NOVA LEGISLATIVA I CYBER SIGURNOST

ŠTA PREDSTAVLJA NIS2 DIREKTIVA ZA JADRANSKU REGIJU



Nova evropska direktiva o cyber sigurnosti predviđa uvođenje strogih mjera zaštite duž cijelog lanca opskrbe, čije se karike mogu pronaći u svim zemljama regije. No, jesu li ovdašnje kompanije spremne za temeljito regulatorno pospremanje u sektoru kibernetičke sigurnosti?

Piše: Mirza Bahić
mirza.bahic@asadria.com



Priča o NIS2 direktivi dominira evropskim kontinentom i za to postoji barem 10,5 biliona razloga izraženih u eurima koji će biti utrošeni na odbranu od cyber napada do 2025. Iste godine, do 17. aprila, članice Evropske unije moraju dovršiti proces kategorizacije tijela koja su obuhvaćena Direktivom, nakon čega im se daje 365 dana da se usklade s novim regulatornim zahtjevima. Stvar je nešto kompliciranija za kompanije izvan EU jer će ih kao kariku lanca nabavke evropskih kompanija NIS2 neminovno "očešati" i tražiti modifikaciju poslovnih praksi.

U nastavku teksta razgovaramo sa stručnjacima i poslovnim ljudima iz regiona koji će nam objasniti zašto je NIS2 prvorazredni događaj za regionalnu cyber sigurnost koja u mjesecima pred nama postaje punokrvna zakonska obaveza, a ne fakultativna poslovna praksa.

Izazov za kompanije izvan Unije

Podsjetimo se, NIS2 je stupio na snagu u januaru 2023. kao zamjena za NIS1. Nova legislativa uvela je znatno strožija pravila i kriterije u zaštiti kibernetičkih sistema unutar Unije. To se posebno odnosi na kritičnu infrastrukturu, usluge i podršku za efikasniju koordinaciju odgovora na cyber incidente koji znatno ugrožavaju ekonomiju i društvo.

Direktivom obuhvaćene organizacije sada moraju provoditi redovne procjene rizika svojih mrežnih i IT sistema i implementirati odgovarajuće tehničke i organizacijske mjere za upravljanje prijetnjama. To uključuje procedure za analizu rizika i upravljanje ranjivostima, kao i efikasnu primjenu kriptografije i enkripcije. Organizacije moraju uvesti procedure za praćenje incidenata i krizno upravljanje, uključujući detekciju, analizu i klasifikaciju povreda sigurnosti. U istom paketu ide i obavještavanje nadležnih državnih tijela o incidentima u zadanim rokovima.

"EU je prepoznala različitu sposobnost i otpornost odgovora na kibernetičke prijetnje po zemljama članicama, a kako su danas tvrtke povezane i kroz lanac opskrbe i sve je više velikih korporacija koje rade u više zemalja EU, cilj NIS2 direktive je smanjiti te razlike", kaže Kristina Oršanić Kopić, savjetnica za kibernetičku sigurnost u kompaniji Combis.

Organizacije moraju donijeti i provoditi planove održavanja kontinuiteta poslovanja i oporavka od napada kako bi osigurale nastavak pružanja usluga i u vanrednim situacijama. Od zemalja regije, navedeni zahtjevi se odnose primarno na Sloveniju i Hrvatsku kao članice Unije, no opisane prakse neće zaobići ni Bosnu i Hercegovinu, Srbiju, Crnu Goru i Sjevernu Makedoniju. Razlog je jednostavan: važna stavka direktive je ona koja sigurnosno osjetljive organizacije imenuje odgovornim za upravljanje rizicima u cijelom lancu opskrbe s kojim rade. To znači da se obaveza primjene odgovarajućih mjera sigurnosti odnosi i na direktne dobavljače i pružaoce usluga koji rade s evropskim kompanijama.

Obavezna primjena

Drugim riječima, ako kompanija izvan EU posluje s partnerima iz Unije ili pruža usluge koje su ocijenjene kao "esencijalne" za tamošnje tržište, ona će morati uskladiti svoje prakse s NIS2 standardima kako bi zadržala ovaj poslovni odnos. To uključuje procjene rizika, upotrebu enkripcije, redovno testiranje sigurnosti i procedure za brzo i efikasno prijavljivanje incidenata.

