Prikazi in analize

Kibernetska varnost bančnega sistema

Avtor: Borut Poljšak

Januar 2024

BANKA SLOVENIJE
EVROSISTEM

Zbirka: Prikazi in analize

Naslov: Kibernetska varnost bančnega sistema

Številka: januar 2024

Leto: 2024

Kraj: Ljubljana

Izdajatelj:
Banka Slovenije
Slovenska 35, 1505 Ljubljana, Slovenija
www.bsi.si

Elektronska izdaja:

https://www.bsi.si/publikacije/raziskave-in-analize/prikazi-in-analize

This publication is also available in English.

Kataložni zapis o publikaciji (CIP) pripravili v Narodni in univerzitetni knjižnici v Ljubljani
COBISS.SI-ID **180451843**
ISBN 978-961-96526-2-6 (PDF)

Kazalo

Povzetek

Z digitalizacijo bančnega sistema se povečuje tudi pomen kibernetske varnosti, zato Banka Slovenije namenja vse več pozornosti identifikaciji in spremljanju kibernetskega tveganja[1] z vidika finančne stabilnosti in makrobonitetne politike. Kibernetski incidenti, ki lahko predstavljajo sistemsko tveganje za finančni sistem, motijo kritične finančne storitve in operacije ter s tem ovirajo opravljanje ključnih gospodarskih funkcij.

Z vidika zagotavljanja finančne stabilnosti je ključno, da kibernetski incident ne vodi do sistemskega dogodka, ki lahko povzroči prekinitev poslovanja finančnih institucij ter posledično finančne izgube in manjše zaupanje javnosti. Zato je pomembno, da tudi centralne banke kot nadzornik bančnega sistema stremijo k povečanju svojih analitičnih sposobnosti glede identifikacije in spremljanja sistemskega kibernetskega tveganja.

Za zagotavljanje finančne stabilnosti je ključna sistemska ublažitev kibernetskega napada. To lahko zagotovimo s pomočjo usmerjene analize sistemskih tveganj, z uporabo in razvojem usmerjenih orodij za analizo sistemskih kibernetskih tveganj, oblikovanjem makrobonitetnih instrumentov za tovrstna tveganja in z ustreznim kriznim upravljanjem.

Ključne besede: kibernetska varnost, odpornost, sistemsko tveganje, kritične finančne storitve, finančna stabilnost, operativno tveganje, makrobonitetna politika

Abstract

As the digitalisation of the banking system increases the importance of cyber security, central banks are paying more and more attention to cyber risk from a financial stability and macro-prudential policy perspective. Cyber incidents, which pose a systemic risk to the financial system, can disrupt critical financial services and operations, thereby impeding the performance of key economic functions.

From the perspective of ensuring financial stability, it is crucial that a cyber incident does not lead to a systemic event that causes disruption to the operations of financial institutions, resulting in financial losses and reduced public confidence. It is therefore important that central banks, as the supervisor of the banking system, also strive to enhance their analytical capabilities with regard to the identification and monitoring of systemic cyber risk.

Systemic mitigation of a cyber-attack is crucial to ensure financial stability. This can be ensured through targeted systemic risk analysis, the use and development of targeted tools to analyse systemic cyber risks, the design of macroprudential instruments for such risks and appropriate crisis management.

Key words: cyber security, resilience, systemic risk, critical financial services, financial stability, operational risk, macroprudential policy

[1] Kibernetsko tveganje lahko opredelimo kot kombinacijo verjetnosti kibernetskih incidentov in njihovega potencialnega vpliva na poslovanje bank, ki se lahko realizira v obliki operativnih prekinitev, finančne škode ali pa prenosa tveganja na ostale sektorje (FSB, 2018).

1 Uvod

Sposobnost napadalcev, da spodkopavajo, motijo in onemogočajo informacijske in komunikacijske tehnološke sisteme, ki jih uporabljajo finančne institucije, predstavlja grožnjo finančni stabilnosti. Napadalci imajo širok dostop do tehnologije, ki jim omogoča čezmejno delovanje ter napade na finančna podjetja in centralne banke z namenom zaslužka ali zgolj operativnih motenj.

Zaradi vse pogostejših napadov, naraščajočih izgub in spoznanja, da lahko pride do resnih motenj v delovanju finančnega sistema, se je kibernetsko tveganje prelevilo v osrednje vprašanje upravljanja tveganj za vse finančne institucije in v tveganje za stabilnost finančnega sistema. Napadalci imajo univerzalen doseg, da ciljajo na velike in majhne institucije, bogate in manj premožne države. Pandemija Covid-19 je le še povečala zavedanje o bistvenem pomenu zaščite digitalnih sistemov in povezljivosti za zagotavljanje neprekinjenega gospodarskega in finančnega delovanja. Kibernetske grožnje so postale bolj zapletene in običajno zajemajo več jurisdikcij, zato jih je težje preiskovati in preganjati.

Pandemija Covid-19, vojna v Ukrajini, širše geopolitično okolje in vse pogostejša uporaba kibernetskih napadov so znatno povečali okolje kibernetskih groženj. Poleg incidentov brez zlonamernega motiva se je povečalo tudi tveganje kibernetskih napadov na finančni sistem, ki jih izvajajo države ali akterji, ki jih sponzorira država. Na podlagi tega nadzorniki vse bolj razmišljajo o različnih pristopih in orodjih za spremljanje sistemskega kibernetskega tveganja. Nadzorniki poleg spremljanja ključnih indikatorjev vse bolj razmišljajo tudi o uporabi kibernetskega kartiranja, ki omogoča pregled medsebojnih operativnih in finančnih povezav različnih subjektov na trgu.

K zagotavljanju višje kibernetske odpornosti bančnega sistema bosta prispevali prihajajoči regulativi, in sicer NIS 2 in DORA. DORA si prizadeva vzpostaviti celovit okvir za digitalno operativno odpornost EU finančnih subjektov. Na drugi strani pa direktiva NIS 2 zagotavlja višjo raven kibernetske varnosti v EU in razširja področje njene uporabe za nove sektorje. Obe regulativi bosta prispevali k višji kibernetski odpornosti finančnega sistema ter zagotovili bolj ustrezen nadzor nad zunanjimi IKT ponudniki storitev. Nenehno razvijajoča se kibernetska tveganja in nedavno povečanje kibernetskih incidentov sta pokazatelja vse večje grožnje finančni stabilnosti v Evropski uniji. To je tudi razlog, da evropske nadzorne institucije posvečajo vse več pozornosti preprečevanju in blažitvi incidentov. Razvijajo instrumente za identifikacijo in spremljanje verjetnosti, da bi kibernetski incident sprožil sistemsko kibernetsko krizo in ogrozil finančno stabilnost.

ESRB-jeva delovna skupina za kibernetsko varnost je v poročilu, ki se nanaša na zmanjšanje sistemskega kibernetskega tveganja (ESRB, 2022a), s ciljem preprečiti neuspešno usklajevanje pri reševanju sistemskih kibernetskih dogodkov priporočila vzpostavitev vseevropskega sistemskega okvira za usklajevanje kibernetskih incidentov (v nadaljevanju EU-SCICF). EU-SCICF se bo aktiviral le med sistemskimi krizami ter bo namenjen reševanju izrednih dogodkov na mednarodni ravni (ESRB, 2022b).

