconLit.

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.

Odziv zakonodajalca na problematiko goljufij pri plačevanju

*Simon Anko**

Delež negotovinskih plačil v evroobmočju zanesljivo raste[1]. Digitalizacija je spremenila nakupovalne in plačilne navade. Vse več kupujemo na spletu, tehnologija pa je pri plačilnih storitvah omogočila uporabniško izkušnjo, ki si je pred 15 leti nismo znali niti predstavljati. Plačila so dosegla hitrost tekstovnih sporočil, kar za ponudnike plačilnih storitev ni bilo tako samoumevno kot (je) za uporabnike.

Razvoju sledijo vzorci goljufij. Nekdaj najpogostejše zlorabe na bankomatih so z opustitvijo magnetne steze na plačilnih karticah praktično izginile. Kartično plačevanje na spletu je z uvedbo močne (dvofaktorske) avtentikacije stranke (t. i. SCA) postalo mnogo varnejše. Zdaj so – in še bolj bodo – »na udaru« takojšnja plačila, ki se poravnajo v nekaj sekundah, podnevi in ponoči, vse dni v letu. Ob tem skrbi porast novih vrst goljufij, posebej primerov „socialnega inženiringa", katerih število se je v zadnjih letih močno povečalo.

V postopku revizije Direktive o plačilnih storitvah (PSD2), ki zadevno področje ureja danes, je bilo ugotovljeno, da je treba zaščito uporabnikov in zaupanje v plačila okrepiti, za to pa bi bil primeren pristop z določitvijo pravil v uredbi, saj se ta uporablja neposredno. Evropska komisija je tako 28. junija 2023 objavila predlog uredbe[2], ki vključuje pravila za ponudnike plačilnih storitev in potrošnike, ter predlog nove direktive[3], ki zajema zlasti pravila o izdajanju dovoljenj plačilnim institucijam in nadzoru nad njimi.[4]

Močna avtentikacija stranke in preverjanje številke IBAN sta pomembna elementa preprečevanja goljufij. Enako pomembno pa je pravočasno odkrivanje goljufivih plačilnih transakcij. Zato predlog uredbe od ponudnikov plačilnih storitev zahteva, da zagotovijo mehanizme za spremljanje transakcij, ki morajo temeljiti na izmenjavi podatkov in odkrivanju netipične uporabe plačilnih storitev, ob upoštevanju elementov, značilnih za uporabnika plačilnih storitev v okoliščinah običajne uporabe osebnih varnostnih elementov, vključno z okoljskimi in vedenjskimi značilnostmi.

Do sem vse lepo in prav. Zahtevane so napredne tehnološke rešitve, ki bodo verjetno vsaj deloma slonele na umetni inteligenci. Predlog uredbe je razburjenje (predvsem ponudnikov plačilnih storitev) povzročil drugje. Zahteva namreč ustrezno zaščito potrošnikov tudi v primerih, ko so plačilne transakcije sicer odobrili, a so bili žrtve prevare. Zavedeni potrošniki lahko odobrijo transakcijo, ki je dejansko niso želeli, ali pa goljufi z zvijačo prevzamejo nadzor nad celotnim postopkom,

* mag. Simon Anko, direktor oddelka Plačilni in poravnalni sistemi v Banki Slovenije. Stališča, izražena v prispevku, so stališča avtorja in niso nujno tudi stališča Banke Slovenije

[1] Še leta 2016 je bil zgolj 21% vseh plačil na prodajnih mestih, leta 2022 že 41%, rezultati za letos pa bodo objavljeni decembra (Vir: ECB: Study on the payment attitudes of consumers in the euro area (SPACE)).

[2] Predlog Uredbe Evropskega parlamenta in Sveta o plačilnih storitvah na notranjem trgu in dopolnitvi Uredbe (EU) št. 1093/2010

[3] Predlog Direktive Evropskega parlamenta in Sveta o plačilnih storitvah in storitvah elektronskega denarja na notranjem trgu, spremembi Direktive 98/26/ES ter razveljavitvi direktiv (EU) 2015/2366 in 2009/110/ES

[4] Predloga sta v postopku pogajanj pri sozakonodajalcih.

vključno z dokončanjem močne avtentikacije stranke. Ker manipulacija vpliva na integriteto odobritve transakcije, ni več mogoče – kot še velja v PSD2 – povračil omejiti samo na neodobrene transakcije.

Izguba zaupanja v sodobne načine plačevanja bi lahko imela sistemske posledice za zaupanje tudi v druge finančne in digitalne storitve. Zato je smiselno vzeti v roke predlog uredbe in se začeti pripravljati na implementacijo ustreznih rešitev in postopkov, ne pa se boriti proti njenim določbam. Zelo verjetno je, da bosta sozakonodajalca šla prej v smeri še večje zaščite potrošnikov kot najranljivejše skupine uporabnikov kot pa nižanja zahtev za ponudnike plačilnih storitev v primerjavi z objavljenim predlogom Evropske komisije[5]. Pomemben del teh zahtev je povezan z ozaveščanjem o trendih in tveganjih goljufij. Vsaj na nacionalni ravni je te aktivnosti smiselno izvajati koordinirano. Spomnimo: varnost plačevanja in ozaveščenost uporabnikov sta del Strategije razvoja trga plačil v Sloveniji za obdobje 2024-2028[6], ki jo je lani sprejel Nacionalni svet za plačila.

Plačila tako že dolgo niso več dolgočasen »nevtralni bančni posel«. Danes so najpogosteje uporabljena finančna storitev, pri kateri je ključna uporabniška izkušnja. Varnost je del nje, ne nasprotni pol, s katerim bi iskali ravnovesje.

[5] Glej npr. poročilo Evropskega parlamenta: https://www.europarl.europa.eu/doceo/document/A-9-2024-0052_EN.html#_section1.

[6] https://www.bsi.si/placila-in-infrastruktura/nacionalni-svet-za-placila/gradiva/temeljni-dokumenti-nacionalnega-sveta-za-placila

Intervju z Davidom Kasabjijem, vodilnim analitikom varnostno-obveščevalnih podatkov:

Grožnje, ki jih omogoča uporaba orodij umetne inteligence

Intervju odpira tematiko groženj, ki jih omogoča uporaba orodij umetne inteligence (AI). Odgovore je podelil strokovnjak David Kasabji iz podjetja NIL, del skupine Conscia. Kasabji deluje v podjetju kot vodilni analitik varnostno-obveščevalnih podatkov.

g. David Kasabji iz podjetja NIL, del skupine Conscia

Naši bralci so tako strokovnjaki s področja kibernetske varnosti kot tudi drugi zaposleni v bančno-finančnem sektorju, ki še ne poznajo vloge analitika varnostno-obveščevalnih podatkov. Katere so vaše glavne naloge in odgovornosti, kako se je vaša vloga razvijala v zadnjih letih glede na hitro spreminjajoče se okolje kibernetske varnosti?

Vloga analitika varnostno-obveščevalnih podatkov ima širok spekter. Znotraj oddelka imamo za vsakega posameznega analitika večkrat različne in specifične fokuse. V tem primeru bom povzel glavne naloge in odgovornosti v celoti.

Primarni cilj varnostno-obveščevalnih podatkov je, da zagotavljajo proaktivno odkrivanje groženj. S pomočjo takšnih podatkov lahko predvidimo potencialne grožnje za naše podjetje, še preden se zgodijo – takšne dogodke lahko preprečimo oziroma bistveno znižamo tveganje za resnejši incident – to je naš »holy grail«.

V podjetju NIL imamo opredeljeno storitev, ki naslavlja prav to področje, in sicer pod imenom Executive Intelligence Briefings. Ta deluje tako, da za naše stranke spremljamo njihove grožnje v okolju (angl. Threat Landscape) in na podlagi opazovanja ugotavljamo, katera grožnja je za njih najbolj relevantna. Ko grožnjo odkrijemo (to so navadno hekerske skupine ali celo APT-ji), analiziramo njihovo delovanje. Ko dobimo informacijo, kdo je najbolj verjetna grožnja ter kako operira, lahko v nadaljevanju na podlagi teh dveh vhodnih podatkov z ustreznimi operativnimi ali strateškimi odločitvami zagotovimo, da grožnja ne bo predstavljala visokega tveganja za digitalno varnost podjetja.

To je torej klasični cilj varnostno-obveščevalnih podatkov na strateški oz. taktični ravni, za katerega verjamem, da ga večina podjetij najbolj pozna.

Tisti manj znani del se pojavlja na operativni ravni, kjer varnostno-obveščevalni podatki služijo kot vir bogatenja podatkov za varnostno operativne centre (angl. SOC), kar analitikom omogoča hitrejšo dedukcijo primerov, ki jih razrešujejo. Prav tako se varnostno-obveščevalni podatki uporabljajo za proaktivno odkrivanje groženj na podlagi t. i. Threat Hunting tehnik, s katerimi ujamejo tiste grožnje, ki se izmuznejo reaktivni zaznavi.
Prav tako so nepogrešljivi pri odzivih na incidente, kjer analitiki varnostno-obveščevalnih podatkov sodelujejo z ekipo odziva na incidente, pri čemer jim pomagajo ugotoviti, kdo stoji za določenim napadom in kako se je tak napad v celoti izvedel (npr. z analizo vzorca zlonamerne programske opreme). S to ugotovitvijo odkrijejo dodatne tehnike napadalca, katere posredujejo ekipi za odzive na incidente. Ta ekipa lahko potem dodatno preveri, ali so res ustrezno in v celoti počistili grožnjo v okolju.
Varnostno-obveščevalni podatki so pravzaprav vpeti v vsak steber kibernetske varnosti in predstavljajo tisto »proaktivno« komponento v kibernetski varnosti, ki postaja vse bolj nepogrešljiva. Iz leta v leto namreč spremljamo naraščanje digitalnega kriminala, tako v volumnu napadov kot v razvoju naprednih tehnik napadov ter infrastrukture. Prav zato tradicionalne metode reaktivne zaznave groženj žal ne bodo več zadoščale. Treba bo začeti predvidevati tiste najbolj očitne in akutne grožnje ter jih ustrezno obravnavati, še preden pride do incidenta.
Veseli me, da se v finančnem sektorju prebuja zavedanje tega izziva in da se v kar nekaj nedavnih pravnih aktih (DORA, TIBER-EU) zahteva vpletenost varnostno-obveščevalnih podatkov v programih za kibernetsko varnost.

Kako ravnate z obveščevalnimi podatki o grožnjah? Kako obveščevalni podatki o grožnjah prispevajo k oblikovanju dolgoročne strategije kibernetske varnosti v banki oz. podjetju?
Sam postopek je večfazni. Sam varnostno-obveščevalne podatke rad definiram kot proces transformacije surovih podatkov v uporabne informacije (angl. Actionable intelligence), ki so ustrezne za določene deležnike. Ni vseeno, ali te informacije prejme CISO, inženir, ki razvija zaznavna pravila, ali pa forenzik v odzivih na incidente. Za isto informacijo moramo tvoriti ustrezne pakete, ki bodo pomenljivi za določenega deležnika.
Banke morajo vključevati strateške varnostno-obveščevalne podatke za oblikovanje dolgoročne strategije kibernetske varnosti. Finančne institucije so žal pogosta tarča digitalnih kriminalcev (zaporedno leto so že med top 3 globalnimi industrijami, če preverjamo različna poročila, kot je IBM-ov Cost of Data Breach). Uspešen vdor lahko za digitalne kriminalce pomeni precejšen denarni izkupiček v fazi izterjave z izsiljevalskim virusom ali odtujenimi podatki.
Za učinkovito zaščito mora takšno sodelovanje potekati neprekinjeno, saj se tudi okolje groženj dinamično spreminja in prilagaja. Tako bi morali analitiki varnostno-obveščevalnih podatkov konstantno spremljati okolje groženj ter prilagajati raven tveganj za finančno inštitucijo glede na trenutne dejavnike in kazalnike, ugotovitve pa ustrezno poročati vodilnim z ustreznimi priporočili. Tako mi ravnamo z našimi storitvami in strankami.
Poleg že omenjene storitve Executive Inteligence Briefings imamo na voljo tudi storitev Brand Protection, ki je zelo popularna v finančnem sektorju. Za naše stranke spremljamo pojave ter spremembe na temnem in navadnem spletu (na ravni domen in identitet), ki bi lahko zlonamerno vplivale na znamko podjetja, v sklopu omenjene storitve pa uspešno zaznavamo tudi morebitne ukradene poverilnice, ki se tam prodajajo.
Za banke je na primer ključno, da hitro zaznamo registracijo nove lažne domene, ki očitno želi prelisičiti komitente preko »phishing« sporočil, da vnesejo svoje prijavne podatke v lažni prijavni portal, ki pa je videti identično kot portal banke. T. i. »typosquatt« domene so lahko zelo prepričljive in na prvo oko verodostojne, takšna uspešna prevara pa bistveno vpliva na ugled banke.

Laiki ne poznamo orodij AI, kot sta WormGPT in FraudGPT. Kaj sta ti »orodji« in kako se razlikujeta od ChatGPT, za katerega smo vsi vsaj slišali?
Predvsem za laike bi opisal ta zla orodja kot »ChatGPT brez varnostnih filtrov« in napajan s podatki o tehnikah napadov. Takšna orodja so zelo koristna pri razvoju zlonamerne programske kode, kjer pri »zlobnih« GPT-jih ni nekih zavor pri odgovorih, kako kakšen sistem ali varovalo prelisičiti – celo še več – prav na podlagi takšnih podatkov so učeni njihovi modeli. So tudi nepogrešljivi pri tvorbi »phishing« sporočil. Tako lahko nedavno opazimo porast uspešnih »phishing« napadov – tudi v Sloveniji lahko opažamo precej bolj sofisticirane verzije »phishing« vsebin. Nekaj let nazaj je bila naše varovalo slovenščina, saj je bila pri »phishing« napadih opazno popačena. Tega varovala sedaj s pomočjo takšnih orodij ni več.

Kako lahko orodja AI prispevajo k povečanemu številu sofisticiranih kibernetskih napadov in kakšni bodo ti? Ali je ta orodja mogoče zaznati s trenutnimi kibernetskovarnostnimi orodji?

Kot sem nakazal že v prejšnjem odgovoru, bodo razna orodja AI bistveno vplivala na volumen napadov ter verjetno tudi na uporabo novih naprednih oblik napadov. Digitalni kriminalci imajo sedaj na voljo asistenta, ki jim pomaga generirati zle vsebine ter kode, kar bistveno pohitri celoten proces kibernetskih napadov. To posledično vpliva na količino izvršenih napadov. Zame je dober primer pohitritve napadov ravno pri izsiljevalskih virusih, ki so najbolj priljubljeni – namreč pri napadih z izsiljevalskimi virusi je del procesa tudi pogajanje glede plačila za ključ za dekriptiranje podatkov ali pa za preprečitev objave odtujenih podatkov. Ta faza napada je lahko za digitalne kriminalce zelo dolgotrajna, saj se morajo svoji žrtvi posvečati več tednov in komunicirati v angleščini, kar jim morda ni najbolj enostavno. No, sedaj imajo naenkrat na voljo orodja AI, ki jih pretvorijo v t. i. Chatbote. Tovrstna orodja bodo omenjeno delo opravljala samostojno in povsem brez njihove intervencije. Celotna faza pogajanja, ki je najbolj dolgotrajna, bo sedaj povsem »outsourced« na AI Chatbote, digitalni kriminalci pa se bodo v tem času lahko fokusirali na nove napade.

Omenil bi še en pomenljiv pojav v svetu digitalnega kriminala, na katerega je vplivala umetna inteligenca. Zaradi bistveno lažjega in hitrejšega razvoja zlonamerne programske kode je na temnem spletu naprodaj vse več paketov te zlonamerne programske opreme, in to po zelo ugodnih cenah, saj je sedaj konkurenčnost produkta večja, ravno zaradi hitrejših iteracij razvoja s pomočjo AI-asistentov. Dostopnost zlonamerne programske opreme je skupaj s padcem cen povzročila nov pojav: amaterskim hekerjem je odprla vrata v svet digitalnega kriminala. Seveda amaterski hekerji niso ravno novost, ampak sedaj je res vsakdo, ki ima v žepu 100 EUR, lahko heker, in za ta znesek dobi sofisticirano zlonamerno programsko opremo, ki se pravzaprav sama izvaja – treba je nastaviti le osnovno konfiguracijo in že je nared za uporabo.

Glede zaznave pa je tako: cilj sofisticirane zlonamerne programske opreme (ki jo danes omogočajo tudi orodja AI) je, da se spretno izogne tradicionalnim oblikam zaznave. Velikokrat se to doseže s posnemanjem delovanja legitimnih orodij na sistemih, na katere se reaktivna zaznavna orodja praviloma ne odzivajo. Analitiki bi se namreč utopili v količini primerov, ki jih morajo pregledati, saj bi največkrat šlo za t. i. »false positive«. Drug primer je izraba neodpravljenih ranljivosti v okoljih, ki omogočajo »tih« vstop. S tradicionalnimi oblikami zaznave je takšne primere tudi sicer težje zaznati, orodja AI pa bodo vse bolj pomagala pri razvoju takšnih zlorab.

Zato velikokrat omenjam, da je pri zaznavanju nujno potrebna proaktivna komponenta. Ključno je vedenje, katere so trenutno najbolj aktivne grožnje za naše okolje, ki se jim moramo ustrezno izogniti pred samim napadom. Proaktivnost vključuje tudi aktiven pregled sistemov in delovnih postaj za grožnje glede na izbrane indikatorje.

Ste zaznali kakšne tehnične ranljivosti ali pomanjkljivosti teh orodij AI, ki bi jih strokovnjaki za kibernetsko varnost lahko izkoristili za obrambo pred napadi in prevarami?

V trenutni fazi, ko še ne poznamo avtonomnega sistema AI (neka raven AGI), imamo prednost, da bijemo bitko s stroji. Le-ti, ne glede na vse zmogljivosti, še vedno delujejo po principu 0 in 1 (biti). Torej na obrambni strani moramo imeti človeško komponento, ustrezno uparjeno z vsaj enako naprednimi tehnologijami ter proaktivnimi komponentami, in tako bomo lahko preprečili resne vdore.

Kako lahko zakonodajalci in regulatorni organi omejijo (zlo)uporabo orodij AI za zlonamerna dejanja? Kako pomembno je po drugi strani vzpostavljanje etičnih standardov pri razvoju in uporabi AI, zlasti ko govorimo o kibernetskih grožnjah?

Po mojem mnenju bi se morali regulatorji osredotočiti na lažje vpeljevanje novih tehnologij v organizacije. Seveda mora obstajati neka regulativa, ampak ne smemo preveč oteževati vpeljave novih tehnologij v legitimne namene, ker nas potem tisti na drugi strani prehitijo in se boj znatno oteži.

Prav tako se moramo usmeriti v vpeljavo boljših tehnologij zaznave naprednih groženj – če ne gre drugače, pa preko zakonov ali regulativ. Kot sem omenil uvodoma, DORA in TIBER-EU sta zelo dobra premika v pravo smer. Imamo pa tudi zametke vpeljave zakonov oz. aktov na ravni EU (kot je na primer EU AI Act), ki poskušajo na svoj način omejevati uporabi orodij AI – menim pa, da to ne bo bistveno vplivalo na svet digitalnega kriminala.

Kakšne preventivne ukrepe lahko organizacije sprejmejo, da zmanjšajo tveganje napadov, ki temeljijo na orodjih AI?

Ukrepov je lahko veliko, izpostavil bi le nekaj pomembnejših:

1. Izobraževanje in ozaveščanje zaposlenih
2. Varnostna preverjanja v kombinaciji z uporabo varnostno-obveščevalnih podatkov
3. Uporaba AI za obrambo
4. Kontinuirano spremljanje varnostnih dogodkov v okolju s pomočjo zaznavnih orodij

Medtem opažamo, da postaja v finančnem sektorju vse bolj popularno varnostno preverjanje v obliki Red Teaming, ki temelji na varnostno-obveščevalnih podatkih. To prepoznava tudi ogrodje TIBER-EU, ki ga je vzpostavila centralna banka (ECB) za krepitev odpornosti finančnega sektorja na kibernetske grožnje.
Takšno storitev izvajamo v podjetju NIL za stranke celo intervalno, kajti grožnje se prilagajajo in razvijajo - še posebej takšne, ki se razvijajo s pomočjo AI.

Kako bo po vašem mnenju razvoj tehnologije umetne inteligence vplival na kibernetsko kriminaliteto v prihodnosti?
Predvidevam, da se bo volumen napadov kontinuirano večal, zaradi vse nižjega vstopnega praga za amaterske hekerje in hitrejšega razvoja zlonamerne programske kode. Prav tako bodo sofisticirane hekerske skupine izvajale bistveno bolj napredne napade s pomočjo AI.