"Vjerujem da kompanije izvan EU čeka značajan zadatak u jačanju svojih sigurnosnih sistema. Ovo uključuje uspostavljanje sistema upravljanja, sveobuhvatno

Ključni subjekti za direktivu

Ključni subjekti su oni koji su obavezni provoditi sve mjere kibernetičke zaštite iz NIS2 direktive, prijavljivati incidente, prolaziti nezavisne revizije i biti pod stalnim nadzorom. Ovi subjekti rade na ili posluju u sektorima poput energetike, prometa, bankarstva, infrastrukture finansijskog tržišta, zdravstva, vode za ljudsku potrošnju, otpadnih voda, digitalne infrastrukture, upravljanja ICT uslugama, javnog sektora i svemira. S druge strane, važni subjekti primjenjuju mjere kibernetičke sigurnosti samostalno i potvrđuju njihovu provedbu kroz samoprocjenu, bez redovnih nezavisnih revizija ili stručnog nadzora. Ovi subjekti su dužni prijavljivati incidente nadležnom tijelu, a nadzor nad njima se provodi samo ako postoje informacije koje ukazuju na nepridržavanje propisa ili obaveza. Važni subjekti uključuju sektore poput poštanskih i kurirskih usluga, upravljanja otpadom, proizvodnje i distribucije hemikalija, proizvodnje hrane, digitalnih usluga, istraživanja i obrazovanja.

Obaveza primjene mjera sigurnosti odnosi se i na direktne dobavljače i pružaoce usluga koji rade s evropskim kompanijama



Većina sektora je srednje spremna. Nije da se ne ulaže ništa, ali premalo da bi se adekvatno odgovorilo na prijetnje koje rastu u frekvenciji, učestalosti i raznolikosti

upravljanje cyber rizicima, zaštitu digitalne infrastrukture koja obuhvata ne samo IT sisteme nego i tehnologije poput SCADA sistema, IoT tehnologija, senzora itd., kao i kontinuirani monitoring i sposobnost kompanije da pravovremeno identificira i odgovori na potencijalne napade", kaže Senad Džananović, direktor cyber sigurnosti u bh. kompaniji ZIRA.

Prema njemu, NIS2 će posebno utjecati na kompanije registrirane izvan Unije koje pružaju usluge u sektorima kao što su ICT (upravljane IT i sigurnosne usluge) i usluge digitalne infrastrukture na teritoriju Unije. Za pružanje usluga u drugim sektorima obuhvaćenim Direktivom, ove kompanije moraju imati fizičko prisustvo u nekoj od zemalja EU. Usklađivanje ostalih kompanija zavisit će od prilagođavanja nacionalnih zakona propisima Unije, ali kako zemlje regije teže članstvu u EU, očekuje se da će se i one uskoro morati uskladiti s novom regulativom.

Tri nivoa implementacije

Za adekvatnu implementaciju Direktive, obuhvaćeni sektori su podijeljeni na ključne i važne, dok će same kompanije morati implementirati mjere na tri nivoa. Prema Oršanić Kopić, prvi nivo je uspostava ključnih procesa upravljanja sigurnošću informacijskog sistema. Tu spadaju upravljanje sigurnosnim rizicima, uključujući one povezane s opskrbnim lancima, zatim kontrola incidenata i zaštita kontinuiteta poslovanja te izrada pratećih politika i procedura zahtijevanih mjerama nove direktive.

Drugi nivo uključuje kontrolne mjere temeljene na procjeni rizika i analizi utjecaja na poslovanje ICT okruženja i poslovanja klijenta. Te kontrolne mjere uključuju tehnološka rješenja i upravljane servise, kao što su višefaktorska autentifikacija, kontrola pristupa, rješenja za kontinuitet poslovanja kao što su IaaS, BaaS, DRaaS i AntiDDoS, te osnovna sigurnosna higijena (firewall i antivirusni softver nove generacije, endpoint detection and response rješenja, firewall web aplikacija, DLP rješenja i dr.). Na kraju, tu je i obaveza podizanja svijesti zaposlenika kroz anti-phishing kampanje i vježbe ljubičastog tima kao važan branik od kibernetičkih prijetnji.

Treći nivo podrazumijeva uspostavu sigurnosnog nadzora i validaciju sigurnosnih kontrola, što omogućuje prevenciju incidenata i ranu detekciju prijetnji. Ove aktivnosti uključuju usluge sigurnosnih operativnih centara (SOC) i MDR-a (Managed Detection and Response) koje će biti dostupne na cjelodnevnoj bazi tokom čitave godine. Za uspostavu SOC-a, kompanije se mogu obratiti pružaocima SOC usluga, jer ih je teško samostalno uspostaviti zbog nedostatka sigurnosnih stručnjaka.

"Za potrebe validacije sigurnosnih kontrola na raspolaganju su usluge svih vrsta penetracijskog testiranja, provjere ranjivosti, lova na prijetnje, kao i već navedene vježbe crvenog i ljubičastog tima kojima se dodatno diže otpornost ICT okoline na kibernetičke prijetnje", kaže Oršanić Kopić.

