Doc. dr. sc. Robertina Zdjelar

Kompetencije, znanje i vještine u kontekstu NIS 2 Direktive

Sažetak

Svijest o osobnoj odgovornosti svakog dionika u kibernetičkom prostoru postala je važna jer prema statistikama upravo ljudski faktor je najčešće uzrok počinjenja propusta iz neznanja i nepažnje, a koji dovode do incidenata koji se mogu prerasti u krizu. Razvoj svijesti treba poticati komuniciranjem o temi, približavanjem konkretnih primjera iz prakse u kojima dionici prepoznaju sebe kao moguću žrtvu iskorištenu u pokušajima kibernetičkih napada. Prepoznavanje mogućih napada te naučeni i uvježbani načini postupanja u takvim situacijama omogućavaju dionicima u sustavu da pravilno postupe s ciljem da se izbjegne nastanak štetnog događaja odnosno incidenta. Takvi obrasci ponašanja razvijaju se kroz održavanje praktičnih treninga i vježbi. Stručnjaci, eksperti, koji se po potrebi angažiraju u slučaju nastanka incidenta moraju imati specijalistička znanja za prepoznavanje sumnjivih nakana napadača, procjenu razine ozbiljnosti situacije i otklanjanje posljedica trebaju se educirati na sustavan i multidisciplinaran način. U ovom članku biti će govora o razvoju kompetencija, širenju znanja i stjecanju praktičnih vještina o čemu govori i NIS 2 Direktiva, ali i nacionalno zakonodavstvo. Rezultati raznih stručnih institucionalnih istraživanja i individualnih znanstvenih istraživanja također su u sažetom obliku prikazani u članku.

Ključne riječi: ***edukacije, kompetencije, NIS 2 Direktiva, program podizanja svijesti, svijest o kibernetičkim napadima, treninzi***

1. Uvod

Područja od značaja koja se moraju sagledavati u okviru kontrola kibernetičke sigurnosti su sigurnost ljudskih resursa, kontrola pristupa, kriptografija i zaštita mrežnih servisa. Područje zaštite ljudskih resursa započinje već kod zapošljavanja raznim provjerama podataka i činjenica vezanih uz kandidate. Nakon provjere kandidata za odabrane kandidate posebno se provodi dodatno upoznavanje s internim pravilima što se uglavnom regulira i kroz ugovor o radu ili drugi dokument izdan s istom svrhom. Treninzima se osiguravaju znanja i vještine potrebne za ispunjenje određenih zahtjeva za kompetencijama. Podizanjem razine svijesti se postiže promjena stavova i ponašanja vezano za primjenu propisanih sigurnosnih pravila i razumijevanje težine prijetnji kojima je sustav ili njegovi segmenti izložen. Edukacijama se postižu specijalizacije za određena područja sigurnosti te se na taj način osiguravaju specijalisti u području kibernetičke sigurnosti. U nastavku će biti govora o obvezama i preporukama iz pravne regulative, kako europske tako i nacionalne, a isto tako i o međunarodnim standardima i dobroj praksi o treninzima i širenju svijesti o važnosti kibernetičke sigurnosti.

2. Pravna regulativa

Recital 50. NIS 2 Direktive govori kako su svijest o kibersigurnosti i kiberhigijena ključni za povećanje razine kibersigurnosti u Uniji, posebno s obzirom na sve veći broj povezanih uređaja koji se sve više upotrebljavaju u kibernapadima. Također preporuča se *uložiti napore kako bi se povećala opća svijest o rizicima povezanima s takvim proizvodima, dok bi ocjenjivanja na razini Unije mogla pomoći u osiguravanju zajedničkog razumijevanja takvih rizika na unutarnjem tržištu.*

Svijest o osobnoj odgovornosti je svijest o sposobnosti za informiranost o stanju u kritičnim i incidentnim situacijama zbog kojih uobičajeni način informiranja javnosti nije u funkciji što je naglašeno Recitalom 72. NIS 2 Direktive.