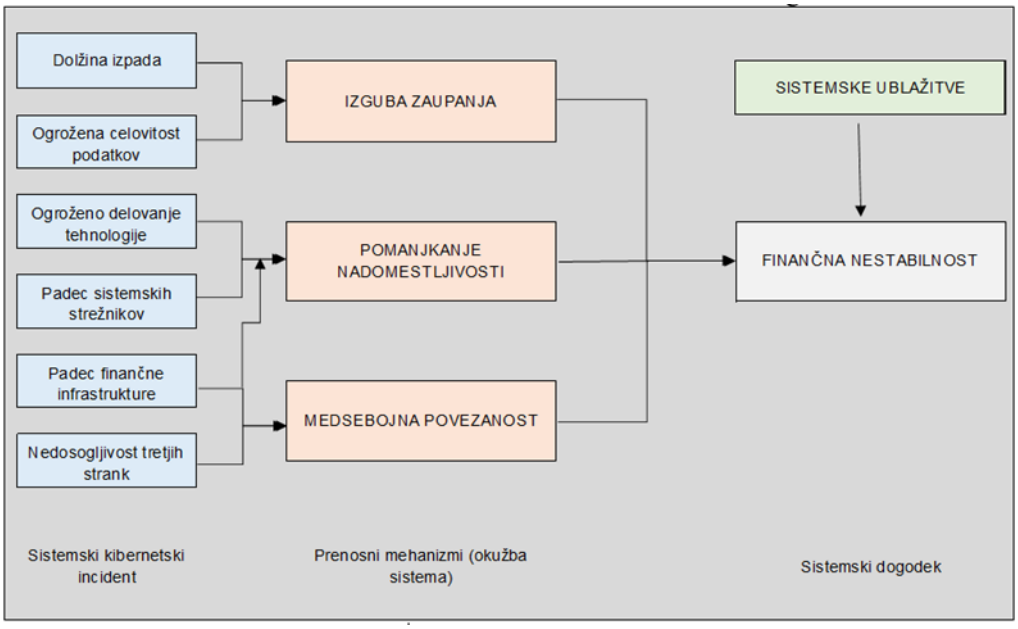
2 Kibernetsko tveganje in vpliv na finančno stabilnost

V zadnjih letih se zaradi vse večje digitalizacije in globalizacije poslovanja povečuje število kibernetskih incidentov in napadov na finančni sistem. Kibernetska varnost postaja vse bolj ključna za zagotavljanje finančne stabilnosti. Kibernetski napadi na sisteme informacijske in komunikacijske tehnologije naraščajo po vsem svetu, pri čemer je panoga finančnih storitev med bolj izpostavljenimi. Z vidika zagotavljanja finančne stabilnosti je ključno, da kibernetski incident ne vodi do sistemskega dogodka, ki lahko povzroči dolgotrajne prekinitve poslovanja finančnih institucij ter posledično finančne izgube in manjše zaupanje javnosti (ESRB, 2020a).

Kibernetsko tveganje lahko vpliva na finančno stabilnost na naslednje načine (ESRB, 2023):

- Dolgotrajni izpadi informacijskega sistema in ogroženost celovitosti podatkov vodijo do izgube zaupanja. Če kibernetski napad za dlje časa ohromi ključne operacije poslovanja, kar lahko na primer pomeni izgubo dostopa do finančnih sredstev in možnosti poravnave obveznosti, lahko stranke in tržni udeleženci izgubijo zaupanje v finančni sistem.
- V primeru incidenta, ki ima sistemske razsežnosti lahko pride do nedelovanja informacijskega sistema posamezne sistemsko pomembne institucije (npr. padec sistemskih strežnikov), kar prav tako vpliva na finančno stabilnost.
- Medsebojna povezanost znotraj finančnega sistema in tudi med različnimi tehnologijami lahko povečuje iz kibernetskih napadov izvirajoče sistemsko tveganje za finančno stabilnost. Pri tehnološki medsebojni povezanosti so problematični predvsem ponudniki tehnoloških storitev (npr. storitve v oblaku), ki lahko ob kibernetskih napadih pospešijo prenos okužbe finančnega sistema.

Slika 1: **Kibernetska varnost in finančna stabilnost finančnega sistema**



Vir: MDS (IMF, 2020) in Banka Slovenije (2021a)

Kibernetski incidenti lahko zaustavijo delovanje kritičnih finančnih storitev in poslovanje ter s tem ovirajo izvajanje ključnih gospodarskih funkcij. Če je poslovanje in izvajanje kritičnih funkcij dlje časa prekinjeno lahko to vodi v finančne izgube in padec zaupanja javnosti. Zavedamo se tudi, da bi kibernetski incident lahko privedel do sistemskega dogodka in ogrozil finančno stabilnost (ESRB, 2020b).

Za zagotavljanje finančne stabilnosti je ključna sistemska ublažitev kibernetskega napada. To lahko zagotovimo s pomočjo usmerjene analize sistemskih tveganj, z uporabo in razvojem usmerjenih orodij za analizo sistemskih kibernetskih tveganj, oblikovanjem makrobonitetnih instrumentov za tovrstna tveganja in z ustreznim kriznim upravljanjem. Ključno pri kibernetski odpornosti[2] je, da finančne institucije in nadzorniki krepijo svojo odzivno funkcijo (sposobnost za ukrepanje po zaznanem kibernetskem incidentu) in tudi obnovitveno funkcijo (obnova okvarjenih sistemov in storitev). Pomembno je tudi, da finančni sistem povečuje svojo kibernetsko odpornost z rednim testiranjem varnosti poslovnih procesov in uporabo orodij za identifikacijo sistemskih groženj ter vpliva kibernetskih incidentov na poslovanje finančnih institucij.

Iz slike 1 je razvidno, na kakšen način lahko kibernetski incidenti vplivajo na finančno infrastrukturo institucij ter kakšni prenosni mehanizmi lahko privedejo do finančne nestabilnosti. Do takih dogodkov lahko pride kadarkoli in kjerkoli, zato je pomembno, da smo na to pripravljeni z vidika, da razpolagamo z orodji, ki omogočajo pravočasno identificiranje in spremljanje kibernetskega tveganja v sistemu. Za zagotavljanje finančne stabilnosti je ključna sistemska ublažitev kibernetskega napada.

Kibernetski napad vpliva na finančno stabilnost na treh ravneh, in sicer na: operativni, finančni, na koncu vpliva tudi na zaupanje v finančni sektor. O operativni okužbi govorimo takrat, ko kibernetski napad povzroči prekinitev več ključnih ekonomskih funkcij, ki jih zagotavlja več finančnih institucij na trgu. Prekinitve ključnih ekonomskih funkcij vplivajo tudi na ostale finančne institucije in gospodarske družbe, kar povzroči grožnjo za zagotavljanje finančne stabilnost (Bank of England, 2021). Cilj kibernetskih napadov je v prvi vrsti onemogočiti delovanje ključnih ekonomskih funkcij ter posledično operativno delovanje finančnega sistema in širšega gospodarstva. Za ustrezno blažitev operativnih prekinitev poslovanja obstajajo določena operativna orodja, in sicer: orodja za izmenjavo informacij, krizno upravljanje in usklajevanje pri reševanju kibernetskih dogodkov ter rezervni sistemi. Operativna orodja zagotavljajo, da so finančne institucije pripravljene na operativne prekinitve na način, da imajo zagotovljeno ustrezne mehanizme za izmenjavo informacij za hitrejše reševanje izrednih dogodkov ter da imajo zagotovljene rezervne sisteme, ki omogočajo hitro povrnitev v prvotno stanje poslovanja. V primeru večjega kibernetskega incidenta je treba zgodaj prepoznati posledice za finančno stabilnost, da se omogoči pravočasna aktivacija sistemskih blažilnikov kibernetskega tveganja, ki preprečijo ali zmanjšajo stopnjo okrepitve finančne okužbe, ki je lahko posledica kibernetskega incidenta. Okužbe v finančnem sistemu so posledica kibernetskih napadov, ki lahko vplivajo na prekinitve poslovanja in finančne izgube. Če so prekinitve poslovanja ter finančne izgube visoke potem, lahko pride do sistemskega kibernetskega dogodka, ki vpliva na zaupanje v finančni sistem (Bank of England, 2022a).

[2] Kibernetska odpornost je sposobnost banke ali druge finančne institucije, da uresničuje poslanstvo s predvidevanjem in obvladovanjem kibernetskih tveganj ter hitrim okrevanjem po kibernetskih incidentih.

3 Različni pristopi in orodja za spremljanje sistemskega kibernetskega tveganja

Za zagotavljanje finančne stabilnosti in izvajanje makrobonitetne politike je pomembna določitev ustreznih orodij in pristopov, ki se lahko uporabljajo za spremljanje kibernetske odpornosti finančnega sistema. Orodja za identifikacijo kibernetskih sistemskih tveganj so še v razvojni fazi in se prilagajajo nadzorniškim spremembam. Za zagotavljanje finančne stabilnosti je ključna tudi izmenjava informacij na področju kibernetske varnosti. Izmenjavo informacij lahko razdelimo na tri dele: obveščanje o grožnjah (vključuje analitiko tveganja, kazalnike in oceno nevarnosti), poročanje o incidentih (ocena finančne institucije, kako obvladuje situacijo) in obrambne tehnike (informacije o tem, kako je bil napad preprečen ali omejen).

