Zmaja od Bosne 47b,
71000 Sarajevo,
Bosna i Hercegovina

T ++ 387 (33) 72 14 00
F ++ 387 (33) 66 88 11

E agencija@fba.ba
W www.fba.ba

BOSNA I HERCEGOVINA
FEDERACIJA BOSNE I HERCEGOVINE
AGENCIJA ZA BANKARSTVO
FEDERACIJE BOSNE I HERCEGOVINE

SPECIJALISTIČKA SUPERVIZORSKA OČEKIVANJA U VEZI SA POSTUPANJEM BANAKA I OSIGURANJEM KONTINUITETA POSLOVANJA U VANREDNIM SITUACIJAMA

Sarajevo, august/kolovoz 2024. godine

Uvod

1. Agencija za bankarstvo Federacije BiH (u daljnjem tekstu: Agencija) objavljuje supervizorska očekivanja u cilju usmjeravanja banaka prema održivom i sigurnom poslovanju, kao i u svrhu upravljanja rizicima i posljedicama eksternih poremećaja koji mogu imati negativan utjecaj na opću sigurnost, ekonomiju i bankarski sistem. Ovaj dokument izdvaja supervizorska očekivanja koja se odnose na postupanja banaka u svrhu osiguravanja kontinuiteta poslovanja u kontekstu saznanja i iskustava iz proteklog perioda. Pažnja se usmjerava na potrebu izdvajanja i održavanja ključnih poslovnih procesa u bankama. Planirane supervizorske aktivnosti opisane u nastavku ovog dokumenta mogu usmjeriti pripremne aktivnosti banaka, osigurati bolju koordinaciju, rezultirati efikasnijom supervizijom i povećanim zadovoljstvom i povjerenjem klijenata u bankarski sistem.

2. 21.6.2024. godine u 12:35, evidentiran je prestanak snabdijevanja električnom energijom većine područja i potrošača u Bosni i Hercegovini, sa postepenim oporavkom koji je trajao narednih 6 sati. Incident je vjerovatno potaknut ispadom interkonektivnog dalekovoda 400 kV između Albanije i Grčke, što je pokrenulo kaskadni niz kvarova koji su se proširili na Crnu Goru, dijelove Hrvatske i Bosnu i Hercegovinu. Ovo je rezultiralo djelimičnim ili potpunim raspadom elektroenergetskog sistema u navedenim zemljama.

3. 19.7.2024. godine u jutarnjim satima po centralnoeuropskom vremenu evidentiran je globalni incident koji je u vezi sa neadekvatnim ažuriranjima i ispadima programskih rješenja koja predstavljaju resurs korištenih informaciono-komunikacionih tehnologija (IKT) i poslovnih procesa u bankama. Ovaj događaj je imao kratkotrajne efekte na rad nekoliko banaka u FBiH sa djelimičnim i potpunim prekidima rada sa klijentima u tim bankama. Potpuni oporavak i stabilizacija poslovnih procesa odvijala se u toku dana.

4. U junu i julu mjesecu 2024. godine evidentirani su ozbiljni cyber napadi na više ustanova u regionu, uključujući i ključnu zdravstvenu ustanovu u Republici Hrvatskoj (26.-27.06.2024. godine), kao i značajan aerodrom (23.07.2024. godine), a što ukazuje i na pojačan rizik od kibernetičkog (*eng. cyber)* napada.

Supervizorska zabrinutost u odnosu na nova saznanja i činjenice

5. Većina telekomunikacijskih operatera koristi izvore neprekidnog napajanja (UPS) i generatore kako bi održavali mrežu u slučaju nestanka električne energije iz javne mreže. Međutim, nakon nekoliko sati, ovi resursi mogu biti iscrpljeni u pojedinim regijama ili dijelovima države, što bi dovelo do smanjenog nivoa ili prekida mobilnih, fiksnih telefonskih i internet usluga. Takva situacija može otežati i koordinaciju u kriznim situacijama ili dodatno odgoditi oporavak poslovnih procesa.

6. Prolongirani prekid u napajanju električnom energijom može rezultirati gubitkom podataka u centrima za obradu podataka koji nemaju adekvatne „backup“ sisteme ili alternativno napajanje. Posebni problemi se mogu pojaviti kod izostanka hlađenja serverskih postrojenja što može imati značajne posljedice i kod oporavka. Moguće su situacije u kojima postojeći planovi obuhvataju kontinuirani rad IKT infrastrukture, ali se

izostavlja međuovisnost sa ostalim potrebnim resursima što može dovesti do značajnijih šteta.