Recital 89. NIS 2 Direktive govori da bi ključni i važni subjekti trebali „usvojiti niz osnovnih praksi računalne kiberhigijene, kao što su načela nultog povjerenja, ažuriranja softvera, konfiguracija uređaja, segmentacija mreže, ***upravljanje identitetima i pristupom ili informiranje korisnika, organizirati osposobljavanje svojeg osoblja i podizati razinu osviještenosti u području kiberprijetnji, phishinga ili tehnika društvenog inženjeringa“***.

Recital 119. NIS 2 Direktive ukazuje na činjenicu da bolju informiranost o kiberprijetnjama treba osigurati i putem redovite razmjene informacija o prijetnjama i ranjivostima među subjektima.

Nacionalna strategija za kibersigurnost propisana je člankom 7. NIS 2 Direktive, a koja između ostaloga sadrži ***plan i potrebne mjere za povećanje opće razine osviještenosti o kibersigurnosti među građanima***. Navedeno je važno osigurati u praksi iz razloga jer e-uključivosti često nije na zadovoljavajućoj razini pogotovo kada je riječ o populaciji 54+, a što je jedan od češćih razloga nesigurnosti pri korištenju informacijsko komunikacijske tehnologije (IKT).

Članak 1. st. 3. Zakona o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24) govori da su od nacionalnog značaja za Republiku Hrvatsku postizanje i održavanje visoke zajedničke razine kibernetičke sigurnosti, posebno kroz razvoj i kontinuirano unaprjeđenje politika kibernetičke zaštite i njihove provedbe, razvoj nacionalnih sposobnosti u području kibernetičke sigurnosti, jačanje suradnje i koordinacije svih relevantnih tijela, jačanje suradnje javnog i privatnog sektora, promicanje razvoja, integracije i upotrebe relevantnih naprednih i inovativnih tehnologija, ***promicanje i razvoj obrazovanja i osposobljavanja u području kibernetičke sigurnosti te razvojne aktivnosti usmjerene na jačanje svijesti o kibernetičkoj sigurnosti***.

Nastavno na obvezu donošenja Nacionalne strategije za kibersigurnost u članku 55. Zakona o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24) propisan je i obvezni sadržaj (II. Dio, Prilog IV. Obvezni sadržaj Nacionalnog akta strateškog planiranja iz područja kibernetičke sigurnosti) koji između ostaloga treba uključiti i politike „– ***za promicanje i razvoj obrazovanja i osposobljavanja u području kibernetičke sigurnosti, vještina u području kibernetičke sigurnosti, informiranja te istraživačkih i razvojnih inicijativa u području kibernetičke sigurnosti, kao i smjernica o dobroj praksi i kontrolama kibernetičke higijene namijenjenih građanima, kao i javnim i privatnim subjektima***”.

Uredbom o kibernetičkoj sigurnosti („Narodne novine“ br. 135/24) propisane su mjere upravljanja kibernetičkim rizicima. Neke od mjera odnose se na kompetencije, znanja i vještine, a definirane su kako slijedi:

- „*1. Predanost i odgovornost osoba odgovornih za provedbu mjera upravljanja kibernetičkim sigurnosnim rizicima“,* a koja operativno podrazumijeva i *„1.9.* ***osigurati odgovarajuće aktivnosti nužne za podizanje svijesti*** *osoba odgovornih za provedbu mjera o kibernetičkoj sigurnosti, a osobito u pitanjima upravljanja kibernetičkim sigurnosnim rizicima i mogućeg učinka tih rizika na usluge koje subjekt pruža, odnosno djelatnost koju obavlja.* ***Ove aktivnosti uključuju edukativne radionice, seminare i druge oblike edukacija o aktualnim kibernetičkim prijetnjama, najboljim kibernetičkim sigurnosnim praksama, te o važnosti poduzimanja proaktivnih mjera upravljanja kibernetičkim sigurnosnim rizicima.*** *Ovim podskupom mjera upravljanja kibernetičkim sigurnosnim rizicima potrebno je osigurati da upravljačko tijelo subjekta bude informirano i kontinuirano angažirano u postizanju i održavanju visoke razine kibernetičke sigurnosti”*
- *„4. Sigurnost ljudskih potencijala i digitalnih identiteta”, a koja nalaže da treba:*
  - *„4.4. osigurati redovnu obuku o osnovnim praksama kibernetičke higijene i podizanje svijesti o rizicima i kibernetičkim prijetnjama za sve zaposlenike, neposredno nakon stupanja osobe u radni odnos u subjektu te kasnije redovito tijekom radnog odnosa. Subjekt mora uspostaviti program podizanja svijesti u skladu s kibernetičkom sigurnosnom politikom, tematski specifičnim politikama i relevantnim procedurama kibernetičke sigurnosti u okviru mrežnog i informacijskog sustava subjekta.* ***Podizanje svijesti mora obuhvatiti osnovne IT vještine i znanja*** *(primjerice svi zaposlenici moraju proći osposobljavanje za sigurno korištenje e-pošte i pretraživanje Interneta).* ***Program podizanja svijesti*** *treba sadržavati poglavlja kao što su:*
    - *uobičajene i dokumentirane upute koje se odnose na sigurnost*
    - *IT sustava i osobne IT imovine što uključuje i mobilne uređaje*
    - *sigurno korištenje autentifikacijskih sredstava i vjerodajnica (primjerice izbjegavanje korištenja istih lozinki na različitim javnim servisima te izbjegavanje korištenja službenih adresa na javnim servisima radi smanjivanja rizika od napada, izbjegavanje spremanja lozinki u web preglednike itd.)*
    - *prepoznavanje i prijavu najčešćih incidenata“.*
  - *„4.11. implementirati testiranje socijalnog inženjeringa, simulacije krađe identiteta (phishing) i programe podizanja svijesti. Ove aktivnosti moraju biti redovite i obuhvatiti sve zaposlenike subjekta kako bi se identificirale ranjivosti i educiralo osoblje o prepoznavanju i odgovoru na takve ranjivosti. Programi podizanja svijesti trebaju uključivati edukativne materijale, radionice i praktične vježbe. Time se jača sigurnosna kultura unutar subjekta i smanjuje rizik od uspješnih napada socijalnog inženjeringa.”*

3. Međunarodni standardi i dobre prakse

Kada je riječ o kvaliteti u poslovanju onda u to svakako treba biti uključen i razvoj ljudskih potencijala, njihovih kompetencija, znanja i vještina. U tom smislu moguće je pratiti preporuke ISO 10015:2019 Upravljanje kvalitetom – Smjernice za upravljanje kompetencijama i razvoj ljudskih potencijala (engl. Quality management — Guidelines for competence management and people development). Ovaj dokument daje smjernice za uspostavu, implementaciju, održavanje i poboljšanje sustava za upravljanje kompetencijama i razvoj ljudskih potencijala kako bi organizacija pozitivno utjecala na ishode povezane s usklađenošću proizvoda i usluga te potrebama i očekivanjima relevantnih zainteresiranih strana. U dijelu definicija ISO 10015:2019 oslanja se na zahtjeve normi skupine ISO 9000, a za ovu temu bitno je pobliže odrediti pojmove:

- kompetencija je „sposobnost primjene znanja i vještina za postizanje željenih rezultata“
- vještina je „naučena sposobnost izvođenja zadatka prema određenim očekivanjima“
- znanje je „ljudska ili organizacijska imovina koja omogućuje učinkovite odluke i djelovanje u kontekstu“.

ISO 22361:2022 Zaštita i otpornost – upravljanje krizama - Smjernice (engl. Security and resilience — Crisis management — Guidelines) u poglavlju 6.2. definira temeljne vještine vođenja kod upravljanja krizama, a o čemu je više bilo govora u poglavlju vezanom uz kibernetičke krize.