Ker so kibernetski napadi globalni pojav in predstavljajo izzive za pregon, zlasti na mednarodni ravni, so ključna tudi načela kriznega upravljanja, ki poleg komunikacije zajemajo tudi koordinacijo aktivnosti ter predloge, kako se morajo finančne institucije in njihovi nadzorniki odzvati v primerih kibernetskih napadov. Centralne banke vse bolj razmišljajo o širši uporabi različnih orodij, ki omogočajo, da se finančni sistem čim bolj ustrezno pripravi (s pomočjo različnih scenarijev) na kibernetske napade in ustrezno blaži njihove posledice. Pri spremljanju sistemskega kibernetskega tveganja se vse več pozornosti namenja opredelitvi orodij za blaženje posledic, ki jih lahko povzročijo kibernetski napadi. Orodja za spremljanje sistemskega kibernetskega tveganja so sledeča:

- Prikaz tveganj, poročila in ostale ad hoc analize (del poslovnega obveščanja).
- Kibernetsko kartiranje je namenjeno prikazu ključnih finančnih in tehnoloških povezav med finančnimi institucijami, podjetji ter neodvisnimi ponudniki tehnologij in storitev. Orodje je namenjeno tako mikrobonitetnim kot tudi makrobonitetnim organom.
- Kibernetski stresni testi pomagajo organom razumeti, ali ima finančni sistem dovolj operativnih zmogljivosti, da se odzove in si opomore od hudega, a verjetnega kibernetskega napada.

3.1 Ključni indikatorji na področju spremljanja kibernetskega tveganja z vidika finančne stabilnosti in makrobonitetne politike

Na področju spremljanja kibernetskega tveganja je ključno, da nadzorniki razpolagajo z ustreznimi podatki in indikatorji. Sistemsko kibernetsko tveganje lahko opredelimo kot kombinacijo verjetnosti kibernetskih incidentov in njihovega potencialnega vpliva na poslovanje bank (ki se lahko realizira v obliki operativnih prekinitev, finančne škode ali okužbe na ostale sektorje). Ključni sprožilec sistemskega kibernetskega dogodka je kibernetski incident, ki lahko ogrozi kibernetsko varnost informacijskega sistema in krši varnostno politiko finančne institucije. Zato je za obvladovanje kibernetskih tveganj ključna kibernetska odpornost. V pristojnosti makrobonitetne politike je spremljanje in blaženje sistemskih kibernetskih dogodkov, ki lahko ogrožajo finančno stabilnost sistema.

Kibernetsko sistemsko tveganje lahko opredelimo kot podkategorijo operativnega tveganja. Zato je treba tudi pri umestitvi indikatorjev slediti vmesnim ciljem, ki se nanašajo

na omejitev sistemskega vpliva izkrivljajočih spodbud[3] in krepitev odpornosti finančnih infrastruktur. Kibernetski indikator meri posledice zlonamernih aktivnosti, ki jih povzročijo notranji ali pa zunanji akterji. Vse te zlonamerne aktivnosti vplivajo na poslovanje finančnih institucij. Medtem ko pa operativni indikatorji merijo operativne prekinitve, ki običajno niso nastale zaradi zlonamernih aktivnosti, ampak nepričakovanega nedelovanja informacijskega sistema finančne institucije. Področje kibernetskega tveganja lahko spremljamo s pomočjo dveh vrst indikatorjev: operativnih in finančnih. Obe vrsti indikatorjev zagotavljajo ustrezne informacije o finančnih in kibernetskih ranljivostih. V primeru večjega kibernetskega incidenta je treba že zgodaj prepoznati posledice za finančno stabilnost, da se omogoči pravočasno aktiviranje sistemskih sredstev za zmanjševanje kibernetskega tveganja, ki preprečujejo ali zmanjšajo stopnjo povečanja finančne okužbe, ki izhaja iz kibernetskega incidenta.

Tabela 1: **Klasifikacija kibernetskih indikatorjev glede na vmesne cilje makrobonitetne politike in metode za analizo indikatorjev**

Vmesni cilj makrobonitetne politike	Kibernetski indikatorji	Metode za analizo indikatorjev
Ublažitev in preprečitev čezmerne rasti kreditiranja in čezmernega finančnega vzvoda	Finančni položaj institucij v različnih kibernetskih scenarijih.	Finančni stresni testi s scenariji kibernetskega tveganja.
Ublažitev in preprečitev čezmernega neskladja v ročnosti strukturi in nelikvidnosti trga	Finančni položaj institucij v različnih kibernetskih scenarijih; izhaja iz stresnega testiranja likvidnosti s kibernetskim scenarijem.	Likvidnostni stresni testi s scenariji kibernetskega tveganja.
Omejiti koncentracijo neposredne in posredne izpostavljenosti	Indikatorji za večje operativne izpostavljenosti	Kibernetsko kartiranje za prepoznavanje tveganj koncentracije in kanalov okužbe.
	Operativna medsebojna povezanost	
	Operativna okužba	
	Medsebojne povezave s sistemskimi vozlišči	
Omejitev sistemskega vpliva izkrivljajočih spodbud in manjši moralni hazard	Identifikacija sistemskih vozlišč po velikosti, kompleksnosti, zamenljivosti in medsebojni povezanosti institucij in tretjih ponudnikov IKT .	Kibernetsko kartiranje za identifikacijo sistemsko pomembnih vozlišč.
	Pri tretjih ponudnikih IKT lahko uvrščamo naslednje indikatorje: tržna koncentracija zunanjih ponudnikov storitev IT (v %), povprečno število ponudnikov storitev v oblaku in številom zunanjih ponudnikov storitev IT.	
	Sodelovanje pri dogovorih o izmenjavi informacij (40. člen DORA).	

[3] Tveganja izkrivljajočih spodbud so praviloma strukturne narave, kar pomeni, da se ne spreminjajo v odvisnosti od faze finančnega cikala, ampak so v večji meri odvisna od strukture finančnega sistema ter so običajno povezana s sistemsko pomembnimi finančnimi institucijami.

Krepitev odpornosti finančnih institucij	Uporaba različnih scenarijev za primere operativnih prekinitev zaradi kibernetskih incidentov.	Kibernetsko stresno testiranje.
		Razvoj posameznih indikatorjev in pragov
	(Podatki) Časovni odziv	
	Sposobnost zagotavljanja celovitosti podatkov po kibernetski nesreči	
	Nadaljnji količinski indikatorji: število naprav z zastarelo programsko opremo, število kibernetskih incidentov, ocena finančne škode (v tisoč evrih) in povprečni odzivni čas za obvladovanje tveganja (v minutah).	

Vir: Banka Slovenije

Z vidika makrobonitetne politike lahko kibernetski incident poslabša likvidnost trga in vodi do tveganja financiranja. Kibernetski incident lahko privede do neposredne izgube ali izgube dostopa do sredstev, kar vpliva na sposobnost institucije za financiranje svojega delovanja. Motnje, ki jih povzroči kibernetski incident so: kraje likvidnosti/sredstev, nepreklicni izbris ali poškodovanje zapisov na tržni infrastrukturi, motnje delovanja infrastrukture. Prekinitve poslovanja bi lahko vplivale na pomanjkanje likvidnosti za druge finančne institucije (možnost prenosa prekinitve poslovanje iz napadene institucije na ostale institucije v finančnem sistemu). Kibernetski incident lahko vpliva tudi na izgubo zaupanja v finančne institucije ali celotne tržne segmente. Učinki okužbe bi lahko bili sorazmerni s sistemsko pomembnostjo prizadetih subjektov, zlasti v primeru kritične finančne infrastrukture, ki služi pretoku likvidnosti.

