Na osnovu člana 44 stav 2 tačka 3 Zakona o Centralnoj banci Crne Gore („Službeni list CG”, br. 40/10, 6/13 i 70/17) i člana 56a stav 3 Zakona o platnom prometu („Službeni list CG”, br. 62/13 i 111/22), Savjet Centralne banke Crne Gore, na sjednici održanoj 28. 04. 2023. godine, donio je

ODLUKU
O SIGURNOSNIM MJERAMA ZA OPERATIVNE I SIGURNOSNE RIZIKE POVEZANE SA PLATNIM USLUGAMA

I. OSNOVNE ODREDBE

Predmet

Član 1

(1) Ovom odlukom se utvrđuju sigurnosne mjere za operativne i sigurnosne rizike povezane sa platnim uslugama, kao i uspostavljanje, sprovođenje i praćenje sigurnosnih mjera.

(2) U smislu ove odluke, operativnim i sigurnosnim rizicima smatraju se rizici informacionog sistema (u daljem tekstu: IS rizici).

Proporcionalnost

Član 2

Pružalac platnih usluga je dužan da postupa u skladu sa odredbama ove odluke uzimajući u obzir, veličinu, unutrašnju organizaciju, prirodu, obim, složenost i rizičnost usluga i proizvoda koje pruža ili namjerava da pruža.

Primjena na kreditne institucije

Član 3

Odredbe ove odluke primjenjuju se na kreditne institucije u dijelu koji nije uređen propisom Centralne banke Crne Gore (u daljem tekstu: Centralna banka) o minimalnim standardima za upravljanje rizicima kojima je kreditna institucija izložena ili bi mogla biti izložena u svom poslovanju.

Značenje izraza

Član 4

Izrazi upotrijebljeni u ovoj odluci imaju sljedeća značenja:

1) **informacioni sistem** (IS) je sveobuhvatni skup tehničke infrastrukture (softverska i hardverska imovina), organizacije, ljudi i postupaka za generisanje, prikupljanje, čuvanje, prenos, prikazivanje, korišćenje, modifikaciju i druge postupke obrade informacija;

2) **IS rizik** je rizik nastanka negativnih efekata na finansijski rezultat i kapital pružaoca platnih usluga, ostvarenje njegovih poslovnih ciljeva, kao i poslovanje u skladu sa propisima, usljed neadekvatnog upravljanja informacionim sistemom ili zbog druge slabosti tog sistema koja negativno utiče na njegovu funkcionalnost ili sigurnost;
3) **informaciona sigurnost** je stanje u kojem samo ovlašćeni korisnici (povjerljivost) imaju pristup tačnim i kompletnim informacijama (integritet) kada za tim imaju potrebu (dostupnost);
4) **operativni ili sigurnosni incident** je jedan ili više povezanih događaja koji nijesu planirani, a koji su ili će vjerovatno imati negativan uticaj na integritet, dostupnost, povjerljivost i/ili autentičnost platnih usluga;
5) **povjerljivost informacije** znači da informacija nije otkrivena ili dostupna neovlašćenim licima;
6) **integritet informacije** znači da informacija, odnosno podatak nije neovlašćeno ili nepredviđeno promijenjen;
7) **dostupnost informacije** znači da ovlašćeno lice može blagovremeno pristupiti informaciji i iskoristiti je;
8) **resursi informacionog sistema** obuhvataju softversku, hardversku i informacionu imovinu, ljude i procese;
9) **softverska imovina** (softverske komponente IS) obuhvata sve tipove aplikativnog i sistemskog softvera, baze podataka, razvojne alate, uslužne programe i ostali softver;
10) **hardverska imovina** (hardverske komponente IS) obuhvata računare i računarsku opremu, komunikacionu opremu, medije za čuvanje podataka i ostalu tehničku opremu koja podržava rad informacionog sistema;
11) **informaciona imovina** obuhvata podatke u bazama podataka, datoteke sa podacima, programski kod, konfiguraciju hardverske imovine, tehničku i korisničku dokumentaciju, izvještaje, strategije, politike, procedure, ostala interna akta i slično;
12) **informaciona tehnologija (IT)** je kombinacija hardverske i softverske imovine koja omogućava automatizovano generisanje, prikupljanje, obradu, čuvanje, prenos, prikazivanje i/ili korišćenje informacija;
13) **IT sistem** je informaciona tehnologija uređena kao dio mehanizma ili međusobno povezane mreže koja pruža podršku poslovanju pružaocu platnih usluga;
14) **IT servis** je usluga koju IT sistem pruža unutrašnjim ili spoljnim korisnicima;
15) **IT projekat** je svaki projekat ili njegov dio u kojem se IT sistemi ili servisi mijenjaju, zamjenjuju, stavljaju van upotrebe ili implementiraju i može biti dio širih IT projektnih programa ili projektnih programa transformacije poslovanja;
16) **sklonost ka preuzimanju rizika** (engl. *risk appetite*) je nivo i vrste rizika koje je pružalac platnih usluga spreman da preuzme u okviru svoje sposobnosti podnošenja rizika kako bi ostvario svoje strateške ciljeve.

