UDK 004.056:336.71.025.13:061.1EU

Nadzorniške prioritete na področju kibernetske varnosti

*Matej Vodopivc**

SUPERVISORY PRIORITIES IN THE CYBER SECURITY AREA

The article presents the supervisory priorities of the European Central Bank (hereafter ECB) for the next period, as well as the consequences of the development of the digital environment for the financial sector, especially in the context of increasing cyber threats. Based on data showing an increase in cyber risks in the recent period, referring to geopolitical events, the document emphasizes the necessity of escalating surveillance measures. The priorities of the supervision of systemically important banks for the period 2023-2025 are discussed, with an emphasis on cyber security and operational resilience. The article offers an insight into the challenges that financial institutions face in this field.

JEL E58 K24 O33

UVOD

Površina kibernetskih groženj se hitro razvija in postaja vse bolj kompleksna. Po nekaterih ocenah se je izpostavljenost kibernetskemu tveganju med leti 2013 in 2020 potrojila, pri tem pa sodi finančni sektor danes med najbolj izpostavljene. Raziskave kažejo, da so kibernetske grožnje vir sistemskega tveganja za podjetja in trge, pri čemer je kibernetsko tveganje vedno bolj upoštevano tudi že na borznih trgih (Panetta, 2022).

RAZVOJ KIBERNETSKIH TVEGANJ

Zunanji dejavniki vplivajo na izpostavljenost kibernetskim grožnjam na načine, ki jih je težko predvideti. Dober primer je ruska invazija na Ukrajino, ki so jo številni akterji kibernetskih groženj uporabili za zlorabo zaupanja posameznikov in podjetij z izvajanjem lažnega predstavljanja ali drugih tehnik socialnega inženiringa, tako pridobljene informacije pa v nadaljevanju uporabili za napade osredotočene na kritično infrastrukturo.

Lažno predstavljanje, socialni inženiring in človeški dejavnik so na splošno še vedno glavni kanali, ki jih kibernetski napadalci uporabljajo za vdor v informacijske sisteme finančnih institucij. Kibernetske grožnje, ki so jim izpostavljeni ponudniki IT-storitev, pa ostajajo vedno prisotna skrb v med seboj povezanih in soodvisnih infrastrukturah in zahtevajo najvišjo stopnjo pozornosti.

V letu 2022 so izzivi, povezani s pandemijo in uvajanjem novih hibridnih načinov poslovanja, postali manj pomembni. Nasprotno pa so negotovosti, ki izhajajo iz vojne v Ukrajini, in vse večjih geopolitičnih napetosti, pomenile, da je bilo okolje za nadzorovane banke še naprej zahtevno z vidika operativne odpornosti (ECB, 2022a).

Pojavnost kibernetskih napadov se je v letu 2022 še povečala in predstavlja povečano grožnjo bančnim operacijam. Število kibernetskih napadov v svetu se je leta 2022 v primerjavi s prejšnjim letom povečalo za približno 45 % in preseglo najvišjo vrednost, zabeleženo med pandemijo. Povečanje javno razkritih kibernetskih napadov se je med regijami močno razlikovalo in se je povečala za 51 % v državah evrskega območja, 23 % v ZDA in 72 % v drugih državah (ECB, 2023).

Tako kot v prejšnjih letih so banke tudi v letu 2022 kazale enak trend k digitalni preobrazbi, kar je pomenilo večjo odvisnost od IT infrastrukture in uporabe storitev tretjih ponudnikov, vključno s storitvami v oblaku, ki so uporabljene za zagotavljanje kritičnih storitev. Čeprav ta trend nedvomno prinaša določene koristi za banke, predstavlja tudi dodatna tveganja in izzive z operativnega vidika, kot sta obvladovanje vse večjega števila naprednih kibernetskih napadov, ki so

* Matej Vodopivc, mag. posl. ved, nadzornik bančnega poslovanja v Banki Slovenije

usmerjeni neposredno na banke ali pa na njihove ponudnike, ter koncentracijo kritičnih tretjih ponudnikov. Iz tega razloga ostajajo kibernetska tveganja in odvisnost od tretjih ponudnikov prednostni nalogi bančnega nadzora. Banke morajo izvesti nadaljnje korake, da bi zagotovile odpornost na morebitne operativne motnje, vključno s hudimi, vendar verjetnimi kibernetskimi incidenti, ki predstavljajo povečana tveganja za celoten finančni sistem (ECB, 2022a).