ISO/IEC 27002:2022 Informacijska sigurnost, kibernetička sigurnost i zaštita privatnosti - kontrole informacijske sigurnosti (engl. Information security, cybersecurity and privacy protection — Information security controls) ističe važnost svijesti o nužnosti očuvanja informacijske sigurnosti i o načinima kako se ona postiže, na što sve korisnik mora obraćati pažnju, koji podaci su povjerljivi i kako postupati s njima. Primjerice upravljanje identitetom (poglavlje 5.16.) jedno je od područja za koje su definirani zahtjevi za subjekte koji se certificiraju po ovoj normi. Također, propisane kontrole vezane uz ljudske resurse koje se trebaju uvesti i provoditi definirane su poglavljem 6., a što je već detaljno opisano u ranije objavljenom članku vezanom uz uspostavu i provedbu kontrole u kontekstu usklade poslovanja s NIS 2 Direktivom.

Iako je u najavi novo izdanje norme o tehnikama zaštite, u kojem je najavljeno detaljnije postavljanje zahtjeva za aktivnosti razvoja kompetencija, važeća je norma ISO/IEC 27031:2011 Informacijska tehnologija – tehnike zaštite – Smjernice za spremnost informacijske i komunikacijske tehnologije za osiguranje kontinuiteta poslovanja (engl. Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity). O osiguranju kontinuiteta poslovanja već je detaljnije bilo govora u ranije objavljenom članku.

IKT spremnost za kontinuitet poslovanja (engl. ICT readiness for business continuity (IRBC)) u upravljanju kontinuitetom poslovanja ključan je preduvjet za uspjeh. IKT spremnost ne nastaje i ne održava se sama po sebi, kako se često puta to podrazumijeva kao što se podrazumijeva i digitalna pismenost. Kako bi spremnost bila na očekivanom nivou i kako bi

efekti od primjene znanja i vještina bili na razini očekivanoga potrebno je navedene aktivnosti planirati, kontinuirano raditi na podizanju razine svijesti zaposlenika o važnosti korištenja (digitalnog) identiteta na siguran način, resursa, razmjene podataka s dužnom pažnjom i stalnom dozom opreza jer prijetnje i napadi su često puta na prvi pogled neprepoznatljivi i nastaju primjenom vrlo vjernih kopija vizualnog identiteta žrtve preko koje se napad vrši na krajnjeg korisnika s ciljem krađe identiteta (engl. phishing). Kako bi korisnici IKTa bili svjesni opasnosti potrebno je informirati ih o napadima i tehnikama napada, slati informacije na što trebaju obratiti pažnju i slično te kako izbjeći „upadanje u zamku“. Phishing je postupak prijevare u kojem napadač pokušava pribaviti povjerljive osobne podatke (identitet) „maskiranjem“ u pouzdanog subjekta u elektroničkoj komunikaciji.

ISO/IEC 27032:2023 Kibernetička sigurnost – Smjernice za Internet sigurnost (engl. Cybersecurity — Guidelines for Internet security) predviđaju uspostavu ***programa za podizanje svijesti*** o ulozi kibernetičke sigurnosti i važnosti odgovornog ponašanja u kibernetičkom prostoru.

U prosincu 2022. godine je ENISA izdala publikaciju grupe autora Christoforatos, N., Ifi genia, L., Rekleitis, E., Van Heurck, C., Zacharis, A. (2022) u kojoj su objavljeni rezultati provedene vježbe spremnosti djelovanja u stanju kibernetičke krize u PAN – Europskom području. ENISA je organizirala niz vježbi vezanih za upravljanje kibernetičkim incidentima i krizama gdje se simulacijom stvorila situacija u kojoj su kibernetički incidenti prerasli u krizu i gdje je analizom incidenata pri korištenju naprednih tehnologija testirana spremnost i sposobnost snalaženja sudionika vježbe u takvim situacijama. Provođenjem vježbe testirana je na razini EU tehnička i operativna suradnja u nastaloj kibernetičkoj krizi, provedeno je testiranje razine spremnosti na lokalnoj razini i plana otpornosti te su uvježbane tehničke sposobnosti na EU i na lokalnoj razini. Nastavno na održane praktične vježbe testiranja spremnosti na kibernetičke incidente i krize donijeti su zaključci kako je potrebno osigurati sredstva za kontinuirano testiranje spremnosti na lokalnoj razini u cilju stalnog poboljšanja i jačanja otpornosti na kibernetičke prijetnje.

