POMURSKA OBZORJA
Vol. 11, No. 20, pp. 33–42, november 2024

Pomurska Obzorja

Ogromne kazni in veliko novih obveznosti glede uvedbe direktive NIS2

Sprejeto
31. 10. 2023

Izdano
22. 11. 2024

Florian de Margan
Symbios Funding & Consulting,
Kriegsstr. 85, 761 33 Karlsruhe, Germany,
e-mail: florian.margan@gmail.com

Dopisni avtor
E-pošta: florian.margan@gmail.com

Povzetek Na tisoč slovenskih podjetij, občin, bolnic, državnih ustanov, čaka kmalu najnovejša kibernetična obveznost imenovana NIS2 (varnost omrežij in informacija ali Network and Information Security). Široko prediskutovana evropska smernica ima za cilj nekompromisno posilit kibernetično varnost podjetjem in državnim organom – ustanov v EU kot celote. Stroške, ki ne bodo majhni bodo morale plačati sama podjetja oziroma državne ustanove s potrebnimi tehničnimi, operativnimi in organizacijskimi ukrepi, ki jih bo zahtevala izvedba odloka oziroma navedena smernica.

Ključne besede:
Direktiva NIS2,
Varnost omrežij in informacij,
kibernetična varnost

https://doi.org/11.18690/po.11.20.33-42.2024

Univerzitetna založba Univerze v Mariboru

1 UVOD

Kibernetična varnost je metoda zaščite kritičnih sistemov in občutljivih podatkov pred digitalnimi grožnjami. Ukrepi kibernetične varnosti, znani tudi kot varnost informacijske tehnologije (IT), so temelji za zaščito omrežnih sistemov in aplikacij pred napadi znotraj in zunaj podjetja. Pričakuje se, da bo svetovni trg kibernetične varnosti rasel zaradi vse večjega števila kibernetičnih groženj in kibernetičnega terorizma, ter nevarnosti pripojevanju na internet.

Direktiva NIS2 je najnovejša politika EU, katere navedeni cilj je izboljšanje skupne kibernetične varnosti držav članic EU. Veljati je začela januarja 2023 in od 18. oktobra 2024 bodo morale vse ustrezne organizacije izpolniti nove zahteve, ki jih predpisuje smernica NSI2 [1]). Kaj natančno pomeni NIS2 in kakšne so njegove morebitne posledice?

Direktiva NIS 2 *(varnost omrežij in informacij - Network and Information Security)* navaja:

- Vsa prizadeta podjetja in organizacije morajo uporabljati pristop k vsem morebitnim kibernetičnim tveganjem, vključno na primer s tveganjem človeškega dejavnika, odpovedjo sistema, zlonamernimi agenti, naravnimi nesrečami, ter tveganja varnostno fizičnih in okoljskih sistemov.
- Uvaja obveznost poročanja o reševanju incidentov in imenovano odgovorno osebo z strani organizacije.
- Imeti mora pripravljene rezervne načrte v primeru kibernetičnega napada, da se aktivnost organizacije lahko nemoteno nadaljuje *(kontinuiteta poslovanja - business continuity)*.

Vse te obveznosti bi morale zadevati srednje in velike organizacije, ki delujejo predvsem v energetiki, omrežnih sektorjih, infrastrukturi, zdravstvu *(tudi na primer zdravilišča)*, državni upravi, prometu in bančništvu. Ti sektorji so označeni kot kritično pomembni. Ne konča se le pri njih, ampak vključuje tudi poštne in kurirske storitve, predelavo odpadkov, kemično, živilsko in druge industrije in končno, digitalne storitve in raziskave.