Vojna v Ukrajini je privedla do povečanja operativnih tveganj in tveganj, povezanih z IT sistemi, zaradi česar so banke prisiljene, da odpravijo pomanjkljivosti v svojih ureditvah zunanjega izvajanja ter v okvirih IT varnosti in kibernetske odpornosti. Banke s kritičnimi operacijami v državah, ki jih je neposredno prizadela vojna v Ukrajini, so aktivirale načrte neprekinjenega poslovanja, ki so se izkazali za učinkovite v hitro spreminjajočih se razmerah v prvi fazi vojne. Sistemsko pomembne institucije so uspele zagotoviti zaščito in po potrebi premestitev ključnega osebja, hkrati pa so nemoteno nadaljevale svoje poslovanje (ECB, 2023).

Nadaljevanje zahtevnih geopolitičnih razmer ohranja splošno raven tveganja za kibernetsko varnost v finančnem sektorju EU na povišani ravni. Še vedno obstajajo možnosti za stopnjevanje kibernetskih napadov, učinki uspešnega napada na večjo finančno institucijo ali kritično infrastrukturo pa bi se lahko razširili po celotnem finančnem sistemu prek treh kanalov: i) neposredno širjenje škodljive programske opreme med sistemi; ii) širjenje likvidnostnega šoka prek operativnih izpadov; iii) negativnega šoka zaupanja vlagateljev, ki bi se verjetno še poslabšal zaradi negotovosti v krizi. Finančni subjekti bi lahko imeli motnje neprekinjenega poslovanja, negativen vpliv na ugled, v skrajnih scenarijih pa bi lahko prišlo do težav z likvidnostjo in finančno stabilnostjo v celotnem sistemu. Kibernetski napadi bi lahko spodkopali tudi kritične storitve in ogrozili podatke potrošnikov zunaj finančnega sektorja (EBA, 2023).

EBA v zadnjem poročilu o tveganjih in ranljivostih v finančnem sistemu EU ohranja kibernetsko varnost kot področje, ki zahteva nadaljnje spremljanje in obravnavo, saj se soočamo z nezmanjšanim številom kibernetskih napadov in nadaljevanjem ruske vojne v Ukrajini (EBA, 2023).

DOSEDANJE NADZORNIŠKE AKTIVNOSTI IN PRIČAKOVANJA

Nadzorniška pričakovanja in aktivnosti na področju kibernetske varnosti so se že v preteklem obdobju stopnjevala. Stopnjevanje nadzorniških aktivnosti in pričakovanj vezanih na upravljanje kibernetske varnosti je v preteklem triletnem obdobju najbolj izrazito sledilo i) nastopu pandemije covida-19 v letu 2020, kar je povečalo obseg dela od doma, ter izpostavljenost bank do IT- in kibernetskih tveganj, ter ii) začetku vojne v Ukrajini v letu 2022 in s tem sovpadajoče povečano število kibernetskih napadov na banke. V letu 2022 so bile nadzorniške prioritete razdeljene v več sklopov, pri tem je bil na področju kibernetskega tveganja poudarek na strukturnih ranljivostih, ki bi jih institucije morale reševati z učinkovitimi digitalnimi strategijami in ukrepi za okrepitev upravljanja (ECB, 2021).

Finančne institucije morajo imeti ustrezna znanja in zmogljivosti za zagotavljanje varnosti IKT ter v ta namen zagotavljati ustrezne vire. Finančne institucije morajo izvajati postopke, ki zmanjšujejo pogostnost in vpliv kršitev varnosti IKT in kibernetskih incidentov. To so na primer redne ocene tveganja in ponavljajoči se preizkusi varnostnih ukrepov za odkrivanje morebitnega uhajanja informacij, preprečevanje zlonamerne kode in drugih varnostnih groženj (EBA, 2023).

Od institucij se v primeru nastopa incidenta pričakuje, da o incidentu poročajo pristojnim organom v opredeljenih rokih. V primeru zamude iz neupravičenega razloga ali malomarnosti se med drugim izpostavljajo tudi tveganju visoke finančne kazni, kot jo je ECB na primer naložila španski banki ABANCA leta 2019 (ECB, 2022c). Na podlagi preteklih nadzorniških aktivnosti ter regulatornih sprememb je ECB izdala nadzorniška pričakovanja ter rezultate izvedenih analiz, ki kažejo na pomembnost ustreznega upravljanja kibernetskih tveganj v finančnih institucijah. V nadaljevanju navajamo nekatera od njih, tj.