Ali menite, da se bo človeštvo v bodoče soočilo z velikim tveganjem, da bi umetna inteligenca z učenjem pridobila svojo samobitnost in je ne bo več mogoče kontrolirati?
Verjamem, da je to utemeljeno tveganje in ga je treba pravočasno obravnavati in urejevati.

Katere industrije so trenutno najbolj izpostavljene napadom z uporabo orodij AI?
Zdravstveni, finančni, bančni ter izobraževalni sektor. Ti prednjačijo, ker so tipično »zanimive« tarče tudi za amaterje, ki bi radi zaslužili hiter denar z nekim kupljenim izsiljevalskim virusom ali »infostealerjem«. Običajno razpolagajo ti sektorji oz. industrije s pomembnimi osebnimi podatki, ki so tudi v hekerskih skupnostih med najbolj cenjenimi.

Kako lahko posamezniki zaščitimo svoje osebne podatke in identiteto pred zlorabami, ki jih omogoča uporaba orodij AI?
Vse to je zelo odvisno od lastnega modela groženj (Threat Modeling). Posamezniki imamo različna merila, kaj nas »boli« v primeru odtujitve osebnega podatka.
Menim, da je tukaj težava bolj v tem, da so naši osebni podatki in identitete precej razpršeni po spletu že samo pri legitimni uporabi popularnih orodij, ki nam konstantno sledijo in nas profilirajo.
Za posameznike bi podal splošna priporočila, kot so:
1. Upoštevanje načel varne uporabe interneta
2. Izogibanje deljenju prevelike količine osebnih podatkov
3. Redno spremljanje svoje digitalne identitete
4. Uporaba šifriranih komunikacijskih kanalov
5. Preverjanje virov informacij
6. Uporaba orodij za zaščito zasebnosti (VPN)
7. Previdnost pri uporabi javnih omrežij

Ali menite, da bi o tveganjih glede zlonamerne uporabe orodij AI morali govoriti že v osnovnih šolah?
Absolutno. Prav tako se mi zdi, da je v osnovnih šolah in tudi kasneje premalo govora o osnovah digitalne varnosti. Zdi se mi, da se vse bolj pričakuje uporaba digitalnih orodij za dosego standardov pri učenju, pri tem pa še zmeraj ne obstaja noben obvezen predmet, ki bi ozaveščal o varni uporabi takšnih produktov in morebitnih grožnjah.

Kakšna je po vašem mnenju stopnja digitalne pismenosti slovenskega prebivalstva?
Moje osebno mnenje je, da obstaja prelomnica, kjer se digitalna pismenost bistveno razlikuje, to prelomnico pa navadno določa starost prebivalca. Pozitivno je, da se iz leta v leto ta prelomnica digitalne pismenosti pomika k višji starosti. Če se ozremo 10 let nazaj in primerjamo povprečnega 70-letnika tedaj in danes, vemo, da smo danes pri 70 letih veliko bolj digitalno ozaveščeni in bolje dojemamo tudi kibernetska tveganja.
Kljub vidnemu pozitivnemu trendu ne moremo mimo številk, ki nam prikazujejo realno stanje in hkrati priložnosti za izboljšave. Po podatkih Statističnega urada Republike Slovenije je v letu 2023 imelo le 19 % prebivalcev Slovenije zelo dobro razvite digitalne veščine, 28 % osnovne, 21 % pomanjkljive, 13 % skromne in 6 % zelo skromne. Med vsemi prebivalci je le dobra polovica (56 %) oseb, ki imajo razvite digitalne veščine za varno uporabo IKT in zaščito podatkov, kar 44 % pa tovrstnih veščin (še) nima. V prizadevanjih za samozavestno, kritično in odgovorno uporabo digitalnih tehnologij imamo torej še veliko možnosti za napredek.

UDK 004.056:343.9(497.4)

Kibernetska varnost v Sloveniji in spremembe Zakona o informacijski varnosti

*URSIV**

CYBERSECURITY IN SLOVENIA AND AMENDMENTS TO THE INFORMATION SECURITY ACT

The Government Office for Information Security (URSIV) plays a crucial role in shaping and implementing cybersecurity strategies in Slovenia. Its responsibilities include ensuring the cybersecurity of critical infrastructure and information systems, aligning legislative changes with EU directives, and connecting key stakeholders. New legislative changes, particularly the NIS 2 Directive, strengthen security requirements and introduce stricter monitoring measures for entities. The NIS 2 Directive expands the scope of cybersecurity obligations to include large and medium-sized companies in highly critical or other critical sectors, as well as entities whose disruptions could impact the functioning of the state.

JEL K24

Uvod

Urad Vlade Republike Slovenije za informacijsko varnost (URSIV) je pristojni nacionalni organ za informacijsko varnost, ki deluje kot samostojna vladna služba. Ima ključno vlogo pri vzpostavitvi celovite strategije informacijske in kibernetske varnosti na nacionalni ravni. Njegove naloge zajemajo širok spekter dejavnosti, ki so osredotočene na krepitev odpornosti kritične infrastrukture in zagotavljanje varnosti ključnih informacijskih sistemov v državi.

URSIV povezuje deležnike v nacionalnem sistemu informacijske varnosti in na strateški ravni koordinira operativne zmogljivosti v sistemu. Posebno pozornost posveča 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.

Na zakonodajni ravni URSIV tesno sodeluje pri pripravi in izboljšavi zakonodajnih okvirjev, ki urejajo področje informacijske varnosti, ter si prizadeva za usklajevanje slovenske zakonodaje z evropskimi direktivami in standardi. S tem zagotavlja, da Slovenija ostaja v koraku z najnovejšimi zahtevami in trendi na področju kibernetske varnosti, kar je ključno za zaščito pred nenehno spreminjajočimi se grožnjami v digitalnem okolju.

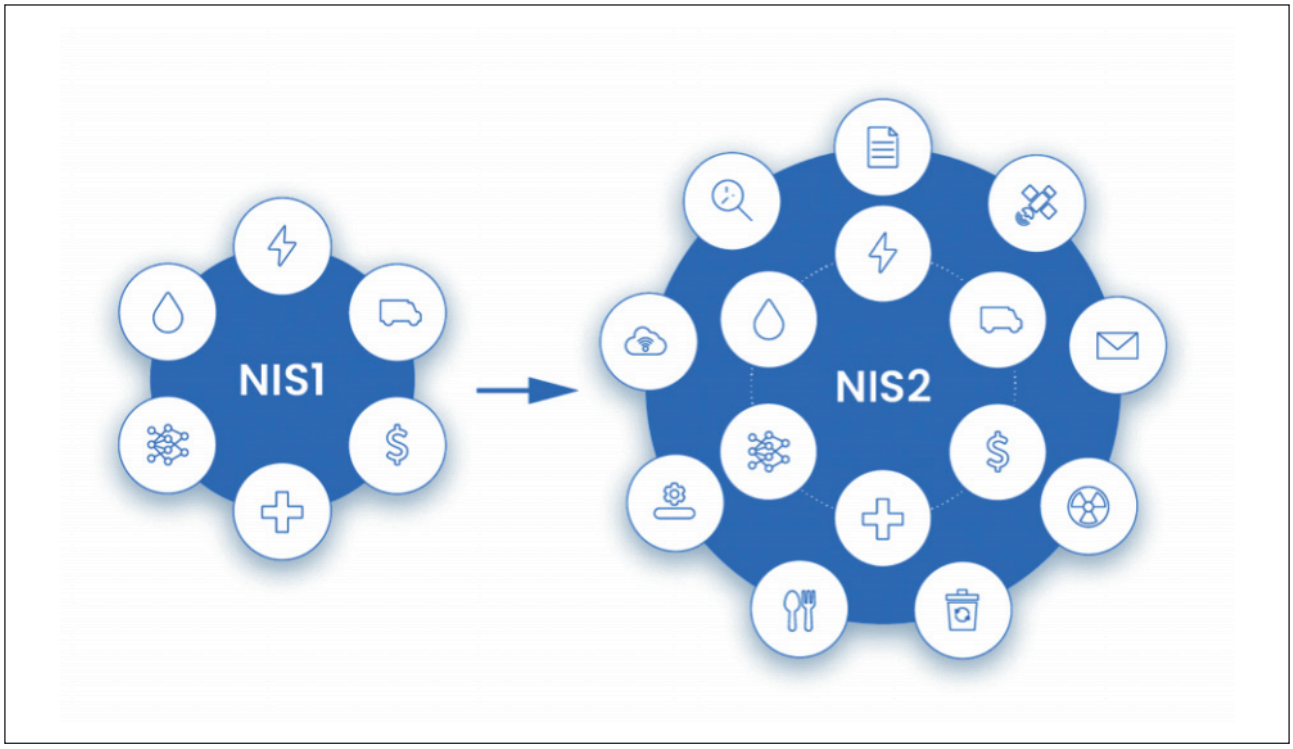
Novi Zakon o informacijski varnosti in ključne spremembe

Direktiva (EU) 2022/2555 (NIS 2) uvaja pomembne spremembe na področju kibernetske varnosti. Njeno področje delovanja je širše, saj zajema več subjektov, ki bodo postali zavezanci. Podjetja, ki spadajo v kategorijo velikih ali srednjih podjetij (več kot 50 zaposlenih in letni promet nad 10 milijonov evrov) ter delujejo v visoko kritičnih ali drugih kritičnih sektorjih, bodo vključena med zavezance direktive oziroma zakona. Prav tako podjetja, kjer bi motnja njihove storitve pomembno vplivala na druge subjekte in delovanje države. Pri tem obstajajo izjeme, ko so subjekti zavezani ne glede na velikost.

Direktiva NIS 2 na novo opredeljuje in dodaja nekaj novih sektorjev ter razdeli zavezance na bistvene in pomembne. Vsak zavezanec se bo moral samoprepoznati oziroma samoregistrirati preko mehanizma, ki ga bo vzpostavil Urad Vlade Republike Slovenije za informacijsko varnost (URSIV), ki je pristojni nacionalni organ za področje informacijske varnosti. URSIV bo na podlagi pridobljenih informacij oblikoval seznam bistvenih in pomembnih subjektov. Dosedanjega predhodnega identificiranja podjetij kot zavezancev ne bo več.

Nova zakonodaja krepi varnostne zahteve za zavezance, uvaja podrobnejše določbe glede poročanja o incidentih,

* Urad Vlade Republike Slovenije za informacijsko varnost, Ulica gledališča BTC 2, 1000 Ljubljana



Vir: https://nis2directive.eu/

vsebine poročil in rokov za njihovo predložitev. Uvedeni bodo strožji nadzorni ukrepi, okrepljena varnost dobavnih verig in osnovni okvir za usklajeno razkrivanje ranljivosti. Direktiva NIS 2 uvaja zgolj minimalno stopnjo harmonizacije in s tem članicam Evropske unije omogoča, da sprejmejo dodatne nacionalne ukrepe za povečanje odpornosti na kibernetske incidente. V skupnem bodo spremembe ob uveljavitvi nove zakonodaje prispevale k boljšemu skupnemu zavedanju in kolektivni sposobnosti odzivanja na kibernetske napade v Evropski uniji (EU).

Strategija kibernetske varnosti v Sloveniji

Temelje za kibernetsko varnost v Republiki Sloveniji postavlja strategija kibernetske varnosti. Poudarja nujnost oblikovanja celovitega sistema za zagotavljanje kibernetske varnosti kot bistvenega elementa državne varnosti. Prispeva k ustvarjanju odprtega, varnega in zaščitenega kibernetskega prostora ter omogoča nemoteno delovanje ključne infrastrukture, pomembne za delovanje državnih organov, gospodarstva in vsakodnevnega življenja posameznikov.

Slovenija je dosegla strateški mejnik na področju nacionalne varnosti z uspešno izgradnjo celovitega sistema kibernetske varnosti. Le - ta vključuje strateško koordinacijsko raven, operativno raven oziroma raven zaznavanja incidentov in odzivanja nanje ter raven zavezancev po zakonih, ki urejajo področje informacijske varnosti in elektronskih komunikacij. Vzpostavili smo sistem, ki zagotavlja zaščito pred vedno bolj kompleksnimi kibernetskimi grožnjami. S tem smo postavili trden temelj za zaščito tako javne kot zasebne infrastrukture pred kibernetskimi tveganji, ki bi lahko ogrozila varnost in delovanje bistvenih storitev družbe in gospodarstva.

Slovenija je okrepila sodelovanje z evropskimi in mednarodnimi organizacijami, kar omogoča še boljšo izmenjavo informacij in skupno reševanje kibernetskih groženj. Ker se področje hitro spreminja, je pomembno spremljati dogajanje tako na mednarodni kot na nacionalni ravni ter temu primerno prilagajati nacionalne rešitve in postopke.

URSIV pomaga z usmeritvami, priporočili in orodji za samooceno krepiti kibernetsko varnost pri zavezancih in drugih subjektih. Izvajalci bistvenih storitev in organi državne uprave ter povezani subjekti so redno obveščeni o zaznanih grožnjah, zanje pa se izvajajo tudi posveti, usposabljanja in vaje. URSIV preko letnih poročil prav tako poroča pristojnemu odboru za obrambo Državnega zbora Republike Slovenije, hkrati pa na svojih spletnih straneh na polletni ravni objavlja poročila o aktualnem dogajanju v slovenskem kibernetskem prostoru.

Obvladovanje tveganj kibernetskih napadov na kritično infrastrukturo

Kibernetski napadi na kritično infrastrukturo so postali ena večjih groženj za nacionalno varnost in delovanje globalnega gospodarstva. Kibernetski incident v sistemih

kritične infrastrukture ima t. i. kaskadni učinek. En dogodek sproži verigo drugih dogodkov, ki se medsebojno ojačujejo in povzročajo širše posledice, kot bi jih imel zgolj prvi dogodek. Na primer uspešen vdor v informacijske sisteme elektroenergetskega omrežja lahko povzroči izpad dobave električne energije. Izpad lahko nato vpliva na druge sektorje kritične infrastrukture, kot so oskrba s pitno vodo, promet, zdravstveni sistemi ali telekomunikacije. Posledica je lahko kriza, ki ima dolgoročne gospodarske in družbene posledice.

V zadnjem desetletju je bilo v mednarodnem okolju kar nekaj kibernetskih napadov na kritično infrastrukturo. Leta 2015 smo bili priče napadu na ukrajinsko elektroenergetsko omrežje, ki je opozoril na ranljivost energetskih distribucijskih omrežij in potrebo po izboljšanju zaščitnih ukrepov. Dve leti kasneje je več kot 300.000 računalnikov v 150 državah prizadela izsiljevalska programska oprema »WannaCry«. Tudi v času covida-19 so bili zaznani napadi zlasti na zdravstvene sisteme in podporne organizacije.

Slovenija celovito obvladuje tveganja kibernetskih napadov na kritično infrastrukturo. Vzpostavljen je pravni in regulativni okvir, ki vključuje zakone in predpise, ki urejajo področje kibernetske varnosti. Sprejeto ima že omenjeno Strategijo za kibernetsko varnost, ki določa cilje, naloge in odgovornosti v zvezi z zaščito kritične infrastrukture. V okviru tega ima vzpostavljen nacionalni odzivni center za kibernetske incidente SI-CERT in ločen odzivni center za državne organe SIGOV-CERT.

Odzivna centra spremljata grožnje, pomagata pri obvladovanju incidentov in izvajata analize ranljivosti, kar je bistveno za pravočasno odzivanje na kibernetske napade.

Slovenija aktivno sodeluje z EU in drugimi mednarodnimi partnerji, da bi izboljšala kibernetsko varnost. Sodelovanje vključuje izmenjavo informacij, skupno reševanje incidentov in udeležbo v mednarodnih vajah ter projektih, kar prispeva k večji pripravljenosti in odpornosti.

Pomemben del dviga odpornosti je tudi izobraževanje in usposabljanje osebja, ki upravlja kritično infrastrukturo. Redna usposabljanja in vaje izboljšajo pripravljenost na kibernetske napade. Zagotovijo, da osebje pozna in razume najnovejše varnostne prakse. Tukaj lahko omenimo nacionalno vajo kriznega upravljanja in odzivanja obrambnega sistema »Odpornost 24«, kjer bodo vsebine tudi s področja kibernetske varnosti.

Zavedati se moramo, da je kritična infrastruktura postala primarna tarča zlonamernih akterjev. Gre za stalno grožnjo, ki zahteva in bo zahtevala ustrezno stopnjo pozornosti in izvedbo blažilnih ukrepov.

Aktualni projekti URSIV na področju kibernetske varnosti v Sloveniji

URSIV se redno udeležuje nacionalnih in mednarodnih dogodkov ter konferenc na temo kibernetske varnosti, saj je mreženje ključno za uspeh na tem področju. Vzpostavlja Nacionalni koordinacijski center za kibernetsko varnost (NCC-SI), ki bo krepil raziskave in inovacije ter njihovo uvajanje na področja kibernetske varnosti. Pomagal bo pri razvoju industrijskih, tehnoloških ter raziskovalnih zmogljivosti države, predvsem z zagotavljanjem možnosti sofinanciranja evropskih projektov.

Velik poudarek bo NCC-SI namenil izobraževanju s področja kibernetske varnosti. Splošno znano je, da na tem področju primanjkuje strokovnjakov, zato bo poudarek predvsem na mladih, ki se odločajo za poklicno pot. V ta namen že potekajo aktivnosti, npr. vsakoletna udeležba na evropskem tekmovanju mladih talentov v kibernetski varnosti »Evropski izziv kibernetske varnosti (European Cybersecurity Challenge)« v okviru projekta »Kibertalent«. Vanj sodi tudi usposabljanje deklet za kibernetsko varnost, ki ga bomo letos izvedli poskusno. Projekt predvideva tudi vzpostavitev mrež srednjih šol za kibernetsko varnost, za kar bomo jeseni s Fakulteto za elektrotehniko izvedli usposabljanje učiteljev oziroma inštruktorjev. V času počitnic smo sodelovali pri izvedbi poletnega tabora s področja kibernetske varnosti za mlade.

URSIV podpira raziskave, razvoj in inovacije na področju kibernetske varnosti tudi s sofinanciranjem projektov. Prvi projekt sofinanciramo z Javno agencijo za znanstvenoraziskovalno in inovacijsko dejavnost Republike Slovenije (ARIS) in Ministrstvom za obrambo. Pokriva napredne analitike podatkov in modeliranje napadov in napadalcev na področju kibernetske varnosti v sektorjih obrambe, notranje varnosti, obveščevalne dejavnosti, zaščite in reševanja ter kritične infrastrukture. Drugi projekt, ki ga sofinanciramo skupaj z ARIS, pa je s področja uporabe umetne inteligence v kibernetski varnosti.

URSIV sodeluje tudi v dveh projektih iz Načrta za okrevanje in odpornost (NOO). Prvi je projekt »SI-EuroQCi« za vzpostavitev nacionalne kvantne komunikacijske infrastrukture za varno distribucijo kvantnih šifrirnih ključev. Projekt, ki obsega zemeljski in vesoljski del, se financira s sredstvi NOO in sredstvi dveh programov EU. Zemeljski del projekta se že izvaja od začetka leta 2023. Drugi projekt, ki ga bo URSIV izvedel z Ministrstvom za digitalno preobrazbo, obsega več različnih aktivnosti, njihova izvedba pa bo pripomogla k dvigu ravni kibernetske varnosti na nacionalni ravni.

Letos je bil URSIV skupaj s partnerji uspešen še pri pridobitvi dveh novih projektov. Prvi je projekt »Akadimos« s po-

dročja pridobivanja veščin kibernetske varnosti, drugi pa projekt »ALiEnS-SOC«, namenjen uporabi novih tehnologij in umetne inteligence v varnostno operativnih centrih.
URSIV uspešno sodeluje tudi v konzorcijih za izvedbo projektov EU. Tako že od začetka leta 2023 sodelujemo v projektu »Atlantis«, katerega cilj je povečati odpornost in kibernetsko-fizično-človeško varnost ključnih kritičnih infrastruktur EU.
Poleg vsega naštetega URSIV koordinira izvajanje storitev zagotavljanja kibernetske varnosti v okviru pilotnega projekta Agencije evropske unije za kibernetsko varnost (ENISA), ki so namenjene zavezancem, tudi upravljalcem kritične infrastrukture. V prihodnje si želimo še več aktivnosti in projektov, ki bodo pripomogli k promociji poklicev s področja kibernetske varnosti in zavedanju pomembnosti dviga kibernetske varnosti v državi. V ta namen smo prisotni tudi na socialnih omrežjih, kjer ozaveščamo širšo javnost.