Također, u 2024. godini je izdana publikacija „Budi pametniji od napadača“ (engl. Be smarter than a hacker) autora Kalenti, M. i Biro, P. (2024). ENISA radi podizanja svijesti o kibernetičkoj sigurnosti kroz cjelogodišnji komunikacijski plan i strategiju kontinuirano provodi razne aktivnosti kampanje. Objavama o društvenom inženjeringu i utjecaju koji može imati na kibernetičku sigurnost svakog pojedinca tijekom 2023. godine radilo se na podizanju svijesti o rizicima društvenog inženjeringa. Medijska prisutnost ENISA-e i teme kibernetičke sigurnosti putem atraktivnih i dobro osmišljenih sadržaja izazvala je interes i angažirala ciljane skupine da u što većoj mjeri prate objave i šire svijest o važnosti kibernetičkih napada. Kampanja pod nazivom „Budi pametniji od napadača“ služila je kao snažan podsjetnik naglašavajući važnost budnosti i razboritosti tijekom korištenja internetskog sadržaja i usluga. Kampanjom se željelo podići svijest o prijetnjama na način da se: *povećava razumijevanje sveprisutne prijetnje; kod pojedinaca razvije sposobnost prepoznavanja prijetnje, održavanja razine opreza i informiranosti o online interakcijama; potiče na oprez: promiče oprezan način razmišljanja, potičući pojedince da pokažu razboritost i kritičko razmišljanje, čime se smanjuje osjetljivost na društveni inženjering; njegovanjem kulture obrazovanja i svijesti potiče se korisnike na kontinuirano učenje i stjecanje znanja o kibernetičkoj sigurnosti.*

4. Preporučene aktivnosti za podizanje svijesti o važnosti kibernetičke sigurnosti

Svaki korisnik IKTa bilo da je zaposlenik ključnog ili važnog subjekta, zaposlenik njegovog poslovnog partnera ili krajnji kupac robe/korisnik usluge bitna je karika u osiguranju otpornosti na kibernetičke napade i održavanju kibernetičke sigurnosti. Što je veći broj uključenih korisnika i frekvencija korištenja IKT usluga veća to je veća vjerojatnost da postoji određena kategorija korisnika koji nisu u potpunosti osviješteni važnosti vlastitih postupaka kada je riječ o aktivnostima u kibernetičkom prostoru.

Sukladno normama i dobroj praksi o čemu je bilo govora u prethodnom poglavlju u nastavku će biti izdvojene neke preporučene aktivnosti za podizanje svijesti o važnosti kibernetičke sigurnosti.

Sveobuhvatan pristup razvoju otpornosti na kibernetičke napade podrazumijeva informiranje i praktične vježbe snalaženja u incidentnoj ili kriznoj situaciji. Posebne kategorije zaposlenika, stručnjaci i eksperti, moraju biti osviješteni svoje uloge i odgovornosti u zaštiti kibernetičke sigurnosti. Osim vlastitih zaposlenika unutar ključnog ili važnog subjekta nužno je informirati i treće strane o njihovoj ulozi u očuvanju kibernetičke sigurnosti jer često puta scenariji kibernetičkih napada iskorištavaju povjerenje koje ključni ili važan subjekt ima u odnosu na treću stranu.

Upravljanje kompetencijama prije svega podrazumijeva utvrđivanje potrebnih kompetencija te procjenu dostignute razine kod postojećih zaposlenika na ključnim radnim mjestima. Neusklađenosti između potrebnih i stečenih kompetencija treba smanjiti kroz provođenje treninga i stjecanje zadanih kompetencija, o čemu je potrebno voditi evidenciju u okviru upravljanja ljudskim resursima.

Dobro je imati na umu da se treninzima i vježbama stječu vještine, no bez razvijene svijesti o praktičnoj primjeni stečenih vještina i djelovanju na promjene ponašanja nema garantiranog učinka.