2 PREDSTAVITEV NEKATERIH VARNOSTNIH UKREPOV Z STRANI NSI2

Navajam deset pomembnih točk za boljše razumevanje, ki predstavljajo minimalne varnostne ukrepe v okviru novega odloka – smernice EU in sicer t.i. NIS2:

1. Načela analize tveganja in varnosti informacijskih sistemov,
2. Reševanje incidentov,

1 https://finmag.penize.cz/byznys/445084-obri-pokuty-a-tuna-novych-povinnosti-smernice-nis2-nema-ve-svete-obdoby?utm_source=www.seznam.cz&utm_medium=sekce-z-internetu#dop_ab_variant=0&dop_source_zone_name=hpfeed.sznhp.context&dop_vert_ab=0&dop_vert_id=leg0&dop_req_id=iR4CMTMsYBN-202309101106&dop_id=22753060

3. Neprekinjenost poslovanja, kot je varnostno kopiranje in upravljanje obnove po katastrofi, ter krizno upravljanje,
4. Varnost dobavne verige, vključno z varnostnimi vidiki, povezanimi z odnosi med posameznimi subjekti in njihovimi neposrednimi dobavitelji ali ponudniki storitev.
5. Varnost pri pridobivanju, razvoju in vzdrževanju omrežij in informacijskih sistemov, vključno z obravnavanjem ranljivosti in njihovim odkrivanjem.
6. Načela in postopki za ocenjevanje učinkovitosti ukrepov za obvladovanje tveganja kibernetične varnosti.
7. Osnovne prakse kibernetične higiene in usposabljanje za kibernetično varnost,
8. Politike in postopki v zvezi z uporabo kriptografije in kjer je primerno šifriranje.
9. Varnost človeških virov, politike nadzora dostopa in upravljanje sredstev,
10. Uporaba večfaktorske avtentikacije ali rešitev za stalno avtentikacijo, varne glasovne, video in besedilne komunikacije, ter varnih komunikacijskih sistemov v mreži znotraj subjekta, kjer je primerno.

Jasno je, da je seznam precej obsežen – tako zelo, da morda tudi velikim podjetjem ne bo povsem enostavno brezhibno izpolniti vseh točk z lastnimi človeškimi viri. Predvsem pa so odlomki o računalniških omrežjih, informacijskih sistemih in kriptografiji precej zahtevni in za nestrokovnjaka nepregledni.*Češka verzija predloga zakona z vsemi spremljajočimi predpisi ima skupaj 151 strani).*

Posledično lahko NIS2 velja tudi za manjše organizacije z manj kot desetimi zaposlenimi in prometom, nižjim od 2 mil. €/leto, če je njihova dejavnost kakorkoli strateško pomembna. Tu je treba dodati, da so kazni za morebitne kršitve lahko izredno visoke: najvišji znesek upravne kazne, lahko doseže 7 mil. € ali 1,4% celotnega prometa določenega podjetja v zadnjem letu in to tista katera je višja *(piše v predlogu)*. Direktiva velja za vsa podjetja, ki delujejo v EU, ne glede na njihov sedež.

Smernica tudi navaja, da bi lahko odsotnost predpisov o varnosti dobavne verige v prihodnosti povzročila poslabšanje položaja poslovnih subjektov, ki delujejo na evropskem trgu, saj ne bi mogli ponuditi enake stopnje varnosti za svoje izdelek ali storitev kot subjekti, ki delujejo v državah, ki so sprejele podobno ureditev. Nesprejetje zakonodaje bi torej lahko povzročilo prisilno zavrnitev dobav slovenskih podjetij s strani tujih kupcev zaradi varnostnih in strateških groženj, ki izhajajo iz dobav podizvajalcev.

Ocenjujem, da bi ti stroški pri uvedbi enega varnostnega sistema stal od 40 do 60 tis. €. Bo to drago, vendar bo to nujna obveznost.

Lahko se vprašamo »ali potrebujemo NIS 2 ?«

Postavlja se vprašanje, v kolikšni meri je direktiva NIS2 *(oziroma nacionalni zakoni, ki izhajajo iz te direktive)* resnično potrebna. Ali ne gre predvsem za zaposlovanje zakonodajalcev in pogodbe za pravno-svetovalni kompleks, kot trdijo nekateri ciniki?

Cybersecurity Ventures s sedežem v Kaliforniji poroča, da bo kibernetski kriminal leta 2023 znašal 8,0 mld.$.[2] ENISA *(Evropska agencija za kibernetično varnost)* poroča, da je količina podatkov, ukradenih po kibernetičnih napadih v letu 2021 dosegla več kot 260 terabajtov [3]. Po podatkih IBM-a je povprečna cena ene kršitve podatkov 4,45 mil. $ [4]

Tudi če bi bile te številke pretirane, varnostnih ukrepov vsekakor ni vredno podcenjevati. Je pa veliko vprašanje, ali je obsežna in nekoliko okorna direktiva, prenesena v slogu EU v nacionalne zakone, najboljša rešitev. ZDA na primer še nimajo zvezne zakonodaje, ki bi bila neposredno primerljiva z evropsko direktivo NIS2.