Sklepna misel

Pomembno je, da se tako fizične kot pravne osebe zavedajo pomembnosti zagotavljanja informacijske in kibernetske varnosti z ustreznimi ukrepi. Na ta način lahko zaščitijo osebne podatke, svoje ali tuje, občutljive podatke, poslovne skrivnosti in finančno premoženje. Slednje največkrat odteka ravno zaradi kibernetskih incidentov, ki so posledica neuvedenih ukrepov zagotavljanja kibernetske varnosti.
Vodstva organizacij nosijo neposredno odgovornost za zagotovitev ustrezne zaščite pred kibernetskimi grožnjami, saj imajo pomembno vlogo pri oblikovanju strateških usmeritev, dodeljevanju sredstev in nadzoru nad izvajanjem varnostnih ukrepov. Nujno je, da odgovorni prepoznajo kibernetska tveganja kot del širšega okvira upravljanja tveganj v organizaciji ter zagotovijo ustrezne vire, tako finančne kot kadrovske, za vzpostavitev in vzdrževanje odpornega sistema kibernetske varnosti. Pri tem pa ne smemo pozabiti na ključni dejavnik kibernetske varnosti znotraj organizacije, to je ustrezno varnostno kulturo, ki ji radi rečemo »kibernetska higiena«.
Žal se pozablja, da je naloga vodstev tudi zagotavljanje skladnosti z zakonodajo in standardi, povezanimi s kibernetsko varnostjo. Direktiva (EU) 2022/2555 (NIS 2) zahteva miselni preskok in pričakuje bolj aktivno vlogo vodstev organizacij na področju kibernetske varnosti.

UDK 004.056:336.71:658

Vloga kibernetske varnosti znotraj procesa korporativne varnosti

*Matic Čaleta in Denis Čaleta**

THE ROLE OF CYBER SECURITY WITHIN THE CORPORATE SECURITY PROCESS

Modern organizations are increasingly facing complex security threats that require a comprehensive approach to ensuring safety. The banking sector is particularly vulnerable due to the transition to digital services. In this context, corporate security plays a crucial role, combining physical, information, and cybersecurity measures to enable organizations to manage risks more effectively. The human factor remains a significant challenge, often being the weakest link in security systems. Cybersecurity must be integrated into an organization's overall security strategy, with clearly defined roles for experts and consistent support from leadership. This article analyzes key challenges and opportunities in the banking sector and highlights the importance of incorporating advanced technologies, such as artificial intelligence, to enhance security.

JEL G21, K22, K24

1. Uvod

Sodobna družba je v svojem delovanju vedno bolj izpostavljena kompleksnim varnostnim grožnjam, ki jih je nemogoče reševati z ločenimi procesi in ukrepi. Če v ta okvir dodamo, da se fizično okolje vedno bolj prepleta z digitalnim in sta le ta med seboj v vedno večji soodvisnosti, potem nam hitro postane jasno, da samo procesi kibernetske varnosti niso več zadostni za učinkovito obvladovanje tveganj, katerim so izpostavljene naše organizacije in uporabniki. Eden od posebej izpostavljenih je bančni sektor, saj je obseg sprememb in prehoda v uporabo digitalno podprtih storitev zelo obsežen. V tem delu pa se hitro soočimo s potrebo po kompleksni vseobsegajoči rešitvi, ki v proces zagotavljanja varnosti in neprekinjenega delovanja vključuje tako strokovnjake iz bančnega sistema kakor tudi uporabnike bančnih storitev ter nenazadnje tudi celotno dobavno verigo, ki je ključna za zagotavljanje te varnosti in neprekinjenosti delovanja. Realni izzivi kompleksnosti varnostnega okolja so potisnili tudi strateško odločevalno raven v smer integralnih postopkov, ki jih lahko razumemo že na ravni zakonodajnih rešitev, saj imamo na ravni EU kar nekaj pomembnih direktiv. Naj navedemo samo nekatere; NIS-2[1], CER[2] in DORA[3], ki jih je nemogoče gledati zgolj s posameznih perspektiv, temveč jih je treba razumeti kot celoto. Ti modeli se morajo sedaj dokončno uveljaviti tudi v nacionalnih aktih, v končni posledici pa se morajo integrirati v procese naših organizacij, katere so odgovorne za neprekinjeno zagotavljanje storitev, ki so ključne za normalno funkcioniranje širše družbene skupnosti in uporabnikov kot končnega deležnika v tem pomembnem ekosistemu. Kljub temu, da ves čas govorimo o dveh sicer ločenih domenah, in sicer fizični in digitalni, ki pa sta posebej povezani skozi vidik človeškega dejavnika, ta pa žal še vedno predstavlja najšibkejši člen naših varnostnih sistemov.

Žal se v praksi še vedno prevečkrat znajdemo v objemu silosnih rešitev, ki pa so že preživet koncept. Je pa ob tem treba jasno poudariti, da so kljub dokazani neučinkovitosti določeni organizacijski vzorci tako močno zakoreninjeni, da jih je nemogoče spremeniti v kratkem časovnem obdobju. Težava, ki pri tem nastaja, je, da je dinamika v sodobnem varnostnem okolju tako izrazita, da imajo organizacije zaradi neučinkovitih načinov upravljanja in obvladovanja celega niza tveganj resne probleme pri svojem poslovanju. To ni samo ugotovitev, ki je posebna

* Matic Čaleta, Certificirani etični heker, ICS Ljubljana, matic.caleta@ics-institut.si
Izr. prof. dr. Denis Čaleta, predsednik Sveta ICS-Ljubljana, denis.caleta@ics-institut.si

[1] NIS-2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).

[2] Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities

[3] REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011

za Republiko Slovenijo (Čaleta in drugi, 2022), temveč te vzorce opažamo tudi pri velikih multinacionalnih podjetjih, ki so zaradi različnih vplivnih dejavnikov vedno bolj zbirokratizirani aparati, ki predvsem zaradi zasledovanja dobička zanemarjajo osnovne postulate zagotavljanja varnosti. Tukaj izpostavljamo resne izzive, ki nastajajo v sistemu upravljanja organizacij in razmerja med lastniki in upravljalci oz. strateškem vodstvu v organizacijah. Vendar je to druga obširna vplivna tema, ki sama potrebuje poseben prispevek (Čaleta, 2022).

Zaradi navedenih izzivov bomo v pričujočem prispevku posebej prikazali pomen razumevanja korporativne varnosti kot ene izmed ključnih dejavnosti znotraj organizacij, v katero bi morale organizacije integrirati cel niz povezanih procesov ter tako doseči ustrezno racionalizacijo porabe virov, povečanja učinkovitosti koordinacije in doseganje ustreznih rezultatov, ki se kažejo v hitrejši prilagodljivosti na vse negativne varnostne pojave, s katerimi se v dinamičnem poslovnem okolju soočajo naše organizacije.

Vsekakor sodi v ta organizacijski okvir tudi proces zagotavljanja informacijske in še ožje kibernetske varnosti. To tezo bomo v nadaljevanju tudi podrobno predstavili. V zadnjem delu prispevka bomo izpostavili še nekatere ključne izzive, s katerimi se bomo na področju kibernetske varnosti morali soočiti, da bomo zagotovili učinkovito obvladovanje le teh.

2. Terminološka opredelitev

Terminologija je temeljna za enovitost razumevanja problemov in izzivov, s katerimi se soočamo v naši družbi. Na tem področju se pojavljajo primarne težave, ki se kasneje kažejo v pomembnih nedoslednostih razumevanja osnovnih problemov in seveda pri iskanju ustreznih rešitev za pojav tako kompleksnih groženj, kot jih prinaša informacijsko okolje.

Problem je večplasten in bi ga generalno lahko opredelili v naslednjih glavnih negativnih dejavnikih. Najprej gre za neustreznost razumevanja in prevodov tuje strokovne terminologije v slovenski jezik. Na eni strani za določene izraze ninamo ustreznih slovenskih terminov, na drugi strani pa, zaradi vedno večje povezanosti v mednarodno okolje, nekateri termini pridobivajo mednarodno naravo in so v svojem izvornem pomenu bolj jasno razumljeni v strokovni javnosti. Večja težava od tega se seveda pojavlja pri napačnem razumevanju posameznih terminov. Verjetno največkrat pomensko zamenjana pojma sta informacijska varnost (information security) in kibernetska varnost (cyber security). V realnem okolju se ta dva termina upravljata z napačnim razumevanjem obsega procesov in kasnejših ukrepov, kar za seboj potegne tudi cel niz težav realnega reševanja problemov, ki jih prinašajo tveganja v teh dveh okoljih. Zaradi navedenega bomo na tem mestu podali nekatere najbolj opredeljujoče terminološke pojasnitve obeh pojmov. Za to pojasnitev bomo uporabili veljavni zakon o informacijski varnosti (ZInf-1), ki sedaj tudi pravno determinira potrebo po pravilnem razumevanje razlik med temi termini. »*Informacijsko okolje*« je namreč skupek družbenih omrežij in kibernetskega prostora, vključno z informacijami. »*Informacijska varnost*« je zaščita, varovanje in obramba informacijskega okolja pred nedovoljenim dostopom, uporabo, razkritjem, motenjem, spreminjanjem ali uničenjem, z namenom zagotavljanja zaupnosti, avtentičnosti, celovitosti in razpoložljivosti.

»*Kibernetski prostor*« je globalno informacijsko okolje, ustvarjeno s pomočjo elektronskih komunikacijskih omrežij in informacijskih sistemov. Kibernetski prostor omogoča nastanek, obdelavo in izmenjavo informacij. »*Kibernetska varnost*« je sposobnost zaščititi, varovati in braniti kibernetski prostor pred kibernetskimi grožnjami, incidenti in kibernetskimi napadi.

Na prvi pogled bi rekli, da gre za zelo sorodna, če ne kar identična pojma, vendar ob podrobnem pregledu vidimo, da gre v primeru informacijske varnosti za mnogo širši obseg, iz katerega sledi tudi širši obseg nalog. Torej velika večina aktivnosti, ki jih v okviru svojih organizacij izvajamo na področju zagotavljanja varnosti informacij in informacijskih sistemov, sodi v širši okvir informacijske varnosti in samo ožji del v okvir kibernetske varnosti. Nasploh sodijo aktivnosti, ki so povezane s področjem usposabljanja in širšega ozaveščanja zaposlenih in naših komitentov, v okvir informacijske in ne kibernetske varnosti, kot imamo velikokrat priložnost videti v našem realnem organizacijskem in tudi medijskem okolju.

Za konec pa si oglejmo še terminološko opredelitev »*korporativne varnosti*«, ki jo v najširšem pomenu besede opredeljujemo kot dejavnost, ki identificira in izvaja vse potrebne sistemske ukrepe za obvladovanje varnostnih tveganj v posameznem podjetju. Kot taka predstavlja eno od osnovnih funkcij za delovanje podjetja in se za njegovo učinkovito delovanje nujno izvaja v tesnem sodelovanju z vsemi drugimi ključnimi funkcijami v podjetju. Celovito področje korporativne varnosti, za ustrezno obvladovanje varnostnih tveganj v korporaciji, nujno vključuje področje varnosti, procese neprekinjenega poslovanja, risk managementa, informacijske varnosti, varovanja ključnih informacij podjetja, varnosti zaposlenih in varnosti pri delu. Procesi zagotavljanja korporativne varnosti so nedeljiva celota krovnega modela upravljanja korporacij, ki se izraža s korporativnim upravljanjem in korporativno družbeno odgovornostjo. Predvsem slednja postavlja korporativno varnost kot proces v širši okvir delovanja v

razmerju korporacije do družbe kot celote v okolju, kjer le ta deluje. Korporativna varnost je zaradi svoje kompleksnosti in umeščenosti v širok spekter raznovrstnih procesov delovanja organizacij še bolj odvisna od uvajanja vedno novih spoznanj. (Čaleta,2018: 5-8)
Korporativna varnost se nanaša na ukrepe, ki jih izvaja organizacija za zaščito fizičnega, finančnega, intelektualnega in človeškega premoženja pred različnimi grožnjami. Ta tveganja lahko vključujejo krajo, goljufijo, kibernetske napade, naravne nesreče, teroristične napade in druge potencialne nevarnosti (Burge, 2023:1).
Korporativno varnost razumemo tudi kot uporabo zaščitnih ukrepov in strateškega načrtovanja v podjetjih, da zagotovijo varnost in celovitost svojih sredstev, osebja, informacij in celotnega delovanja. Ta večplastna disciplina ni omejena na fizične prostore, ampak se razteza v digitalno sfero, pri čemer priznava vse večji pomen kibernetske varnosti. (Burge, 2024:2)
Razumevanje zgoraj navedenih terminoloških opredelitev bo pomembno za razumevanje naslednjih delov prispevka.

3. Procesi in vloga korporativne varnosti

Funkcija korporativne varnosti uporablja za zagotavljanje svojega delovanja ljudi, procese in tehnologijo za zaščito organizacije pred negativnimi dogodki in situacijami. Korporativna varnost prepoznava, spremlja in odvrača notranje in zunanje grožnje osebju, lastnini in sredstvom organizacije ter obvladuje fizične krize, ko se le te pojavijo. Ocenjuje tudi tveganja za organizacijo, jih posreduje vodilnim in vodstvu ter jih ustrezno obvladuje.
Ni neobičajno, da se nekatere odgovornosti funkcije korporativne varnosti delijo z drugimi oddelki. Medtem ko sodijo na primer tveganja za varnost informacij in informacijskih sistemov v nekaterih organizacijah pod okrilje službe za korporativno varnost, jih v drugih pogosto organizacijsko upravljajo ločeno. V vsakem primeru pa je treba zagotoviti razumevanje skupnega delovanja funkcije kibernetske varnosti ali varnosti informacij skupaj s korporativno varnostjo znotraj korporacije. Medtem ko sodita neprekinjenost poslovanja in odpornost pogosto pod okrilje korporativne varnost, je lahko v nekaterih organizacijah informacijska varnost organizirana ločeno od funkcije korporativne varnosti. V vsakem primeru pričakujemo, da je delovanje usklajeno. (SEC, 2024)
Z gotovostjo lahko ugotovimo, da so varnostne krize in drugi varnostno izpostavljeni dogodki, ki si kar po tekočem traku sledijo v 21. stoletju, korporativni varnosti zagotovili ustrezno organizacijsko mesto v vsaki resni organizaciji. To pomeni umeščenost te dejavnosti v neposredno bližino strateškega nivoja vodenja, saj le ta predstavlja pomembno orodje v procesu obvladovanja raznovrstnih tveganj, katerim so izpostavljene organizacije v tem kompleksnem mednarodnem okolju. V praksi je, kot je zgoraj navedeno, še vedno zaznati določene variante oblikovanja služb korporativne varnosti in predvsem umeščenosti informacijske in ožje kibernetske varnosti v okvir zagotavljanja procesov korporativne varnosti. Temu smo priče tudi v bančnem sektorju. Lahko sicer ugotovimo, da se je informacijska varnost dokončno umaknila in ločila od služb informatike in informacijske podpore, s čimer smo zagotovili potrebno ločenost, da izvajalci pri izvajanju informacijske varnosti ne nadzirajo samih sebe. Seveda je predvsem v tistih organizacijskih sredinah, kjer sta informacijska varnost in vodja informacijske varnosti (CISO) ločena v svoj segment, zaznati določene izzive vezane na koordinacijo potrebnih ukrepov pri zagotavljanju celovitega načina obvladovanja tveganj. Žal tukaj vse prevečkrat opažamo ponovno vzpostavitev novih oblik silosnih rešitev in zmanjšanje potrebne koordinacijske vloge enovitega upravljanja zahtevnih postopov za zagotavljanje korporativne varnosti. V praski najdemo tudi izraz, ki celovite postopke korporativne varnosti opredeljuje kot integralno varnost (Vršec, 1993). V vsakem primeru na žalost uspešnost preprečevanja vedno bolj kompleksnih tveganj, ki se izražajo v hibridnih pojavnih oblikah, v organizacijah vzpostavljamo entropijo in zgubljamo že tako zelo omejene vire.
Tudi v bančnem sektorju so organizacije zaznale pomanjkljivosti take organiziranosti, zato smo soočeni z oblikovanjem teh procesov v skupno organizacijsko obliko, imenovano proces korporativne varnosti. Katere dejavnosti in procesi so združeni v celovito (integralno) obliko zagotavljanja korporativne varnosti, smo predstavili že v poglavju o terminološki opredelitvi ključnih procesov. Kar želimo v tem delu posebej izpostaviti, pa so izzivi, ki se kažejo pri uveljavljanju in zagotavljanju korporativne varnosti in so povezani z ustreznim kompetenčnim modelom strokovnjakov, ki zagotavljajo aktivnosti v tem okviru.
Izraženi izzivi in ugotovitve, ki jih že vrsto let spremljamo v okviru Instituta za korporativne varnostne študije, so naslednji:

- Izredne izzive predstavljajo kompetenčni okviri strokovnjakov, ki vodijo službe korporativne varnosti (CSO). Tisti, ki prihajajo iz bolj tradicionalnih varnostnih institucij in okolij ter bolj razumejo zagotavljanje varnosti v fizičnem okolju, imajo izredno velike izzive pri razumevanju in integriranju varnosti informacijskih in še posebej kibernetskih okolij v celotno dejavnost. To lahko

v organizacijah brez zavedanja o teh izzivih povzroči, da so procesi in ukrepi zagotavljanja informacijske varnosti neustrezni in so zato organizacije izpostavljene dodatnim tveganjem na tem področju. Na drugi strani pa vodstveni kader v teh službah ob prihodu iz kompetenčnih okvirov informacijske varnosti ne razume pomembnosti fizičnega okolja in s tem povezanih specifičnih dejavnosti.

- Trenutno so ustrezni izobraževalni programi še v fazi oblikovanja, tako da lahko ustrezen kompetenčni kader na tem področju šele pričakujemo. Seveda pa se tukaj pojavlja cel niz težav. Od tega, da država ne prepozna potrebe po koncesioniranju teh kompleksnih študijskih vsebin in so le te obsojene na vzpostavitev v okviru zasebnih izobraževalnih institucij, ki pa ne premorejo dovolj kadrovskih in drugih virov za učinkovito izvedbo izobraževanja (Čaleta, 2019:30-31).
- Naslednje zaskrbljujoče dejstvo pa je, da mlajše generacije ne prepoznavajo v tej profesiji priložnosti za graditev uspešnih kariernih priložnosti. To pomeni, da tudi niso pripravljene vložiti dodatnih finančnih vložkov v svoje izobraževanje in izpopolnjevanje, kar kadrovski bazen močno siromaši. Sploh je to pomembno glede na vedno večje kadrovske potrebe v tej dejavnosti.
- V nekaterih organizacijskih okoljih so procesi upravljanja s tveganji izločeni iz okvira korporativne varnosti. To pomeni, da so tveganja preširoko opredeljena in ocenjena samo na strateški ravni. Izpostavljanje pomembnosti je pomanjkljivo, kar pomeni, da so tudi ukrepi za upravljanje teh tveganj nerealno in precej birokratsko zasnovani. Primer, kjer je ta proces v okviru upravljanja procesa korporativne varnosti, so tveganja, tudi tista strateška, bolj realno zasnovana in upravljana.
- Kljub hitremu tehnološkemu razvoju človek ostaja tisti segment, ki ima v procesu obvladovanja varnostnih tveganj ključno vlogo. V večini primerov še vedno predstavlja tisti najšibkejši člen v celovitem sistemskem zagotavljanju kibernetske varnosti. Odtekanje ključnih poslovnih informacij in poslovnih tajnosti ter s tem povezani socialni inženiring, malomarnost, nizka organizacijska in varnostna kultura, neizobraženost in namerno izvajanje protizakonitih aktivnosti so tisti dejavniki, ki silijo podjetja k učinkovitejšemu izvajanju ukrepov korporativne varnosti, povezane z nadzorom zaposlenih v njihovih osnovnih delovnih okoljih.
- Naslednji pomemben dejavnik, na katerega moramo biti še posebej pozorni pri zagotavljanju korporativne varnosti, so zunanji izvajalci in pogodbeni partnerji. V zadnjem obdobju se podjetja namreč vedno bolj poslužujejo prenosa določenih procesov na zunanje pogodbene izvajalce. Pri prvi kalkulaciji se lahko ta oblika zmanjšanja stroškov delovanja podjetja zdi zelo vabljiva, vendar je treba na proces oddajanja ključnih funkcij gledati tudi z drugačnega zornega kota, saj za delovanje podjetja lahko prinese zelo velika tveganja, katerih pa se pogosto lastniki in menedžment ne zavedajo. V zadnjem obdobju se je predvsem pri večjih organizacijskih okoljih ta trend bistveno obrnil v smer organiziranja lastnih zmogljivosti.