Razvoj kompetencija ljudskih resursa složen je zadatak koji se realizira u nekoliko faza. Prije svega treba utvrditi potrebne kompetencije po radnim mjestima i provesti analizu imaju li postojeći zaposlenici zahtijevanu razinu kompetencija. Ukoliko se pokaže da postoje radna mjesta kod kojih postoji neusklađenost zadanih i stvarnih kompetencija potrebno je donijeti plan razvoja kompetencija kojim se utvrđuje tip i struktura mjera za podizanje kompetencija. Mjere edukacije i osvješćivanja potrebno je provesti u praksi nakon čega je neophodno, radi mjerenja postignutih rezultata, provesti evaluaciju. Ovisno o radnim zadacima odnosno radnom mjestu, odgovornostima i ulogama kompetencije treba razmatrati na organizacijskoj razini, na razini tima i na osobnoj razini.

Moguće aktivnosti za razvoj kompetencija uključuju provođenje praktičnih ciljanih vježbi, konferencije, stručne forume ili slične događaje za umrežavanje stručnjaka u cilju širenja znanja i iskustava, radionice, samostalno učenje i rad na temama ključnim za podizanje razine kompetentnosti. S druge strane kod kreiranja plana razvoja kompetencija aktivnosti treba podijeliti na ciljane skupine kako bi se uložena sredstva ciljano koristila za razvoj određenih kompetencijskih osobina. Programi usavršavanja mogu se podijeliti i prema tome što im je cilj. Ukoliko je potrebno razviti neku novu kompetenciju tada je potrebno zaposlenika uputiti

na opću edukaciju, ako je dovoljna samo informativna razina tada se najčešće koriste konferencije, uvodna predavanja i slično, dok u slučaju potrebe kontinuiranog razvoja treba kontinuirano pratiti edukacijske aktivnosti (periodično usvajanje novih znanja i informacija ovisno u razvoju područja).

Svaka vrsta edukacije i informiranja treba imati zadani cilj i definirane očekivane rezultate koje organizatori sučeljavaju s procijenjenom dosegnutom razinom kompetencija određenog zaposlenika. Takav pristup osigurava mjerljivost za praćenje napretka u razvoju kompetencija, nakon provedene evaluacije. Evaluacija postignutih rezultata provedenih treninga za podizanje kompetencija osigurava utvrđivanje koji je učinak provedene mjere dosegnut. Evaluaciju je moguće provoditi u više faza. Prva povratna informacije je odmah nakon provedenih vježbi/treninga kako bi se dobila informacija o općem dojmu polaznika na prezentirane materijale i pristup prenošenju informacija. Moguće je testirati znanje odnosno sposobnosti prije i nakon edukacije, pa se time dobiva povratna informacija koja su poboljšanja u kompetencijama postignuta nakon edukacije u odnosu na stanje prije. Evaluacija primjene stečenog znanja u praksi nakon određenog vremenskog odmaka po održanoj edukaciji govori o tome jesu li polaznici stjecanjem znanja promijenili i svoje navike u skladu sa stečenim znanjem.

O edukacijama za specijalistička znanja iz područja kibernetičke sigurnosti pisala je Blažič (2022). U tom znanstvenom radu prikazani su rezultati istraživanja provedenog s ciljem da se utvrdi koliko obrazovni sustav u području kibersigurnosti zadovoljava potrebe stjecanja potrebnih vještina kod studenata na diplomskim studijima. Metoda primijenjena u istraživanju temelji se na podacima prikupljenima iz anketa koje su proveli europski centri za stručnost o kibersigurnosti i Europske organizacije za kibersigurnost. Rezultati istraživanja govore da je potrebno poboljšati kurikulume visoko obrazovnih ustanova novim sadržajima iz područja znanja kao što su organizacijski ili ljudski aspekti kibersigurnosti. Također potrebno je osigurati korištenje radnog područja - poligona za praktične vježbe za osposobljavanje i izgradnju vještina.