V ZDA se kibernetična varnost obravnava na različnih ravneh vlade in med sektorji, vendar ni enotnega zveznega standarda. Nekatere zvezne agencije, kot npr Cybersecurity and Infrastructure Security Agency (CISA), izdajajo smernice in standarde, ki pa pogosto niso zavezujoči. Po drugi strani pa obstaja več zakonov na zvezni ravni, ki obravnavajo kibernetično varnost v določenih sektorjih, kot sta zdravstvo (HIPAA)[5,6,7]) in finančne storitve (GLBA). Pravilo o zasebnosti HIPAA določa zvezne standarde za varovanje zasebnosti osebnih zdravstvenih podatkov in daje pacientom vrsto pravic v zvezi s temi informacijami, vključno s pravicami do pregleda in pridobitve kopije njihove zdravstvene kartoteke ter do zahtevanja popravkov.Nekatere države imajo tudi svoje zakone o kibernetični varnosti, vendar se ti lahko razlikujejo od države do države.

V naslednjih grafih prikazujem nekoliko primerov velikost bodočega globalnega varno-

2 Steve MORGAN, (2022), „Cybercrime To Cost The World 8 Trillion Annually In 2023“, Cibercrime Magazine, 17.10.2022, 83 Main Street, Suite 5, Northport NY 11768 https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/

3 European Union Agency for Cybersecurity, (2022), “ENISA Threat Landscape 2022“, 3.11.2022, https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

4 Cassy LALAN, (2023), „*IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend, Despite Soaring Breach Costs*“, 24.7.2023, Cambridge, IBM Newsroom, https://newsroom.ibm.com/2023-07-24-IBM-Report-Half-of-Breached-Organizations-Unwilling-to-Increase-Security-Spend-Despite-Soaring-Breach-Costs

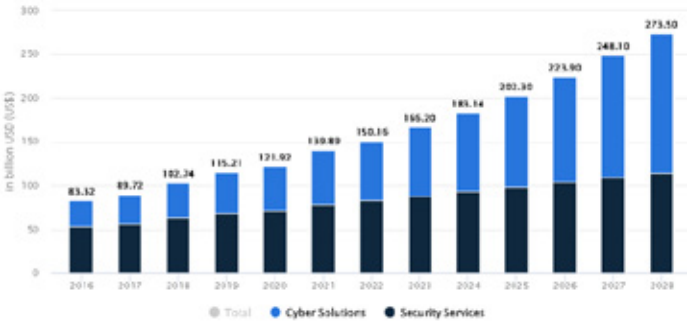
5 PrimeFactors, (2016), “*HITECH vs. HIPAA: What You Need to Know*”, September 2016, Global Industries Served, https://secureframe.com/request-demo/demo- secureframe?utm_source=google&utm_medium=cpc&utm_campaign=19904721815&utm_content=-147606704596-g-eur&utm_term=hipaa%20compliance%20rules&hsa_acc=8812124833&hsa_cam=19904721815&hsa_grp=147606704596&hsa_ad=677158932695&hsa_src=g&hsa_tgt=kwd-370143517917&hsa_kw=hipaa%20compliance%20rules&hsa_mt=p&hsa_net=adwords&hsa_ver=3&gad=1&gclid=Cj0KCQjwm66pBhDQARIsALIR2zCipGyf6d9BiivFLfWelRqnztfnJk1ZwtYYMnClVVlDSy5ExRjeIz0aAixtEALw_wcB

6 U.S. Department of Health and Human Services, “The HIPAA Privacy Rule“, HHS Headquarters, 200, Independence Avenue, S.W. Washington, D.C. https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