II. MJERE ZA RIZIKE INFORMACIONOG SISTEMA POVEZANE SA PLATNIM USLUGAMA

Sistem upravljanja

Član 5

(1) Pružalac platnih usluga je dužan da sistemom upravljanja koji uspostavlja u skladu sa zakonom, a koji uključuje upravljačku organizaciju sa jasno definisanim, preglednim i dosljednim linijama ovlašćenja i odgovornosti, obezbijedi jasno definisana ovlašćenja i odgovornosti, za efikasno i sigurno upravljanje informacionim sistemom (IT operacijama, IT razvojem, informacionom sigurnošću, itd.), IS rizicima i kontinuitetom poslovanja, kojim se izbjegava sukob interesa, obezbjeđuje efikasna komunikacija i saradnja u vezi sa obavljanjem tih aktivnosti i uspostavlja jasan i dokumentovan proces donošenja odluka.

(2) Pružalac platnih usluga je dužan da obezbijedi da je u kontinuitetu angažovan odgovarajući broj lica sa potrebnim stručnim kvalifikacijama i kompetencijama za obavljanje poslova iz stava 1 ovog člana i za sprovođenje strategije razvoja informacionog sistema iz člana 7 ove odluke.

(3) Pružalac platnih usluga je dužan da internim aktima propiše sadržaj, periodičnost i način izvještavanja nadležnih organa tog pružaoca platnih usluga o značajnim činjenicama u vezi sa obavljanjem poslova iz stava 1 ovog člana.

(4) Organizacioni djelovi pružaoca platnih usluga koji obavljaju operativne poslove i aktivnosti u kojima IS rizici nastaju, a naročito organizacioni dio ili djelovi koji su zaduženi za obavljanje IT operacija, odgovorni su za uspostavljanje odgovarajućih procesa i kontrola kojima su ovi rizici, u skladu sa sklonošću ka preuzimanju IS rizika, svedeni na prihvatljiv nivo, kao i za usklađenost servisa i sistema koje pružaju i aktivnosti koje obavljaju sa internim i spoljnim zahtjevima.

(5) Pružalac platnih usluga je dužan da odredi organizacioni dio i/ili lica koja su neposredno odgovorna za koordinaciju, praćenje i nadziranje primjene pravila za upravljanje IS rizicima, odnosno da obezbijede da se ovi rizici utvrđuju, mjere, procjenjuju, kontrolišu, prate i da se o njima izvještava.

(6) Pružalac platnih usluga je dužan da obezbijedi nezavisnost i objektivnost organizacionog dijela i/ili lica iz stava 5 ovog člana, na način da taj organizacioni dio i/ili lica ne obavljaju operativne poslove i aktivnosti u kojima rizik nastaje (koje prate i nadziru), a naročito poslove i aktivnosti koje obavlja organizacioni dio pružaoca platnih usluga koji je zadužen za IT operacije.

(7) Organizacioni dio i/ili lica iz stava 5 ovog člana su dužni da blagovremeno izvještavaju nadležne organe pružaoca platnih usluga o redovnim i vanrednim aktivnostima vezanim za upravljanje IS rizicima.

Korišćenje usluga trećih strana

Član 6

(1) Pružalac platnih usluga je dužan da na adekvatan način upravlja IS rizicima koji proizilaze ili mogu proizaći iz poslovnog odnosa sa trećom stranom koja mu pruža uslugu ili proizvod u vezi sa informacionim sistemom, bez obzira da li taj poslovni odnos predstavlja eksternalizaciju ili ne, što obuhvata i sprovođenje mjera za ublažavanje rizika koje su utvrđene ovom odlukom.