4. Kibernetska varnost in njena umeščenost v korporativno varnost

Sodobna podjetja se soočajo z vedno bolj zapletenimi grožnjami v digitalnem okolju, kar jih prisili, da kibernetsko varnost postavijo v središče svojih celovitih varnostnih politik. Tradicionalno je bila kibernetska varnost pogosto ločena od drugih področij korporativne varnosti, vendar so podjetja z naprednimi tehnološkimi rešitvami ugotovila, da to ni več izvedljivo. Integracija tehničnih in operativnih varnostnih ukrepov je ključnega pomena za gradnjo robustne obrambe pred nenehno evolucijo kibernetskih groženj. Povezovanje fizične, pravne in digitalne varnosti omogoča boljšo koordinacijo znotraj organizacije, kar zmanjšuje možnosti za neodkrita tveganja in ranljivosti. Tako lahko podjetje hitro in učinkovito reagira na incident, pri čemer je ključno, da vse enote podjetja razumejo svojo vlogo v tem procesu, od upravljanja tveganj do varovanja ključnih podatkov. Pri integraciji kibernetske varnosti v varnostne politike je bistveno, da se podjetje osredotoči na razumevanje specifičnih tveganj, s katerimi se sooča. Globalizacija poslovnih procesov in digitalna preobrazba ustvarjata številna področja ranljivosti, kar pomeni, da splošna varnostna politika ne more biti statična, temveč mora biti prilagodljiva in odzivna na spremembe v poslovnem in tehnološkem okolju.

Medtem ko je tehnični del varnosti pogosto v rokah IT-strokovnjakov, mora biti vodenje podjetja tisto, ki zagotovi jasno usmeritev in podpira oblikovanje ter izvajanje celovite kibernetske strategije. Vodstvo igra ključno vlogo pri zagotavljanju ustreznih virov, od finančnih do kadrovskih, saj brez te podpore niti najboljše varnostne rešitve ne morejo učinkovito delovati. Ključnega pomena je, da vodstveni kader razume širši kontekst kibernetskih groženj ter njihov vpliv na poslovne operacije, kar vključuje vse od izgube podatkov do prekinitve poslovanja. Ustrezno vključevanje varnostnih strokovnjakov v odločevalne procese omogoča razvoj strategij, ki se prilagajajo hitro spreminjajočim se digitalnim grožnjam, hkrati pa ostajajo v skladu s poslovnimi cilji podjetja.

5. Glavni izzivi, kako v organizaciji zagotavljati kibernetsko varnost

Sodobna podjetja se soočajo z izzivi zaradi vedno večje kompleksnosti tehnoloških rešitev, ki vključujejo razpršena omrežja, oblačne storitve in mobilne naprave. Ta razpršenost otežuje zaščito občutljivih podatkov, ki so pogosto shranjeni na več različnih lokacijah, kar zahteva centralizirano upravljanje varnosti in skladnost z varnostnimi standardi. Poleg tega zahteva dinamično okolje groženj, kjer se napadi, kot so ribarjenje in izsiljevalska programska oprema, nenehno razvijajo, proaktivne ukrepe, kot so redni pregledi sistemov in simulacije napadov. Poleg tega pa prinaša skladnost z zakonodajo, kot je GDPR, še dodatne zahteve glede upravljanja zaupnih podatkov. Podjetja morajo vlagati v varnostne postopke, ki zagotavljajo zaščito pred kršitvami, saj lahko te zahtevajo finančne kazni in škodujejo ugledu. Kljub zavedanju o pomenu kibernetske varnosti pa se mnoga podjetja soočajo z omejenostjo virov, bodisi kadrovskih bodisi finančnih. Varnostne tehnologije in usposabljanje zaposlenih zahtevajo znatna vlaganja, vendar so dolgoročni stroški varnostnih incidentov običajno veliko višji kot preventivni ukrepi. Zato morajo podjetja kljub omejitvam dati prednost vlaganju v varnost, da zaščitijo svojo poslovno stabilnost in podatke.

5.1 Vpliv kibernetske varnosti na poslovno kontinuiteto in zaščita podatkov

Neprekinjeno poslovanje je eden ključnih ciljev vsakega uspešnega podjetja, pri čemer ima kibernetska varnost pomembno vlogo. Podjetje, ki ni pripravljeno na kibernetske napade, tvega hude motnje, kar lahko vodi v finančne izgube, zmanjšano produktivnost in izgubo zaupanja strank. ENISA(2024). Napadi, kot je izsiljevalska programska oprema, lahko hitro ohromijo poslovanje, če ni vzpostavljenih ustreznih varnostnih mehanizmov za hitro okrevanje. Poleg preprečevanja napadov se morajo podjetja osredotočiti tudi na učinkovite strategije obvladovanja posledic in vlagati v načrte za neprekinjeno poslovanje (BCP) ter obnovitvene ukrepe, ki pokrivajo vse vidike kibernetske varnosti.

Zaščita podatkov je drugo ključno področje, na katerega kibernetska varnost neposredno vpliva. Zaradi digitalizacije in obsežnega shranjevanja podatkov v oblaku je njihova varnost nujna. Zakonodaje, kot sta GDPR in druge regulative, zahtevajo strogo varovanje podatkov, saj kršitve prinašajo finančne kazni in izgubo zaupanja, kar negativno vpliva na dolgoročno uspešnost podjetja. Kibernetska varnost mora biti vključena v vse plasti poslovanja, od IT-sistemov do pravnih in upravljavskih praks.

5.2 Umetna inteligenca in tveganja

Umetna inteligenca (UI) postaja eno ključnih orodij v boju proti nenehno razvijajočim se kibernetskim grožnjam. V zadnjih letih je uporaba UI za zaznavanje in preprečevanje varnostnih napadov doživela velik razcvet, saj lahko te napredne tehnologije prepoznajo vzorce in anomalije, ki bi jih tradicionalni varnostni sistemi spregledali. Algoritmi strojnega učenja, ki temeljijo na obdelavi velikih količin podatkov, lahko hitro analizirajo promet v omrežjih in prepoznajo odstopanja, ki kažejo na potencialne napade, kot so vdor v sistem ali kraja podatkov. Na ta način UI omogoča organizacijam, da zgradijo proaktivne obrambne mehanizme, ki lahko zgodaj odkrijejo zlonamerne aktivnosti in preprečijo širše posledice.

Posebna prednost umetne inteligence je njena zmožnost neprekinjenega učenja. Medtem ko so tradicionalni varnostni sistemi pogosto omejeni na prepoznavanje vnaprej določenih groženj, lahko sistemi, ki temeljijo na UI, sproti prilagajajo svoje algoritme in se učijo iz novih napadov ter posodobljenih taktik hekerjev. Tako se umetna inteligenca nenehno razvija in postaja vedno bolj učinkovita pri preprečevanju napadov. Poleg tega UI omogoča avtomatizacijo številnih varnostnih procesov, kar močno olajša delo varnostnim ekipam, saj lahko sistemi z UI v realnem času spremljajo dogajanje v omrežju, prepoznajo grožnje in sprožijo ustrezne protiukrepe, še preden napad povzroči škodo. Kljub tem prednostim pa je pomembno poudariti, da uporaba UI za zaznavanje groženj ne more popolnoma nadomestiti človeškega nadzora. Za optimalno učinkovitost je potrebna kombinacija napredne tehnologije in strokovnega znanja varnostnih strokovnjakov, ki lahko pravilno interpretirajo rezultate in se pravočasno odzovejo. Poleg sprememb v varnostni arhitekturi pa umetna inteligenca prinaša tudi izzive na področju zasebnosti. Ker sistemi UI temeljijo na zbiranju in obdelavi velikih količin podatkov, je varovanje teh podatkov ključnega pomena za preprečevanje zlorab, kajti sistem, ki nenehno analizira podatkovne tokove in spremlja aktivnosti v omrežju, lahko posega v zasebnost posameznikov, če ni ustrezno nadzorovan. (ENISA, 2024)

5.2.1 Tveganja povezana z implementacijo umetne inteligence (deepfakes, avtomatizirani napadi)

Kljub temu, da umetna inteligenca omogoča napredne rešitve za zaznavanje groženj, pa sama predstavlja tudi nova tveganja za varnost, saj jo napadalci uporabljajo za izvedbo sofisticiranih napadov. (ENISA, 2024). Ena izmed najbolj zaskrbljujočih tehnologij, ki je povezana z UI, so tako imenovani "deepfakes" – ponarejeni video in zvočni

posnetki, ki jih je skoraj nemogoče ločiti od resničnih. S pomočjo teh tehnik lahko napadalci ustvarijo lažne posnetke, ki so videti povsem verodostojno, kar predstavlja nevarnost za integriteto informacij in zaupanje v digitalne vsebine. Deepfakes se lahko uporabijo za razne manipulacije, kot so zavajanje javnosti, izsiljevanje podjetij ali posameznikov, kar kaže na globoko vpetost UI v nove oblike napadov.
Poleg tehnologije deepfakes pa umetna inteligenca omogoča tudi avtomatizacijo napadov na obsežni ravni. Napadalci lahko uporabijo UI za ustvarjanje samodejnih programov, ki izvajajo napade brez človeškega posredovanja. Ti programi lahko v kratkem času analizirajo na tisoče tarč, iščejo ranljivosti in izvajajo napade, kar varnostnim ekipam onemogoča, da bi se hitro odzvale na vse hkrati. Dodatno tveganje pa je tudi uporaba UI za ustvarjanje prilagojenih napadov ribarjenja, kjer algoritmi zbirajo podatke o posameznikih ali podjetjih in nato ustvarjajo zelo prepričljiva sporočila, ki jih je težko prepoznati za lažna. To ustvarja veliko grožnjo, saj lahko takšni napadi dosežejo visoko stopnjo uspešnosti in pridobijo zaupne informacije neposredno od tarče. Ti primeri kažejo, da napadalci uporabljajo UI prav tako inovativno kot varnostni strokovnjaki, kar ustvarja novo dinamiko v kibernetski varnosti. Organizacije se tako soočajo z izzivom, da se branijo pred napadi, pri katerih se uporabljajo iste napredne tehnologije, kot jih same uporabljajo za zaščito.

5.3 Varnostni izzivi digitalizacije bančnega sektorja

Vedno večji obseg bančnega poslovanja se premika v virtualno okolje. S hitrim napredkom digitalizacije bančni sektor vse bolj prehaja v virtualno okolje, kjer prevladujejo spletne storitve in mobilne aplikacije. Digitalna transformacija prinaša številne prednosti, kot so večja dostopnost storitev, izboljšana uporabniška izkušnja in večja učinkovitost poslovnih procesov. Vendar pa te spremembe ustvarjajo tudi nove varnostne izzive. Bančne institucije so še posebej privlačne tarče za kibernetske napade zaradi količine in občutljivosti podatkov, ki jih obdelujejo. V zadnjih letih smo bili priče porastu napadov na finančne institucije, kjer napadalci uporabljajo sofisticirane metode, kot so ribarjenje, napadi DDoS (Distributed Denial of Service) in izsiljevalska programska oprema. Digitalizacija je spremenila tudi način, kako banke obvladujejo tveganja. Z naraščajočo uporabo oblačnih storitev in povečanjem obsega oddaljenega poslovanja se morajo banke zanašati na varnostno infrastrukturo, ki omogoča zaščito pred napadi znotraj kompleksnih in razpršenih omrežij. Poleg tega so banke pod nenehnim pritiskom regulatornih organov, ki zahtevajo skladnost z vedno bolj zapletenimi predpisi o varovanju podatkov. To predstavlja dodaten izziv, saj morajo banke vlagati v rešitve, ki ne le zagotavljajo varnost, ampak tudi omogočajo preglednost in skladnost z zakonodajo. Digitalizacija bančnega poslovanja tako prinaša stalno potrebo po nadgrajevanju varnostnih protokolov in orodij, ki morajo biti prilagojeni hitro spreminjajočemu se okolju kibernetskih groženj.

5.3.1 Naraščajoča odvisnost od spletnih storitev in mobilnih aplikacij

Z digitalno preobrazbo bančništva so spletne storitve in mobilne aplikacije postale ključni kanali, preko katerih komitenti dostopajo do bančnih storitev. Ta prehod je bil pospešen z naraščajočim povpraševanjem po priročnih in hitrih rešitvah, kjer lahko uporabniki izvajajo transakcije, preverjajo stanje na računu ali upravljajo svoje finance z nekaj dotiki na svojem pametnem telefonu. Hkrati pa ta naraščajoča odvisnost od digitalnih platform povečuje površino napadov, saj postajajo spletne platforme in mobilne aplikacije priljubljena tarča kibernetskih kriminalcev. Ranljivosti v aplikacijah, nezadostna šifriranja podatkov in slaba uporabniška praksa pri upravljanju gesel so le nekateri od dejavnikov, ki prispevajo k povečanju tveganj v digitalnem bančnem okolju.
Mobilne aplikacije, ki omogočajo takojšnje transakcije in dostop do občutljivih podatkov, morajo vključevati najnaprednejše varnostne mehanizme, kot so dvofaktorska avtentikacija, biometrična avtentikacija (npr. prstni odtis ali prepoznavanje obraza) in šifriranje komunikacije med uporabnikom in bančno infrastrukturo. Kljub temu je varnost mobilnih aplikacij odvisna tudi od uporabnikov, ki so pogosto manj ozaveščeni o varnostnih tveganjih, kot so napadi ribarjenja ali nameščanje zlonamerne programske opreme. Banke so se zato prisiljene prilagajati in zagotavljati nenehne posodobitve ter izobraževanja uporabnikov, saj je varnost odvisna tako od tehnoloških rešitev kot od pravilne uporabe teh rešitev s strani komitentov.

5.3.2 Varstvo osebnih in finančnih podatkov v virtualnem okolju

Varnost osebnih in finančnih podatkov predstavlja osrednji izziv v virtualnem bančnem okolju. S povečanjem števila uporabnikov, ki uporabljajo spletne storitve za upravljanje svojih financ, se povečuje tudi količina občutljivih podatkov, ki jih banke hranijo in obdelujejo. Ti podatki vključujejo osebne podatke strank, transakcijske zgodovine, finančna poročila in drugo pomembno dokumentacijo, ki mora biti strogo varovana. V primeru

vdora ali zlorabe teh podatkov so posledice lahko zelo resne, saj lahko kršitev zasebnosti in varstva podatkov privede do kazenskih sankcij, pravnih posledic in izgube zaupanja komitentov. Zaradi strogih zakonodaj, kot je splošna uredba o varstvu podatkov (GDPR), so banke dolžne zagotavljati, da so vsi osebni in finančni podatki zavarovani pred nepooblaščenim dostopom, zato morajo banke vzpostaviti tudi učinkovite politike varovanja podatkov, ki vključujejo nadzor dostopa do podatkovnih baz in redno preverjanje skladnosti z zakonodajo. Pomembno je, da so vse tehnološke rešitve, ki jih banke uporabljajo za obdelavo podatkov, skladne z varnostnimi standardi, ki preprečujejo zlorabe in omogočajo hitro odzivanje v primeru napadov.
Poleg varnostno-tehničnih rešitev pa je pomembno tudi izobraževanje komitentov o pravilnem ravnanju z njihovimi osebnimi podatki. Banke morajo komitente obveščati o nevarnostih, kot so napadi ribarjenja, ter jim svetovati, kako zaščititi svoje bančne račune in finančne podatke. Ozaveščeni komitenti predstavljajo prvo obrambno linijo proti kibernetskim grožnjam, saj lahko s pravilnim ravnanjem zmanjšajo možnosti za uspešne napade. Vse to poudarja, da varstvo osebnih in finančnih podatkov v virtualnem okolju ni le odgovornost banke, temveč tudi njenih komitentov, kar zahteva stalno sodelovanje med obema stranema.

5.4 Izobraževanje zaposlenih in komitentov

Eden ključnih vidikov kibernetske varnosti je ozaveščanje zaposlenih o možnih grožnjah. Čeprav podjetja pogosto vlagajo v tehnične rešitve, je človeški dejavnik še vedno najpogostejši vir varnostnih incidentov. Napadi, kot so ribarjenje, socialni inženiring ter zlonamerna programska oprema, pogosto ciljajo neposredno na zaposlene. Z napačnim klikom na povezavo ali šibkimi gesli lahko pride do vdora v celoten sistem podjetja. Zato je ključno, da organizacije vzpostavijo redne programe izobraževanja, kjer zaposleni spoznajo, kako prepoznati sumljiva sporočila, kako uporabljati močna gesla in ohranjati varnost tudi na fizični ravni.
Poleg ozaveščanja je enako pomembno tudi praktično usposabljanje. Redne simulacije varnostnih incidentov, kot so napadi ribarjenja in napadi z izsiljevalsko programsko opremo, zaposlenim omogočajo, da se v varnem okolju naučijo pravilno reagirati na te situacije. S tem ne samo krepijo svoje znanje, ampak podjetje tudi preveri učinkovitost obstoječih varnostnih protokolov in ugotovi, kje so potrebne izboljšave. Tako podjetja postanejo bolj pripravljena na resnične varnostne grožnje in lahko hitreje in bolj učinkovito ukrepajo.

Vzpostavitev močne varnostne kulture je prav tako ključnega pomena za dolgoročno odpornost organizacije proti kibernetskim napadom. (ENISA, 2022) Zaposleni morajo biti spodbujeni, da kadar opazijo nenavadno aktivnost, kot je klik na phishing povezavo ali zaznavanje zlonamerne programske opreme na napravi, o tem čim prej obvestijo odgovorne osebe. Ključno je, da zaposleni ne občutijo strahu ali zadržkov pred tem, da bi prijavili napako, saj je hitra reakcija ključna za omejevanje škode in preprečevanje večjih težav. Z gradnjo takšne varnostne kulture, kjer so vsi člani podjetja proaktivno vključeni v varnostne procese, podjetje ne le krepi zaščito svojih podatkov in sistemov, temveč se dolgoročno postavi v boljšo pozicijo za obrambo pred nenehno spreminjajočimi se kibernetskimi grožnjami.

6. Sklepne misli

Sodobna organizacijska okolja, še posebej v bančnem sektorju, se soočajo z vse bolj kompleksnimi in raznolikimi varnostnimi grožnjami, ki zahtevajo celovite in strateške rešitve. Razumevanje korporativne varnosti kot širokega koncepta, ki zajema tako fizične kot digitalne varnostne vidike, je ključno za uspešno obvladovanje tveganj. Integracija informacijske in ožje kibernetske varnosti v širše varnostne strategije ni več opcija, temveč nuja. Organizacije, ki zanemarjajo to potrebo, tvegajo ne le finančne izgube, temveč tudi dolgoročno erozijo zaupanja strank in partnerjev. Človeški dejavnik ostaja osrednji izziv, saj ne glede na tehnološke inovacije, kot je umetna inteligenca, še vedno predstavlja najšibkejši člen varnostnih sistemov. Usposabljanje in ozaveščanje zaposlenih ter komitentov morata postati stalnica v vsaki varnostni politiki. Poleg tega je ključno, da se na vodstvenih ravneh zavedajo pomembnosti kompetenčnih okvirov strokovnjakov, ki vodijo procese korporativne in kibernetske varnosti. Bančni sektor, kot eden izmed najbolj izpostavljenih, mora nenehno vlagati v napredne varnostne rešitve in se prilagajati hitro spreminjajočemu se okolju kibernetskih groženj. Digitalizacija prinaša številne prednosti, vendar brez ustreznih varnostnih mehanizmov ne moremo zagotoviti neprekinjenega poslovanja in zaščite podatkov. V prihodnje bo ključno najti ravnovesje med tehnološkimi rešitvami in človeško komponento, saj bo le tako možno zagotoviti celovito varnost v dinamičnem poslovnem okolju.

Viri in literatura / References:

- Burge Simon (2023). What is Corporate Security? International Security Jurnals https://internationalsecurityjournal.com/what-is-corporate-security/

- Burge Simon (2024). What is Corporate Security? Security Jurnal Americas https://securityjournalamericas.com/corporate-security/
- Čaleta Denis (2018). Korporativna varnost je še v iskanju ustreznega mesta v poslovnem okolju. Revija Korporativna varnost, št 17. letnik 2018, strani 5-8.
- Čaleta Denis (2019) ocenjevanje tveganj v kritični infrastrukturi – vpliv izobraževalnega procesa na kvaliteto izvedbe, št.18, letnik 2018, strani 30-34
- Denis Čaleta (2022). Kriza je postala realnost našega operativnega okolja Revija Korporativna varnost, št 30. letnik 2022, strani 16-18.
- Čaleta Denis, Bertoncelj Brane, Kandžič, Aljoša, Podgoršek Žiga, Čaleta Eva, Čaleta Matic (2022). Analiza potencialov kibernetske varnosti v Republiki Sloveniji. Študija izvedena za URSIV.
- 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
- Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities
- ENISA (2024). Cyber Insurance - Models and methods and the use of AI. https://www.enisa.europa.eu/publications/cyber-insurance-models-and-methods-and-the-use-of-ai
- ENISA (2022). Cybersecurity Education Initiatives in the EU Member States. https://www.enisa.europa.eu/publications/cybersecurity-education-initiatives-in-the-eu-member-states
- ENISA (2024). Best Practices for Cyber Crisis Management. https://www.enisa.europa.eu/publications/best-practices-for-cyber-crisis-management
- NIS-2 Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive).
- 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
- REGULATION (EU) 2022/2554 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 14 December 2022 on digital operational resilience for the financial sector and amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011.
- Security Executive Council (2024) What Is Corporate Security? https://www.securityexecutivecouncil.com/?utm_source=insWhatIsCorpSecPpr&utm_medium=PDF&utm_campaign=insWhatIsCorpSec
- Vršec Milan (1993). Varnost podjetja – tokrat drugače. Viharnik : Ljubljana
- Zakon o informacijski varnostni (ZInfV) Uradni list RS, št. 30/18, 95/21, 130/22 – ZEKom-2, 18/23 – ZDU-1O in 49/23.