Sve navedeno nužno je kako bi se prijetnje rano detektirale, a posljedice kibernetičkih napada svele na minimum. Time se osigurava usklađenost s NIS2 direktivom i zakonima koje će zemlje članice EU usvojiti do 17. oktobra ove godine.

No, u kojoj su mjeri kompanije s obje strane granice EU spremne za poduhvat koji traži kako značajne tehnološke i stručne resurse tako i temeljitu promjenu svijesti o važnosti cyber sigurnosti?

Hrvatska: neki sektori imaju startnu prednost, neki nikakvu

Za početak, treba napomenuti da NIS2 neće imati istovjetne učinke na hrvatske i slovenske kompanije u poređenju s



Aleksandar Kotevski, vlasnik i izvršni direktor, Advanced Cyber Security



Branko Džakula, direktor informacijskih tehnologija, BrightMarbles Grupa, i suosnivač, UN1QUELY



Kristina Oršanić Kopić, savjetnica za kibernetičku sigurnost, Combis



Matic Knuplež, regionalni direktor za Jadransku regiju, Group-IB

ostatkom Jadranske regije. Čak i ograničavanje procjene spremnosti na primjenu Direktive unutar samo jedne zemlje neće dati reprezentativnu sliku jer su neki sektori na temelju zahtjeva poslovanja već u startu opremljeniji za NIS2.

"Većina sektora je u nekoj srednjoj spremnosti. Nije da se ne ulaže ništa, ali premalo da bi se adekvatno odgovorilo na prijetnje koje rastu u frekvenciji, učestalosti i raznolikosti. S druge strane, pružatelji usluga nemaju dovoljno stručnjaka za uskladu u ISMS dijelu (upravljanje sigurnošću informacijskog sustava) da bi mogli odgovoriti na potrebe tržišta, posebno u segmentu malih i srednjih tvrtki koje su sad pred izazovom da će se od trenutka primitka obavijesti o kategorizaciji od nadležnih tijela, morati uskladiti s NIS2 zahtjevima, odnosno sa Zakonom o kibernetičkoj sigurnosti u roku od godinu dana od trenutka primitka iste", kaže Oršanić Kopić.

Neke industrije, poput bankarstva, financijske infrastrukture i zračnog prometa, već su regulirane u oblasti kibernetičke sigurnosti u Hrvatskoj i drugim članicama EU. Ovi sektori su bolje pripremljeni za prilagodbu novim zahtjevima NIS2 direktive te već posjeduju strožije regulative nego što ona podrazumijeva. S druge strane, nešto šarenija slika je u tzv. poluautonomnim sektorima poput elektronskih komunikacija, javnog sektora i pružatelja usluga povjerenja, u kojima je cyber sigurnost djelimično regulirana na evropskom ili nacionalnom nivou, ali opet nedovoljno u odnosu na zahtjeve Direktive.

Više optimizma ima hrvatska Sigurnosno-obavještajna agencija, koja na naš upit o percepciji trenutnog stanja na terenu u pogledu organizacijske svijesti o NIS2 direktivi odgovara da je trenutno stanje posljedica jačanja svijesti o potrebi zaštite poslovnih mrežnih i IT sistema koje jača iz godine u godinu. "Utjecaj na takav razvoj su svakako imali i brojni izazovi koje je donijela COVID kriza i prilagodbe na nove modele rada koje je ona donijela", navodi se u odgovoru SOA-e.

Slovenija: tržište nije spremno za nagli skok

U susjednoj Sloveniji situacija nije mnogo drugačija od one u Hrvatskoj. Slovenski je industrijski insajderi opisuju kao zbir varijacija. Kao eho stava koji je iznijela njegova hrvatska kolegica Oršanić Kopić, Matic Knuplež, regionalni direktor za Jadransku regiju u kompaniji Group-IB, navodi da spremnost slovenskog tržišta znatno varira, uz viši nivo svijesti i resursa među većim kompanijama s razvijenijim politikama kibernetičke sigurnosti.

"Smatram da će mala i srednja preduzeća imati probleme zbog ograničenih resursa i stručnosti. Konsultanti za kibernetičku sigurnost i država ulažu napore na podizanju svijesti i davanja, ali će se, uprkos tome, značajan dio tržišta suočiti s poteškoćama kada je u pitanju unapređenje kapaciteta sigurnosti za ispunjavanje standarde iz Direktive", kaže Knuplež. Kompanije koje su se već prilagodile spomenutim zahtjevima imat će mnogo lakši zadatak nego one koje su prvi put obuhvaćene sličnom regulativom. U tom smislu, NIS2 za slovenske kompanije koje su prema NIS1 već bile označene kao "kritične organizacije" zapravo neće donijeti mnogo toga novog. Isto važi i za one koje upravljaju rizicima u oblasti cyber sigurnosti na osnovu standarda ISO/IEC 27001.