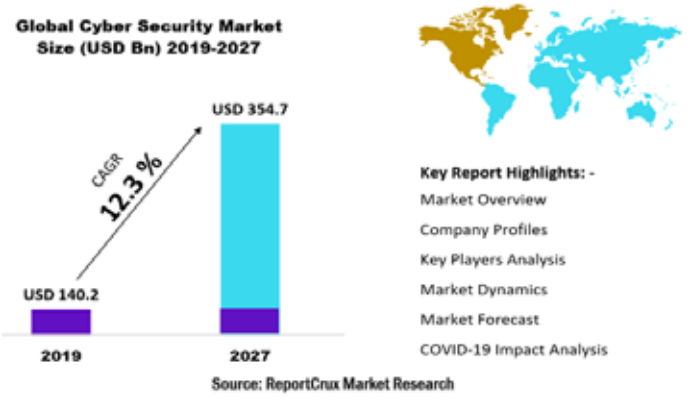
7 https://www.google.com/search?sca_esv=573613501&cs=0&sxsrf=AM9HkKnaD-rWMHHtNQrYTxtZzN6ADLezDQg:1697382847396&q=global+security&tbm=isch&chips=q:global+security,online_chips:cybersecurity:t7mymCksDXo%3D&usg=AI4_-kQiomI_kvifZD7My0m-FuT4yk1tQA&sa=X&ved=2ahUKEwjXiqrtq_iBAxU0g_0HHSpMAgQ4ChCAigMoAXoECCcQFg&biw=1344&bih=723&dpr=1.25

stno kibernetičnega trga po regionih in rast globalnega kibernetičnega trga v milijardah USA $. Podatki raznih virov se zelo razlikujejo, vendar podajam nekoliko primerov.

Prihodek na trgu kibernetičnih varnosti naj bi leta 2023 dosegel $166,20 mld. Varnostne storitve prevladujejo na trgu s predvidenim tržnim obsegom $87,97 mld. v letu 2023. Pričakuje se, da bo prihodek pokazal letno stopnjo rasti (CAGR 2023–2028) v višini 10,48 % , zaradi česar bo obseg trga do leta 2028 znašal $273,60 mld.



Graf št. 1: Prihodki po segmentu kibernetične rešitve in kibernetični servis (mld. $)
Vir: statista.com



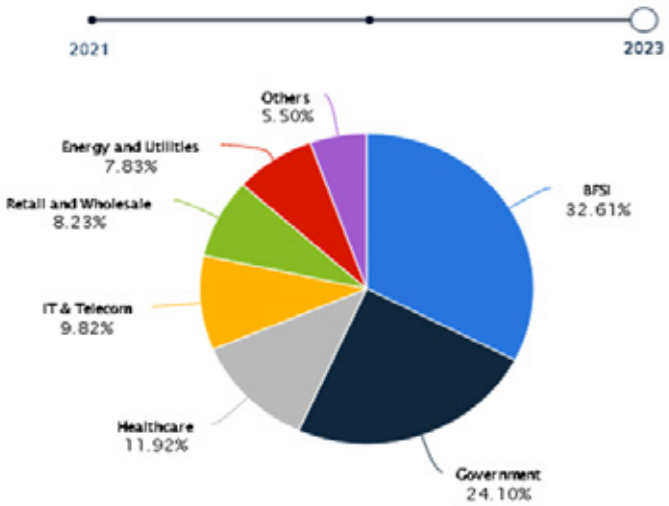
Graf št.2: Globalna kibernetična varnost v mld. USD

Velikost treh kibernetičnih varnosti je bila v letu 2021 ocenjena na $218,2 mld. in bi naj do leta 2030 dosegla $431,5 mld., ki bo v letu 2022 do 2030 znašala 11,50 % CAGR[8].

Velikost svetovnega trga kibernetične varnosti naj bi se povečala s $172,32 milijard leta 2023 na $424,97 milijard leta 2030, pri CAGR 13,8 %[9]).

8 https://www.verifiedmarketresearch.com/product/global-cybersecurity-market-size-and-forecast/

9 Fortune Business Insights, https://www.fortunebusinessinsights.com/industry-reports/cyber-security-market-101165



Graf št.3: Procentna udeležba kibernetične varnosti po sektorjih (*predpoved*)
Vir: Statista Market Insights, IX/2023

Iz grafa je razvidno, da bo najbolj potrebna zaščita před kibernetično nevarnostjo v zavarovalnicah (32,61%) in državnemu aparatu (24,10%). Priporočam z pregledom daljših virov[10,11,12,13,14]).