V primeru sistemskega kibernetskega tveganja se okužba ne pojavlja le na finančni, temveč tudi na operativni ravni. Kibernetski incidenti vplivajo tako na neposredno izpostavljenost (poslovni odnosi med različnimi finančnimi institucijami) kot tudi posredno (medsebojna povezanost različnih informacijskih sistemov ali skupnih ponudnikov storitev in operativnih sistemov). Poleg tega je kibernetsko tveganje lahko tudi vir kreditnega tveganja, povezanega z izpostavljenostmi do nefinančnih družb, katerih sposobnost izpolnjevanja kreditnih obveznosti je lahko močno odvisna od njihovih lastnih operacijskih sistemov IKT.

V ESRB poročilu o sistemskem kibernetskem tveganju je navedeno, da finančne institucije kibernetski varnosti ne namenjajo zadostnih sredstev in namesto tega raje razporedijo sredstva na bolj »vidna« področja (tj. osredotočanje na dobiček in rast). Drug primer neusklajenih spodbud je, da finančne institucije ne želijo izmenjati informacij o kibernetskih incidentih zaradi strahu pred izgubo ugleda in konkurenčnosti na trgu. Reševanje, povezano s kibernetskim tveganjem, se lahko izvede z operativnimi ukrepi, na primer s povečano ali pravočasno dodelitvijo omejenih sredstev za reševanje incidentov (ESRB. 2020a).

Odpornost finančnih institucij na kibernetske incidente je ključna za zagotavljanje finančne stabilnosti. Za zagotavljanje odpornosti je potreben ustrezen nadzor nad zunanjimi IKT ponudniki storitev. Spremljati je treba tudi tržno koncentracijo IKT ponudnikov na trgu (tudi oblačnih). Opredelitev »odpornosti« je treba prilagoditi kibernetskemu kontekstu, ki se nanaša predvsem na hitro okrevanje po kibernetskih incidentih. Pri krepitvi

odpornosti finančnih institucij je ključna tudi ustrezna zaščita zaupnosti, celovitosti in razpoložljivosti informacij (podatkov), ki jo lahko kibernetski incidenti ogrožajo.

3.2 Kibernetsko kartiranje

Kibernetsko kartiranje (kvalitativno orodje) vključuje ključne tehnologije, storitve, zunanje ponudnike storitev in njihove povezave z institucijami finančnega sektorja. Na konceptualni ravni je namen kartiranja poudariti ključne finančne in tehnološke povezave med finančnimi institucijami, podjetji ter neodvisnimi ponudniki tehnologij in storitev. S kibernetskim kartiranjem dobimo pregled nad finančnimi institucijami in povezavami med finančnimi institucijami ter drugimi kritičnimi objekti. Te informacije se lahko uporabijo za nadzor in analizo kibernetskih tveganj za finančno stabilnost. Slabost kibernetskega kartiranja se kaže v tem, da bolj kot je podrobno, bolj je drago in časovno zahteven.

Kibernetsko kartiranje omogoča identifikacijo sistemskih vozlišč v sistemu s spremljanjem in analizo ključnih tehnologij, storitev in povezav med institucijami finančnega sektorja, ponudniki storitev in sistemi tretjih oseb. Orodje je namenjeno tako mikrobonitetnemu kot tudi makrobonitetnemu nadzoru finančnega sistema. Kibernetsko kartiranje prinaša dodano vrednost na naslednji način:

- osredotočanje nadzorniških aktivnosti na ključne točke finančnega sistema,
- izboljša preglednost in operativno odpornost finančnega sistema,
- omogoča zaščito kritične infrastrukture na nacionalni ravni in
- zagotavlja lažje upravljanje sistemskih kibernetskih tveganj.

Tabela 2: **Terminologija kibernetskega kartiranja (določitev vozlišč)**

Terminologija	Opis
Subjekti finančnih storitev	Centralne banke, banke, zavarovalnice, investicijski skladi, borznoposredniške hiše
Subjekti finančne infrastrukture	Upravljavci plačilnih sistemov, borze, depozitarji, ponudniki informacijskih storitev
Finančni sektor	Vse od naštetega (subjekti finančnih storitev in infrastrukture)
Subjekti IKT	Prodajalci strojne in programske opreme, ponudniki storitev v oblaku, ponudniku telekomunikacijskih storitev, ponudniki storitev IT
Komponente IKT	Strojna in programska oprema, omrežja, podatkovni centri

Vir: Banka Slovenije

Pri definiranju ključnih vozlišč je pomembna tudi definicija zemljevidnih slojev, ki so definirani na naslednji način: podatkovni tok, organizacijska in tehnološka odvisnost, ki tvorijo mrežo povezav ter vozlišč med finančnim in tehnološkim sektorjem (za bolj podrobne informacije glej sliko 3). Mreže povezav med finančnim in tehnološkim sektorjem je treba tudi ustrezno utežiti na podlagi tržnega deleža in sintetičnih matrik, saj s tem dobimo bolj realno sliko tveganja v finančnem sektorju.

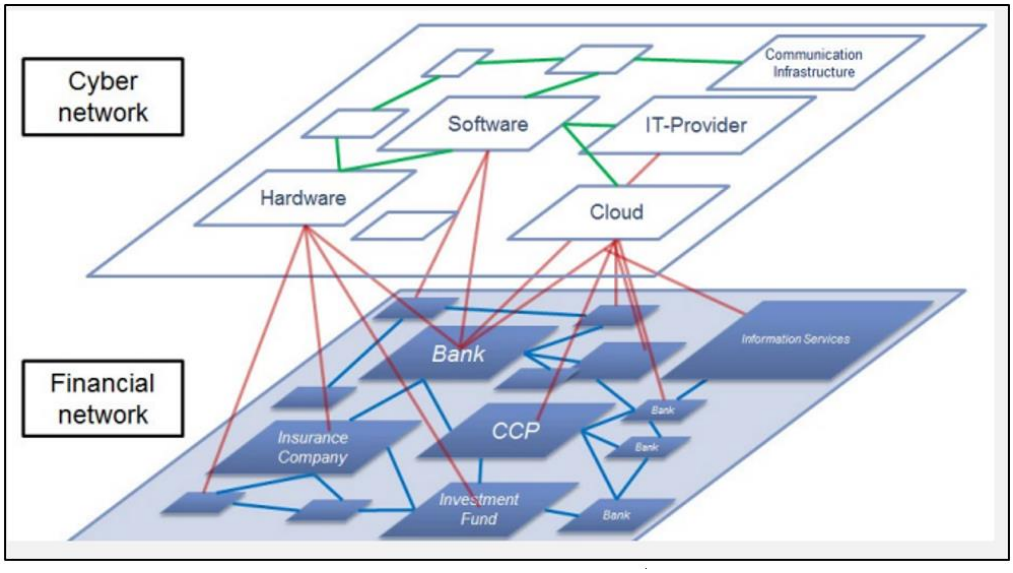
Tabela 3: **Subjekti na zemljevidu**

Nivo	Prikaz subjektov	Opomba
Tok podatkov	Subjekti finančnega nadzora	Osredotočenost na tehnične povezave
	Finančna infrastruktura	
Organizacijska odvisnost	Subjekti finančnih storitev	V finančnem sektorju
	Finančna infrastruktura	Finančni sektor – IKT
	Subjekti IKT	IKT - IKT
Tehnološka odvisnost	Subjekti finančnih storitev	Vpliv organizacijske odvisnosti
	Finančna infrastruktura	
	Subjekti IKT	
	Strojna oprema	
	Programska oprema	
	Omrežje	

Vir: Banka Slovenije

Kibernetsko kartiranje lahko temelji na funkcionalnem ali institucionalnem pristopu. Institucionalni pristop zajema dve omrežji, in sicer: kibernetsko in finančno omrežje. Kibernetsko omrežje je mogoče obravnavati kot virtualno plast finančnega omrežja, ki jo sestavljajo vse komponente IKT,[4] ki jih finančne institucije uporabljajo za svoje poslovanje. S kartiranjem finančnega omrežja (tj. finančnega sistema) na kibernetsko omrežje lahko ugotovimo povezave med ponudniki IKT tretjih oseb, ki jih uporabljajo finančne institucije. Ta pristop omogoča razkritje skupnih ponudnikov IKT (npr. ponudnikov storitev v oblaku) v finančnem sektorju. Te informacije omogočajo nadzornikom finančnega sektorja pregled nad koncentracijo tveganja v kibernetskem omrežju kot tudi kanale prenosa kibernetskega tveganja v finančni sistem.