S druge strane, Mitja Trampuž, direktor slovenske kompanije CREAPLUS, predviđa veće probleme za subjekte koji su se sada našli na listama važnih ili kritičnih organizacija. Kao i u Hrvatskoj, jedan od ključnih problema u ovom segmentu bit će nedostatak osoblja.

Rješenje u uvozu kadrova?

Mišljenje kolega o deficitu kadrova dijeli i Tomislav Kosanović, direktor za Hrvatsku u kompaniji Telelink, koji smatra da je regionalno tržište i bez NIS2 direktive već neko vrijeme u "deficitu vezanom za ljudske resurse, posebno u sferi kibernetičke sigurnosti". Prema njemu, riječ je o dobro poznatom i širem problemu pronalaženja i, jednako važno, zadržavanja stručnih resursa koje region nasušno treba, posebno u ambijentu u kojem mlađi stručnjaci masovno odlaze u inozemstvo.

Da bi se ovaj problem adekvatno riješio, neće biti dovoljno uvoziti kvalificirani kadar nego i mijenjati percepciju direktive kod dva ključna dionika: IT i sigurnosnih odjela i menadžmenta kompanija. "Prvi moraju prestati djelovati kao isključive adrese za probleme informatičke sigurnosti, dok će uprava morati širiti kulturu sigurnosti na nivou cijele organizacije", smatra Džananović.



"U Sloveniji se, naprimjer, broj obveznika povećao više od 30 puta i vjerujem da tržište nije spremno za takav skok. Možda u smislu prodaje sigurnosnih rješenja, ali svakako ne kada je u pitanju ponuda usluga upravljanja kibernetičkom sigurnošću, savjetovanja o upravljanju rizicima i ranjivostima i sl. Jednostavno nema dovoljno osoblja za to. Nedostaje certificiranih IT revizora i stručnjaka za cyber sigurnost, dok administratori sistema i baza podataka ne posjeduju dovoljno znanja. U našem regionu potreban je jedan ovlašteni revizor za više od stotinu NIS2 obveznika, što je fizički nemoguće isporučiti", kaže Trampuž.

Manjak kvalificiranog osoblja za provedbu i nadzor

Priča o manjku kvalificiranog osoblja tema je koja privlači pažnju i kompanija koje posluju izvan Evropske unije na koje se NIS2 indirektno odnosi. Procjena stanja na tom planu neodvojiva je od konteksta višegodišnjih problema u oblasti cyber sigurnosti s kojim se suočava regija, a koji su vidljivi i u rastu broja napada na kompanije i pojedince u ovom dijelu svijeta.

"Možemo govoriti o kompanijama koje posluju u državama kandidatima za članstvo u EU na teritoriji Zapadnog Balkana gdje vidimo veliku nespremnost za prilagođavanje novim zahtjevima Direktive, što je evidentno iz velikog broja uspješnih sajber napada na državne infrastrukture u posljednjih nekoliko godina", kaže Branko Džakula, direktor informacijskih tehnologija u BrightMarbles Grupi i suosnivač i izvršni direktor kompanije UN1QUELY. Slika je to, smatra on, nedostatka stručnog kadra u domenu cyber sigurnosti, kao i neadekvatnih mjera za sanaciju štete od napada, što je jedna od važnih stavki Direktive.

> U Sloveniji se broj obveznika povećao više od trideset puta. Tržište nije spremno za takav skok

Džakula smatra da će glavni izazovi biti vezani za stručnost, odnosno angažman adekvatnog kadra za obavljanje poslova implementacije i održavanja sistema za informacijsku sigurnost koji će biti u potpunosti usklađen sa ISO 27001 standardom i specifičnim NIS2 kontrolama.

Pored nedostatka stručnjaka u ovoj oblasti jedan od većih izazova bit će i kvalitet dostupnog kadra koji mora posjedovati znanja da pomogne organizacijama da se usklade s NIS2 direktivom u upravljačkom dijelu. To se posebno odnosi na izrade procjena rizika i planova kontinuiteta poslovanja, upravljanja incidentima i validacije sigurnosnih kontrola. Prema Oršanić Kopić, pitanje osposobljenosti nije ograničeno na primjenu regulative nego i na praćenje njene usklađenosti. "Broj revizora, točnije stručnjaka koji će moći provoditi revizije kibernetičke sigurnosti, također je ograničen", navodi ona.