Obljuba ali grožnja v imenu NIS2

Kot je običajno pri kompleksnih zakonih in sistemih, se hudič skriva v podrobnostih. Za zdaj ni mogoče ugotoviti, ali je NIS2 nepogrešljivo orodje v boju proti kibernetski kriminaliteti ali pa bo na koncu bolj kot formalnost, ki ne pomaga in ustvarja le dodatne stroške.

Pri tem je treba omeniti direktivo GDPR, ki ni naredila ničesar za zaščito naših osebnih

10 https://www.statista.com/outlook/tmo/cybersecurity/worldwide#revenue
11 https://www.marketsandmarkets.com/Market-Reports/cyber-security-market-505.html https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2- trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers
12 Polaris Market Research, (2023), "Report Summary", 30 Wall Street, 8th Floor, New York City, NY 10005, United States https://www.polarismarketresearch.com/industry-analysis/cyber-security-market
13. Spherical Insights LLP, (2023), "Global Cybersecurity Market Insights Forecasts to 2030", East Fountain, Circle Drive, Mason, Ohio 45040, USA https://www.sphericalinsights.com/reports/cybersecurity-market
14 Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel, (2023), "New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers ", McKinsey & Company, https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/new-survey-reveals-2-trillion-dollar-market-opportunity-for-cybersecurity-technology-and-service-providers

podatkov. Samo zapravlja vaš čas s tem, da morate klikati stran od stalnih soglasij za piškotke. Ampak to ni najhujši del. Škoda, da je GDPR postala ovira za napredek pri razvoju novih sistemov, predvsem umetne inteligence. Za povprečnega uporabnika morda ni opazno, a razvijalcem je GDPR varovanje nedokončnih idej. Na koncu je GDPR postal ukrep, ki je podjetjem povečal stroške in odpravil polovico novih prijav [1515)].

Z rastjo digitalnega gospodarstva se z njim povečuje tudi digitalni kriminal. Naraščajoče število spletnih in mobilnih interakcij ustvarja milijone priložnosti za napade. Mnogi vodijo do kršitev podatkov, ki ogrožajo ljudi in podjetja. Pri trenutni stopnji rasti bo škoda zaradi kibernetskih napadov do leta 2025 znašala približno $10,5 mld./ letno – kar je 300 % povečanje glede na raven iz leta 2015.[16)]

Ob soočenju s temi kibernetičnimi napadi so organizacije po vsem svetu leta 2021 za kibernetično varnost porabile približno $150 mld., kar je letno rast za 12,4 %. Vendar pa je glede na obseg problema tudi to »prebujanje varnosti« verjetno nezadostno. Raziskava med 4.000 srednje velikimi podjetji kaže, da se bo obseg groženj od leta 2021 do leta 2022 skoraj podvojil. Glede na raziskavo je skoraj 80 % testiranih skupin bilo ogroženih, ki so delovala leta 2021, in več kot 40 % opazovane programske opreme še nikoli ni bilo ogrožene.[17)]

Ta dinamika kaže na pomemben potencial na razvijajočem se trgu. Trenutno razpoložljive komercialne rešitve ne ustrezajo v celoti zahtevam strank v smislu avtomatizacije, cen, storitev in drugih zmogljivosti. Posledično je današnja vrzel med prodajnim trgom v vrednosti $150 mld. in potencialnim trgom velika. Pri približno 10-% prodoru varnostnih rešitev danes, skupna priložnost znaša $1,5 do 2,0 bil. trga *(graf 1)*. To ne pomeni, da bo trg kmalu dosegel tolikšno velikost *(trenutna stopnja rasti je 12,4 %/letno od osnove približno $150 mld. leta 2021)*, temveč da tako ogromna delta od ponudnikov in vlagateljev zahteva, da »odklenejo« večji vpliv z strankami z boljšim izpolnjevanjem potreb slabo pokritih segmentov, nenehnim izboljševanjem tehnologije in zmanjševanjem zapletenosti in za kupce lahko predstavlja edinstven trenutek za inovacije v industriji kibernetične varnosti.