Osim obrazovanja i stjecanja vještina potrebno je raditi na podizanju svijesti jer kako je već naglašeno samo posjedovanje kompetencija nužno ne znači i njihovu praktičnu primjenu. Promotivne aktivnosti s ciljem podizanja razine svijesti o važnosti osobne odgovornosti u kontekstu kibernetičke sigurnosti i otpornosti potrebno je provoditi na svim organizacijskim razinama, sa svim kategorijama zaposlenika. Poznavanje regulative, postupaka i procedura, politika i standarda koji su primjenjuju unutar nekog ključnog i važnog subjekta preduvjet je shvaćanje individualne odgovornosti za postupanje u kibernetičkom prostoru.

Akcije podizanja razine svijesti o važnosti kibernetičke sigurnosti trebaju se provoditi kontinuirano za sve zaposlenike, obavezno kod zapošljavanja za nove zaposlenike i obavezno nakon riješenih incidentnih/kriznih stanja, jer se iz toga najbolje uči na primjeru i shvaća prava težina počinjenih propusta iz neznanja ili nerazumijevanja poštovanja sigurnosnih protokola i procedura. Zaposlenike treba povremeno upućivati i podsjećati što trebaju posebno čuvati (lozinke, podatke o primanjima, podatke o policama osiguranja, podatke o kupcima, podatke o zdravstvenim dijagnozama, financijske podatke i podatke o računima i sl.). Kako bi ciljane skupine lakše prihvatile pravila ponašanja treba ih informirati o zaštiti

zaposlenika od krađe identiteta, sigurnosti elektroničke pošte, zaštiti intelektualnog vlasništva, o mogućim najčešćim napadima koji se u svim spomenutim segmentima događaju. Kod podizanja razine svijesti o kibernetičkoj sigurnosti treba sve ciljane skupine informirati o tome da se incidenti događaju bez najave, da oprez mora biti stalno prisutan kada je riječ o osobnim ili drugim povjerljivim podacima, da napadi najčešće budu izvedeni preko osoba od povjerenja čiji identitet je ukraden i kredibilitet iskorišten u svrhu prijevare.

5. Zaključak

Svaki društveni problem potencijalno se može smanjiti, ako već ne do kraja riješiti, provođenjem ciljanih kampanja kojima se utječe na svijest dionika. Kampanje usmjerene informiranju i obavještavanju pojedinaca o permanentnom postojanju kibernetičkih prijetnji, o mogućim načinima zloupotrebe osobnih ili drugih povjerljivih podataka važan su dio strategije za razvoj otpornosti na kibernetičke napade.

Usklađivanje poslovanja s odredbama NIS 2 Direktive uključuje i aktivan pristup jačanju kompetencija svih zaposlenika po pitanju shvaćanja važnosti kibernetičke sigurnosti, jačanju znanja i vještina eksperata što zahtijeva dodatno sustavno obrazovanje kroz akreditirane programe. Osim edukacije i treninga kojima se doprinosi kvaliteti znanja i shvaćanja područja kibernetičke sigurnosti treba djelovati i na svijest svih dionika da stečena znanja i vještine upotrijebe u kritičnom trenutku kada nastupi napad ili kad već dođe do incidenta.

Pri implementaciji NIS 2 Direktive se definiraju različite uloge i odgovornosti pojedinih radnih mjesta, a da bi se utvrdile potrebne kompetencije potrebno je uzeti u obzir specifičnosti koje ovise o djelatnosti kojom se ključni ili važan subjekt bavi. Kod stručnjaka iz domene kibernetičke sigurnosti i eksperata za incidentna i/ili krizna stanja potrebno je dodatno razviti vještine za sustavan pristup u rješavanju takvih stanja.

Nastavno na regulativu za očekivati je da će ponuda programa izobrazbi biti standardizirana u cilju što uspješnije implementacije NIS 2 Direktive i postizanja globalnih ciljeva kibernetičke sigurnosti.