7. Ako neki dijelovi mreže ostanu operativni, moglo bi doći do preopterećenja zbog povećane potražnje, što bi dodatno smanjilo kvalitet usluga ili povećalo šanse za greške u obradama i prijenosu podataka. Platni sistemi mogu biti naročito usporeni ili nedostupni.

8. Uslijed sve većeg oslanjanja na informacione komunikacione tehnologije (IKT) u svakodnevnom životu i poslovanju banaka, korištenja modernih tehnoloških usluga poslovanja u oblaku (*eng. cloud computing*), globalnih pružatelja IKT usluga i uključenih lanaca podizvođača/trećih strana, te međusobne povezanosti IKT sistema, proširuje se prostor za iskorištavanje njihove ranjivosti. Zbog toga dolazi do ubrzanog širenja incidenata. Očekuje se da će se učestalost incidenata koji imaju utjecaj na dostupnost informacionih sistema, odnosno dostupnost poslovnih usluga banaka, u budućnosti povećavati. Navedenom doprinosi i visoka prijetnja od cyber napada u Europi, koja je očigledna kroz sabotaže, poremećaje u sistemima velikih banaka i trećih strana, te rastuću sofisticiranost i učestalost cyber napada.

9. Bankomati i POS terminali obično imaju alternativno napajanje za kratkotrajne nestanke struje. Međutim, protokom vremena, većina bi prestala s radom, što bi ograničilo pristup gotovini i mogućnostima plaćanja.

10. Dugotrajni prekidi internet i mobilnog bankarstva mogu predstavljati izniman izazov jer bez električne energije, serveri, sistemi za internet i mobilno bankarstvo bi prestali funkcionirati, onemogućavajući klijentima pristup njihovim računima i izvršavanje transakcija.

11. Dugotrajan prekid može povećati rizik od sigurnosnih incidenata, uključujući cyber napade i fizičke upade, jer bi sistemi osnovnog sigurnosnog nadzora mogli prestati s radom (video nadzor, alarm i sl.). Obavljanje procesa bez adekvatnih sigurnosnih mjera može biti posebno neprihvatljivo ukoliko bi bila ugrožena fizička sigurnost.

Specijalistička supervizorska očekivanja za postupanje banaka

12. Prioritet u kriznim situacijama je zaštita fizičke sigurnosti klijenata i zaposlenika banke. Banke imaju obavezu osigurati da poslovne prostorije budu sigurne, što uključuje kontinuitet rada sigurnosnih sistema za fizičku zaštitu, pravovremenu evakuaciju, pružanje pomoći i komunikaciju. Rizici koji se odnose na fizičku sigurnost moraju biti uvaženi i definirani, što uključuje i kriterije za prekid i nastavak rada sa klijentima u prostorijama banke.

13. Kod razmatranja opcija kontinuiteta poslovanja i dostupnosti usluga za klijente, princip dostupnosti „24/7“ treba biti razmotren ili omogućen za sve usluge koje ne uključuju fizički pristup prostorijama banke.

14. Osim preispitivanja slabosti i kapaciteta vlastite IKT infrastrukture, od banaka se očekuje da pitanja kontinuiteta i dostupnosti budu obuhvaćena i kroz ugovorne aranžmane sa

ključnim poslovnim partnerima i klijentima, uključujući telekomunikacijske operatere i značajne trgovačke lance i objekte. Ovo se posebno odnosi na POS terminale koji bi trebali biti dostupni i aktivni i u kriznim situacijama.

15. Očekuje se preispitivanje otpornosti infrastrukture internet i mobilnog bankarstva, te utvrđivanje prioriteta ovog modela rada sa klijentima i u okolnostima značajnih eksternih poremećaja ili kriza. POS infrastruktura, internet i mobilno bankarstvo moraju se razmatrati kao opcija rada za slučajeve višednevnih ili produženih kriznih stanja koja mogu biti vezana za fizičku sigurnost.

16. Ovisno o poslovnom modelu banke i specifičnostima poslovne mreže, od banaka se očekuje da utvrde prioritete kod osiguranja dostupnosti i ostalih usluga banke, uključujući i usluge koje uključuju direktni kontakt i rad s gotovinom.