Slika 2: **Shema kibernetskega zemljevida, ki temelji na institucionalnem pristopu**



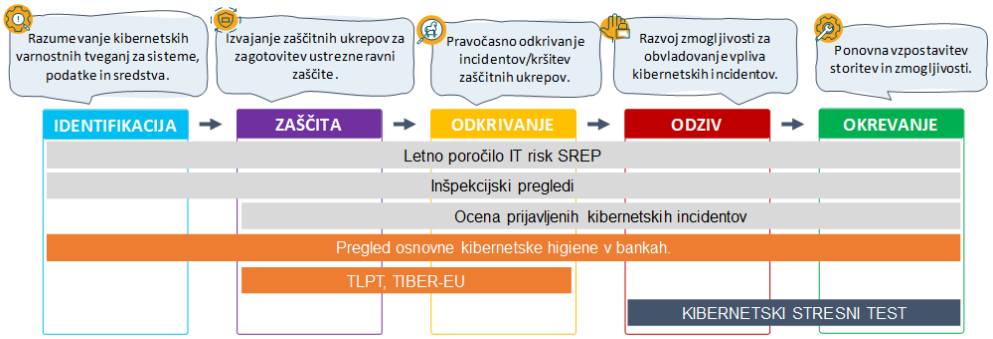
Vir: ESRB (ESRB, 2022a)

[4] Kratica IKT je oznaka za informacijsko in komunikacijsko tehnologijo, ki zajema vse naprave ali sisteme, ki omogočajo shranjevanje, priklic, obdelavo, prenos in sprejemanje informacij, torej ne le računalnike, ampak tudi radio, televizijo, telefone itd. Združuje naprave in programsko opremo, ki jo na teh napravah uporabljamo.

3.3 Kibernetski stresni testi

Kibernetski stresni testi so nadzorniško orodje za preizkušanje zmogljivosti finančnega sistema za podporo neprekinjenosti ključnih gospodarskih funkcij s pravočasnim in učinkovitim odzivom in okrevanjem po hudem, vendar verjetnem kibernetskem scenariju, ki povzroči znatne motnje ter bi lahko vplival na finančno in operativno stabilnost (Bank of England, 2022b). Nadzorniki lahko z izvajanjem kibernetskih stresnih testov prepoznajo morebitne kibernetske ranljivosti, ki bi lahko povzročile tveganja za finančno in operativno stabilnost, ter ocenili potrebo po ukrepanju na ravni podjetja in celotnega sistema. Še pomembneje pa je, da kibernetski stresni testi dopolnjujejo in podpirajo nadzornike pri delu, ki ga bodo opravili za izvajanje nadzornih zahtev, kot je DORA. Dodana vrednost kibernetskih stresnih testov je, da lahko nadzorniki na podlagi rezultatov opredelijo morebitne ukrepe na nivoju finančnega sistema za zagotavljanje kibernetske odpornosti. Kibernetski stresni testi običajno vključujejo finančne institucije, finančno infrastrukturo, podjetja, ki podpirajo delovanje finančnega sistema vključno z IKT ponudniki storitev.

Slika 3: **Načrt za zagotovitev popolne pokritosti cikla kibernetske varnosti**



Vir: ECB (2018)

Kibernetski stresni testi se kot običajno izvedejo v štirih korak, in sicer:

- Oblikovanje kibernetskega scenarija → običajno je scenarij sestavljen iz več faz, znotraj katerih je opisano postopno širjenje informacij o kibernetskem napadu. Scenarij mora biti standardiziran, saj je le tako lahko relevanten za vse udeležence testiranja, ne glede na vrsto IKT infrastrukture. V scenarij so lahko vključeni tudi zunanji IKT ponudniki, ki za finančne institucije nudijo svoje storitve na področju informacijskega sistema.

- Izvedba kibernetskega scenarija → Udeleženci testiranja se preko kibernetskega scenarija soočijo s kibernetskim napadom. Za pravilno izvedbo testiranja morajo zavezanci najprej ugotoviti, kateri poslovni procesi in funkcije so ogrožene ter v kolikšni meri. V ta namen naj izvedejo teste neprekinjenega poslovanja (ang. continuity tests on the basis of the scenario). Dobljene rezultate testiranja poročajo nadzorniku.

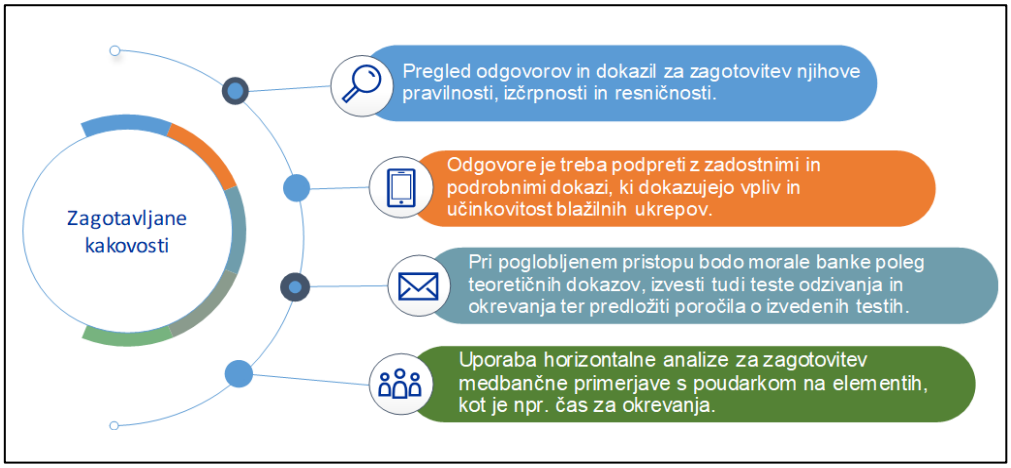
- Poročanje o odzivu na kibernetski scenarij → za zagotovitev skladnosti poročanja med bankami mora nadzornik pripraviti enoten vprašalnik. Vprašalnik od udeležencev testiranja običajno zahteva informacije, ki se nanašajo na:
  - opis vseh korakov za ohranitev delovanja poslovnih procesov in ponovno vzpostavitev normalnega delovanja,
  - razloge za uveljavitev posameznih korakov,
  - časovni okvir za vzpostavitev potrebnih ukrepov,
  - navedbo udeleženih subjektov v procesu testiranja,

- podatke, ki izhajajo iz testiranja, za boljše razumevanje vpliva kibernetskega scenarija in učinkovitosti sprejetih ukrepov (npr. čas izpada, čas izvajanja posameznih korakov, čas izvajanja korakov za vzpostavitev normalnega delovanja).

- Ocena nadzornikov → Nadzorniki imajo v procesu kibernetskega stresnega testiranja pomembno vlogo, saj so odgovorni za ocenjevanje odpornosti finančnega sistema na kibernetske napade. Njihova ocena temelji na rezultatih kibernetskega stresnega testa in oddanih vprašalnikih s strani finančnih institucij. Nadzorniki na podlagi zbranih informacij ocenijo operativno zmogljivost posamezne institucije za obvladovanje kibernetskega scenarija. Za vsakega udeleženca testiranja pripravijo ugotovitve in nadzorniška priporočila v zvezi z ugotovljenimi ranljivostmi okvira kibernetskega odzivanja in okrevanja (npr. pomanjkanje varnostnih kopij, ki zajemajo kritične podatke, čas okrevanja, ki presega cilje okrevanja, pomanjkljivi načrti neprekinjenega poslovanja ali zmogljivost testiranja - tudi pri zunanjih izvajalcih). Na podlagi ocene lahko nadzorniki od udeležencev testiranja zahtevajo, da sprejmejo določene ukrepe za izboljšanje svoje kibernetske odpornosti. Rezultate lahko kasneje tudi uporabijo pri svojih nadzorniških dejavnostih.