a) V povezavi s pandemijo covida-19 in prepoznanimi aktualnimi tveganji je ECB bankam svetovala, da proaktivno ocenijo in testirajo sposobnosti lastne IT infrastrukture v luči potencialnega povečanja kibernetskih napadov in potencialne velike odvisnosti od izvajanja bančnih storitev na daljavo. Banke so bile pozvane, da ocenijo povečano tveganje kibernetskih zlorab, ki ogrožajo njih ali njihove stranke (ECB, 2020).
b) V sklopu nadzorniškega pregledovanja (SREP) za leto 2020 je ECB objavila analizo IT tveganj, ki temelji na samoocenah bank. Med drugim je bilo prepoznano, da je upravljanje IT tveganj boljše v bankah, kjer člani uprave razpolagajo z višjo stopnjo znanja IT in izkušenj, da pri številnih bankah kritični bančni procesi temeljijo na zastarelih sistemih ter da se odvisnost od zunanjega izvajanja IT povečuje, pri tem številne banke povečujejo odvisnost od posameznih ponudnikov (ECB, 2020b).

c) V sklopu SREP 2022 in izsledkov objavljene analize so bile prepoznane pomanjkljivosti pri upravljanju zunanjega izvajanja IT in kibernetski odpornosti. Oboje je ECB opredelila kot ključni ranljivosti, ki ju bo bančni nadzor obravnaval prednostno v obdobju 2022–2024. Primernost upravljanja IT varnosti v bankah ostaja skrb nadzornikov in nadzorovanih institucij, kar je podkrepljeno z ugotovitvami inšpekcijskih pregledov kibernetske varnosti. Ugotovitve pregledov so pokazale slabosti na številnih področjih, med drugim i) pri upravljanju IKT sredstev, ii) pomanjkljivosti pri zaščiti sredstev, iii) v omejenih zmogljivostih za odkrivanje incidentov ter iv) omejenem odzivu na kibernetske incidente in pripravljenosti na obnovo po katastrofi (ECB, 2022d).
d) V sklopu kvartalnega poročanja EBA o tveganjih skupaj z rezultati iz vprašalnika o oceni tveganj (RAQ) je bilo ugotovljeno, da banke v EU skrbi naraščajoča raven kibernetskega tveganja. Večina bank pričakuje povečanje operativnega tveganja predvsem zaradi povečanih kibernetskih tveganj. Tveganja, povezana s kibernetsko ter informacijsko in komunikacijsko tehnologijo (IKT), so bila med pandemijo še vedno visoka, izgube zaradi realizacije operativnega tveganja pa so se povečale. Zanašanje na zunanje izvajanje omenjena tveganja še povečuje (EBA, 2022).
e) Smernice EBA o upravljanju tveganj povezanih z IKT, ki opredeljujejo pričakovanja glede obvladovanja notranjih in zunanjih IKT in varnostih tveganj. Smernice omogočajo institucijam, da bolje razumejo nadzorniška pričakovanja glede upravljanja IKT in varnostnih tveganj, vključno z notranjim upravljanjem, zahtevami glede informacijske varnosti, operacij IKT, upravljanja projektov in sprememb ter upravljanja neprekinjenega poslovanja (EBA, 2020).

NADZORNIŠKA PRIČAKOVANJA (2023–2025)

Glede načrtovanja ima ECB vzpostavljen letni proces presoje nadzorniških prioritet za naslednje triletno obdobje. V primeru potreb ali povečevanja posameznih tveganj lahko ta postopek izvede tudi kadarkoli prej. Prioritizacija posameznega področja tveganj temelji na oceni ECB, ki opredeli ključna tveganja in ranljivosti, s katerimi se institucije soočajo v trenutnem poslovnem, regulatornem in nadzorniškem okolju.
Namen nadzorniških prednostnih nalog enotnega mehanizma nadzora (EMN) za obdobje 2023–2025 je okrepiti nadzorniška prizadevanja pri doseganju srednjeročnih nadzorniških strateških ciljev ob hkratnem prilagajanju osredotočenosti na spreminjajoče se izzive.