Kao i u Hrvatskoj i Sloveniji, nivo svijesti o važnosti NIS2 izvan Unije varira geografski i sektorski, pri čemu su u prednosti kompanije koje već posluju s Unijom. "Spremnost tržišta izvan Evropske unije na prilagodbu novim zahtevima iz Direktive NIS2 je različita. Kompanije koje već posluju unutar Unije uglavnom su svesne Direktive, ali nivo svesti i pripremljenosti varira od zemlje do zemlje. Glavni izazovi u implementaciji uključuju usklađivanje sa tehničkim i organizacionim zahtevima, kao i obezbeđivanje adekvatne obuke zaposlenih. Takođe, neophodno je uspostaviti efikasne mehanizme za praćenje i prijavljivanje sigurnosnih incidenata", kaže Aleksandar Kotevski, vlasnik i izvršni direktor kompanije Advanced Cyber Security iz Beograda.

Te varijacije se, ipak, mogu podvesti pod jedan zajednički sadržalac: kompanije izvan EU su općenito manje zrele kada je u pitanju cyber sigurnost u odnosu na one koje posluju unutar Unije. Iako nema egzaktnih podataka, Džananović smatra da je veliki broj organizacija čuo za NIS2 direktivu, ali da se manjina usklađuje s njenim odredbama.

"Govoreći o NIS2 direktivi i njenoj primjenjivosti na organizacije koje imaju sjedište ili posluju u zemljama koje su potpisale pristupne sporazume s EU, vjerovatno je da će se takve organizacije u skoroj budućnosti morati uskladiti s normama



Mitja Trampuž, direktor, CREAPLUS



Senad Džananović, direktor cyber sigurnosti, ZIRA



Tomislav Kosanović, direktor za Hrvatsku, Telelink

i zahtjevima NIS2 direktive", kaže on. Prema njemu, kod procjene zrelosti ovih kompanija važno je naglasiti da se NIS2 direktiva primarno odnosi na organizacije koje nude usluge unutar EU ili imaju značajan utjecaj na tržište EU u sektorima poput energetike, transporta, bankarstva, zdravstva i digitalne infrastrukture.

Implementacija je skupa

Bez obzira na meridijane, eksperte s obje strane evropske granice objedinjuje zajednička bojazan da problem manjka osoblja neće biti jedina prepreka glatkoj implementaciji NIS2 direktive. Jer, čak i da problemi s kadrom budu riješeni, povećanje troškova poslovanja će biti dodatni izazov za sve kompanije u doticaju s NIS2. To se posebno odnosi na one koje prethodno nisu bile uključene u NIS1. Evropska komisija procjenjuje da će troškovi za ovu kategoriju porasti blizu 22%, dok će za kompanije obuhvaćene direktivom NIS1 iznositi oko 12%. Direktni troškovi primjene za preduzeća iz EU procijenjeni su na 31,2 milijarde eura godišnje u 2023. godini, što predstavlja 0,31% ukupnog prometa u svim sektorima na koje utječe direktiva NIS2. Treba znati i da je riječ o konzervativnim procjenama koje u obzir ne uzimaju faktore poput inflacije.

Istovremeno, povećanje za sektore koje tretira NIS2 procjenjuje se na 29,9 milijardi eura godišnje, što predstavlja 0,32% njihovog ukupnog prometa. "Cyber otpornost se ne može postići s jednom ili dvije investicije, to je proces koji traje. Uostalom, cyber prijetnje i rizici se stalno mijenjaju i rastu uvođenjem novih digitalnih tehnologija. Mislim da kompanije nisu dovoljno svjesne toga, a opet nemaju ni znanja za to. Mislim da će najviše problema imati srednje i velike kompanije, gdje je cyber sigurnost tretirana kao sporedna aktivnost IT odjela, a bez definiranog budžeta za nju", kaže Trampuž.

Fiktivna usaglašenost

I za slovenske kompanije troškovi će neizbježno biti značajni, smatra Knuplež te dodaje da će glavni izvori tih troškova biti primjena novih sigurnosnih mjera, uvođenje programa podizanja svijesti i angažmana konsultanata za kibernetičku sigurnost. Utjeha leži u činjenici da se ovi troškovi mogu promatrati kao investicije koje su, prema Knupležu, opet znatno jeftinije nego skupi incidenti povezani s narušavanjem sigurnosti. Za Džakulu, veći problem bi, zapravo, mogla biti "fiktivna usaglašenost" kakva se javila nakon stupanja GDPR-a na snagu. Prema njemu, nemali broj kompanija bi mogao pokušati preko noći i bez većih ulaganja postići usaglašenost "na papiru", a to s ciljem da se nastavi neometano poslovati bez adekvatnog tretmana rizika. Vođeni iskustvom s primjenom GDPR-a, za očekivati je da će neke kompanije i ovaj put paušalno reklamirati usaglašenost s regulativom na svojim stranicama, što će biti teško za provjeriti zbog nedostatka inspekcijskog nadzora i kadra za provođenje kontinuiranih provjera, smatra on.