Kibernetski stresni test je v primerjavi z običajnimi stresnimi testi kvalitativne narave (opisen). Tukaj ne obstaja kvantitativni model od zgoraj navzdol, ki bi omogočal preverjanje odgovorov, ki jih posredujejo udeleženci testiranja. Postopek zagotavljanja kakovosti temelji na oceni dokazil, ki jih morajo finančne institucije predložiti. Načini za zagotavljanje kakovostne izvedbe kibernetskega stresnega testa so prikazani na sliki 4.

Slika 4: **Zagotavljanje kakovosti kibernetskega stresnega testa**



Vir: ECB (2018) in Banka Slovenije

4 Kibernetska odpornost bančnega sistema

Z digitalizacijo bančnega sistema se povečuje tudi pomen kibernetske varnosti (Banka Slovenije, 2019), zato je Banka Slovenije v zadnjih letih (2019, 2021 in 2023) med slovenskimi bankami izvedla več anket s področja kibernetske varnosti. Z anketami merimo kibernetsko odpornost bančnega sistema. Slovenske banke izpostavljajo, da so v zadnjih letih namenile dodatna sredstva za zagotavljanje kibernetske varnosti bančnih informacijskih sistemov. Banke se kljub temu še vedno srečujejo s težavami glede pomanjkanja nadzora nad zunanjimi izvajalci in dobavitelji, zastarelostjo informacijskih sistemov in kibernetske higiene, vendar manj kot v preteklih letih (Banka Slovenije, 2023b).

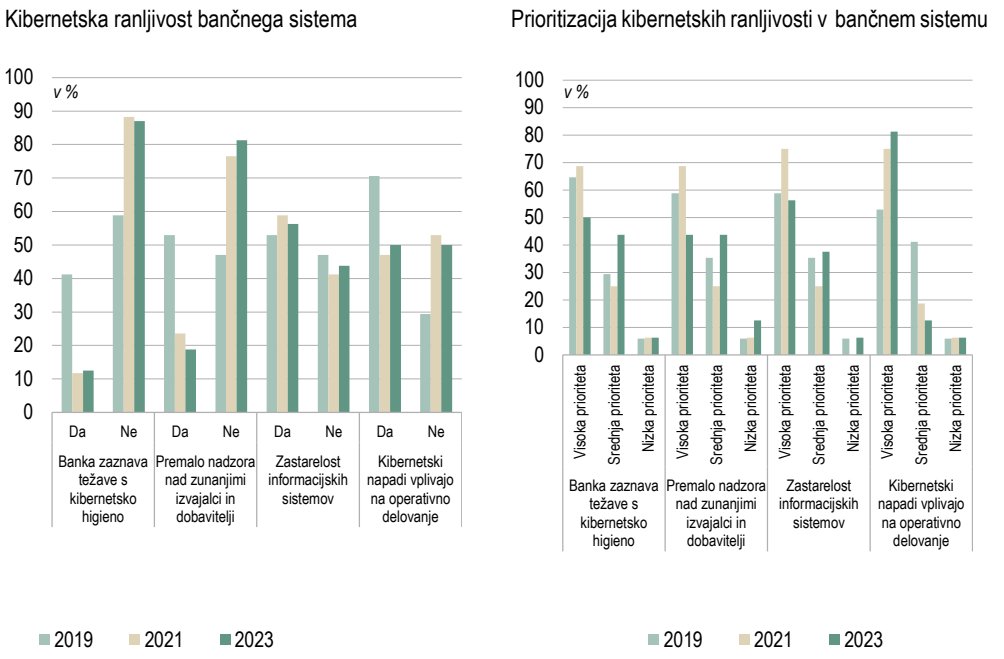
Globalni trend gre v smer najemanja informacijskih rešitev ter podpore zanje pri zunanjih izvajalcih in dobaviteljih, s čimer se lahko povečuje njihova izpostavljenost kibernetskim napadom in incidentom. Banke nadzor nad zunanjimi izvajalci izvajajo na podlagi sprejete politike uporabe zunanjih izvajalcev, ki sledi zahtevam EBA smernic o zunanjem izvajanju[5], kar pripomore k izboljšanju odpornosti bančnega sistema. Za kritične zunanje izvajalce banke naročajo neodvisne revizijske preglede, kar pripomore k izboljšanju odpornosti bančnega sistema. Banke imajo sicer v pogodbah opredeljene klavzule, ki zunanje izvajalce zavezujejo k uvedbi in izvajanju organizacijskih ter tehničnih varnostnih ukrepov za zagotavljanje varovanja informacij. Bančni sistem se še zmeraj sooča z zastarelostjo informacijskih sistemov, kar predstavlja določena tveganja za lažje kibernetske vdore (Banka Slovenije, 2020). Banke poročajo, da intenzivno nadgrajujejo in posodabljajo informacijske sisteme, tudi s ciljem boljše zaščite pred napadi.

Banke poročajo, da občasno identificirajo težave s kibernetsko higieno[6] zaposlenih, ki se kaže v različnih manjših deviacijah od varnostne politike banke. Za obvladovanje tega tveganja se poleg različne programske opreme uporablja tudi redno usposabljanje zaposlenih. Če primerjamo rezultate kibernetske ranljivosti bančnega sistema z letom 2019, se je kibernetska odpornost bančnega sistema izboljšala. V anketi smo poskušali izvedeti tudi, kako se banke lotevajo kibernetskih ranljivosti glede na prednostne naloge, in ocenili, da resno obravnavajo ranljivosti, ki smo jih identificirali z uporabo rezultatov ankete. Kibernetska odpornost bančnega sistema se je od leta 2019 izboljšala, kar kaže, da je bančni sistem na kibernetske napade dobro pripravljen in je zmožen blažiti njihove posledice, če do njih pride (slika 5).

[5] EBA smernice o zunanjem izvajanju IKT ponudnikov so dostopne na naslednjem naslovu: EBA BS 2019 04 (Final draft Guidelines on ICT and security risk management).docx (europa.eu).

[6] Kibernetska higiena je sklicevanje na prakse in korake, ki jih uporabniki računalnikov in drugih naprav sprejmejo, da ohranijo zdravje sistema in izboljšajo spletno varnost.

Slika 5: **Kibernetska ranljivost bank**



Vir:: Banka Slovenije.

Večina bank je med pandemijo povečala sredstva za kibernetsko varnost na naslednji način: (i) uvedba dodatne zaščite pred kibernetskimi napadi (kot so na primer napadi DDoS), (ii) uporaba novih finančnih tehnologij za zaznavanje potencialnih varnostnih dogodkov in napadov ter (iii) projektni načrti za dvig ravni kibernetske varnosti. Vse več je tudi kibernetskih napadov, v katerih napadalci intenzivno uporabljajo umetno inteligenco, s pomočjo katere lahko preko spletne registracije ustvarijo račune namišljenih oseb. V zadnjih letih se je močno povečalo število lažnih SMS sporočil, v katerih se prevaranti izdajajo za banke. Prevaranti želijo prejemnike sporočila s klikom na priloženo spletno povezavo preusmeriti na lažno spletno stran banke, na kateri od njih zahtevajo vnos zaupnih osebnih podatkov. Gre za spletne goljufije, s katerimi želijo komitente slovenskih bank prepričati, da jim posredujejo dovolj podatkov, da se lahko v njihovem imenu namesti aplikacija, ki omogoča potrjevanje teh transakcij in izvedbo phishing napadov. Tako pridobljene podatke zlorabijo za izvrševanje nepooblaščenih plačilnih transakcij, ki bremenijo njihov osebni bančni račun. Število kibernetskih napadov in incidentov na bančne informacijske sisteme se zaradi geopolitičnega tveganja (vojne v Ukrajini) v zadnjem letu ni povečalo. Kljub temu pa ostajajo kibernetske grožnje še zmeraj na visoki ravni, zato je spremljanje sistemskega kibernetskega tveanja ključno.

5 Pravna ureditev področja kibernetske varnosti

K zagotavljanju višje kibernetske odpornosti bančnega sistema bosta prispevali prihajajoča pravna akta, in sicer NIS 2[7] in DORA.[8] DORA si prizadeva vzpostaviti celovit okvir za digitalno operativno odpornost EU finančnih subjektov. Na drugi strani pa direktiva NIS 2 zagotavlja višjo raven kibernetske varnosti v EU in razširja področje njene uporabe za nove sektorje. Po novem med ključne izvajalce storitev spadajo tudi kreditne institucije, ki jih nadzoruje Banka Slovenije. Z novimi direktivami se izboljšuje nadzor nad subjekti finančnega sektorja, ponudniki tehnologij in tehnološkimi rešitvami, kar posledično prispeva k dvigu kibernetske odpornosti bančnega sektorja.