Za obdobje 2023–2025 se bo od nadzorovanih institucij na področju IT in kibernetskih tveganj prioritetno zahtevalo, da okrepijo svojo odpornost na nenadne makrofinančne in geopolitične pretrese, da obravnavajo izzive digitalizacije in okrepijo usmerjevalne zmogljivosti organov upravljanja ter okrepijo svoja prizadevanja pri obravnavi podnebnih sprememb. Banke se morajo spoprijeti s strukturnimi izzivi in tveganji, povezanimi z delovanjem v vse bolj digitalnem okolju, da bi zagotovile odpornost in vzdržnost svojih poslovnih modelov (ECB 2022b).
V nadaljevanju izpostavljamo nadzorniške prioritete, ki so posredno ali neposredno povezane s kibernetsko varnostjo in vključene v sklop nadzorniških prioritet za obdobje 2023–2025 (ECB 2022b). ECB od nadzorovanih institucij pričakuje, da prednostno obravnavajo in rešujejo i) pomanjkljivosti v strategijah digitalne preobrazbe, ii) pomanjkljivosti v okvirih operativne odpornost (v katere se prednostno šteje upravljanje zunanjega izvajanja IT ter IT/kibernetska tveganja) ter iii) pomanjkljivosti pri upravljanju s podatki oz. agregaciji podatkov o tveganjih ter poročanju o tveganjih (ECB, 2023).
Nadzorovane institucije se morajo še naprej močno osredotočati na obravnavanje strukturnih izzivov in tveganj, ki izhajajo iz digitalizacije njihovih bančnih storitev, da bi zagotovile odpornost in vzdržnost svojih poslovnih modelov. Medtem ko sta močno notranje upravljanje in učinkovito strateško usmerjanje s strani upravljalnih organov ključna za razvoj in izvajanje uspešnih strategij digitalne preobrazbe, se morajo banke spoprijeti tudi z ranljivostmi in tveganji, ki izhajajo iz večje operativne odvisnosti od informacijskih sistemov, storitev tretjih ponudnikov in inovativnih tehnologij. Hkrati banke delujejo v nestanovitnih in negotovih razmerah. Z odločnimi ukrepi za doseganje močnega strateškega usmerjanja, dobrega upravljanja ter ustreznega zagotavljanja agregacije podatkov o tveganjih in zmogljivosti poročanja lahko banke podprejo vzdržnost svojih poslovnih modelov.

1) Banke morajo razviti in izvajati trdne strategije digitalizacije

Banke morajo razviti in izvajati načrte za digitalno preobrazbo z ustreznimi ureditvami, da bi okrepile vzdržnost svojih poslovnih modelov in zmanjšale tveganja, povezana z uporabo inovativnih tehnologij.
Digitalizacija ni le ključno gonilo povečanja učinkovitosti, temveč je ključnega pomena tudi za zagotavljanje konkurenčnosti bank. Skladno s tem morajo banke prilagoditi strategije digitalne preobrazbe, da naslovijo nenehno spreminjajoče se potrebe in želje potrošnikov ter

vzdržijo pritiske konkurence. Čeprav so nadzorovane institucije nedavno poročale o večji dobičkonosnosti, lahko okrepitev konkurence v bančnem sektorju in digitalnih ponudnikov zunaj sektorja – npr. finančna tehnološka podjetja in veliki tehnološki akterji – ogrozi poslovne modele bank, če se ne bodo pravočasno prilagodili novim razmeram. Nenazadnje, uvajanje novih tehnologij lahko hkrati podpre tudi povečanje učinkovitosti, ki prispeva k izboljšanju dobičkonosnosti bank.
V sklopu delovnega programa prednostnih nalog nadzora namerava ECB i) objaviti nadzorniška pričakovanja glede strategij digitalne preobrazbe in rezultatov primerjalne analize, izvedene v letu 2022, ii) izvesti ciljno usmerjene preglede strategij digitalne preobrazbe in njihove uporabe inovativnih tehnologij, ki jih dopolnjujejo aktivnosti spremljanja skupnih nadzorniških skupin za banke, v katerih bodo ugotovljene bistvene pomanjkljivosti.

2) Banke se morajo prednostno ukvarjati s tveganji, ki jih predstavljajo IT storitve oddane v zunanje izvajanje ter povečane kibernetske grožnje

