Kibernetička sigurnost – zašto je važna i koja je uloga HAKOM-a vezano uz kibernetičku sigurnost

Kibernetička sigurnost je skup mjera, tehnologija i procesa kojima se štite računalni sustavi, mreže, podaci i aplikacije od kibernetičkih prijetnji, hakiranja, neovlaštenog pristupa i oštećenja. Cilj je osigurati povjerljivost, integritet i dostupnost digitalnih informacija i sustava, a sve veća povezanost uređaja čini je ključnom za zaštitu osobnih podataka i poslovanja.

Kibernetički napadi su zlonamjerni akti usmjereni na računalne sustave, mreže ili uređaje, a ciljevi su im krađa, promjena ili uništavanje podataka, prekidanje rada sustava ili iznuđivanje novca. Mogu se usmjeriti na kritičnu infrastrukturu poput energetike, prometa, bankarstva i zdravstva, ali i na državne funkcije, klasificirane podatke ili pojedince putem krađe identiteta.

Najčešći kibernetički napadači nisu samo pojedinci (često koriste socijalni inženjering, poput phishinga, kako bi ostvarili brz dobitak), već i organizirane kriminalne grupe (napadaju u velikim razmjerima s ciljem krađe financijskih sredstava ili podataka te ucjenjivanja) i državno potpomognuti hakeri (mogu napadati zbog špijunaže, sabotaže ili političkih motiva).

Najčešće vrste kibernetičkih napada su phishing (slanje lažnih e-poruka ili poruka u ime poznatih tvrtki kako bi se ukrali osjetljivi podaci), ransomware (zlonamjerni softver koji zaključava podatke i traži otkupninu za njihovo oslobađanje), DDoS (Distributed Denial of Service, preopterećivanje sustava velikim brojem zahtjeva kako bi postao nedostupan), krađa identiteta (neovlašteno korištenje tuđih osobnih podataka za prijevaru), napad na kritičnu infrastrukturu (usmjeren na sustave poput električne mreže, vodoopskrbe ili prometne signalizacije), napad na državne funkcije (cilja na obranu, upravljanje institucijama, izbore ili diplomaciju).

S rastućim oslanjanjem na digitalne sustave za sve, od komunikacije i trgovine do kritične infrastrukture, kibernetička sigurnost je ključna za sprječavanje financijskih gubitaka, štete po ugled i prekida usluga.

Primjena odgovarajućih učinkovitih mjera kibernetičke sigurnosti u današnjem svijetu istovremeno je iznimno važna i iznimno zahtjevna. Broj različitih digitalnih uređaja koje koristimo veći je od ukupnog broja ljudi na svijetu, a isti mogu poslužiti kao ranjive ulazne točke za kibernetičke prijetnje. Istovremeno, napadači su sve domišljatiji, a uspješni napadi mogu uzrokovati značajne financijske gubitke, prekide poslovanja, krađe identiteta, objavu privatnih informacija i drugu štetu.

Operatori javnih elektroničkih komunikacijskih mreža i usluga pružaju svoje usluge i infrastrukturu velikom broju privatnih i poslovnih korisnika. Stoga raspolažu velikom količinom osobnih podataka krajnjih korisnika, a o radu njihovih mreža ovise poslovni procesi drugih sektora. Kibernetičke ugroze mreža kojima upravljaju operatori stoga utječu na veliki broj korisnika i/ili sustava i potencijalno mogu izazvati velike štete.

Upravo zbog navedenih razloga, kibernetička sigurnost u elektroničkim komunikacijama je iznimno važna te je na razini Europske unije (EU) kreiran regulatorni okvir[1] koji obuhvaća i pružatelje javnih elektroničkih mreža i usluga.