Nenehno razvijajoča se kibernetska tveganja in nedavno povečanje kibernetskih incidentov sta pokazatelja vse večje grožnje finančni stabilnosti v Evropski uniji. To je tudi razlog, da evropske nadzorne institucije posvečajo vse več pozornosti preprečevanju incidentov. Razvijajo instrumente za zmanjšanje verjetnosti, da bi kibernetski incident sprožil sistemsko kibernetsko krizo in ogrozil finančno stabilnost. ESRB-jeva delovna skupina za kibernetsko varnost je v poročilu, ki se nanaša na zmanjšanje sistemskega kibernetskega tveganja (ESRB, 2022a), s ciljem preprečiti neuspešno usklajevanje pri reševanju sistemskih kibernetskih dogodkov priporočila vzpostavitev vseevropskega sistemskega okvira za usklajevanje kibernetskih incidentov (v nadaljevanju EU-SCICF).[9]

5.1 Akt o digitalni operativni odpornosti (DORA)

EU zaradi vse večjih kibernetskih groženj krepi informacijsko varnost finančnih institucij (kot so banke, zavarovalnice in investicijska podjetja). H krepitvi informacijske varnosti finančnih institucij bo prispeval akt o digitalni operativni odpornosti (DORA), ki bo zagotovil, da bo lahko finančni sektor v Evropi odporen tudi ob resnih operativnih motnjah. Akt o digitalni operativni odpornosti določa enotne zahteve za varnost omrežij in informacijskih sistemov podjetij in organizacij, ki delujejo v finančnem sektorju, ter ključnih tretjih strani, ki jim zagotavljajo storitve, povezane z IKT (informacijske komunikacijske tehnologije), kot so platforme v oblaku ali storitve podatkovne analitike. Vzpostavlja regulativni okvir za digitalno operativno odpornost, pri čemer morajo vsa podjetja zagotoviti, da lahko vzdržijo vse vrste motenj in groženj, povezane z IKT, ter se nanje odzovejo in si opomorejo zaradi kibernetskih napadov. Glavni cilj okvirja je preprečiti in ublažiti posledice kibernetskih napadov (Banka Slovenije, 2023a).

Ključni gradniki akta o digitalni operativni odpornosti (DORA) so naslednji (EP, 2022):

- Dvig ravni upravljanja z IKT tveganjem na strani finančnih subjektov,
- Dvig ozaveščenosti nadzornikov o kibernetskih tveganjih in IKT incidentih institucij (uskladitev poročanje o incidentih, nadgradnja poročanja),
- Udejanjanje temeljitega preverjanja IKT sistemov (izmenjava informacij in podatkov o kibernetskih grožnjah),

[7] Direktiva NIS 2 je vseevropska horizontalna zakonodaja o kibernetski varnosti. Veljati je začela 16. januarja 2023, med tem ko je rok za njen prenos v nacionalno zakonodajo in notifikacijo te zakonodaje Evropski komisiji 17. oktober 2024.

[8] DORA (Digital Operational Resilience Act) naj bi se začela uporabljati januarja 2025. Ključni gradniki DORA so: (i) upravljanje tveganj, povezanih z IKT, (ii) incidenti, povezani z IKT, (iii) test digitalne operativne odpornosti, (iv) upravlja-nje tveganj zunanjih ponudnikov IKT in (v) izmenjava informacij med nadzornimi organi v EU.

[9] Kratica EU-SCICF pomeni EU-Pan-European systemic cyber incident coordination framework (vseevropski sistemski okvir za usklajevanje kibernetskih incidentov).

- Podlaga za nadzor nad tveganji, ki jih predstavljajo IKT storitve tretjih oseb (spremljanje tveganj zunanjih ponudnikov storitev in pregled pogodbenih določb) in

- Izmenjava informacij med nadzornimi organi v EU in drugimi ključnimi akterji na trgu.

Akt o digitalni operativni odpornosti (DORA) stremi k vzpostavitvi celovitega okvira za digitalno operativno odpornost EU finančnih subjektov. DORA je stopila v veljavo januarja 2023 (njena uporaba je predvidena v roku dveh let). DORA naj bi se začela uporabljati januarja 2025. Področje rabe zakona o digitalni operativni odpornosti bo poleg kreditnih in plačilnih institucijami zajemala še institucije za izdajo e-denarja, investicijska podjetja, ponudnike storitev kriptosredstev, centralne depotne družbe vrednostnih papirjev, družbe za upravljanje, zavarovalnice in pozavarovalnice, bonitetne agencije in zunanje ponudnike IKT storitev. Načelo sorazmernosti je del uredbe.

5.2 Vseevropska horizontalna zakonodaja o kibernetski varnosti (NIS 2)

Direktiva o varnosti omrežij in informacij (NIS) je bila prvi del vseevropske zakonodaje o kibernetski varnosti, njen cilj pa je bil doseči visoko skupno raven kibernetske varnosti v državah članicah. Čeprav je povečala zmogljivosti držav članic na področju kibernetske varnosti, se je izkazalo, da je njeno izvajanje težavno, kar je povzročilo razdrobljenost na različnih ravneh celotnega notranjega trga. To je bil tudi povod, da so se odločili za nadgradnjo direktive. Direktiva NIS 2 je vseevropska horizontalna zakonodaja o kibernetski varnosti. V veljavo je stopila 16. 1. 2023, medtem ko je rok za njen prenos v nacionalno zakonodajo ter notifikacijo te zakonodaje Evropski komisiji 17. 10. 2024. NIS 2 bo izboljšala odpornost in zmogljivost odzivanj na incidente na področju kibernetske varnosti in zaščite kritične infrastrukture. Direktiva določa tudi strožje nadzorne ukrepe nad zavezanimi subjekti, okrepljeno varnost dobavnih verig ter vzpostavlja osnovni okvir za usklajeno razkritje ranljivosti. Ključna novost direktive NIS 2 je razširitev njene uporabe za nove sektorje. Določa tudi pravne ukrepe za povečanje splošne ravni kibernetske varnosti v EU prek določanja usklajenih okvirov za kibernetsko varnost, pri čemer imajo države članice v njej določene obveznosti. Istočasno z Direktivo NIS 2 je sprejeta neposredno uporabljiva uredba o digitalni operativni odpornosti (DORA), ki se šteje za sektorski pravni akt, ki ima že določene zahteve za obvladovanje tveganj.

5.3 Vzpostavitev vseevropskega sistemskega okvirja za usklajevanje kibernetskih incidentov (EU-SCICF)

Cilj EU-SCICF je omogočiti učinkovito komunikacijo in usklajevanje med evropskimi nadzornimi organi ter drugimi organi, vključenimi v reševanje sistemske kibernetske krize. Za uspešno reševanje kibernetskih incidentov je potrebno usklajevanje na vseh ravneh (nacionalnem, mednarodnem in evropskem). Da bi zmanjšali tveganje neuspešnega usklajevanja, morajo nadzorniki finančnega sistema povečati svojo stopnjo pripravljenosti na sistemsko kibernetsko krizo na način, da izboljšajo svoje komunikacijske in usklajevalne zmogljivosti na ravni EU. Ključna načela, h katerim morajo evropski nadzorni organi stremeti, da ne bi prišlo do napak pri usklajevanju, so: (i) enotno razumevanje situacije, (ii) pravočasno usklajevanje med finančnimi nadzorniki, (iii) ustrezno komuniciranje z javnostjo in mediji (hitro širjenje sistemskih kibernetskih incidentov

lahko povzroči izgubo zaupanja v delovanje finančnega sistema) ter (iv) redno testiranje in nadgradnja okvira (redno testiranje zagotavlja, da je okvir ves čas primeren za uporabo in da se z njim izboljšuje pripravljenost na reševanje kibernetskih incidentov). Cilj EU-SCICF ni nadomestiti obstoječe zakonodajne okvire, temveč omogočiti premostitev vrzeli v usklajevanju in komunikaciji med finančnimi institucijami ter drugimi ključnimi akterji na mednarodni ravni. EU-SCICF naj bi se aktiviral le med sistemskimi kibernetskimi krizami. Uveden bo do konca leta 2025, vanj pa bodo vključeni nacionalni makrobonitetni organi (Banka Slovenije, 2022).