Banke morajo imeti trdne ureditve upravljanja tveganja zunanjega izvajanja ter okvire upravljanja IT varnosti in kibernetske odpornosti, da lahko proaktivno obravnavajo vsa tveganja, ki bi lahko povzročila bistvene motnje v kritičnih dejavnostih ali storitvah, hkrati pa zagotovile spoštovanje regulatornih zahtev in nadzorniških pričakovanj.
Digitalna preobrazba, ki poteka v bančnem sektorju, ter večja odvisnost od tehnologij in tretjih ponudnikov storitev pri zagotavljanju bančnih storitev sta prinesli dodatno prepletenost in medsebojne povezave znotraj finančnega sistema, kar bankam po vsem svetu povečuje izzive pri zagotavljanju operativne odpornost. Medtem ko so nadzorovane institucije med pandemijo pokazale visoko stopnjo odpornosti z omejenimi operativnimi izgubami, prinaša geopolitična situacija nove izzive. Nekateri konkretni pomisleki, ki so jih izrazile tudi številne skupne nadzorniške skupine v okviru procesa SREP za leto 2022, so povezani s povečanimi tveganji, ki izhajajo iz zunanjega izvajanja nekaterih dejavnosti ali kritičnih storitev v državah, na katere negativno vplivajo režimi sankcij ali ki se soočajo z večjimi geopolitičnimi tveganji, saj obstaja povečana verjetnost kibernetskih napadov s strani akterjev, ki jih podpirajo države, proti katerim so uveljavljene sankcije.
Banke morajo zlasti obravnavati tveganja, ki izhajajo iz velike odvisnosti od tretjih ponudnikov pri ključnih IT storitvah in pomanjkljivosti v ureditvah IT zunanjega izvajanja, saj bi nerazpoložljivosti ali slaba kakovost storitev lahko povzročile pomembne izgube. Prav tako se morajo proaktivno spopadati s kibernetskimi tveganji, povezanimi z IT varnostjo.
Bančni nadzor v ECB bo v naslednjem obdobju i) zbiral podatke in izvajal horizontalne analize registrov zunanjega izvajanja z namenom prepoznave medsebojnih povezav med pomembnimi institucijami in tretjimi ponudniki ter prepoznave morebitne koncentracije ponudnikov, ii) izvajal ciljno usmerjene preglede dogovorov o zunanjem izvajanju, ukrepov za kibernetsko varnost in nadzora tveganj na področju informacijske tehnologije.
Z namenom preverjanja sposobnosti odziva bank na uspešen kibernetski napad in postopkov okrevanja po njem bo ECB v začetku leta 2024 izvedla tematski stresni test kibernetske odpornosti v sistemsko pomembnih bankah. Rezultati vaje bodo predvideno objavljeni do sredine leta 2024 (ECB, 2023b).

3) Banke morajo obravnavati in prioritetno nasloviti dlje prisotne pomanjkljivosti na področju združevanja podatkov o tveganjih in poročanja o tveganjih

Dostop do pravočasnih in točnih podatkov in poročil ni le prvi pogoj za učinkovito strateško usmerjanje, temveč tudi za obvladovanje tveganja in kvalitetno sprejemanje odločitev. Nadzorniške aktivnosti v zadnjih letih so večkrat opozorile na pomembne pomanjkljivosti na področju združevanja podatkov o tveganju in poročanja o tveganju. Banke so pokazale počasen in nezadosten napredek pri odpravljanju vrzeli v zvezi z nadzorniškimi pričakovanji in skladnostjo z načeli baselskega odbora za bančni nadzor za to področje (BCBS 239). Bančni nadzor v ECB bo zato okrepil svoja prizadevanja in nadzorniške aktivnosti za zagotovitev znatnega napredka nadzorovanih institucij pri odpravljanju ugotovljenih pomanjkljivosti.

SKLEP

V sedanjih gospodarskih in geopolitičnih okoliščinah ter ob povečanem obsegu kibernetskih groženj sta bistvenega pomena preudarnost in pravočasen odziv na hitro spreminjajoče se okolje. Nadzorniške aktivnosti bodo usmerjene v nadzor zagotavljanja robustnega okvira upravljanja IT in kibernetskih tveganj ter upravljanja tveganj zunanjega izvajanja. Prednostne nadzorniške naloge se lahko spremenijo, kolikor bo to potrebno zaradi hitro spreminjajočih se makrofinančnih razmer. Nadzorni organi pa bodo še naprej podrobno obravnavali institucije, pri katerih se kažejo bistvene pomanjkljivosti, in odločno ukrepali, kadar banke teh pomanjkljivosti ne bodo odpravile.