[1] EU regulatorni okvir za kibernetičku sigurnost uključuje Akt o kibernetičkoj sigurnosti (Cybersecurity Act), Direktivu NIS2 i Plan za upravljanje kibernetičkim krizama. Akt o kibernetičkoj sigurnosti uspostavlja okvir za

➢ NIS2 Direktiva

Direktivom (EU) 2022/2555, odnosno NIS2 Direktivom (dalje: NIS2), EU nastoji uspostaviti ujednačeni, visoki zajednički standard kibernetičke sigurnosti. NIS2 znatno proširuje opseg zahtjeva kibernetičke sigurnosti u odnosu na raniju NIS1 Direktivu. Također, NIS2 obuhvaća znatno širi krug sektora što znači da zahtjevi kibernetičke sigurnosti postaju primjenjivi na veći broj ključnih i važnih subjekata odnosno uspostavlja se jedinstveni pravni okvir za očuvanje kibernetičke sigurnosti u 18 ključnih sektora diljem EU-a. NIS2 se između ostalih primjenjuje i na pružatelje javnih elektroničkih komunikacijskih mreža i usluga, te obuhvaća veći broj digitalnih usluga, kao što su primjerice društvene mreže te poštanske i dostavne usluge. U skladu s NIS2 subjekti se kategoriziraju kao određeni tip subjekta na kojeg se primjenjuje pripadajući set mjera vezan uz kibernetičku sigurnost, a uključuju odgovarajuće tehničke, operativne i organizacijske mjere za upravljanje kibernetičkim rizicima, upravljanje incidentima, sigurnost opskrbnog lanca i kontinuitet poslovanja. Također, propisano je obvezno izvješćivanje o značajnim kibernetičkim incidentima i prijetnjama koje subjekti moraju prijaviti nadležnim nacionalnim tijelima u propisanim rokovima. NIS2 uvodi i odgovornost članova upravljačkih tijela subjekata organizacija za neusklađenost s mjerama upravljanja kibernetičkim sigurnosnim rizicima, čime se skreće pozornost uprava na kibernetičku sigurnost.

NIS2 posebno naglašava sigurnost opskrbnog lanca, zahtijevajući od subjekata procjenu i upravljanje rizicima povezanim s njihovim dobavljačima. NIS2 daje nacionalnim nadležnim tijelima šire ovlasti za njezinu provedbu, uključujući mogućnost izricanja značajnih novčanih kazni za nepoštivanje propisanih obveza. NIS2 potiče suradnju i razmjenu informacija među državama članicama, nacionalnim tijelima i subjektima radi jačanja zajedničke otpornosti. To se postiže jačanjem sigurnosti i otpornosti kritičnih sektora kako bi se osiguralo funkcioniranje ključnih usluga čak i u uvjetima ozbiljnih prijetnji i poremećaja.

➢ Primjena NIS2 Direktive u Republici Hrvatskoj

Države članice bile su obvezne prenijeti NIS2 u nacionalno zakonodavstvo do 17. listopada 2024.
Republika Hrvatska prenijela je NIS2 u nacionalno zakonodavstvo Zakonom o kibernetičkoj sigurnosti[2] i Uredbom Vlade Republike Hrvatske o kibernetičkoj sigurnosti[3]. Zakon i Uredba detaljno propisuju mjere kibernetičke sigurnosti *koje moraju poduzeti subjekti obuhvaćenim NIS2 Direktivom.*

HAKOM-u je dodijeljena ulogu nadležnog tijela za provedbu zahtjeva kibernetičke sigurnosti za **pružatelje javnih elektroničkih komunikacijskih mreža** i **pružatelje javno dostupnih elektroničkih komunikacijskih usluga**, što uključuje i pružatelje brojevno neovisnih interpersonalnih komunikacijskih usluga.

➢ Sigurnost elektroničkih komunikacija i NIS2 Direktiva

Implementacijom NIS2 u nacionalno zakonodavstvo stavljene su izvan snage pravila povezana sa sigurnosnim mjerama utvrđena u člancima 40. i 41. Direktive (EU) 2018/1972[4] odnosno Direktive o Europskom zakoniku elektroničkih komunikacija. Time je izvan snage stavljen članak 41. Zakona o elektroničkim komunikacijama koji je uređivao nadležnost HAKOM-a u provedbi tehničkih i organizacijskih

---

certifikaciju proizvoda i usluga, dok NIS2 direktiva postavlja zajedničke sigurnosne standarde i obvezuje na izvještavanje o incidentima u ključnim sektorima. Plan za kibernetičke krize pruža okvir za učinkovit i koordiniran odgovor na velike kibernetičke napade.