I naši sagovornici iz Hrvatske smatraju da će finansijski nešto bolje proći obveznici prema NIS1 regulativi jer su se, makar u manjem opsegu, već susreli sa sličnim sigurnosnim zahtjevima koje sada trebaju nadograditi. Za ostale, veća odgovornost će biti prevedena i u veće finansijske posljedice.

"Te brojeve možemo isključivo shvatiti kao neke pokazatelje, jer će tvrtke koje do sada nisu trebale biti usklađene, a spadaju po segmentaciji u srednje i male, zasigurno trebati uložiti značajnija sredstva kako bi se uskladile s NIS2", kaže Oršanić Kopić. Njen kolega Kosanović misli da će veći troškovi biti neizbježni, ali da je to već dio "higijene svakodnevnog poslovanja, gotovo poput komunalija".

Troškovi se moraju pravdati

Ipak, ostaje pitanje u kojoj mjeri će menadžerske strukture kompanija uvođenje novih mjera tretirati na ovaj način. Iako su dodatne investicije i značajan finansijski pritisak usklađivanja s NIS2 na troškove poslovanja neminovni, ovi troškovi će se naposljetku opet morati pravdati pred direktorima i vlasnicima kompanija. Za Džananovića, ove troškove je jako teško kvantificirati, osim u slučaju cyber napada, što otežava posao osoblju koje bude tražilo izdvajanja pred upravom kompanija. Rast troškova će neminovno osjetiti i kompanije izvan EU i one će, prema njemu, osjetiti rast troškova proporcionalan veličini kompanije. Obrnuto proporcionalan, pak, bit će odnos troškova i stepena zrelosti koji je neka organizacija dostigla po pitanju implementacije praksi cyber sigurnosti, smatra on.

No, ovo i nije nova praksa jer dobar dio ovih kompanija već ulaže u usklađivanje s međunarodnim standardima kakav je, naprimjer, ISO 27001. Još od ranije postoji praksa da se harmonizacija s ovim standardom tretira kao preduvjet nastavka saradnje s velikim kompanijama, pri čemu je one manje reguliraju kao stavku u ugovoru o pružanju usluga. Ipak, Džakula ne vjeruje da će ova praksa biti primjenjiva i kod NIS2, ali da će veći troškovi vjerovatno biti pravdani kroz promociju naprednijih sigurnosnih praksi. "Sve češće viđamo napredne bezbjednosne kontrole u SaaS rješenjima u okviru enterprise planova subskripcije i očekujem da će takav trend samo nastaviti i osnažiti", navodi Džakula.



Ignoriši NIS2, zaboravi tržište

Nepridržavanje odredbi NIS2 direktive iz bilo kojeg od ovih razloga neće biti opravdano i povući će teške pravne i poslovne posljedice. U članu 34. Direktiva propisuje opće uslove za izricanje administrativnih novčanih kazni ključnim i važnim subjektima. Ključni subjekti mogu biti kažnjeni s najmanje 10 miliona eura ili 2% ukupnog godišnjeg prihoda na svjetskom nivou iz prethodne finansijske godine, zavisno od toga koji je iznos veći. Važni subjekti mogu biti kažnjeni s najmanje sedam miliona eura ili 1,4% ukupnog godišnjeg prihoda na svjetskom nivou iz prethodne godine, opet prema načelu većeg iznosa.

Osim toga, član 32. NIS2 direktive dodatno definira nadzorne mjere i mjere izvršavanja u vezi sa ključnim subjektima. Između ostalog, predviđene su privremene suspenzije certifikata ili ovlaštenja za dio ili kompletne usluge koje pruža ključni subjekt, kao i privremene zabrane obavljanja upravljačkih dužnosti za svako fizičko lice na nivou glavnog izvršnog direktora ili pravnog zastupnika u tom ključnom subjektu.

"Važno je napomenuti da lokalni zakoni mogu propisati strožije mjere od onih definisanih NIS2 direktivom, ali ne i blaže", navodi Oršanić Kopić u komentaru na predviđene kazne.