(2) Pružalac platnih usluga je dužan da prije stupanja u poslovni odnos iz stava 1 ovog člana, sa trećom stranom zaključi ugovor u vezi sa tim poslovnim odnosom, i da pri tome vodi računa da su sadržaj i obim ugovornih odredbi definisani u skladu sa kompleksnošću i obimom poslova koji se povjeravaju trećoj strani i sklonošću ka preuzimanju IS rizika pružaoca platnih usluga.

(3) Ugovor iz stava 2 ovog člana, naročito treba da sadrži odredbe u vezi sa:

1) mjerama informacione sigurnosti, kao što su zahtjevi po pitanju sajber sigurnosti, kriptovanja podataka pružaoca platnih usluga i njihovog životnog ciklusa, sigurnosti računarske mreže, lokacije na kojoj će se nalaziti podaci, zahtjeva po pitanju kontinuiteta pružanja usluge, nadgledanja sigurnosti sistema i slično;
2) načinom i dinamikom rješavanja operativnih i sigurnosnih incidenata, uključujući postupke eskalacije i izvještavanja.

(4) Pružalac platnih usluga je dužan da prati kvalitet i sigurnost obavljanja poslova koji su predmet ugovora iz stava 2 ovog člana i ispunjenost ugovorenog nivoa usluge.

Strategija razvoja informacionog sistema

Član 7

(1) Pružalac platnih usluga je dužan da utvrdi strategiju razvoja informacionog sistema, za vremenski period koji nije kraći od tri godine, koja je usklađena sa opštom poslovnom strategijom i koja, najmanje, treba da:

1) kroz prikaz postojećeg i željenog stanja opiše način na koji bi informacioni sistem trebalo da se razvija, uključujući promjene u vezi sa IT sistemima, IT arhitekturom, organizacionom i operativnom strukturom i korišćenjem usluga trećih strana;
2) definiše jasne ciljeve po pitanju informacione sigurnosti, sa naglaskom na IT sisteme, IT servise, zaposlene i procese;
3) opiše način na koji će se pružalac platnih usluga posvetiti upravljanju informacionim sistemom u cilju očuvanja kontinuiteta poslovanja.

(2) Pružalac platnih usluga je dužan da strategiju iz stava 1 ovog člana detaljnije razradi donošenjem godišnjih operativnih planova aktivnosti koji sadrže mjere za realizaciju ciljeva definisanih u strategiji razvoja informacionog sistema.

(3) Godišnji operativni plan aktivnosti iz stava 2 ovog člana treba, kao minimum, da sadrži opis aktivnosti i projekata, izvođače, odgovorna lica, budžet i rokove za izvršenje planiranih aktivnosti.

(4) Pružalac platnih usluga je dužan da obezbijedi finansijska sredstva dovoljna za sprovođenje strategije iz stava 1 ovog člana.

(5) Pružalac platnih usluga je dužan da uspostavi proces kontinuiranog mjerenja i nadgledanja efikasnosti sprovođenja strategije iz stava 1 ovog člana.

Interna akta za upravljanje IS rizicima

Član 8

Pružalac platnih usluga je dužan da u internim aktima utvrdi pravila za upravljanje IS rizicima kojima, kao minimum, definiše:

1) sklonost ka preuzimanju IS rizika, u skladu sa sklonošću ka preuzimanju rizika tog pružaoca platnih usluga;
2) metode i parametre (prijetnja, ranjivost, vjerovatnoća, uticaj itd.) za utvrđivanje i mjerenje, odnosno procjenjivanje IS rizika kojima je pružalac platnih usluga izložen;
3) postupke za definisanje mjera za kontrolisanje rizika, uključujući uvođenje novih i/ili modifikaciju postojećih kontrola u cilju ublažavanja rizika;
4) postupke praćenja realizacije mjera iz tačke 3 ovog člana i njihove efikasnosti, kao i broja utvrđenih operativnih ili sigurnosnih incidenata, uključujući i incidente koji su prijavljeni Centralnoj banci u skladu sa zakonom, i preduzimanja radnji za prilagođavanje tih mjera kada je to potrebno;
5) obavezu utvrđivanja i mjerenja, odnosno procjenjivanja rizika relevantnog dijela informacionog sistema koji proizilaze iz bilo kakvih većih promjena informacionog sistema, servisa i/ili procesa upravljanja informacionim sistemom, prije donošenja odluke o realizaciji tih promjena;
6) obavezu utvrđivanja i mjerenja, odnosno procjenjivanja rizika relevantnog dijela informacionog sistema nakon svakog značajnog operativnog ili sigurnosnog incidenta;
7) vremenski okvir za sprovođenje redovnog, sveobuhvatnog utvrđivanja i procjene IS rizika, a najmanje jednom godišnje;
8) način i periodičnost pripreme i dostavljanja izvještaja nadležnim organima pružaoca platnih usluga o značajnim činjenicama u vezi sa aktivnostima za upravljanje IS rizicima i izloženosti pružaoca platnih usluga ovim rizicima;
9) ovlašćenja i odgovornosti za upravljanje IS rizicima za sve nivoe radnog procesa i odlučivanja, na način kojim se izbjegava sukob interesa.

Mapiranje poslovnih funkcija, procesa, IT sistema i IT servisa

Član 9

(1) Pružalac platnih usluga je dužan da utvrdi i redovno ažurira mapu svojih poslovnih funkcija i procesa koji se izvršavaju u okviru tih funkcija, koja:

1) opisuje međusobnu povezanost različitih funkcija i procesa;
2) sadrži pregled informacione imovine koju određena funkcija i/ili proces koristi ili kreira;
3) opisuje odlazni i dolazni tok informacija između različitih funkcija i procesa.

(2) Pružalac platnih usluga je dužan da utvrdi i redovno ažurira i mapu povezanosti između poslovnih funkcija i procesa iz stava 1 ovog člana i IT sistema, IT servisa,

zaposlenih i drugih angažovanih lica kod pružaoca platnih usluga koji podržavaju i/ili omogućavaju funkcionisanje tih funkcija i procesa.

Utvrđivanje važnosti resursa informacionog sistema

Član 10

(1) Pružalac platnih usluga je dužan da klasifikuje i dokumentuje poslovne funkcije, procese, informacionu imovinu, IT sisteme, IT servise, zaposlene i spoljne pružaoce usluga iz člana 9 ove odluke prema njihovoj važnosti, odnosno kritičnosti.

(2) Prilikom utvrđivanja važnosti, odnosno kritičnosti resursa iz stava 1 ovog člana pružalac platnih usluga je dužan da, kao minimum, uzme u obzir zahtjeve po pitanju njihove dostupnosti, povjerljivosti i integriteta.

(3) Pružalac platnih usluga je dužan da jasno definiše zaduženja i odgovornosti za resurse iz stava 1 ovog člana i za utvrđivanje njihove klasifikacije.

(4) Važnost resursa iz stava 1 ovog člana se uzima u obzir i preispituje prilikom vršenja procjene IS rizika.

Definisanje korektivnih mjera

Član 11

(1) Pružalac platnih usluga je dužan da, na osnovu rezultata procjene rizika, u skladu sa sklonošću ka preuzimanju IS rizika, utvrdi koje su mjere potrebne kako bi se IS rizici sveli na prihvatljiv nivo, i da li je potrebno izvršiti promjene postojećih poslovnih procesa, kontrolnih mjera, IT sistema i/ili IT servisa.

(2) Pružalac platnih usluga je dužan da procijeni vrijeme potrebno za sprovođenje promjena iz stava 1 ovog člana, i da u skladu sa sklonošću ka preuzimanju IS rizika, ako je potrebno, definiše privremene mjere za ublažavanje rizika koje će se primjenjivati dok se planirane promjene ne sprovedu.

Revizija

Član 12

(1) Pružalac platnih usluga je dužan da obezbijedi reviziju informacionog sistema, upravljanja informacionim sistemom i IS rizicima od strane nezavisnog revizora koji ima znanje i iskustvo u oblasti IS rizika i oblasti platnog prometa.

(2) Učestalost i predmet revizije iz stava 1 ovog člana treba da budu srazmjerni IS rizicima kojima je pružalac platnih usluga izložen.

(3) Pružalac platnih usluga donosi i redovno ažurira plan revizije iz stava 1 ovog člana.