[2] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_02_14_254.html

[3] https://narodne-novine.nn.hr/clanci/sluzbeni/2024_11_135_2217.html

[4] https://eur-lex.europa.eu/legal-content/HR/ALL/?uri=CELEX:32018L1972

sigurnosnih mjera koje su bili u obvezi primjenjivati operatori javnih komunikacijskih mreža i javnih elektroničkih komunikacijskih usluga.

Kako je sektor elektroničkih komunikacija i ranije bio značajno reguliran, pretpostavka je kako operatorima elektroničkih komunikacija NIS2 donosi najmanje izazova. Naime, Pravilnikom o načinu i rokovima provedbe mjera zaštite sigurnosti mreža i usluga kojeg je donio HAKOM, implementirani su zahtjevi iz 5G Toolboxa-a.[5] Operatori su temeljem ovog Pravilnika već imali određene zahtjeve za sigurnost njihovih mreža i usluga, a osobito prijave incidenata.

NIS2 proširuje područje primjene i na brojevno neovisne interpersonalne komunikacijske usluge tzv. OTT usluge kako su definirane u Direktivi (EU) 2018/1972, uzimajući u obzir kako je potrebno osigurati da se i na takve usluge primjenjuju odgovarajući sigurnosni zahtjevi. Budući da se prostor za napad nastavlja širiti, brojevno neovisne interpersonalne komunikacijske usluge, kao što su usluge razmjene poruka, primjerice Whatsapp, postaju sve češći ciljevi kibernetičkih napada. Zlonamjerni počinitelji služe se platformama za komuniciranje i poticanje potencijalnih žrtava na otvaranje nesigurnih internetskih stranica, čime se povećava vjerojatnost incidenata koji uključuju iskorištavanje osobnih podataka, a time i sigurnosti mrežnih i informacijskih sustava. S obzirom na to da pružatelji brojevno neovisnih interpersonalnih komunikacijskih usluga obično nemaju stvarnu kontrolu nad prijenosom signala odnosno ne posjeduju vlastitu infrastrukturu, stupanj rizika za takve usluge može se u nekim aspektima smatrati nižim od rizika za tradicionalne elektroničke komunikacijske usluge.

➢ Nadležnost HAKOM-a prema novom zakonodavnom okviru kibernetičke sigurnosti

HAKOM je nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti za pružatelje javnih elektroničkih komunikacijskih mreža i javno dostupnih elektroničkih komunikacijskih usluga (skr. ECN/S), a nadležni CSIRT[6] (eng. *Computer Security Incident Response Team*) nadležno tijelo koje odgovara na kibernetičke prijetnje) za ECN/S postaje Nacionalni centar za kibernetičku sigurnost pri SOA-i.

HAKOM kao nadležno tijelo:

- provodi kategorizaciju subjekata te utvrđuje i vodi popise ključnih i važnih subjekata
- provodi stručni nadzor nad ključnim i važnim subjektima u provedbi zahtjeva kibernetičke sigurnosti
- u poslovima kategorizacije subjekata, postupanja u slučaju značajnih incidenata te poslovima stručnog nadzora usko surađuje i koordinira svoj rad s Nacionalnim centrom za kibernetičku sigurnost
- surađuje i razmjenjuje relevantne informacije s tijelima za zaštitu osobnih podataka u rješavanju incidenata koji su doveli do povrede osobnih podataka odnosno s tijelima kaznenog progona kada su incidenti rezultat kriminalnih aktivnosti
- surađuje s nadležnim CSIRT-ovima
- sudjeluje u međunarodnim i nacionalnim vježbama kibernetičke sigurnosti.

[5] https://digital-strategy.ec.europa.eu/en/library/eu-toolbox-5g-security
[6] Nadležni CSIRT određuje se za svaki od 18 ključnih sektora, pri čemu jedan CSIRT može biti nadležan za više sektora.