UDK 004.056:658:343.9

Zahteve NIS 2: prilagoditev poslovnih procesov za izboljšanje kibernetske odpornosti

*Igor Mlakar**

NIS 2 REQUIREMENTS: ADAPTING BUSINESS PROCESSES TO ENHANCE CYBER RESILIENCE

The article will explore how organizations can adapt to the NIS 2 Directive (Network and Information Systems Directive 2), introduced to enhance cyber resilience within the EU members. The focus will be on the impact of NIS 2 requirements on existing processes within organizations and what changes or improvements are necessary to achieve compliance with this legislation.

The article will provide readers a clear and practical guidelines for successfully adapting business processes in line with NIS 2 requirements and related legislation, with the goal of improving organizations' cyber resilience.

JEL K22, K24

Namesto uvoda – Trenutno stanje in trendi kibernetske varnosti

Razvoj informacijskih tehnologij prispeva k izjemnemu razvoju na številnih področjih družbenega in gospodarskega življenja. Organizacijam pomaga krepiti inovativnost in produktivnost, uvajanje novih informacijskih tehnologij pa vse bolj predstavlja osnovni dejavnik konkurenčnosti poslovanja. Digitalna transformacija omogoča organizacijam, da hitreje in učinkoviteje zadostijo potrebam trga ter odpirajo nove priložnosti za rast in razvoj. Napredne tehnologije so korenito spremenile načine komuniciranja in poslovanja med podjetji, njihovimi dobavitelji in strankami. Enako velja za posameznika, katerega vse večji del osebnega in družbenega udejstvovanja je tesno prepleten z uporabo in obvladovanjem sodobnih informacijskih tehnologij. Posledično narašča pomen kibernetske varnosti, kar zahteva vse večjo pozornost vseh deležnikov v organizacijah – od ključnih strokovnih kadrov, poslovodstev in odločevalcev do zaposlenih, partnerjev, strank in regulatorjev.

Trenutno stanje kibernetske varnosti v Evropski uniji (EU) in globalno zaznamuje hiter napredek tehnoloških inovacij, ki poleg prednosti prinaša tudi nove izzive na področju kibernetskih groženj. Razširjena uporaba oblačnih storitev, umetne inteligence in interneta stvari (IoT) ustvarja nove priložnosti za napade, ki postajajo vse bolj sofisticirani in organizirani. Kibernetski napadi, kot so izsiljevalska programska oprema in napadi na dobavne verige, so postali pogostejši in bolj uničujoči, kar ogroža ključno infrastrukturo. To ne vpliva zgolj na posamezne organizacije, pač pa ima lahko katastrofalen vpliv na celotne panoge, regije in nacionalno varnost.

Konkreten primer nedavnega kibernetskega napada, ki izpostavlja pomembnost kibernetske varnosti, je napad preko programske opreme podjetja SolarWinds (TechTarget, 2023). Ta napad je prizadel več kot 30.000 javnih in zasebnih organizacij po vsem svetu, vključno s podjetji in vladnimi agencijami. Incident je razkril potrebo po okrepljeni varnosti in boljši koordinaciji mednarodnih prizadevanj za zaščito pred kibernetskimi grožnjami. Napadalci, ki jih je domnevno podprla Rusija, čeprav ta to vztrajno zanika, so prevzeli nadzor nad programskim orodjem Orion proizvajalca SolarWinds, ki se uporablja za nadzor zmogljivosti sistemov IT. V programsko kodo Oriona so napadalci vnesli zlonamerno programsko kodo, ki je ustvarila t. i. stranska vrata (ang. Backdoor Malware), kar jim je omogočilo neavtoriziran dostop do sistemov, ki jih orodje nadzira. Prizadete niso

* Igor Mlakar, mag. med. posl., direktor operative, igor.mlakar@smart.com.si, Smart Com d.o.o.

bile le stranke podjetja SolarWinds, temveč tudi njihovi partnerji, saj so hekerji pridobili dostop do podatkov in omrežij znotraj napadenih sistemov. Možnosti za nadaljnje izkoriščanje te podtaknjene programske kode so se tako eksponentno povečale. Napadalci so pridobili neavtoriziran dostop do omrežja SolarWinds že septembra 2019, marca 2020 pa je napadeno podjetje nevede začelo razpošiljati okuženo različico izdelka Orion svojim strankam. Informacija o vdoru je bila razkrita šele konec leta 2020, posledice napada pa tudi konec leta 2023 še niso bile v celoti odpravljene. Preiskovalci so morali pregledati ogromne količine podatkov, številne napadene organizacije pa tudi še niso uspele zagotoviti, da bi bila vsa stranska vrata odkrita in odstranjena. Različico iste škodljive programske kode in metodo napada naj bi zlorabile tudi druge skupine napadalcev. V istem obdobju je tako skupina, ki izhaja s Kitajske, izvedla napad na zvezno agencijo za obračun plač znotraj Ministrstva za kmetijstvo ZDA (National Finance Center, okr. NFC). Potencialno so bili ogroženi podatki o plačah več kot 600.000 zveznih uslužbencev, vendar obseg dejansko ukradenih podatkov ostaja nerazkrit (Bing *idr.,* 2021).

Napad še vedno velja za enega največjih napadov na dobavno verigo ter zelo dober primer pomembnosti nadzora nad dobavitelji storitev in sistemov IT za zagotavljanje varnosti poslovanja.

Opisani primer nikakor ni osamljen, je pa pomemben kazalnik, kako povezano in ranljivo je postalo svetovno gospodarstvo. To dokazuje tudi incident s programsko opremo za kibernetsko varnost proizvajalca CrowdStrike, ki je julija letos zaradi napake v novi različici programske opreme povzročil večji izpad prek 8 milijonov računalniških sistemov po vsem svetu. Prizadeta so bila številna proizvodna podjetja, vladne institucije, energetski sektor, letališča, hoteli, bolnišnice, banke, borze in druge finančne ustanove. V tem primeru ni šlo za kibernetski napad, pač pa je incident povzročila človeška napaka, pomanjkljiv nadzor pri proizvajalcu programske opreme in prevelika soodvisnost kritične infrastrukture. Ponuja se sklep, da vsaj nekateri upravljavci prizadete infrastrukture niso primerno obvladovali tveganj povezanih z dobavno verigo oz. z izvajalci kritičnih storitev IT. Seveda je pri oceni treba dopustiti možnost, da so posamezni upravljavci tveganje ustrezno obravnavali in je bil izpad znotraj dopustnih možnosti za obnovitev sistemov.

Obseg napadov na zaupnost, celovitost in dostopnost podatkov (ang. Confidentiality, Integrity and Availability), vse bolj pa tudi na pristnost podatkov (ang. Authenticity), je že na evropski ravni težko dojemljiv. Zgolj v znanih, javno razkritih incidentih, ki se jih je v obdobju od novembra 2023 do časa priprave tega članka zgodilo že 905, je prišlo do zlorabe več kot 2,5 milijarde zapisov (IT Governance Europe, 2024). Največ zlorab je bilo zabeleženih v javnem sektorju in zdravstvu, po obsegu zapisov pa je takoj za javnim sektorjem področje storitev IT. Pri tem je pomembno vedeti, da javno razkriti incidenti predstavljajo le manjši del vseh zlorab. Velik del napadov ostane prikrit, mnogi uspešni napadi pa sploh niso oz. še niso prepoznani. Napadalci pogosto poskušajo ostati neodkriti in uporabljajo okuženo infrastrukturo kot odskočno desko za pomembnejše napade.

V EU se s temi izzivi soočamo s krepitvijo regulativnega okvira, pri čemer ima ključni pomen uvajanje standardov, certificiranje in povečanje ozaveščenosti o kibernetskih tveganjih. Posledično se povečuje potreba, da kibernetsko varnost obravnavamo kot prednostno nalogo tako regulatorjev kot poslovodstev v organizacijah. Uspeh poslovanja in celo obstoj organizacij je vse bolj odvisen od uspešno uvedenih politik in sistemov za obvladovanje kibernetskih tveganj. Kot smo videli iz primerov, lahko tveganja hitro presežejo meje posamezne organizacije in postanejo grožnja na ravni celotne panoge, družbenih sistemov, nacionalne varnosti in celo globalne ekonomije.

Julija 2016 je bila sprejeta prva različica Direktive o varnosti omrežij in informacijskih sistemov (ang. Network and Information Systems Directive, okr. NIS). Ta direktiva je uvedla vrsto regulativnih ukrepov za povišanje kibernetske odpornosti organizacij v EU. Osredotočila se je na krepitev zmogljivosti kibernetske varnosti na nacionalni ravni, izboljšanje sodelovanja med državami članicami EU in vključevanje kibernetske varnosti v jedro organizacij. Organizacije, ki so morale zagotoviti skladnost z direktivo NIS, so bili operaterji bistvenih storitev (ang. Operators of Essential Services, okr. OES) in pomembni ponudniki digitalnih storitev (ang. Digital Service Providers, okr. DSP). Prvotna direktiva NIS je sprožila spremembo miselnosti znotraj institucionalne in regulativne obravnave kibernetske varnosti. Kljub temu pa se je soočala z nekaterimi izzivi, na katere obstoječa zakonodaja ni imela ustreznih odgovorov. To je povzročilo razdrobljeno obravnavo na ravni držav članic EU. V zadnjih letih so okoliščine, vključno z naglim tehnološkim razvojem, napredkom kibernetskega vojskovanja, pandemijo koronavirusne bolezni covid-19 ter rusko-ukrajinskim vojaškim konfliktom, močno spremenile digitalno okolje. Ti dejavniki so vplivali na povečanje varnostnih groženj in posledično na naraščanje kibernetskih napadov, usmerjenih proti organizacijam in državam članicam EU.

Januarja 2023 je EU sprejela drugo različico Direktive o varnosti omrežij in informacij o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, in sicer direktivo (EU) 2022/2555, znano kot NIS 2 (Uradni list Evropske unije, 2022). Osnovni namen direktive je izboljšati zaščito enotnega evropskega trga in prispevati k pospešitvi prizadevanj za vzpostavljanje višje ravni kibernetske varnosti in odpornosti organizacij v EU.

Kratek pregled direktive NIS 2: ključne zahteve in cilji za izboljšanje kibernetske odpornosti

Države članice EU bodo morale direktivo NIS 2 prenesti v svojo nacionalno zakonodajo do 17. oktobra 2024. V Sloveniji bomo to storili z novim Zakonom o informacijski varnosti (ZInfV-1), o katerem je že potekla javna razprava in je od 15. 5. 2024 v fazi medresorskega usklajevanja (eUprava, 2024). Namen zakona je, da organizacije od njegove uveljavitve v najkrajšem možnem času, vendar ne več kot v šestih mesecih, vzpostavijo ustrezne mehanizme za celovito izpopolnjevanje regulativnih zahtev, kot predlaga trenutna različica zakona.

Organizacije se morajo že sedaj pripravljati, da bodo zagotovile skladnost z direktivo.

NIS 2 bistveno širi obseg zavezancev in uvaja samoprepoznavo kot mehanizem za določanje zavezancev, ki bodo po novem postali bistveni ali pomembni subjekti. Če se organizacija ne prepozna kot zavezanec, to ne pomeni, da njeno poslovodstvo ni odgovorno za skladnost poslovanja. Organizacije se namreč ne bodo izognile visokim kaznim v primeru, da bi zaradi nespoštovanja, opustitve ali izogibanja predpisanim ukrepom predstavljale grožnjo lastnemu poslovanju ali okolju, v katerem poslujejo.

Kaznovalna politika v novi direktivi je zelo konkretna, pri čemer so kazni za organizacije precej visoke. Kljub temu je treba poudariti, da so višine kazni primerljive ali nižje od škode, ki jo lahko žrtve utrpijo v primeru uspešno izvedenega kibernetskega napada. Ta je po zadnjem poročilu o škodi iz naslova kršitev varstva podatkov (IBM Corporation, 2024) v globalnem povprečju za leto 2023 4,88 milijona USD, kar predstavlja 10-odstotno povečanje v primerjavi z letom 2022 in je najvišja doslej. Povprečna škoda v gospodarsko bolj razvitih državah je še bistveno višja, pri čemer beležijo najvišjo povprečno škodo v ZDA, kjer dosega 9,36 milijona USD. Po panogah je najbolj izpostavljeno zdravstvo, kjer je povprečna globalna škoda 9,77 milijona USD (kar predstavlja znatno znižanje v primerjavi z letom 2022), na drugem mestu pa je finančni sektor s škodo v višini 6,08 milijona USD (prav tam).

Med številnimi novostmi, ki jih prinaša NIS 2, bo z uveljavitvijo ZInfV-1 zagotavljanje kibernetske varnosti postalo primarna odgovornost članov poslovodnih organov oziroma odgovornih pravnih oseb, ki se bodo prepoznali kot bistveni ali pomembni subjekti. To pomeni, da bodo ti prevzeli neposredno odgovornost za obvladovanje tveganj na področju kibernetske varnosti, odobritev ukrepov in nadzor nad njihovim izvajanjem. Zakon jim nalaga obveznost izobraževanja oziroma usposabljanja za obvladovanje tveganj kibernetske varnosti ter njihovega vpliva na dejavnosti oziroma storitve, ki jih izvaja subjekt. Hkrati zakon nalaga, da morajo zagotoviti redno usposabljanje zaposlenim, da s tem pridobijo dovolj znanj in spretnosti za prepoznavanje in ocenjevanje tveganj, za skrbnike informacijsko-komunikacijskih sistemov pa zakon predpisuje redno letno usposabljanje.

Poleg navedenega so poslovodstva zavezana k zagotavljanju ustrezne organizacijske strukture in zadostnih virov, da lahko organizacija v celoti izpolnjuje zahteve zakona. Poslovodstva morajo tudi poskrbeti, da organizacija učinkovito sledi spremembam na področju kibernetskih tveganj, tehnološkemu razvoju in uvajanju ustreznih rešitev. Namen nove zakonodaje je v prvi vrsti zvišati varnostno pripravljenost v celotnem okolju EU, kar je mogoče doseči le s povečanjem odpornosti večine organizacij, tako institucij kot gospodarskih družb. Pomembno je zavedanje, da napadalci iščejo pot do uspešnega napada skozi najmanj zavarovane sisteme, varnostne pomanjkljivosti, neprevidne ali premalo usposobljene posameznike, pri čemer uporabljajo vse razpoložljive načine in tehnologije. Ocenjena skupna škoda tovrstnih napadov je primerljiva s prihodki pomembnih gospodarskih panog, medtem ko predstavljata neposredna in posredna škoda za napadeno organizacijo pogosto veliko grožnjo njenemu nadaljnjemu poslovanju. Prav zato je cilj regulative povečati zavedanje poslovodstva o nujnosti vključitve kibernetskih tveganj v ocenjevanje poslovne uspešnosti. Hkrati mora biti kibernetska varnost obravnavana kot ključni dejavnik za poslovno uspešnost in konkurenčno prednost v njihovi dejavnosti. Skladnost z zakonskimi določili, upoštevanje dobrih praks ter visoka stopnja varnostne zrelosti organizacij ne zagotavljajo le varnejšega poslovanja, temveč tudi pozitivno vplivajo na delovne odnose, poslovne procese, ugled pri poslovnih partnerjih in dojemanje blagovne znamke pri odjemalcih in kupcih, kar prispeva k dolgoročni uspešnosti poslovanja.

Področje, ki mu tako direktiva NIS 2 in posledično novi zakon posvečata posebno pozornost, je nadzor in upravljanje tveganj, povezanih z dobavno verigo. Kot je razvidno iz zgoraj navedenih primerov, so dobavitelji, ne le tisti na področju storitev in opreme IT, ključni dejavnik tveganja. Agencija Evropske unije za kibernetsko varnost

(ENISA) izpostavlja v svoji zadnji objavljeni študiji groženj kibernetske varnosti do leta 2030 izkoriščanje odvisnosti od programske opreme v dobavni verigi (ang. Supply Chain Compromise of Software Dependencies) kot najpomembnejšo grožnjo. Visoko na lestvici groženj so tudi napadi na programsko opremo za odkrivanje globokih ponaredkov (ang. Deepfake), katerih cilj je preprečiti zaznanje tovrstnih ponaredkov ter omogočiti napadalcem zlorabo varovanih sistemov in vstavljanje zlonamerne programske opreme, kar lahko moti dobavno verigo, še posebej na področju proizvodnje hrane (ENISA, 2024).

Direktiva NIS 2 pri tem seveda ne nastopa samostojno. Spremlja in dopolnjuje jo vrsta drugih pravnih aktov, direktiv, uredb, priporočil, tako na ravni EU kot na nacionalnih ravneh. Posebej pomembna je Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor (okr. DORA), ki se začne uporabljati od 17. januarja 2025. Ta uredba je v celoti neposredno zavezujoča za vse države članice (Uradni list Evropske unije, 2022) in se obravnava kot posebni zakon (lex specialis), ki prenaša zahteve NIS 2 na področje finančnih subjektov, kot so banke, zavarovalnice in investicijska podjetja. Uredba bo zagotovila, da bo finančni sektor v Evropi sposoben ohraniti odpornost v primeru resnih motenj v delovanju. DORA prinaša poenotenje pravil glede operativne odpornosti za finančni sektor, ki velja za 20 različnih vrst finančnih subjektov in zunanjih ponudnikov storitev IKT. Organizacije, ki jih DORA zavezuje k izvajanju ukrepov, so večinoma že preverile svojo pripravljenost in uskladile postopke ali pa intenzivno izvajajo potrebne ukrepe. Vendar pa je položaj na drugih področjih precej drugačen. Marsikatera organizacija, ki ni bila vključena med zavezance po prvotnem zakonu o informacijski varnosti, še čaka na ZinfV-1. Pojavljajo se tudi vprašanja glede neposredne vključitve med bistvene ali pomembne subjekte po NIS 2. Precej razmišljanj je usmerjenih v izpolnjevanje formalnih zahtev direktive oz. novega zakona, medtem ko bodoči zavezanci, pa tudi tisti, ki jih novi zakon neposredno ne bo zadeval, bodo pa kot del dobavne verige pod drobnogledom svojih kupcev, žal v mnogih primerih povsem spregledajo osnovni namen direktive, ki namerava zagotoviti boljšo pripravljenost javnega in zasebnega sektorja za obvladovanje kibernetskih groženj. K temu cilju vodi poenotenje mehanizmov za vzpostavitev visoke ravni kibernetske varnosti v vseh državah članicah ter dvig splošne zavesti in usposobljenosti vseh deležnikov. Zgolj izpolnjevanje formalnih pogojev organizacijo ne bo zaščitilo pred kibernetskimi grožnjami, saj so dejanske grožnje, ki jih predstavljajo kibernetska tveganja, pogosto daleč večje od morebitnih kazni.

Pregled ključnih korakov za prilagoditev procesov in dosego skladnosti z NIS 2

Organizacije, ki so bodisi zavezane k izpolnjevanju zahtev direktive NIS 2 ali menijo, da bodo preko dobavne verige vključene v ukrepe svojih ključnih partnerjev, oziroma tiste, ki verjamejo, da bo prilagoditev zahtevam NIS 2 prispevala k višji stopnji kibernetske varnosti, okrepila varnostno ozaveščenost znotraj organizacije ter posledično povečala ugled in izboljšala ali vsaj pomagala ohraniti konkurenčni položaj, naj preverijo svoje obstoječe postopke za obvladovanje tveganj, odzivanje na incidente, zaščito infrastrukture in varnosti podatkov.