3 SPREMEMBA PRI UVEDBI SNI2 JE VEČJA KOT PA ŽE SPREJETA SMERNICA GDPR EU

Na tisoče podjetij se bo kmalu soočilo z novo obveznostjo, imenovano NIS2. Široko

15 Brian Chau, (2023), *„The Costs of Europe's GDPR Regime"*, Pirate wires, 28.8.2023, https://www.piratewires.com/p/the-costs-of-europes-gdpr-regime https://bowtiesecurity.com/webinar-nis2-13062023/?gclid=Cj0KCQjwm66pBhDQARIsALIR2zCLVBPY5DciRh38jbblvohGTLiPnrrMJz6mNEBPsJ1zVaOV3Q-Hf0YaAlXiEALw_wcB

16 Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel, (2023), *"New survey reveals $2 trillion market opportunity for cybersecurity technology and service providers "*, McKinsey & Company,

17 McKinsey & Company (2023), "What is cybersecurity? - Which cybersecurity trends are projected over the next three to five years?", https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-cybersecurity

obravnavana evropska direktiva želi drastično okrepiti kibernetično zaščito podjetnikov in državnih organizacij v EU. Stroške njegovega povečanja bodo nosile družbe same, in sicer s potrebnimi tehničnimi, operativnimi in organizacijskimi ukrepi, ki jih bo zahtevala uveljavitev uredbe. Na kaj se torej pripraviti?

Koga točno bo zajela nova dajatev, še ni jasno; trenutno čaka na vključitev direktive NIS2 slovenski pravni sistem. To je treba storiti z novim zakonom o kibernetični varnosti (NZKB) in izvedbenimi odloki, ki jih moral pripraviti, **recimo** Državni urad za kibernetično in informacijsko varnost (DUKIV). Ocene, koliko podjetij bo nova obveznost prizadela, so torej različne. Odvisno je med drugim od tega, kako DUKIV pristopi k ureditvi. Najmanjši obseg obveznih subjektov določa sama direktiva NIS2, vendar se ta obseg lahko še razširi na državni ravni.

Vvsakem primeru je gotovo, da bodo nova pravila veljala za vse subjekte kritične infrastrukture, izbrane storitve, ki jih določa zakon, pa tudi za večino srednjih in velikih podjetij v ključnih sektorjih *(z več kot 50 zaposlenimi in/ali prometom, ki presega €10 mil./leto)*. Vsekakor se bo pa končni krog zavezancev nedvomno razširil, predvsem na manjše organizacije, ki poslujejo v enem od kritičnih sektorjev.

Natančneje, direktiva NIS2 bi lahko prizadela več tisoč slovenskih podjetij. Učinek direktive bo ogromen. Zavedajmo se, da govorimo o tisočih entitetah. Pri največjih lahko investicijski stroški narastejo na nekaje milijonov eur, operativni stroški pa na desetine. V primerjavi z NIS2 je z vidika stroškov implementacije tudi GDPR majhna.

Nova pravila bodo veljala tudi za segmente, ki se do sedaj praktično niso ukvarjali s kibernetsko varnostjo. Je res, da številne organizacije dolgo časa zanemarjajo svojo kibernetsko varnost. Glavna prednost je očitna. Prejeli bodo zunanji impulz, ki jih bo prisilil, da ponovno razmislijo o tej praksi in začnejo bolje varovati svoje premoženje. Tako lahko preprečijo večkrat večje izgube in s tem opozarjam na vse bolj naraščajoče in bolj sofisticirane kibernetske napade.

Študija PwC Global Economic Crime and Fraud 2022[18] s konca lanskega leta je na primer izpostavila, da je skoraj polovica podjetij v zadnjih dveh letih doživela neko vrsto gospodarskega kibernetičnega kriminala. Najbolj ogrožena so podjetja, ki delujejo z tehnologijami, v medijskem prostoru ali telekomunikacijah, je pokazala raziskava med 1300 najvišjimi menedžerji v 53 državah po svetu. Medtem ko število napadenih podjetij v zadnjih dveh letih bolj ali manj ni naraslo (46 %), so izjema tehnološka podjetja, kjer se skokovito povečuje kibernetični kriminal. Skoraj dve tretjini (64 %) podjetij, ki se ukvarjajo s tehnologijo, komunikacijo ali delujejo v medijskem prostoru, priznava, da je doživelo kibernetični napad.