> Za kompanije koje posluju izvan EU kazna bi mogla doći i u vidu uskraćivanja pristupa jednom od najvažnijih i najbogatijih tržišta na svijetu

Istovremeno, za kompanije koje posluju izvan EU, kazna bi mogla doći i u vidu uskraćivanja pristupa jednom od najvažnijih i najbogatijih tržišta na svijetu, sve uz "gubitak ugovora, potencijalnu zabranu pružanja usluga EU i odgovornost rukovodstva za nepoštivanje sigurnosnih zahtjeva", navodi Džakula.

Pitanje "odgovornosti" ima još jednu važnu komponentu kada je u pitanju NIS2, a to je praksa prikrivanja kada su u pitanju sigurnosni incidenti zarad zaštite poslovne reputacije i interesa. Džakula ovu praksu opisuje kao "kopanje još dublje jame" i dodaje da nova direktiva predviđa kratke rokove za prijavu sigurnosnih incidenata. Oni podrazumijevaju uspostavljanje jasnih koraka za prijavljivanje incidenata: početno prijavljivanje u roku od 24 sata, detaljan izvještaj unutar 72 sata te redovno ažuriranje i konačni izvještaj nakon mjesec dana. Ovi izvještaji trebaju sadržavati informacije o ozbiljnosti incidenta, njegovom utjecaju i poduzetim mjerama, za šta će biti preporučljivo tražiti angažman profesionalnih sigurnosnih konsultanata.

Udar na mala i srednja preduzeća

I Knupleš dijeli ovaj stav, uz opasku da će ova stavka posebno pogoditi mala i srednja preduzeća čiji je glavni problem "nedostatak resursa" koji je sada kombiniran s već postojećim opterećenjem potrebama da se prate najnoviji sigurnosni trendovi. Tu bi, na pola puta između suprotstavljenih potreba zaštite budžeta i usklađenosti s NIS2, kompanijama ruku pomoći mogla pružiti tehnologija. U nju nadu polaže i Džakula.

"S tehničke strane, to može uključivati implementaciju sistema za praćenje sigurnosnih incidenata (SIEM), naprednih antivirusnih rješenja za računare i serversku infrastrukturu, uređaje za zaštitu mrežne infrastrukture kao i alate i procedure za kontinuirano testiranje softvera i interne mreže na bezbjednosne ranjivosti. Kompanije se često opredijele za angažovanje trećih lica, tj. MSP-jeva (Managed Security Providers), za kompletnu implementaciju, upravljanje i održavanje bezbjedonosnih sistema", kaže Džakula.

Njegov kolega Trampuž sličnu ulogu predviđa za pristup nultog povjerenja

(Zero Trust) i zaštitu digitalnih identiteta. Isto važi i za primjenu hardverskih sigurnosnih modela koji bi po stupanju na snagu NIS2 direktive mogli doživjeti pravi bum. "Postoje dodatna tehnička rješenja koja pomažu kompanijama da ograniče i odvoje korištenje mreža i IT sredstava na fizičkom nivou, upravljaju sigurnošću cjelokupnog portfelja krajnjih tačaka i, u konačnici, osiguraju sigurnost kopija podataka", kaže Trampuž.

Prilike nadmašuju prepreke

Na kraju, svi naši sagovornici dijele mišljenje da će direktiva NIS2 imati dubinski utjecaj na sve pore cyber sigurnosti u regiji u godinama pred nama. Najteže prepreke na putu njene primjene bit će nedostatak kvalificiranog osoblja i finansijskih sredstava kojim ne pomažu ni manjak svijesti o rasponu primjene direktive i ulozi države u ovom procesu.

Izvan granica Unije, NIS2 je još veća nepoznanica čije bi ignoriranje regionalne kompanije moglo lako lišiti pristupa lukrativnom tržištu EU. S druge strane, NIS2 je i prilika da se zamalo preko noći povećaju ulaganja u nedovoljno korištene sigurnosne tehnologije i prakse, poput enkripcije podataka, automatiziranih alata, sistema za praćenje ranjivosti, upravljanje identitetima i simulacije napada. Važan momenat tiče se i pojačanog outsourcinga cyber sigurnosnih usluga, kao i angažmana privatnih sigurnosnih kompanija za edukaciju, konsalting i upravljanje kao prijeke mjere za problem manjak kadra u ovoj oblasti. Sve ovo bi u optimističnijoj varijanti moglo dovesti do širenja ulaganja i ponude na tržištu cijele Jadranske regije uz do sada neviđenu brzinu i intenzitet.