Načinov za doseganje skladnosti z NIS 2 je več, pri čemer vsak prinaša svoje prednosti in omejitve. Nekateri so usmerjeni bolj v formalno izpolnjevanje zahtev, kar vključuje pripravo politik, pravilnikov, postopkov ter analizo vrzeli ter zapisane usmeritve za nadaljnje ukrepanje. Prepogosto je tak načrt preveč splošen in ne doseže dejanskega načina dela v organizaciji, prav tako ne doseže ključnih ljudi. Ti se sicer prilagodijo formalnim postopkom, vendar se ukrepom v resnici izogibajo, saj ne ponotranjijo njihovega bistva. Drugi postopki so izrazito tehnično naravnani. Uvedba elektronskih varnostnih sistemov ali najem zunanjih storitev za zagotavljanje kibernetske varnosti ali kombinacija obojega lahko prispeva k povečanju ravni kibernetske zaščite organizacije. Vendar pa je to učinkovito le, če je pred tem opravljena temeljita analiza trenutne organizacijske zrelosti na področju varovanja informacij. Pogosta slabost tehničnih ukrepov so pomanjkljiva organizacijska struktura, premalo osebja z ustreznim strokovnim znanjem ter neustrezna koordinacija in nadzor nad zunanjimi storitvami. Pomanjkljivo uvedeni tehnični ukrepi lahko povzročijo lažen občutek varnosti, povečajo tveganja in zmanjšajo odpornost organizacije pri odzivanju na kritične dogodke zaradi neustrezne koordinacije in nejasne strukture odgovornosti. Da bi bili ukrepi zares uspešni, mora organizacija najprej preveriti in oceniti tveganja, opraviti analizo poslovnih učinkov ter se soočiti z vrzelmi, ki jo ločijo od višje stopnje zrelosti informacijske varnosti. Šele nato lahko določi konkretne ukrepe in časovnice za uvedbo sprememb. Na podlagi pridobljenih informacij in ustreznih ocen se lahko poslovodstvo po tehtnem premisleku odloči za uvedbo ukrepov tam, kjer organizaciji preti največja grožnja oziroma na področju, kjer bo učinek spremembe največji. Oceno stanja in razmislek lahko organizacija opravi sama, lahko pa poišče pomoč pri zunanjih strokovnjakih za

posamezno tehnološko področje ali za presojo in oblikovanje procesov.
Pomembno je, da ta način preverjanja postane stalnica v okviru procesa nenehnega izboljševanja. Vsaka sprememba mora biti po uvedbi ovrednotena, da se ugotovi dejanski učinek in po potrebi izpelje korektivne ukrepe za doseganje načrtovanega stanja. Eden od načinov, kako se spopasti s to izjemno zahtevno nalogo, je uporaba metode „13 področij uporabe“[1] (Smart Com, 2024). Ta metoda načrtno modelira področja uporabe in ob ustrezni prilagoditvi pokriva vse organizacijske vidike katerekoli organizacije. Hkrati v preseku obravnava vsa področja, ki so ključnega pomena za obvladovanje kibernetskih groženj.
Priporočljivo je, da organizacija za oceno skladnosti z direktivo NIS 2 preveri področja uporabe z odgovori na vprašanja, ki so del metodologije za ugotavljanje zrelostne ravni kibernetske varnosti. Ta vprašanja se, po predhodnih razgovorih in izvedeni analizi, prilagodijo konkretni organizaciji z namenom, da poslovodstvo ob pomoči svetovalca kar najbolj učinkovito pridobi vpogled v dejanske potrebe svojega poslovanja. Na podlagi teh informacij lahko oblikuje zahteve za uvedbo potrebnih sprememb v organizaciji, procesih in sistemih.
Vsako področje uporabe je podrobno razdelano po vsebini, primerih dobre prakse in pomembnih ukrepih, ki naj jih organizacija uvede za optimalno zaščito. Področja uporabe so nadalje razdeljena na štiri sklope, kar povečuje preglednost in omogoča lažje obvladovanje ter spremljanje uvedenih ukrepov.
Prvi sklop področij zajema vodstveni in organizacijski vidik. V ta del sodijo:

- vključenost poslovodstva,
- varnostna politika organizacije,
- ozaveščanje osebja o varnostnih grožnjah,
- upravljanje ključnih virov IKT.

Drugi sklop področij zajema uporabniški vidik. V ta del sodijo:

- posodabljanje programske opreme,
- upravljanje dostopa do delovnih postaj in omrežja,
- zaščita delovnih postaj in prenosnih naprav.

Tretji sklop področij zajema omrežno in podatkovno infrastrukturo, vključno z oddaljenim dostopom. V ta del sodijo:

- arhiviranje podatkov,
- zaščita strežnikov in omrežnih komponent,
- varen oddaljeni dostop.

Četrti sklop področij obravnava varovanje pred grožnjami in neprekinjenost poslovanja. V ta del sodijo:

- zaščita pred zlonamerno programsko kodo,
- zaščita pred drugimi grožnjami,
- neprekinjenost poslovanja in upravljanje incidentov.

Področja uporabe in sklopi področij so oblikovani v smiselne, povezane enote, kar predvsem olajša obvladovanje celote. Gre za enega izmed možnih načinov, pri čemer je razdelitev na sklope le ena od možnosti, ki se lahko prilagodi glede na organizacijski ustroj in potrebe organizacije. Vsak sklop zajema določeno organizacijsko strukturo znotraj generične organizacijske oblike in zahteva drugačne tehnološke postopke in strokovna znanja pri uvajanju sprememb. Področja uporabe ne obravnavajo posameznih zahtev neposredno, temveč kot celota pokrivajo vse zahteve. Na primer, obvladovanje dobavne verige ni zajeto v enem samem področju uporabe, ker skrb za informacijsko varnost dobavne verige pri tipični organizaciji nastopa na več področjih uporabe. Urejanje formalnih odnosov v povezavi z dobavitelji, določanje strategije in ocenjevanje dobaviteljev so naloge poslovodstva, medtem ko je obvladovanje informacijskih tveganj dobavne verige vključeno v varnostno politiko. Odnose z dobavitelji je treba obravnavati tudi na področju ozaveščanja osebja o varnostnih grožnjah, kritične sisteme in z njimi povezane dobavitelje pa obravnavamo v sklopu upravljanja ključnih virov IKT. Glede na potrebe in prakse v organizaciji se lahko posamezen vidik obvladovanja dobavne verige pojavi tudi znotraj preostalih področij uporabe.

Sklep

V članku smo, glede na razpoložljiv obseg, obravnavali vplive nove direktive NIS 2 na organizacije in njihovo kibernetsko varnost. Ugotavljamo, da prinaša NIS 2 pomembne spremembe, ki zahtevajo prilagoditev obstoječih procesov za krepitev varnostnih mehanizmov. Predstavljeni so ključni koraki, ki jih morajo organizacije izvesti za doseganje skladnosti z direktivo, vključno z revizijo varnostnih politik, tehnološkimi nadgradnjami in izboljšanjem notranjega sodelovanja. Čeprav so te prilagoditve lahko zahtevne, prinašajo dolgoročne koristi v obliki večje kibernetske odpornosti, večjega zaupanja strank in skladnosti z zakonodajo. Skladnost z NIS 2 ni zgolj nujnost, temveč tudi priložnost za organizacije, da izboljšajo svoje varnostne procese in tako okrepijo svoj položaj na trgu.

[1] Metoda „13 področij uporabe“ je razvita in uporabljena v podjetju Smart Com d.o.o.

Viri / References

Bing, C. *idr.* (2021) *„Suspected Chinese hackers used SolarWinds bug to spy on U.S. payroll agency – sources“*. Reuters. Dostopno: https://www.reuters.com/article/technology/exclusive-suspected-chinese-hackers-used-solarwinds-bug-to-spy-on-us-payroll-idUSKBN2A22K8/ (Dostopano: 23. avgust 2024.).

ENISA (2024) „Foresight Cybersecurity Threats for 2030 - Update“ Dostopno: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024 (Dostopano: 20.8.2024.).

eUPRAVA (2024) „Zakon o informacijski varnosti“ Dostopno: https://e-uprava.gov.si/si/drzava-in-druzba/e-demokracija/predlogi-predpisov/predlog-predpisa.html?id=16290 (Dostopano: 27.8.2024.).

IBM Corporation (2024) *„Cost of a Data Breach Report 2024“* Dostopno: https://www.ibm.com/au-en/reports/data-breach (Dostopano: 23. avgust 2024.).

IT Governance Europe (2024) *„ Data Breaches and Cyber Attacks – Europe 2024 Report.“* Dostopno: https://www.itgovernance.eu/blog/en/data-breaches-and-cyber-attacks-in-2024-in-europe (Dostopano: 20. avgust 2024.).

Smart Com (2024) „Priporočila za učinkovito prilagoditev zahtevam direktive NIS 2“ Dostopno: https://www.smart-com.si/ocena-nis2/ (Dostopano: 13.2.2024.).

TechTarget (2023) *„SolarWinds hack explained: Everything you need to know.“* Dostopno: https://www.techtarget.com/whatis/feature/SolarWinds-hack-explained-Everything-you-need-to-know (Dostopano: 22. avgust 2024.).

Uradni list Evropske unije (2022) „ Direktiva (EU) 2022/2555 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o ukrepih za visoko skupno raven kibernetske varnosti v Uniji, spremembi Uredbe (EU) št. 910/2014 in Direktive (EU) 2018/1972 ter razveljavitvi Direktive (EU) 2016/1148 (direktiva NIS 2)“ Dostopno: https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX:32022L2555 (Dostopano: 26.10.2023.).

Uradni list Evropske unije (2022) „Uredba (EU) 2022/2554 Evropskega parlamenta in Sveta z dne 14. decembra 2022 o digitalni operativni odpornosti za finančni sektor in spremembi uredb (ES) št. 1060/2009, (EU) št. 648/2012, (EU) št. 600/2014, (EU) št. 909/2014 in (EU) 2016/1011“ Dostopno: https://eur-lex.europa.eu/legal-content/sl/TXT/?uri=CELEX:32022R2554 (Dostopano: 28.8.2024.).

UDK 57.087.1:004.382.745

Varna uporaba biometrije na telefonu

*Robert Grabrijan**

USING BIOMETRICS SECURELY ON YOUR PHONE

Biometric technologies are revolutionising how we use and secure our phones. Despite its many advantages, we need to be aware of the risks of using biometrics inappropriately. Being aware of how biometrics works, its advantages and disadvantages, and following the recommendations for safe use help us to keep our phones and data safe. With the right understanding and approach, biometrics is a powerful tool to protect our digital identity.

JEL K24, O33

Uvod

Biometrija je tehnologija, ki uporablja fizikalne in vedenjske značilnosti posameznika za njegovo identifikacijo. Biometrični podatki, ki se običajno uporabljajo, vključujejo prstne odtise, obrazne poteze, šarenico in očesno mrežnico, glas ter vzorce tipkanja ali gibanja. Uporaba biometrije je razširjena v različnih aplikacijah, kot so varnostni sistemi, nadzor dostopa, mobilne naprave, pravosodni sistemi in celo v zdravstvenem varstvu. Biometrični sistemi zagotavljajo visoko stopnjo varnosti, saj je težko ponarediti ali ukrasti edinstvene fizične lastnosti posameznika. Uporaba biometrije prinaša izzive, povezane z zasebnostjo in varstvom podatkov posameznika. Poleg varne uporabe biometrije je pomemben tudi zakonodajni vidik, ki ureja uporabo biometrije in upošteva varnostne ukrepe za zmanjšanje tveganj za zlorabo biometričnih podatkov. Med prenosne naprave, ki omogočajo biometrijo, ne glede na tip in vrsto proizvajalca, v večini primerov prevladujejo prenosni telefoni, bolj ali manj »pametni«, zato v nadaljevanju uporabljamo za vse različne prenosne naprave, ki omogočajo uporabo biometrije, eno samo besedo »telefon«.

Zakonodajni vidik

Za uporabo biometrije na telefonu, kot so prstni odtisi ali prepoznavanje obraza, sta potrebna privolitev uporabnika in telefon, ki omogoča biometrijo. Privolitev posameznika mora biti prostovoljna, ozaveščena in dana za določen namen (Kdaj je privolitev veljavna?). V Sloveniji ureja področje varstva osebnih podatkov zakon o varstvu osebnih podatkov (ZVOP-2), ki je usklajen z evropsko splošno uredbo o varstvu podatkov (Varstvo osebnih podatkov). Biometrični podatki se obravnavajo kot občutljivi osebni podatki, zato je njihova obdelava strogo regulirana (Ureditev biometrijskih ukrepov po ZVOP-2). Privolitev za uporabo biometrije na telefonu običajno vključuje obvestilo o vrsti biometričnih podatkov, ki jih naprava zbira (npr. prstni odtisi, obrazne značilnosti), in kako bodo ti podatki uporabljeni. Prav tako obvestilo razloži, katera aplikacija ali storitev bo do zapisa biometrije dostopala in zakaj. Privolitev pogosto vključuje tudi informacije o tem, kako lahko uporabnik upravlja ali briše svoje biometrične podatke ter kakšne so možnosti za odstop od uporabe biometričnih metod.

Vrste privolitev uporabe biometrije na telefonu

Pri uporabi biometrije na telefonu se srečamo z različnimi vrstami privolitev, ki so odvisne od namena uporabe biometričnih podatkov, vrste podatkov in pravil zasebnosti, ki jih uporabljajo posamezne aplikacije ali operacijski sistemi. Poznamo naslednje vrste privolitev:

Privolitev ob prvem nastavljanju: Ta vrsta privolitve se pojavi, ko prvič nastavljamo biometrične funkcije na telefonu, kot je prstni odtis ali prepoznava obraza. V tem koraku izvemo, kaj biometrija pomeni, kako bo uporabljena in kako lahko upravljamo svoje podatke.

* Robert Grabrijan, svetovalec za skladnost poslovanja, Skladnost poslovanja in krepitev integritete, Varovanje informacij - NLB

Ločene privolitve za posamezne aplikacije: Nekatere aplikacije zahtevajo posebno privolitev za uporabo biometrije za specifične funkcije znotraj aplikacije, kot so bančne aplikacije za avtentikacijo transakcij ali aplikacije za varno shranjevanje dokumentov. V tem primeru se od uporabnika zahteva, da posebej privoli v uporabo biometrije znotraj te aplikacije.

Privolitev za posodobitve funkcij: Ko se posodobijo funkcije biometrije ali se spremenijo pogoji uporabe, lahko telefon od uporabnika zahteva, da ponovno potrdi svojo privolitev. Na ta način je uporabnik seznanjen s spremembo in jo tudi potrdi oziroma zavrne.

Začasna ali enkratna privolitev: V nekaterih primerih, na primer pri gostujočih uporabnikih ali pri uporabi določenih funkcij, se lahko zahteva začasna ali enkratna privolitev, ki velja samo za določen čas ali za posamezno sejo.

Implicitna privolitev: Ko je uporabnik telefona že sprejel splošne pogoje uporabe naprave ali aplikacije, se lahko šteje, da je implicitno privolili v uporabo biometrije, če so informacije o biometriji jasno vključene v te pogoje.

Vsaka vrsta privolitve je namenjena zagotavljanju, da uporabniki telefona razumejo, kako bodo njihovi biometrični podatki uporabljeni in kako jih lahko kontrolirajo, pri tem pa se spoštuje zakonodaja o zasebnosti in varstvu podatkov.

Zapis in hranjenje biometričnega podatka na telefonu

Ko se biometrični podatki, kot so odtisi prstov ali prepoznava obraza, shranjujejo na telefonu, je postopek običajno zelo varovan in zasnovan tako, da zaščiti zasebnost uporabnika. Zapis in shranjevanje biometričnih podatkov v spomin telefona poteka po naslednjih korakih:

- zajem biometričnih podatkov,
- pretvorba v digitalni podatek,
- šifriranje,
- shranjevanje v zaščitenem prostoru telefona.

Telefon z uporabo posebnih senzorjev (npr. senzorja prstnih odtisov ali kamere za prepoznavanje obraza) zajame biometrični vzorec. Pri odtisu prsta to pomeni pridobitev podrobne slike prstnega odtisa, pri prepoznavanju obraza pa se ustvari podrobna 3D mapa obraza. Zajeti biometrični vzorec se nato pretvori v digitalni zapis, ki se imenuje biometrična predloga. To je digitalna reprezentacija biometričnih značilnosti, izvedenih iz prvotnega vzorca.
Biometrični predloga se šifrira, kar pomeni, da se podatki zapišejo na način, da jih ni mogoče enostavno prebrati ali spremeniti brez ustreznega ključa (dekripcija).
Šifrirani biometrični podatki se shranijo v varnem, izoliranem prostoru znotraj telefona, znanem kot Trusted Execution Environment (TEE) ali Secure Enclave. Ta prostor je ločen od glavnega operacijskega sistema in aplikacij, kar zagotavlja, da tudi če nekdo pridobi dostop do telefona, ne more enostavno dostopati do shranjenih biometričnih podatkov. Ko želimo odkleniti telefon ali avtorizirati določeno dejanje v nameščeni aplikaciji telefona, naprava ponovno zajame biometrični vzorec in ga primerja s shranjenim šifriranim zapisom. Če se podatki ujemajo, se izvede želeno dejanje (npr. odklepanje telefona). Opisani proces zagotavlja, da se biometrični podatki obdelujejo in shranjujejo na način, ki varuje našo zasebnost in zmanjšuje tveganje za zlorabo.

Shranjevanje biometričnih podatkov v zaščitenem prostoru telefona pomeni, da so podatki fizično in logično ločeni od drugih delov sistema, kar dodatno poveča varnost.

Branje biometričnih podatkov na telefonu

Ko želimo odkleniti telefon s prstnim odtisom, se sproži proces zbiranja podatkov. Senzor na našem telefonu (npr. prstni odtisni senzor, senzor za prepoznavanje obraza) zajame biometrične podatke. Telefon pretvori podatke v matematični model, ki predstavlja naš prstni odtis, obraz ali iris. Ta model je shranjen v varnem delu našega telefona (običajno v Secure Enclave). Ko želimo dostopati do želene aplikacije, se zbrani podatek ponovno pretvori v matematični model. Ta model se nato primerja s shranjenim modelom. Če se modela ujemata z dovolj veliko natančnostjo, aplikacija dovoli dostop.

Kako nameščene aplikacije na telefonu dostopajo do biometričnih podatkov

Operacijski sistemi, kot sta Android in iOS, ponujajo posebne API-je (Application Programming Interfaces), ki omogočajo aplikacijam, da zahtevajo biometrično avtentikacijo. Ko aplikacija zahteva dostop, se prikaže pojavno okno, v katerem uporabnik potrdi ali zavrne zahtevo. API-ji so zasnovani tako, da preprečujejo neposreden dostop do aplikacij oziroma biometričnih podatkov. Aplikacije prejmejo le informacijo o tem, ali je avtentikacija uspela ali ne.

Obdelava biometričnih podatkov se izvaja v telefonu in ne v aplikaciji, kar pomeni, da banke za potrebe uporabe e-bančnih storitev ne obdelujemo biometričnih podatkov, ki so hranjeni v telefonu.

Nastavitve biometrije na telefonu

Biometrija na telefonu vsebuje dodatne varnostne nastavitve, ki so prednastavljene s politiko proizvajalca telefona. Za svojo varnost moramo občasno vnesti svoj vzorec, PIN ali geslo, kot varnostno preverjanje biometričnih podatkov. V operacijskih sistemih Android je za prstni odtis ponastavljena vrednost na vsakih 72 ur. Vnos vzorca, PIN-a ali gesla je kot varnostno preverjanje biometričnih podatkov potreben iz več razlogov:

- biometrični sistemi niso popolni. Koda PIN, geslo ali vzorec dodajo dodatno plast varnosti. Ta način zagotavlja, da obstaja, če biometrična avtentikacija odpove ali je ogrožena, še en močan varnostni ukrep, kar za uporabnika pomeni dodatno varnost;
- senzorji za biometrijo občasno ne prepoznajo prstnega odtisa, obraza ali drugih biometričnih funkcij zaradi različnih vzrokov (umazanija, vlaga, sprememba videza, poškodba senzorja). V takih primerih omogoča PIN ali geslo nemoten dostop do telefona;
- večina naprav zahteva vnos kode PIN, gesla ali vzorca, če telefon ni bil dalj časa v uporabi. Nastavljena politika proizvajalcev telefonov nam pomaga zaščititi telefon pred nepooblaščenim dostopom, če je telefon izgubljen ali ukraden, ko je izklopljen ali dolgo časa ni bil uporabljen;
- po posodobitvi ali spreminjanju varnostnih nastavitev telefona moramo največkrat ponovno vnesti PIN, vzorec ali geslo. Ta ukrep zagotavlja preverjanje, ali je oseba, ki izvaja spremembe, dejansko lastnik telefona;
- v nekaterih pravnih okoljih se standardi za dostop do telefona z biometrijo oziroma z geslom razlikujejo. Na primer, v pravnem kontekstu je lahko zahteva za uporabo biometrije lažja kot zahteva za uporabo PIN-a. Zahteva za vnos gesla, kot varnostne kopije, pomaga uravnotežiti skrbi glede zasebnosti oziroma načina dostopa do telefona;
- hranjeni biometrični podatki se s časom lahko razlikujejo od dejanskih biometričnih značilnosti posameznika (npr. staranje, brazgotine itd.). Redno potrjevanje varnostne metode pomaga, da uporabnik obnavlja in si zapomni izbrano metodo, kar preprečuje zaklepanje telefona.