Reference

1. Blažič, B. J. (2022). Changing the landscape of cybersecurity education in the EU: Will the new approach produce the required cybersecurity skills?. *Education and information technologies*, *27*(3), 3011-3036.
2. Europska Komisija, (2022). 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), preuzeto https://eur-lex.europa.eu/eli/dir/2022/2555/oj, pristupljeno 10. svibnja 2024.
3. Christoforatos, N., Ifi genia, L., Rekleitis, E., Van Heurck, C., Zacharis, A., (2022). Cyber Europe 2022: After Action Report, ENISA, dostupno na https://www.enisa.europa.eu/publications/cyber-europe-2022-after-action-report, pristupljeno 5. studenoga 2024

4. Kalenti, M. i Biro, P. (2024). European Cybersecurity Month 2023 - Campaign report, ENISA, dostupno https://www.enisa.europa.eu/publications/european-cybersecurity-month-2023-campaign-report, pristupljeno 5. studenoga 2024.
5. ISO 10015:2019 Quality management - Guidelines for competence management and people development, dostupno https://www.iso.org/standard/69459.html, pristupljeno 10. studenoga 2024.
6. ISO 22361:2022 Security and resilience - Crisis management - Guidelines, dostupno https://www.iso.org/standard/50267.html, pristupljeno 12. studenoga 2024.
7. ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls, dostupno https://www.iso.org/standard/75652.html, pristupljeno 12. studenoga 2024.
8. ISO/IEC 27031:2011 Information technology - Security techniques - Guidelines for information and communication technology readiness for business continuity, dostupno (https://www.iso.org/standard/44374.html, pristupljeno 12. studenoga 2024.
9. ISO/IEC 27032:2023 Cybersecurity - Guidelines for Internet security - (ISO/IEC 27032:2023(en), Cybersecurity - Guidelines for Internet security, dostupno https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27032:ed-2:v1:en, pristupljeno 12. studenoga 2024.
10. Uredba o kibernetičkoj sigurnosti („Narodne novine“ br. 135/24)
11. Zakon o kibernetičkoj sigurnosti („Narodne novine“ br. 14/24)

O autorici

Doc. dr. sc. Robertina Zdjelar doktorirala je u području društvenih znanosti, polje informacijske i komunikacijske znanosti 2022. godine. Tijekom 2024. godine autorica je izabrana u znanstveno-nastavno zvanje naslovni docent. Bavi se istraživanjem u području informacijskih i komunikacijskih znanosti, stručnim radovima u području javnih politika, financija i računovodstva. Angažirana je kao vanjski suradnik na Sveučilištu u Zagrebu na Fakultetu organizacije i informatike Varaždin te na Pravnom fakultetu u Zagrebu te na Geotehničkom fakultetu u Varaždinu. Djelovanje na Fakultetu organizacije i informatike odnosi se na upravljanje kvalitetom u informatici, kvalitetu i mjerenja u informatici, upravljanje primjenom informacijske tehnologije u poslovanju, odgovornost, inkluzija i održivost u informatici. Na Pravom fakultetu u Zagrebu autorica je održala nekoliko predavanja na temu upravljanja projektima. Na Geotehničkom fakultetu u Varaždinu održala je tribinu pod naslovom "Umjetna inteligencija i gospodarenje otpadom".

U poslovnom okruženju autorica je zaposlenik Gradskog komunalnog poduzeća Komunalac d.o.o. kao direktorica Sektora financija, računovodstva i EU projekata, a u okviru kojega se nalaze i druge poslovne funkcije važne za poslovanje društva. Zadnjih osam godina zaposlena je u društvu Komunalac, čemu je prethodilo dvadeset godišnje radno iskustvo u Koprivničko-križevačkoj županiji na raznim pozicijama, od pripravnika, suradnika do pročelnice za financije, proračun i javnu nabavu.

Autorica posjeduje brojne stručne certifikate od kojih treba istaknuti ***NIS2 DirectiveLeadImplementer, ISO 27001 interni auditor, ISO 9001 Lead auditor***, ESG akademija, voditelj financijskog kontrolinga, voditelj pripreme i provedbe EU projekata.