17. Ovisno o bančinoj procjeni kapaciteta infrastrukture, ne dovodeći u pitanje potrebu neprekidne dostupnosti POS, internet i infrastrukture mobilnog bankarstva, od banaka se očekuje da imaju spremne preglede kapaciteta i projicirane dostupnosti poslovne mreže u slučajevima realizacije specifičnih rizika. Gdje god je moguće, banke trebaju odrediti lokacije i dijelove poslovne mreže koji će biti prioritetno dostupni, ovisno o specifičnim okolnostima, a posebno uzimajući u obzir proporcionalnost. Ovaj zahtjev uključuje određivanje i transparentno obavještavanje klijenata o „dežurnim“ poslovnicama i uslovima u kojima se može očekivati rad banke u izmijenjenom ili smanjenom kapacitetu. Koncepti i načini informisanja klijenata moraju biti planirani i provedivi i u slučajevima značajnih kriznih stanja (koncept notifikacija i usmjeravanja klijenata u vanrednim okolnostima).

18. U skladu sa Odlukom o sistemu internog upravljanja u bankama i Odlukom o upravljanju informacionim sistemima, banke su dužne imati spremne planove oporavka za različite očekivane događaje, što uključuje i prirodne katastrofe, tehničke incidente, uključujući nedostatak električne energije, komunikacionih kanala, kao i druge sigurnosne prijetnje. U okviru navedenih planova oporavka, banke su dužne definirati i parametre očekivanog vremena oporavka poslovnih procesa.

19. Osiguranje pravovremenih, jasnih i potpunih informacija o dostupnim uslugama klijentima je od ključne važnosti, kako za osiguranje pravovremenog obavljanja neophodnih hitnih usluga unutar rokova koje određuju važeći zakoni, tako i za izbjegavanje dezinformacija ili panike u pogledu dostupnosti usluga. Od banaka se očekuje da imaju razvijene planove za krizno komuniciranje. Takvi planovi i njihova operativna primjena trebaju uključiti i edukaciju zaposlenika banke i klijenata o načinima mogućeg djelovanja i dostupnosti usluga banke.

20. Održavanje povjerenja u snagu i stabilnost bankarskog sistema treba se proširiti na način da se u svakoj kriznoj situaciji zaposlenicima banke i klijentima omogući adekvatna informacija ili procjena potrebnog vremena za oporavak usluga banke. Od iznimne je važnosti razvoj svijesti o postojanju koncepta kontinuiteta poslovanja koji štiti interese i imovinu klijenta i u uvjetima značajnih kriznih stanja.

21. Unaprijeđena saznanja i činjenice o rizicima koji mogu ugroziti kontinuitet poslovanja banke moraju biti predmet razmatranja od strane organa upravljanja banke. Uočene slabosti trebaju biti povod za preispitivanja i unaprjeđenja postojećih planova i infrastrukture. Od organa upravljanja se očekuje preispitivanje spremnosti poslovnih modela i infrastrukture banke za kontinuirano pružanje usluga klijentima, što uključuje i preispitivanje prioriteta.

Supervizorski prioriteti i aktivnosti

Nadzor sigurnosti IKT sistema u bankama je kontinuiran. Agencija očekuje dodatnu podršku i jačanje funkcija u bankama koje se odnose na sigurnost IKT. Rizici koji se razmatraju u kontekstu kontinuiteta poslovanja i IKT će biti predmet ciljanih kontrola od strane Agencije. Pažnja će se posvetiti stanju sistema internih kontrola u dijelu koji se odnosi na upravljanje rezervnim kopijama (*eng. backup*), posebno u dijelovima infrastrukture koja se oslanja na poslovanje u oblaku (*eng. cloud computing*) i druge eksternalizirane servise.

Posvećenost principima održavanja kontinuiteta poslovanja će se dodatno razmatrati, a eventualni izostanak primjene plana kontinuiteta poslovanja će se smatrati slabošću ili propustom sistema internih kontrola u dijelu odgovornosti organa upravljanja banke.

Koncept komunikacije i upravljanja incidentima će se unaprijediti, što uključuje preispitivanje postojećih protokola za dostavljanje i razmjenu informacija unutar bankarskog sistema. Inicijative i preporuke svih učesnika u komunikacijskim protokolima će se pažljivo razmatrati i uvažavati od strane Agencije.

U nastavku 2024. godine, Agencija će prikupljati dodatne informacije koje se odnose na supervizorska očekivanja i njihove efekte u praksi, planove kontinuiteta poslovanja, ključnu infrastrukturu i dijelove poslovne mreže banaka koji su označeni kao značajni u kriznim i vanrednim okolnostima. Ovisno o procjeni, takve informacije mogu biti iskorištene za informisanje banaka, institucija i javnosti u specifičnim okolnostima.

AGENCIJA ZA BANKARSTVO FEDERACIJE BIH