Navedeni ukrepi nam zagotavljajo varen in zanesljiv dostop do telefona in ohranijo ravnovesje med udobjem in integriteto varnosti.

Nasveti za varno rabo biometrije na telefonu

Biometrična tehnologija je postala ključni del varnosti telefonov, ki nam omogoča dostop do naprav, aplikacij in storitev na hiter in udoben način. Vendar pa, kot pri vseh tehnologijah, je tudi pri biometriji pomembno razumeti, kako jo varno uporabljati.

Proizvajalci pametnih telefonov redno izdajajo posodobitve, ki vključujejo izboljšave varnosti in popravke glede znanih ranljivosti. Redne posodobitve zagotavljajo, da so tudi biometrične funkcije telefona zaščitene pred najnovejšimi grožnjami, zato moramo **svojo napravo redno posodabljati**. Telefoni omogočajo izbiro, katere aplikacije lahko dostopajo do naših biometričnih podatkov. Pri dodeljevanju dovoljenj moramo biti previdni in **omogočiti dostop samo tistim aplikacijam, ki jim zaupamo,** saj na ta način omejimo dostop do biometričnih podatkov.

Biometrične tehnologije niso enake. Nekateri telefoni uporabljajo naprednejše in varnejše biometrične senzorje, kot so infrardeči skenerji obraza ali ultrazvočni prstni odtisi, ki so bolj zanesljivi in jih je težje ponarediti. **Novejši telefoni imajo praviloma bolj napredno biometrično tehnologijo**. Pozorni moramo biti na kombinacijo, kje in kako uporabljamo biometrijo skupaj z vzorcem, PIN-om ali geslom oz. v kombinaciji z drugimi varnostnimi elementi. V javnih ali nezavarovanih okoljih se lahko izpostavimo tveganju, da nekdo opazuje vnos vzorca ali PIN-a ter tako posname naše zaupne podatke oziroma avtentikacijske elemente. **Bodimo previdni pri uporabi varnostnih elementov in zaupnih podatkov v javnosti.** Kljub temu, da biometrija ponuja visoko stopnjo varnosti, je priporočljivo, da **uporabljajmo dvofaktorsko avtentikacijo** (2FA), kjer nam tehnologija to omogoča.

Uporabljajmo kombinacijo biometričnih podatkov z drugimi elementi, kot so geslo, vzorec, PIN ali enkratno geslo (OTP), saj tako dodatno zavarujemo svoje podatke. V primeru, da je eden od elementov kompromitiran, nas morebitni goljuf ne more zlorabiti, saj potrebuje še drugi element, ki pripada dvofaktorski avtentikaciji.

Z upoštevanjem naštetih nasvetov lahko izboljšamo varnost in zasebnost pri uporabi biometrične tehnologije na pametnem telefonu.

Prednost uporabe biometrije

Uporaba biometrije na telefonu prinaša številne varnostne prednosti, ki izboljšajo zaščito osebnih in podatkovnih informacij. Biometrični podatki, kot so prstni odtisi, obrazne lastnosti ali šarenica, so edinstveni za vsako osebo. Ta

edinstvenost otežuje potencialnim napadalcem, da bi ponaredili ali ukradli našo identiteto, kar je velik varnostni plus v primerjavi s tradicionalnimi gesli ali kodami PIN. Biometrični podatki se težko ponaredijo ali kopirajo, kot to velja za tradicionalna gesla ali PIN. Tehnologija, ki je potrebna za uspešno ponarejanje biometričnih podatkov, je precej zapletena in običajno nedostopna potencialnim napadalcem. Biometrična avtentikacija omogoča hitro in enostavno odklepanje naprav, kar izboljša uporabniško izkušnjo, hkrati pa ohranja visoko stopnjo varnosti.
Uporabnik biometrije lahko hitro dostopa do svojih naprav, ne da bi moral vtipkati geslo, kar zmanjšuje možnost, da bi ga kdo opazoval in posnel njegovo geslo ali PIN.
Biometrija omogoča tudi samodejno avtentikacijo v različnih aplikacijah in storitvah, kar nam omogoča lažji dostop do storitev brez ponovnega vnosa gesel. To ne samo da izboljša uporabniško izkušnjo, ampak tudi poveča varnost, saj se zmanjša število gesel, ki so lahko izpostavljena.

Biometrični podatki ne morejo biti ukradeni ali pridobljeni preko tradicionalnih metod socialnega inženiringa, kot so phishing ali lažno predstavljanje. To zmanjšuje tveganje, da bi kdo pridobil naše geslo ali PIN.

Tveganja uporabe biometrije

Tveganja uporabe biometrije se nanašajo na zasebnost, varnost in etične vidike.
Biometrični podatki so zelo osebni, saj izhajajo iz fizičnih in vedenjskih značilnosti posameznika, kot so prstni odtisi, obrazne poteze in glasovni vzorci. Neavtoriziran dostop ali zloraba teh podatkov lahko privede do kršitev zasebnosti. Čeprav biometrični sistemi pogosto veljajo za varne, so izpostavljeni tveganjem, kot so lažna sprejemanja in lažne zavrnitve. Z uporabo novejše tehnologije se možnost ponarejanja prstnih odtisov oz. vdora v podatkovne zbirke zmanjšuje.
Biometrični sistemi niso popolni in lahko prihaja do napak. Na primer, nekateri ljudje imajo lahko prstne odtise, ki so težko berljivi, ali obrazne značilnosti, ki jih sistem težje prepozna, kar lahko privede do težav pri identifikaciji ali avtentikaciji.
Biometrični sistemi so lahko pristranski, če podatki, uporabljeni za njihovo učenje, niso dovolj raznoliki. To lahko privede do višje stopnje zavrnitev ali nepravilne identifikacije pri določenih skupinah ljudi, kar je lahko oblika diskriminacije.
Biometrične lastnosti posameznika se s časom redko spremenijo, kar pomeni, da če biometrični podatek enkrat uide v javnost, ga ni mogoče enostavno "spremeniti" ali "zamenjati", kot je to mogoče pri geslih ali PIN-u.

Vključevanje biometrije v vsakdanje tehnologije in procese odpira vrsto etičnih vprašanj, kot so obseg nadzora, ki ga družba sprejema, in pravica posameznikov do zavrnitve uporabe biometrije.

Potrjevanje finančnih in nefinančnih transakcij v storitvah, ki jih ponujajo banke

Potrjevanje finančnih transakcij samo z varnostnim elementom PIN ali geslom predstavlja tveganje, saj lahko ti načini avtentikacije postanejo tarča napadov, kot so phishing, keylogging ali napadi brute-force. Če napadalci pridobijo dostop do PIN-a ali gesla, lahko izvedejo nepooblaščene transakcije, povedano drugače, izpraznijo stanje na našem računu.
Banke že od leta 2019 zmanjšujemo opisana tveganja zlorab posameznega varnostnega elementa z uporabo dvofaktorske avtentikacije. Dvofaktorska avtentikacija (2FA) je varnostni postopek, ki zahteva dva ločena načina preverjanja identitete, da se uporabnik lahko prijavi v e-banko in izvede transakcijo. 2FA vključuje kombinacijo dveh od treh možnih vrst avtentikacijskih faktorjev:

- **nekaj, kar veš** (nekaj, kar ve samo uporabnik, kot je geslo, PIN ali varnostno vprašanje),
- **nekaj, kar imaš** (nekaj, kar ima uporabnik v svoji posesti, kot je pametni telefon, varnostni ključ (npr. USB-ključek), kartica z žetoni ali drugo strojno napravo, na primer telefon),
- **nekaj, kar si** (biometrični podatki, kot so prstni odtis, prepoznavanje obraza, glasovna prepoznava ali očesna mrežnica).

Uporaba dvofaktorske avtentikacije je zelo učinkovita pri preprečevanju nepooblaščenih dostopov, saj tudi če napadalec pridobi geslo, še vedno potrebuje drugi faktor, da se uspešno prijavi. Uporaba dvofaktorske avtentikacije močno zmanjša verjetnost nepooblaščenega dostopa in povečuje varnost izvajanja finančnih in nefinančnih transakcij.

Uporaba biometrije kot enega od elementov dvofaktorske avtentikacije preprečuje možnost, da bi nepooblaščene osebe uporabile naše e-bančne storitve oziroma izvedle nepooblaščene plačilne transakcije.

UDK 004.8:004.62:343.9:336.71

Uporaba strojnega učenja pri preprečevanju prevar s kreditnimi karticami

*Lovro Brulec**

THE USE OF MACHINE LEARNING IN CREDIT CARD FRAUD PREVENTION

In this study, we examined the effectiveness of four machine learning models –logistic regression, naive Bayes classifier, random forest, and neural network – in detecting credit card fraud. We used the SMOTE technique to balance the data. The results showed that the random forest achieved the best performance with precision 0.85, recall 0.77, and F1-score 0.81, while logistic regression and naive Bayes exhibited low precision. The neural network achieved solid results with a precision of 0.73 and an F1-score of 0.74 but was slightly outperformed by the random forest.

JEL G21, K24

1. Uvod

V današnji digitalni dobi so transakcije s kreditnimi karticami nepogrešljivi del vsakdanjega poslovanja, kar prinaša številne prednosti, a tudi nove izzive, med katerimi izstopa grožnja prevar. Izgube zaradi goljufij s kreditnimi karticami vsako leto dosegajo milijarde evrov, leta 2021 je bila skupna vrednost goljufivih transakcij znotraj območja evrskega plačevanja (angl. Single Euro Payments Area – SEPA) 1,53 milijarde evrov (European Central Bank, 2023). Na splošno poznamo dve vrsti goljufij s kreditnimi karticami: krajo fizične kartice in krajo občutljivih informacij, kot so številka kartice, varnostna koda CVV in tip kartice. Z zlorabo teh podatkov lahko goljufi hitro dvignejo velike zneske ali opravijo večje nakupe, še preden imetnik kartice opazi nepravilnosti, zato je pomembno, da obstaja sistem, ki imetnika kartice obvesti, da je bil tarča prevare.

Posledice goljufivih transakcij so resne tako za uporabnike kot za banke. Uporabniki lahko utrpijo finančne izgube, imajo težave pri dostopu do računov in stroške, povezane z zamenjavo kartic ter reševanjem goljufije. Banke pa poleg povračila sredstev tvegajo tudi izgubo zaupanja strank. Neučinkoviti sistemi zaznavanja goljufij lahko vodijo do povečanja lažnih negativnih primerov (neprepoznane goljufije), kar povzroča še večje finančne izgube, ali lažnih pozitivnih primerov (zavrnitev zakonitih transakcij), kar zmanjšuje zadovoljstvo strank (Hashim et al., 2020).

Strojno učenje omogoča gradnjo modelov, ki z analizo velikih količin podatkov samodejno prepoznavajo sumljive transakcije. Tradicionalni modeli za odkrivanje goljufij temeljijo na vnaprej določenih pravilih, ki jih je treba nenehno posodabljati, kar otežuje sledenje novim vzorcem goljufij. Ključna prednost strojnega učenja je v tem, da se modeli ne le samodejno prilagajajo novim podatkom, temveč se tudi učijo iz vsake nove transakcije, kar povečuje njihovo zmožnost prepoznavanja prej neznanih oblik goljufij. Strojno učenje omogoča tudi zaznavanje subtilnih vzorcev in anomalij, ki bi jih tradicionalni sistemi lahko spregledali, kar vodi do natančnejšega in učinkovitejšega zaznavanja prevar v realnem času.

Kljub temu so neuravnoteženi podatki, pri čemer goljufije predstavljajo majhen delež vseh transakcij, poseben izziv za modele strojnega učenja. Ti modeli se namreč pogosto osredotočajo na večinski razred (zakonite transakcije), zaradi česar spregledajo manjšinskega (goljufive transakcije), kar zmanjšuje učinkovitost sistema pri zaznavanju prevar.

Namen te raziskave je primerjati učinkovitost štirih algoritmov strojnega učenja – logistične regresije, naivnega Bayesovega klasifikatorja, naključnega gozda in nevronske mreže – pri zaznavanju goljufivih transakcij po uporabi metode SMOTE (angl. Synthetic Minority Over-sampling Technique, v nadaljevanju: SMOTE) za obravnavo neuravnoteženih podatkov. V analizi bomo preučili, kateri algoritem je najučinkovitejši pri prepoznavanju prevar, ko je porazdelitev podatkov ustrezno uravnotežena. Uporabljena metodologija vključuje standardizacijo podatkov, izbor značilk, uporabo SMOTE

* Lovro Brulec, študent, Univerza v Ljubljani, lovro.brulec@gmail.com

za uravnoteženje razredov ter delitev podatkov na učno in testno množico za preverjanje uspešnosti modelov. Modeli bodo ovrednoteni z uporabo različnih meril, kot so natančnost, priklic, F1-mera in AUC-ROC (angl. Area Under the Receiver Operating Characteristic Curve, v nadaljevanju: AUC-ROC).
Naša hipoteza je, da bodo kompleksnejši modeli, kot sta naključni gozd in nevronske mreže, uspešnejši od logistične regresije ter naivnega Bayesovega klasifikatorja pri zaznavanju prevar.
Na podlagi rezultatov lahko našo hipotezo potrdimo, saj sta kompleksnejša modela, kot sta naključni gozd in nevronske mreže, dosegla boljše rezultate v primerjavi z logistično regresijo in naivnim Bayesovim klasifikatorjem. Naključni gozd je dosegel najboljše rezultate pri natančnosti, priklicu in F1-meri. Nevronska mreža je prav tako pokazala solidno zmogljivost, z boljšimi rezultati kot enostavnejša modela, predvsem pri priklicu in AUC-ROC. Logistična regresija in naivni Bayes sta dosegla slabšo uspešnost, predvsem zaradi nizke natančnosti in večjega števila lažno pozitivnih napovedi.
Raziskava prinaša tudi praktične implikacije za bančni sektor, saj s primerjavo modelov predstavlja vpogled v to, katere metode strojnega učenja so najučinkovitejše pri zaznavanju goljufij in zmanjšanju napačnih zaznav (lažno pozitivni in lažno negativni primeri). Izsledki bodo bankam in finančnim ustanovam pomagali pri izboljšanju njihovih varnostnih sistemov ter zmanjševanju finančnih izgub in povečanju zaupanja strank.

2. Metode

2.1 Zbirka podatkov

V tej raziskavi je bil uporabljen nabor podatkov Credit Card Fraud Detection, ki je dostopen na platformi Kaggle (2013). Nabor vsebuje podatke o transakcijah, ki so jih opravili evropski imetniki kreditnih kartic, in sicer v dveh dneh septembra 2013. Skupno je v naboru 284.807 transakcij, med katerimi je 492 goljufivih, kar pomeni, da je približno 0,17 % vseh transakcij goljufivih.
Podatki vključujejo 31 numeričnih značilnosti, pri čemer so bile nekatere spremenljivke preoblikovane s pomočjo metode glavnih komponent (angl. Principal Component Analysis, v nadaljevanju: PCA), da bi ohranili anonimnost finančnih informacij. Tri spremenljivke niso bile transformirane. Prva je spremenljivka "time", ki prikazuje čas, ki je pretekel od prve transakcije do vsake naslednje transakcije v naboru. Druga je "amount", ki predstavlja znesek transakcije. Tretja in najpomembnejša spremenljivka je "class", ki je oznaka in zavzame vrednost 1, če je transakcija goljufiva, ali 0, če je zakonita.
Ker predstavljajo goljufive transakcije tako majhen delež celote, je ta nabor podatkov izrazito neuravnotežen. To lahko negativno vpliva na uspešnost modelov, saj se ti osredotočajo na večinski razred, kar vodi v dobro prepoznavanje zakonitih transakcij, a slabše prepoznavanje goljufij. Predobdelava podatkov je zato bistvena, saj vključuje tehnike, ki lahko izboljšajo ravnotežje med razredi.

2.2 Predobdelava podatkov

Za izvedbo analize smo uporabili programski jezik Python, skupaj z knjižnicami Pandas, Matplotlib, Scikit-learn in Imblearn. Pandas je bil uporabljen za obdelavo podatkov, Matplotlib za vizualizacijo rezultatov, Scikit-learn za implementacijo modelov strojnega učenja in Imblearn za uporabo metode SMOTE pri obravnavi neuravnoteženih podatkov.

Standardizacija

Da bi podatke pripravili za uporabo v modelih strojnega učenja, smo izvedli standardizacijo. Standardizirali smo spremenljivki čas in znesek transakcij, da bi zagotovili, da imajo vse spremenljivke enako merilo. Tako smo izboljšali skladnost podatkov, kar omogoča modelom, da učinkovito obravnavajo vse vhodne podatke in tako dosežejo boljše rezultate pri zaznavanju goljufij. Nato smo podatkovni nabor razdelili na učno in testno množico v razmerju 70 : 30, pri čemer je učna množica uporabljena za treniranje modelov, testna pa za oceno njihove uspešnosti.

Izbira značilk

Izbira značilk (angl. feature selection) je postopek, s katerim določimo najpomembnejše spremenljivke v podatkovnem naboru in tako zmanjšamo kompleksnost modela ter izboljšamo njegovo učinkovitost. Modelu tako omogočimo, da se osredotoči na ključne informacije, kar vodi do natančnejših in hitrejših napovedi, hkrati pa preprečimo preprileganje (angl. overfitting). V tej raziskavi smo se za izbor značilk odločili uporabiti metodo informacijskega prispevka (angl. information gain). Metoda meri količino informacij, ki jo posamezna spremenljivka prispeva glede na ciljno spremenljivko. Na podlagi tega smo izbrali najpomembnejše spremenljivke za zaznavanje goljufij in odstranili pet spremenljivk z najnižjo informacijsko vrednostjo ("V22", "V13", "V15", "V26", "V25"), saj so imele minimalen vpliv na model.

Spopadanje z neuravnovešenostjo podatkov

Glede na to, da so goljufije redke v primerjavi z zakonitimi transakcijami, je pomembno obravnavati neuravnoteženost podatkov, saj bi model sicer lahko ignoriral goljufive

primere. V literaturi se pogosto uporablja metoda podvzorčenja (angl. undersampling) (Awoyemi, Adetunmbi in Oluwadare, 2017), pri kateri se zmanjša število primerov večinskega razreda, da postanejo podatki bolj uravnoteženi. Vendar pa ta metoda pogosto pripelje do izgube pomembnih podatkov o zakonitih transakcijah, kar lahko negativno vpliva na učinkovitost modela. V raziskavi smo se namesto tega odločili za uporabo metode SMOTE, ki sintetično ustvarja nove primere manjšinskega razreda (goljufij) z interpolacijo med obstoječimi primeri. SMOTE tako povečuje število goljufivih transakcij, ne da bi preprosto podvajal obstoječe primere, kot to počne naključno nadvzorčenje (angl. random oversampling). SMOTE omogoča boljšo generalizacijo modela, saj ustvarja nove, bolj realistične primere goljufij in pomaga modelu bolje prepoznati vzorce, značilne za goljufive transakcije (Fernández et al., 2018).

2.3 Modeli strojnega učenja

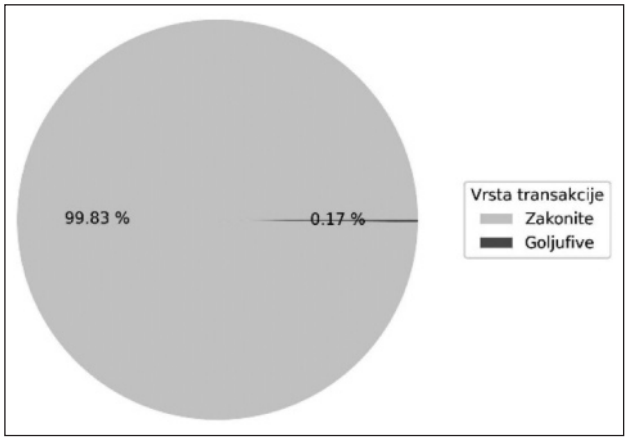
Logistična regresija je priljubljen algoritem za binarne klasifikacijske naloge, kot je zaznavanje prevar s kreditnimi karticami. Temelji na linearni regresiji, vendar napoveduje verjetnost, da spada primer v enega od dveh razredov (goljufiva ali zakonita transakcija). Njena prednost sta preprostost in jasna interpretacija koeficientov, vendar se pogosto izkaže za neučinkovito pri zaznavanju nelinearnih vzorcev med spremenljivkami.