6 Zaključek

V zadnjih desetletjih je finančni sistem postal bolj digitaliziran in medsebojno povezan ter s tem posledično bolj ranljiv za kibernetske napade. Realno gospodarstvo za svoje delovanje od finančnega sistema zahteva, da zanesljivo opravlja vrsto ključnih gospodarskih funkcij. Finančni sistem postaja vse bolj odvisen od zanesljive infrastrukture informacijske in komunikacijske tehnologije (IKT) ter zaupnosti, celovitosti in razpoložljivosti podatkov in sistemov. Iz tega sledi, da so lahko ključne gospodarske funkcije motene zaradi kibernetskih incidentov, ki vplivajo na informacijske sisteme in podatke finančnih institucij ter infrastrukturo finančnega trga. Čeprav se je kibernetsko tveganje povečalo (pandemija in vojna v Ukrajini), finančni sistem do zdaj še ni doživel kibernetskega dogodka, ki bi ogrozil finančno stabilnost. Vendar pa lahko kibernetski incident povzroči operativne motnje, škoduje ugledu bančnega sistema in povzroči finančno škodo. Zato je ključno, da finančni regulator prispeva k zmanjšanju verjetnosti kibernetskega incidenta, ki bi sprožil sistemsko kibernetsko krizo in ogrozil finančno stabilnost.

Pomanjkanje kibernetske odpornosti lahko pomembno vpliva na finančno stabilnost. Zato je jasno, da je treba na kibernetsko odpornost gledati z makrobonitetnega vidika. To ne vključuje le opredelitve finančnih operacij ter storitev, ki so kritične na ravni sistema, temveč tudi ocenjevanje, spremljanje in testiranje same operativne odpornosti celotnega sistema. Glede na trenutno stanje finančnega sistema je tehnologija med najbolj oprijemljivimi in verjetnimi vzroki za motnje, ki lahko vplivajo na kibernetsko odpornost finančnega sistema. Z vidika zagotavljanja finančne stabilnosti je ključno, da kibernetski incident ne vodi do sistemskega dogodka, ki lahko povzroči dolgotrajne prekinitve poslovanja finančnih institucij ter posledično finančne izgube in manjše zaupanje javnosti. Za zagotavljanje finančne stabilnosti in izvajanje makrobonitetne politike je pomembna določitev ustreznih orodij in pristopov, ki se lahko uporabljajo za spremljanje kibernetske odpornosti finančnega sistema. Orodja za identifikacijo kibernetskih sistemskih tveganj so še v razvojni fazi in se prilagajajo nadzorniškim spremembam.

Nadzorniki finančnega sistema si prizadevamo povečati analitične sposobnosti pri spremljanju in identifikaciji sistemskega kibernetskega tveganja. Za dosego tega cilja nadzorniki razpolagamo z orodji, ki omogočajo bolj učinkovito spremljanje in analitične preglede, ter identificiramo tveganja. Orodja, ki jih uporabljamo za spremljanje tega področja so sledeča: prikazi tveganj s kibernetskimi kazalniki, ki omogočajo spremljanje tveganja na ravni bančnega sistema, kibernetsko kartiranje, ki vključuje ključne povezave med subjekti finančnega sektorja, ponudniki tehnologij in tehnološkimi rešitvami in kibernetski stresni testi.

K dvigu kibernetske odpornosti finančnega sektorja bosta prispevala prihajajoča pravna akta, in sicer NIS 2 in DORA, s katerima se izboljšuje nadzor nad subjekti finančnega sektorja, ponudniki tehnologij in tehnološkimi rešitvami, kar posledično prispeva k dvigu kibernetske odpornosti finančnega sektorja (Prenio in Restoy, 2022). Za zagotavljanje finančne stabilnosti je ključna tudi izmenjava informacij na področju kibernetske varnosti. Na EU ravni se bo do leta 2025 vzpostavil vseevropski sistemski okvir za usklajevanje kibernetskih incidentov (EU-SCICF). Ta bo izboljšal komunikacijo in usklajevanje med evropskimi nadzornimi organi ter drugimi organi pri reševanju sistemskih kriz.

7 Viri

Bank of England (2021). Operational resilience: Impact tolerances for important business services. Marec 2021. Dostopno na https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/policy-statement/2021/march/ps621.pdf?la=en&hash=A15AE3F7E18CA731ACD30B34DF3A5EA487A9FC11

Bank of England (2022a). Operational resilience: Impact tolerances for important business services. Marec 2022. Dostopno na https://www.bankofengland.co.uk/-/media/boe/files/prudential-regulation/supervisory-statement/2021/ss121-march-22.pdf

Bank of England (2022b). Prudential Regulation Authority statement on the 2022 cyber stress test: Retail payment system. December 2022. Dostopno na https://www.bankofengland.co.uk/prudential-regulation/publication/2021/december/cyber-stress-test-2022-retail-payment-system

Banka Slovenije (2019). Poročilo o finančni stabilnosti. December 2019. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/gdhbThgfwjcjdv_fsr-december-2019-lektorirano.pdf

Banka Slovenije (2020). Poročilo o finančni stabilnosti. Oktober 2020. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/fsr-oktober-2020_objava1.pdf

Banka Slovenije (2021a). Poročilo o finančni stabilnosti. April 2021. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/fsr_april_2021_sl.pdf

Banka Slovenije (2021b). Poročilo o finančni stabilnosti. Oktober 2021. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/fsr_oktober_2021.pdf

Banka Slovenije (2022). Poročilo o finančni stabilnosti. Maj 2022. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/porocilo-o-financni-stabilnosti-2022_maj_l.pdf

Banka Slovenije (2023a). Poročilo o finančni stabilnosti. Maj 2023. Dostopno na https://bankaslovenije.blob.core.windows.net/publication-files/fsr-2023_maj_le.pdf

Banka Slovenije (2023b). Poročilo o finančni stabilnosti. Oktober 2023.

ECB (2018). Cyber resilience oversight expectations for financial market infrastructures. December 2018. Dostopno na https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

EP (2022). Digital Operational Resilience Act (DORA). November 2022. Dostopno na https://www.europarl.europa.eu/doceo/document/TA-9-2022-0381_EN.pdf

ESRB (2020a). Systemic cyber risk. Februar 2020. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf

ESRB (2020b). The making of a cyber crash: a conceptual model for systemic risk in the financial sector. Maj 2020. Dostopno na https://www.esrb.europa.eu/pub/pdf/occasional/esrb.op16~f80ad1d83a.en.pdf

ESRB (2022a). Mitigating systemic cyber risk. Januar 2022. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.SystemiCyberRisk.220127~b6655fa027.en.pdf

ESRB (2022b). ESRB recommends establishing a systemic cyber incident coordination framework. Januar 2022. Dostopno na https://www.esrb.europa.eu/news/pr/date/2022/html/esrb.pr.220127~f1548f677e.en.html

ESRB (2023). Advancing macroprudential tools for cyber resilience. Februar 2023. Dostopno na https://www.esrb.europa.eu/pub/pdf/reports/esrb.macroprudentialtoolscyberresilience220214~984a5ab3a7.en.pdf

Financial Stability Board (2018). Cyber Lexicon. November 2018. Dostopno na https://www.fsb.org/wp-content/uploads/P121118-1.pdf

IMF (2020). Cyber Risk and Financial Stability: It's a Small World After All. December 2020. Dostopno na https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2020/12/04/Cyber-Risk-and-Financial-Stability-Its-a-Small-World-After-All-48622

Prenio, J. and Restoy, F. (2022). Safeguarding operational resilience: the macroprudential perspective. Avgust 2022. FSI Briefs, Financial Stability Institute, Bank for International Settlements. Dostopno na https://www.bis.org/fsi/fsibriefs17.pdf