REFERENCE

1. af Jochnick, K. and Quagliariello, M. (2022). Charting the course: our supervisory priorities. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/press/blog/2022/html/ssm.blog221212~52bd154288.en.html [Accessed 21 Aug. 2023].
2. BIS (2013). *Basel Committee on Banking Supervision Principles for effective risk data aggregation and risk reporting*. [online] Available at: https://www.bis.org/publ/bcbs239.pdf.
3. CERT-EU (2023). *THREAT LANDSCAPE REPORT 2023Q2 – MAIN MALICIOUS ACTIVITIES*. [online] https://cert.europa.eu/. Available at: https://cert.europa.eu/static/threat-intelligence/TLP-CLEAR-TLR2023-Q2-ExecSum-1.0.pdf.
4. EBA (2020). *FINAL REPORT ON GUIDELINES ON ICT AND SECURITY RISK MANAGEMENT FINAL REPORT EBA Guidelines on ICT and security risk management FINAL REPORT ON GUIDELINES ON ICT AND SECURITY RISK MANAGEMENT 2 Contents*. [online] Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Guidelines/2020/GLs%20on%20ICT%20and%20security%20risk%20management/872936/Final%20draft%20Guidelines%20on%20ICT%20and%20security%20risk%20management.pdf.
5. EBA (2022). *Asset quality has further improved, but cyber risk remains a source of concern for EU banks*. [online] European Banking Authority. Available at: https://www.eba.europa.eu/asset-quality-has-further-improved-cyber-risk-remains-source-concern-eu-banks [Accessed 18 Aug. 2023].
6. EBA (2023). *RISKS AND VULNERABILITIES IN THE EU FINANCIAL SYSTEM*. [online] Available at: https://www.eba.europa.eu/sites/default/documents/files/document_library/Publications/Reports/2023/1054918/JC%202023%2007%20%28Spring%202023%20Report%20on%20Risks%20and%20Vulnerabilities%29.pdf [Accessed 18 Aug. 2023].
7. ECB (2020a). *Contingency preparedness in the context of COVID-19*. [online] ECB Banking Supervision. Available at: https://www.bankingsupervision.europa.eu/press/letterstobanks/shared/pdf/2020/ssm.2020_letter_on_Contingency_preparedness_in_the_context_of_COVID-19.en.pdf.
8. ECB (2020b). Guarding against IT and cyber risk. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/press/publications/newsletter/2020/html/ssm.nl200513_1.en.html [Accessed 18 Aug. 2023].
9. ECB (2021). ECB Banking Supervision – Supervisory priorities for 2022-2024. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities2022~0f890c6b70.en.html.
10. ECB (2022a). *ECB Annual Report on supervisory activities ECB Annual Report on supervisory activities 2022 -Contents*. [online] Available at: https://www.bankingsupervision.europa.eu/press/publications/annual-report/pdf/ssm.ar2022~e4b57f3b89.en.pdf [Accessed 18 Aug. 2023].
11. ECB (2022b). ECB Banking Supervision: SSM supervisory priorities for 2023-2025. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/banking/priorities/html/ssm.supervisory_priorities202212~3a1e609cf8.en.html#toc1.
12. ECB (2022c). ECB sanctions ABANCA for failing to report cyber incident within deadline. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/press/pr/date/2022/html/ssm.pr221216_1~4742bce1b3.en.html [Accessed 18 Aug. 2023].
13. ECB (2022d). *IT and cyber risk - key observations*. [online] Available at: https://www.bankingsupervision.europa.eu/banking/srep/2022/html/ssm.srep2022_ITandcyberrisk.en.pdf.
14. ECB (2023a). *Financial Stability Review*. [online] ECB. Available at: https://www.ecb.europa.eu/pub/pdf/fsr/ecb.fsr202305~65f8cb74d7.en.pdf.
15. ECB (2023b). Interview with Verslo žinios. *www.bankingsupervision.europa.eu*. [online] Available at: https://www.bankingsupervision.europa.eu/press/interviews/date/2023/html/ssm.in230309~5f39ac5267.en.html [Accessed 21 Aug. 2023].
16. Europa.eu. (2022). *EUR-Lex - 32022R2554 - EN - EUR-Lex*. [online] Available at: https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32022R2554.
17. Panetta, F. (2022). Adapting to the fast-moving cyber threat landscape: no room for complacency. *www.ecb.europa.eu*. [online] Available at: https://www.ecb.europa.eu/press/key/date/2022/html/ecb.sp220601~89cc3f518c.en.html [Accessed 18 Aug. 2023].
18. SI-CERT (2023). *Statistika SI-CERT za prvo polovico leta 2023*. [online] SI CERT. Available at: https://www.cert.si/statistika-si-cert-za-prvo-polovico-leta-2023/ [Accessed 18 Aug. 2023].