Naivni Bayesov klasifikator temelji na Bayesovem teoremu in predpostavlja neodvisnost spremenljivk, kar redko velja v praksi. V tej raziskavi smo uporabili Gaussov naivni Bayesov klasifikator, ki je prilagojen za delo z zveznimi spremenljivkami. S tem smo predpostavili, da so spremenljivke normalno porazdeljene. Čeprav ta predpostavka omogoča hitro in enostavno usposabljanje modela, lahko v primeru, da podatki ne sledijo normalni porazdelitvi, zmanjša natančnost modela pri zaznavanju prevar.

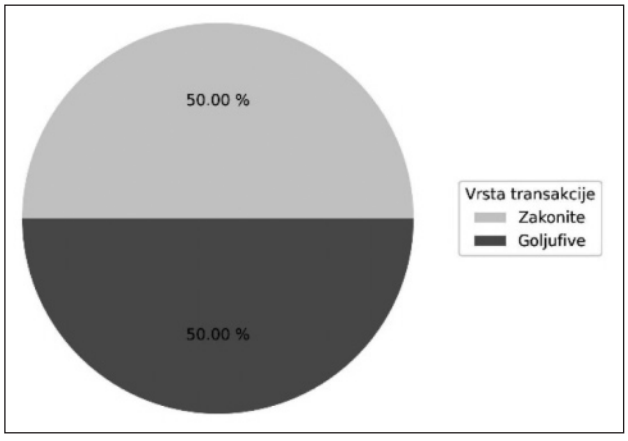
Naključni gozd je algoritem, ki združuje več odločitvenih dreves in tako izboljšuje natančnost ter zmanjšuje čezmerno prileganje. Uporablja naključne podmnožice podatkov, kar povečuje raznolikost dreves in posledično robustnost modela. Glavna prednost naključnega gozda je njegova sposobnost obdelave kompleksnih, nelinearnih podatkov, a ima visoko računsko zahtevnost, kar lahko oteži interpretacijo rezultatov.

Nevronske mreže posnemajo delovanje bioloških nevronskih sistemov in so sestavljene iz več plasti nevronov, ki obdelujejo podatke skozi vhodno plast, skrite plasti in izhodno plast. So zelo prilagodljive in sposobne zaznati kompleksne vzorce, vendar imajo pomanjkljivosti, kot so visoka računska zahtevnost, težja interpretacija in nagnjenost k preprileganju, zlasti pri manjših naborih podatkov. Pri uporabi nevronskih mrež smo v raziskavi uporabili arhitekturo z dvema skritima plastema, pri čemer je prva plast vsebovala 50 nevronov, druga pa 100 nevronov. Kot aktivacijsko funkcijo smo izbrali rektificirano linearno enoto ReLU (angl. Rectified Linear Unit), ki je priljubljena zaradi svoje enostavnosti in učinkovitosti pri reševanju nelinearnih problemov.

Slika 1: Porazdelitev zakonitih in goljufivih transakcij po uporabi metode SMOTE



Slika 2: Porazdelitev zakonitih in goljufivih transakcij v začetnem naboru podatkov



2.4 Merila uspešnosti

Namen raziskave je primerjati uspešnost zgoraj omenjenih modelov strojnega učenja pri prepoznavanju goljufivih transakcij s kreditnimi karticami. Pri ocenjevanju učinkovitosti modela za zaznavanje prevar se na prvi pogled zdi, da je naloga preprosta, idealen sistem bi moral zaznati čim večje število pravilnih klasifikacij in zaznati vse goljufive transakcije. Po navadi se za merjenje tega uporablja točnost (angl. accuracy), vendar je zaradi narave problema zaznavanja prevar, pri čemer gre za neuravnotežene podatke in je napačna klasifikacija goljufivih transakcij veliko večje breme, uporaba samo tega merila nezadostna

(Guo in Viktor, 2004). Na primer model, ki vse transakcije označi za zakonite, bi pri zelo nizkem deležu prevar (npr. 0,1 %) dosegel visoko natančnost, čeprav ne bi zaznal nobene goljufije. V literaturi o zaznavanju prevar je zato splošno sprejeto, da so potrebna ustreznejša merila (Dal Pozzolo et al., 2017; Elkan, 2001). Da bi dobili vpogled v rezultate vsakega algoritma, smo zato upoštevali naslednja merila ocenjevanja:

Natančnost (angl. precision) je razmerje med pravilno pozitivnimi primeri (angl. true positive, v nadaljevanju: TP) in vsoto pravilno pozitivnih ter lažno pozitivnih primerov (angl. false positive, v nadaljevanju: FP). Natančnost meri, koliko od napovedanih prevar je v resnici prevar. Natančnost zavzema vrednosti med 0 in 1, pri čemer je vrednost bližje 1 boljša, saj to pomeni, da je večina zaznanih prevar pravilno zaznanih (manj lažno pozitivnih primerov). Formula:

$$natančnost = \frac{TP}{TP + FP}$$

Priklic (angl. recall) je razmerje med pravilno pozitivnimi primeri (TP) in vsoto pravilno pozitivnih ter lažno negativnih primerov (angl. false negative, v nadaljevanju: FN). Prikazuje, kolikšen delež dejanskih prevar je bil pravilno odkrit. Tudi priklic zavzema vrednosti med 0 in 1, pri čemer je višja vrednost boljša, saj pomeni, da model zazna večino dejanskih prevar (manj lažno negativnih primerov). Formula:

$$priklic = \frac{TP}{TP + FN}$$

F1-mera (angl. F-score) je harmonično povprečje natančnosti in priklica, kar pomeni, da združuje obe vrednosti v eno vrednost, ki upošteva tako pravilno zaznane prevare kot tiste, ki jih model spregleda. F1-mera zavzema vrednosti med 0 in 1, pri čemer je višja vrednost boljša. Visoka F1-mera pomeni, da model uravnoteženo dobro prepoznava prevare, hkrati pa prepozna malo zakonitih prevar za lažne.

$$F1 - mera = \frac{2 \times natančnost \times priklic}{natančnost + priklic}$$

AUC-ROC je merilo, ki prikaže, kako dobro ločuje model med razredi pri različnih pragih odločanja. Krivulja ROC primerja priklic in lažno pozitivne napovedi (angl. false positive rates – FPR) za vsak prag. Model, katerega krivulja ROC prevladuje v grafu, je natančnejši, idealen model pa doseže točko (0,1), kar pomeni brez lažnih pozitivnih in negativnih napovedi. Naključni model bi imel krivuljo vzdolž diagonale. Ker je primerjava krivulj lahko težavna, se za jasnejšo oceno modela uporablja površina pod krivuljo (AUC). Mera AUC je zlasti uporabna pri neuravnoteženih podatkovnih naborih in predstavlja standardno merilo uspešnosti klasifikatorjev (Chawla et al., 2008).

3. Rezultati

Za oceno uspešnosti štirih algoritmov strojnega učenja – logistične regresije, naivnega Bayesovega klasifikatorja, naključnega gozda in nevronske mreže – pri zaznavanju goljufivih transakcij s kreditnimi karticami so bila analizirana merila uspešnosti, predstavljena v poglavju 2.4. Poleg tega so predstavljene matrike zmede, ki prikazujejo uspešnost modelov pri ločevanju med zakonitimi in goljufivimi transakcijami. Rezultati so združeni v skupni preglednici, ki omogoča neposredno primerjavo med algoritmi.

3.1 Logistična regresija

Na podlagi preglednice 1 lahko opazimo, da logistična regresija pravilno klasificira večino zakonitih transakcij, vendar pa je pri zaznavanju goljufivih transakcij učinkovitost bistveno nižja. Pravilno prepozna 129 goljufivih primerov, hkrati pa označi 2016 zakonitih transakcij za goljufive (lažno pozitivni primeri) in 19 goljufivih transakcij za zakonite (lažno negativni primeri).

Preglednica 1: Matrika zmede logistične regresije

		Napovedano	
		Zakonite	Goljufive
Dejansko	Zakonite	83.279	2016
	Goljufive	19	129

3.2 Naivni Bayesov klasifikator

Preglednica 2 prikazuje matriko zmede naivnega Bayesovega klasifikatorja. Model uspešno prepozna 83.250 zakonitih transakcij in 123 goljufivih transakcij. Vendar pa napove 2045 zakonitih transakcij za goljufive (lažno pozitivni primeri) in zgreši 25 goljufivih transakcij (lažno negativni primeri).

Preglednica 2: Matrika zmede naivnega Bayesovega klasifikatorja

		Napovedano	
		Zakonite	Goljufive
Dejansko	Zakonite	83.250	2045
	Goljufive	25	123

3.3 Naključni gozd

Kot prikazuje preglednica 3, dosega naključni gozd visoko stopnjo pravilne klasifikacije tako zakonitih kot goljufivih transakcij. Model pravilno prepozna 85.275 zakonitih transakcij in 114 goljufivih transakcij. Le 20 zakonitih transakcij je bilo označenih za goljufive (lažno pozitivni primeri), model pa ni prepoznal 34 goljufivih transakcij (lažno negativni primeri).

Preglednica 3: Matrika zmede naključnega gozda

		Napovedano	
		Zakonite	Goljufive
Dejansko	Zakonite	85.275	20
	Goljufive	34	114

3.4 Nevronska mreža

Matrika zmede nevronske mreže je predstavljena v preglednico 4. Model pravilno klasificira 85.253 zakonitih transakcij in 111 goljufivih transakcij. Označi 42 zakonitih transakcij za goljufive (lažno pozitivni primeri), ne prepozna pa 37 goljufivih transakcij (lažno negativni primeri).

Preglednica 4: Matrika zmede nevronske mreže

		Napovedano	
		Zakonite	Goljufive
Dejansko	Zakonite	85.253	42
	Goljufive	37	111

3.5 Rezultati uspešnosti

V spodnji preglednici so prikazani rezultati štirih uporabljenih modelov: logistične regresije, naivnega Bayesovega klasifikatorja, naključnega gozda in nevronske mreže. Rezultati iz preglednice 5 kažejo precejšnje razlike v uspešnosti med modeli. Logistična regresija in naivni Bayes kažeta zelo nizko natančnost (0,06), kar pomeni, da prepoznata veliko število zakonitih transakcij za goljufive. Kljub temu oba modela dosegata visok priklic (0,87 pri logistični regresiji in 0,83 pri naivnem Bayesu), kar pomeni, da uspešno prepoznata večino goljufivih transakcij. Njuna nizka F1-mera (0,11) nakazuje neuravnoteženost med natančnostjo in priklicem, kar zmanjšuje njuno celotno učinkovitost pri prepoznavanju goljufij.

Naključni gozd se izkaže za najboljši model, saj dosega visoko natančnost (0,85), kar pomeni, da je le malo zakonitih transakcij napačno prepoznanih za goljufive. Poleg tega doseže model priklic 0,77, kar pomeni, da uspešno prepozna večino goljufivih transakcij. Njegova F1-mera (0,81) in AUC-ROC (0,965) kažeta na uravnoteženost med natančnostjo in priklicem ter splošno visoko zmogljivost modela.

Preglednica 5: Primerjava uspešnosti modelov

Model	Natančnost	Priklic	F1-mera	AUC-ROC
Logistična regresija	0,06	0,87	0,11	0,961
Naivni Bayes	0,06	0,83	0,11	0,956
Naključni gozd	0,85	0,77	0,81	0,965
Nevronska mreža	0,73	0,75	0,74	0,954

Nevronska mreža dosega solidne rezultate z natančnostjo 0,73, kar kaže, da napačno prepozna nekoliko več zakonitih transakcij za goljufive v primerjavi z naključnim gozdom. Priklic modela je 0,75, kar pomeni, da prepozna večino goljufivih transakcij, F1-mera pa je 0,74. AUC-ROC vrednost (0,954) je konkurenčna, vendar nekoliko nižja od naključnega gozda, kar kaže na dobro sposobnost zaznavanja goljufij, a manjšo robustnost v primerjavi z najboljšim modelom.

4. Razprava

Rezultati raziskave kažejo, da je naključni gozd dosegel najboljše rezultate med analiziranimi modeli strojnega učenja. Z natančnostjo 0,85, priklicem 0,77 in F1-mero 0,81 je model izkazal dobro sposobnost prepoznavanja goljufivih transakcij ob hkratnem majhnem številu lažno pozitivnih primerov. Prav tako je dosegel najvišjo vrednost AUC-ROC (0,965), kar potrjuje njegovo visoko učinkovitost pri ločevanju med zakonitimi in goljufivimi transakcijami. Nevronska mreža je z natančnostjo 0,73, priklicem 0,75 in F1-mero 0,74 dosegla solidne rezultate, vendar nekoliko zaostaja za naključnim gozdom, čeprav je AUC-ROC (0,954) še vedno visoka. Logistična regresija in naivni Bayesov klasifikator pa sta dosegla nizko natančnost (0,06), kar pomeni veliko število lažno pozitivnih napovedi. Kljub visokemu priklicu (0,87 in 0,83) je njuna nizka F1-mera (0,11) pokazala pomanjkanje uravnoteženosti med natančnostjo in priklicem.

Rezultati v celoti podpirajo našo začetno hipotezo, da bodo kompleksnejši modeli, kot sta naključni gozd in nevronska mreža, uspešnejši od logistične regresije in naivnega Bayesovega klasifikatorja pri zaznavanju prevar. Pri primerjavi rezultatov naše raziskave z drugimi študijami opazimo nekaj razlik. V raziskavi Varmedja et al. (2019) so za logistično regresijo dosegli boljše ravnotežje med natančnostjo (0,5882) in priklicem (0,9184) v primerjavi z našo študijo (natančnost 0,06, priklic 0,87). Podobno poroča raziskava Mim et al. (2024) o nizki natančnosti (0,0814), vendar visokem priklicu (0,8878), kar nakazuje težave logistične regresije pri zaznavanju goljufij.

Naivni Bayesov klasifikator je prav tako pokazal nizko natančnost v vseh raziskavah. Naša študija je dosegla natančnost 0,06, medtem ko so Varmedja et al. (2019) poročali o natančnosti 0,1617, Mim et al. (2024) pa še o nižji natančnosti 0,1429, kar kaže na izzive pri uporabi tega modela za kompleksne probleme.

Naključni gozd je v vseh raziskavah pokazal najboljše rezultate. Naša raziskava je dosegla natančnost 0,85, priklic 0,77 in AUC-ROC 0,965, kar je skladno z rezultati Varmedja et al. (2019) (natančnost 0,9638, priklic

0,8163) in Mim et al. (2024) (natančnost 0,8723, F1-mera 0,8542, AUC-ROC 0,9650).
Nevronska mreža je v naši študiji dosegla natančnost 0,73, priklic 0,75 in AUC-ROC 0,954, kar je primerljivo z Varmedja et al. (2019) in nekoliko zaostaja za boljšimi rezultati Mim et al. (2024) (AUC-ROC 0,9881, priklic 0,9286).
Omejitve te raziskave so povezane predvsem z omejeno uporabo metod za obravnavo neuravnoteženih podatkov in omejenim obsegom testiranih algoritmov. Čeprav je bila uporabljena metoda SMOTE za izboljšanje zmogljivosti modelov, ta ne odpravi vseh težav, povezanih z neuravnoteženimi podatkovnimi nabori, kot je čezmerno generiranje sintetičnih podatkov, kar lahko pripelje do pristranskega učenja modelov.
Dodatna omejitev je transformacija podatkov s pomočjo PCA zaradi anonimnosti, kar otežuje natančno interpretacijo spremenljivk. Zaradi tega je težje razumeti vpliv posameznih spremenljivk na rezultate modelov, kar omejuje možnosti za izboljšanje modelov ali prilagajanje parametrov v praktičnih aplikacijah.
V prihodnjih raziskavah bi bilo smiselno razširiti obseg algoritmov in vključiti metode, kot so XGBoost, AdaBoost in LightGBM, ki so znane po svoji uspešnosti pri klasifikacijskih nalogah. Prav tako bi lahko raziskali vpliv uporabe drugih tehnik obravnave neuravnoteženih podatkov, kot je hibridno podvzorčenje in nadvzorčenje. Najpomembnejša smer nadaljnjih raziskav bi bila pridobitev transparentnih podatkov o transakcijah, kar bi omogočalo razumevanje dejanskih vplivov posameznih faktorjev na zaznavanje prevar.
Praktične implikacije te raziskave so pomembne za finančne ustanove, ki se spoprijemajo z zaznavanjem goljufij s kreditnimi karticami. Naključni gozd, ki je izkazal najboljše rezultate, bi lahko zmanjšal število napačno označenih zakonitih transakcij za goljufive, s čimer bi povečal zadovoljstvo strank in zmanjšal stroške bank. Nevronske mreže z dobrimi rezultati pa predstavljajo učinkovito alternativo, zlasti pri večjih podatkovnih naborih, s čimer bi lahko prispevale k zaznavanju bolj sofisticiranih prevar.

Sklep

Raziskava je pokazala, da je med analiziranimi modeli naključni gozd izstopal kot najučinkovitejši, saj je dosegel najvišje vrednosti pri vseh merilih, kar potrjuje njegovo primernost za tovrstne klasifikacijske naloge. Nevronska mreža je prav tako pokazala solidne rezultate, čeprav nekoliko slabše od naključnega gozda. Po drugi strani sta logistična regresija in naivni Bayesov klasifikator dosegla nizko natančnost in visoko število lažno pozitivnih napovedi, kljub visokemu priklicu.
Praktične implikacije teh rezultatov so ključne za finančne ustanove, saj lahko uvedba modelov, kot je naključni gozd ali nevronske mreže, pomembno izboljša zaznavanje prevar ob hkratnem zmanjšanju napačno označenih zakonitih transakcij, kar bi prispevalo k višjemu zadovoljstvu strank in znižanju stroškov, povezanih z vračili sredstev.
Nadaljnje raziskave bi morale vključevati podrobnejše podatke, ki niso anonimni, saj bi to omogočilo boljšo interpretacijo spremenljivk in izboljšanje modelov. Prav tako bi bilo smiselno raziskati uporabo naprednejših algoritmov, kot so XGBoost, AdaBoost in LightGBM ter vpliv drugih tehnik obravnave neuravnoteženih podatkov na uspešnost modelov.

Viri in literatura / References:

1. Awoyemi, J. O., Adetunmbi A. O. in Oluwadare, S. A. (2017) "Credit card fraud detection using machine learning techniques: A comparative analysis", *International Conference on Computing Networking and Informatics (ICCNI)*, pp. 1-9. doi: 10.1109/ICCNI.2017.8123782.
2. Chawla, V. N., Cieslak, A. D., Hall, O. L. in Joshi, A. (2008) "Automatically countering imbalance and its empirical relationship to cost", *Data Min. Knowl. Discov*, 17, pp: 225-252. doi: 10.1007/s10618-008-0087-0.
3. Dal Pozzolo, A., Boracchi, G., Caelen, O., Alippi, C. in Bontempi, G. (2017) "Credit Card Fraud Detection: A Realistic Modeling and a Novel Learning Strategy", *IEEE Transactions on Neural Networks and Learning Systems*, pp: 1-14. doi: 10.1109/TNNLS.2017.2736643.
4. Elkan, C. (2001) "The foundations of cost-sensitive learning", *Proceedings of the Seventeenth International Conference on Artificial Intelligence*, pp: 4-10.
5. European Central Bank (2023) *Seventh report on card fraud*. Dostopno na: https://www.ecb.europa.eu/press/cardfraud/html/ecb.cardfraudreport202305~5d832d6515.en.html.
6. Fernández, A., Garcia, S., Herrera, F. in Chawla, N. (2018) "SMOTE for Learning from Imbalanced Data: Progress and Challenges", *Marking the 15-year Anniversary. Journal of Artificial Intelligence Research,* 61, pp. 863-905. doi: 10.1613/jair.1.11192.
7. Guo, H. in Viktor, H. L. (2004) "Learning from imbalanced data sets with boosting and data generation: the databoost-im approach", *ACM SIGKDD Explorations Newsletter*, 6(1), pp: 30-39. doi: 10.1145/1007730.1007736.
8. Hashim, H. A., Salleh, Z., Shuhaimi, I. in Ismail, N. A. N. (2020) "The risk of financial fraud: a management perspective", *Journal of Financial Crime*, 27(4), pp. 1143-1159. doi: 10.1108/JFC-04-2020-0062.
9. Kaggle (2013). *Credit Card Fraud Detection*. Dostopno na: https://www.kaggle.com/datasets/mlg-ulb/creditcardfraud.
10. Mim, M. A., Majadi, N. in Mazumder, P. (2024) "A soft voting ensemble learning approach for credit card fraud detection", *Heliyon*, 10(3), pp: e25466. doi: 10.1016/j.heliyon.2024.e25466.
11. Varmedja, D., Karanovic, M., Sladojevic, S., Arsenovic, M. in Anderla, A. (2019) "Credit Card Fraud Detection - Machine Learning methods", pp. 1-5. doi: 10.1109/INFOTEH.2019.8717766.