18 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html
PwC's Global Economic Crime and Fraud Survey 2022
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://www.pwc.com/gx/en/forensics/gecsm-2022/PwC-Global-Economic-Crime-and-Fraud-Survey-2022.pdf

V zadnjih dveh letih se podjetja ne le v tujini, ampak tudi v Sloveniji soočajo z največ goljufijami v kibernetskem prostoru, ki so presegle goljufije, ki jih povzročijo stranke na vrhu namišljenega seznama. Ključno je, da se podjetja bolj prožno odzovejo na te spremembe in uvedejo nove postopke in tehnologije, ki jim bodo omogočili boljše soočanje s tovrstnimi goljufivimi dejanji. Sem prepričan, da se bo število napadov v prihodnosti povečalo.

Poleg tega naraščajoče število kibernetičnih incidentov kaže, da še zdaleč ni le to teorija. Čeprav je uvedba novih mehanizmov lahko težavna za podjetja, ki jih bo NIS2 na novo prizadel *(na primer v živilski industriji ali ravnanju z odpadki)*, po mnenju strokovnjakov s pripravami ni priporočljivo odlašati. Po mojem pa brez spremembe miselnosti ne gre.

Nova pravila bodo lastnikom podjetij pomagala razumeti, da je lahko kdorkoli tarča napada, da kibernetična varnost ni samoumevna, da so proaktivni ukrepi nujno potrebni, da so s tem povezani stroški vendar ni zapravljen denar, ampak da bodo bogato poplačani v obvladovanih incidentih in izgubah, ki se zaradi uvedbe ukrepov, ki jih zagotavla smernica SIN2 ne bodo zgodile. Stroške implementacije NIS2 za največje kritične infrastrukturne subjekte ocenjujem na desetine milijonov evrov, operativne stroške pa na nekaj sto tisoč evrov. Ne bo treba vlagati le v strojno in programsko opremo, temveč predvsem v ljudi in organizacijske ukrepe, kar zahteva zahtevnost novih pravil.

3 Zaključek

Za tiste, ki aktivno obvladujejo tveganja in ne podcenjujejo svoje zaščite, lahko NIS2 služi kot dobro merilo. Z vidika celotne družbe bo ta zakonodaja nedvomno prispeval k splošni krepitvi odpornosti slovenske kritične infrastrukture, kar je v interesu države, državljanov in podjetij.

Predvidevam pa, da bodo podjetja nova pravila začela izvajati že v prihodnjem letu, saj je obseg novih obveznosti zelo širok in vpliva tako rekoč na celotno delovanje podjetja, ob dejstvu, da že zdaj primanjkuje strokovnjakov na trgu, ki so sposobni zagotoviti potrebne rešitve. Prepričan sem, da bo poenotenje pravil, ki jih NIS2 prinaša na področju kibernetične varnosti, zelo nujno. Pravočasno obravnavanje kibernetičnih groženj je nujno in pomembno za večjo varnost vseh državljanov in subjektov v Sloveniji.

Viri in literatura

Bharath Aiyer, Jeffrey Caso, Peter Russell, and Marc Sorel, (2023), "*New survey reveals $2 trillion market portunity for cybersecurity technology and service providers* ", McKinsey & Company,

Brian Chau, (2023), „*The Costs of Europe's GDPR Regime*", Pirate wires, 28.8.2023,

European Union Agency for Cybersecurity, (2022), "ENISA Threat Landscape 2022", 3.11.2022,

Cassy LALAN, (2023), „*IBM Report: Half of Breached Organizations Unwilling to Increase Security Spend Despite Soaring Breach Costs*", 24.7.2023, Cambridge, IBM Newsroom,

Steve MORGAN, (2022), „Cybercrime To Cost The World 8 Trillion Annually In 2023", Cibercrime Magazine, 17.10.2022, 83 Main Street, Suite 5, Northport NY 11768

Polaris Market Research, (2023), "*Report Summary*", 30 Wall Street, 8th Floor, New York City, NY 10005, United States

Prime Factors, (2016), "*HITECH vs. HIPAA: What You Need to Know*", September 2016, Global Industries Served,

Spherical Insights LLP, (2023), "*Global Cybersecurity Market Insights Forecasts to 2030*", East Fountain-Circle Drive, Mason, Ohio 45040, USA