➢ Kategorizacija subjekata po Zakonu o kibernetičkoj sigurnosti

U okviru postupka kategorizacije subjekata, HAKOM provodi nacionalnu procjenu kibernetičkih sigurnosnih rizika za svakog subjekta. Cilj nacionalne procjene rizika je definirati razinu mjera upravljanja kibernetičkim sigurnosnim rizicima koju je dužan provoditi subjekt koji je kategoriziran kao ključni, odnosno važni subjekt. Sukladno provedenoj kategorizaciji, dodjeljuje se razina kibernetičke sigurnosti koju subjekt mora postići: osnovna, srednja ili napredna.

Obavijest o kategorizaciji s dodijeljenom razinom kibernetičke sigurnosti dostavlja se svakom pojedinačnom subjektu.

➢ Specifičnost sektora elektroničkih komunikacija

U odnosu na druge sektore obuhvaćene ZKS-om, svi subjekti koji pripadaju sektoru elektroničkih komunikacija obuhvaćeni su zahtjevima kibernetičke sigurnosti neovisno o njihovoj veličini odnosno ukupnom godišnjem prihodu i broju zaposlenih. Dodatno, pružatelji javnih elektroničkih komunikacijskih mreža ili javno dostupnih elektroničkih komunikacijskih usluga podliježu nadležnostima i ovlastima propisanim ZKS-u ako svoje usluge pružaju na teritoriju Republike Hrvatske, neovisno o državi poslovnog nastana. Dakle, podliježu propisima kibernetičke sigurnosti svih 27 država članica.

Subjekti mogu biti kategorizirani u više sektora, podsektora i vrsta te mogu dobiti više obavijesti o kategorizaciji. U tom slučaju, nadležna tijela sklapaju protokol kojim se određuje glavno nadležno tijelo za takvu vrstu subjekta.

➢ Primjena mjera kategoričke sigurnosti

S obzirom na utvrđenu razinu kibernetičkih sigurnosnih rizika, operatori su dužni provesti osnovnu, srednju ili naprednu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima. Dodijeljenu razinu mjera upravljanja kibernetičkim sigurnosnim rizicima operatori su dužni provesti u roku od godine dana od dana zaprimanja obavijesti o kategorizaciji.

Osnovna razina mjera primjenjuje se na subjekte s nižim profilom rizika te se temelji na lako dostupnim tehnologijama i dobro poznatim sigurnosnim praksama. Cilj je zaštita od najčešćih globalnih napada koje provode napadači s prosječnim vještinama.

Srednja razina mjera nadograđuje osnovnu razinu dodatnim mjerama radi povećane otpornosti. Namijenjena je subjektima iz sektora gdje postoji veći rizik od ciljanih napada prosječno vještih napadača.

Napredna razina mjera je najviša razina zaštite, uključuje napredne tehničke i organizacijske mjere. Cilj je obrana od sofisticiranih i resursno jakih napadača s visokim razinama vještina.

➢ Revizija mjera kibernetičke sigurnosti

Ključni subjekti dužni su provoditi reviziju kibernetičke sigurnosti najmanje jednom u dvije godine, a moguće je provođenje revizije i prije isteka roka kada to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti.

Reviziju kibernetičke sigurnosti ključnih i važnih subjekata provode revizori kibernetičke sigurnosti. Revizori su pružatelji upravljanih sigurnosnih usluga koji posjeduju nacionalni certifikat za reviziju kibernetičke sigurnosti ili odgovarajući kibernetički sigurnosni certifikat na temelju mjerodavne europske sheme kibernetičke sigurnosne certifikacije.

Iznimno, revizor kibernetičke sigurnosti za tijela državne uprave i druga državna tijela je Zavod za sigurnost informacijskih sustava (ZSIS) kao središnje državno tijelo za obavljanje poslova u tehničkim područjima informacijske sigurnosti.

Nacionalni sigurnosni certifikat za reviziju kibernetičke sigurnosti izdaje ZSIS u ulozi središnjeg državnog tijela za obavljanje poslova u tehničkim područjima informacijske sigurnosti u postupku i prema zahtjevima koji će biti propisani pravilima sigurnosne certifikacije.