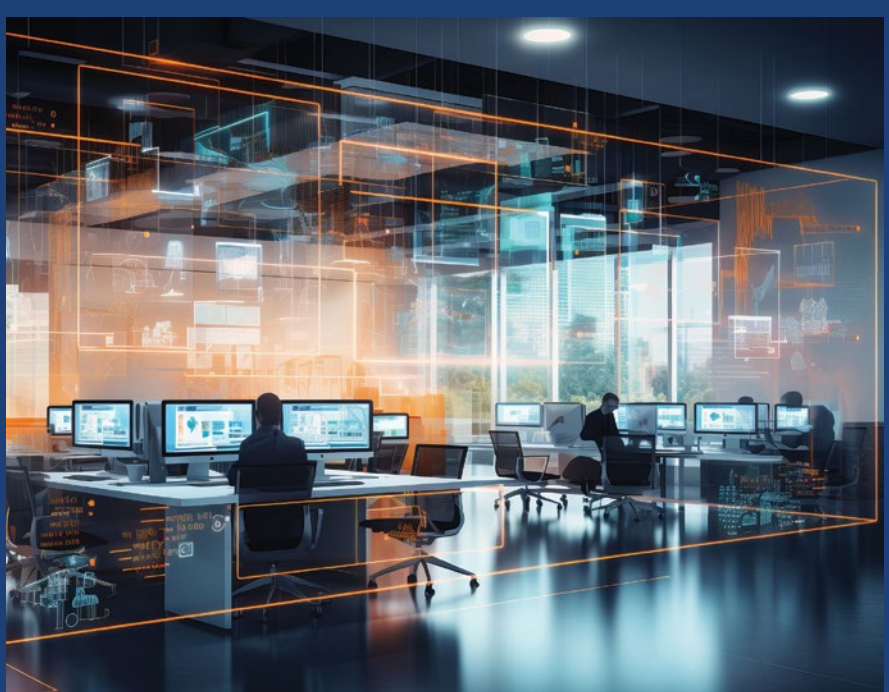
"Jasno je da će doći do znatnog povećanja ulaganja i zbog činjenice da je Direktiva u svojim mjerama adresirala sigurnost lanca opskrbe, uključujući sigurnosne aspekte odnosa između svakog subjekta i izravnih dobavljača ili pružatelja usluga. Subjekti će morati raditi procjenu rizika svojih dobavljača i pružatelja usluga te će se okretati onima koji i sami poštuju mjere zahtijevane NIS2 direktivom te tako umanjiti vjerojatnost incidenta za subjekte s kojima rade. Osim subjekata koji se moraju uskladiti sukladno kategorizaciji koja je definirana NIS2, a koja je obuhvatila i male i srednje velike tvrtke, tu će se naći i tvrtke koje čine lanac opskrbe obveznika. Dakle, veći broj nego što možemo procijeniti temeljem same kategorizacije definirane Direktivom", navodi Kopić.

Sve u svemu, implementacija NIS2 Direktive treba donijeti značajne promjene u regionalnoj industriji cyber sigurnosti, s fokusom na povećana ulaganja, unapređenje tehnoloških rješenja i poboljšanu saradnju između različitih sektora. U svjetlu prijetnji kojima administrativne granice nikada nisu ni bile prepreka, ovo može biti važan korak ka podizanju kontinentalnog odbrambenog zida u kojem je i regija ništa manje važan bedem. ◄

Podrška države: između obaveze i manjka resursa

U proceduralnom smislu, u Hrvatskoj i Sloveniji i državna tijela su jedan od aktera od kojih se očekuje pružanje podrške barem u inicijalnoj fazi primjene. Naši sagovornici su tu podijeljeni po liniji očekivanja i realnih mogućnosti. Za Knupleža iz Slovenije, država bi trebala odigrati važnu ulogu, barem u davanju detaljnih smjernica i najboljih praksi, kao i u podršci organizacije obuke i razmjene informacija između organizacije i sektora. Njegov zemljak Trampuž očekuje da će nacionalni CERT-ovi (timovi za hitne računarske intervencije) primarno biti od koristi kod detekcije ranjivosti, reakcija na incidente i izvještavanja.

Ipak, nije realistično očekivati da će država slati stručnjake u svaku kompaniju da prati primjenu direktive. Tu ulogu će, po njemu, ipak preuzeti tržište. Nešto drugačiji ton u odnosu na očekivanja od državne podrške iznosi Kosanović iz Hrvatske: "Slabo, nacionalna tijela tek nemaju dovoljno resursa niti načina da privuku stručni kadar", zaključuje on. U Bosni i Hercegovini situacija je još složenija jer na državnom nivou nije usvojen Zakon o cyber sigurnosti, kao ni propisi o obaveznom prijavljivanju incidenata, osim ako oni ne predstavljaju krivično djelo u nadležnosti policije u skladu sa Zakonom o krivičnom postupku.



Nemali broj kompanija bi mogao pokušati preko noći i bez većih ulaganja postići usaglašenost "na papiru" kako bi nastavili neometano poslovati