- **Samoprocjena mjera kibernetičke sigurnosti**

Važni subjekti dužni su provoditi samoprocjenu kibernetičke sigurnosti najmanje jednom u dvije godine, dok su reviziju kibernetičke sigurnosti dužni provesti samo kada to zatraži nadležno tijelo za provedbu zahtjeva kibernetičke sigurnosti kao nadzornu mjeru.

Samoprocjene kibernetičke sigurnosti provodi subjekt s vlastitim ljudskim potencijalima ili za provedbu samoprocjene može angažirati vanjskog davatelja usluge.

Pravila, tehnički zahtjevi, norme, obrasci i postupci koji se primjenjuju u postupcima samoprocjene kibernetičke sigurnosti propisani su Uredbom o kibernetičkoj sigurnosti.

- **Obavještavanje o značajnim incidentima i prijetnjama**

Subjekti su dužni, nakon što zaprime obavijest o kategorizaciji, u roku od 30 dana započeti s obavještavanjem o značajnim incidentima. Smjernice o obavijestima o incidentima, kibernetičkim prijetnjama i izbjegnutima incidentima javno su objavljene na mrežnoj stranici Nacionalnog centra za kibernetičku sigurnost.[7] Za sektor elektroničkih komunikacija nadležan je CSIRT pri središnjem državnom tijelu za kibernetičku sigurnost odnosno Nacionalni centar za kibernetičku sigurnost (NCSC).

Obavijesti o incidentima prijavljuju se putem nacionalne platforme za prikupljanje, analizu i razmjenu podataka o kibernetičkim prijetnjama i incidentima (dalje: PiXi). Preduvjet za korištenje PiXi platforme je da pravna osoba ima uspostavljeno e-Poslovanje koje omogućava autentifikaciju poslovnim vjerodajnicama, odnosno autentifikaciju korisnika u svojstvu poslovnog subjekta, a pri tome se moraju koristiti vjerodajnice visoke ili značajne razine sigurnosti.

- **Obavještavanje korisnika o značajnim prijetnjama i incidentima**

Ključni i važni subjekti dužni su obavijestiti primatelje svojih usluga o značajnim incidentima ili ozbiljnoj kibernetičkoj prijetnji na koje bi takav incident ili prijetnja mogla utjecati.

[7] https://ncsc.hr/hr/smjernice-i-upute

Ključni i važni subjekti su dužni, bez odgode, a najkasnije u roku od 72 sata od saznanja za značajan incident, na jasan i lako dokaziv način, o značajnom incidentu obavijestiti primatelje svojih usluga na koje bi takav incident mogao utjecati.

Obavijest o značajnom incidentu mora sadržavati sljedeće podatke :

- vrstu i kratki opis incidenta
- uzrok incidenta
- mogući utjecaj incidenta na uslugu
- kontakt podatke subjekta
- upute o postupanju primatelja usluga u svrhu ublažavanja učinka nastalog incidenta i naknade uzrokovane štete.

U slučaju pojave ozbiljne kibernetičke prijetnje, ključni i važni subjekti dužni su primatelje svojih usluga, na koje bi takva prijetnja mogla utjecati, obavijestiti o svim mogućim mjerama zaštite ili pravnim sredstvima koje mogu uporabiti u svrhu sprečavanja ili naknade uzrokovane štete te, po potrebi, obavijestiti primatelje usluga i o samoj ozbiljnoj kibernetičkoj prijetnji. Na obavještavanje primatelja usluga o ozbiljnim kibernetičkim prijetnjama na odgovarajući način se primjenjuje postupak obavještavanja primatelja usluga o značajnim incidentima.

U određenim slučajevima, značajni incidenti ili ozbiljnije kibernetičke prijetnje mogu se kategorizirati kao kaznena djela protiv računalnih sustava, programa i podataka. Na naknadu štete primjenjuju se opća pravila o naknadi štete sukladno posebnim propisima.