(4) Pružalac platnih usluga je dužan da uspostavi proces u skladu sa kojim se vrši sprovođenje mjera za otklanjanje nepravilnosti i nedostataka utvrđenih revizijom iz stava 1 ovog člana, kao i praćenje tog sprovođenja.

Politika informacione sigurnosti

Član 13

(1) Pružalac platnih usluga je dužan da usvoji i sprovodi politiku informacione sigurnosti, kojom su definisana opšta načela i pravila za zaštitu povjerljivosti, integriteta i dostupnosti podataka i informacija pružaoca platnih usluga i njegovih klijenata, a kojom se naročito utvrđuju:

1) cilj i obuhvat politike informacione sigurnosti;
2) načela upravljanja informacionom sigurnošću;
3) opis glavnih uloga, opštih i posebnih odgovornosti u vezi sa upravljanjem informacionom sigurnošću.

(2) Pružalac platnih usluga je dužan da politikom iz stava 1 ovog člana definiše odgovornost svih zaposlenih, izvođača i drugih angažovanih lica po pitanju zaštite informacija, kao i mjere koje može prema njima preduzeti u slučaju narušavanja sigurnosti informacionog sistema.

(3) Pružalac platnih usluga je dužan da upozna lica iz stava 2 ovog člana sa politikom informacione sigurnosti.

(4) Pružalac platnih usluga je dužan da politikom informacione sigurnosti obezbijedi povjerljivost, integritet i dostupnost logičkih i fizičkih resursa informacionog sistema u skladu sa njihovom kritičnošću, kao i osjetljivih podataka, nezavisno od toga da li se nalaze u stanju mirovanja, prenosu ili u upotrebi.

(5) Pružalac platnih usluga je dužan da kontinuirano usklađuje politiku informacione sigurnosti sa promjenama u informacionom sistemu i njegovoj okolini, u slučajevima narušavanja sigurnosti informacionog sistema, kao i na osnovu rezultata procjene rizika.

(6) Pružalac platnih usluga je dužan da na osnovu politike informacione sigurnosti iz stava 1 ovog člana, internim aktima propiše i primijeni detaljna pravila koja se odnose na sve aspekte informacione sigurnosti, i to na:

1) organizaciju i upravljanje u skladu sa čl. 5 i 12 ove odluke;
2) logičku sigurnost;
3) fizičku sigurnost;
4) sigurnost IT operacija;
5) praćenje informacione sigurnosti;
6) provjeru, procjenu i testiranje informacione sigurnosti;
7) obuku i podizanje svijesti o informacionoj sigurnosti.

(7) Pružalac platnih usluga koji platne usluge pruža kao platna institucija politiku iz stava 1 ovog člana utvrđuje u okviru politike sigurnosti koju donosi u skladu sa zakonom.

Logička sigurnost

Član 14

(1) Pružalac platnih usluga je dužan da internim aktima definiše i primijeni pravila za upravljanje logičkim kontrolama pristupa (upravljanje identitetima i pristupom) kojima se obezbjeđuje najmanje da:

1) se pristup informacionom sistemu vrši u skladu sa principom neophodnosti pristupa informacijama (engl. *need to know*), uključujući i pristup na daljinu;
2) su korisnicima informacionog sistema dodijeljena prava pristupa na osnovu definisane poslovne potrebe, tako da su minimalno potrebna za nesmetano obavljanje zadataka;
3) dodijeljena prava pristupa omogućavaju adekvatnu segregaciju dužnosti, odnosno da korisnicima nije dodijeljena kombinacija prava pristupa koja im omogućava zaobilaženje kontrola;
4) su, gdje je to moguće, korisnicima informacionog sistema dodijeljeni personalizovani korisnički nalozi po kojima ih je lako identifikovati, i da jedan nalog koristi samo jedan korisnik kako bi se aktivnosti koje se sprovode u informacionom sistemu mogle jasno povezati sa tim korisnikom i kako bi mogla da se utvrdi odgovornost;
5) je korišćenje privilegovanog pristupa strogo kontrolisano tako što se ograničavaju i pažljivo prate aktivnosti naloga sa povišenim pravima pristupa (kao što su nalozi administratora sistema), i da se privilegovani pristup na daljinu odobrava samo na osnovu principa neophodnosti pristupa informacijama uz upotrebu rješenja za pouzdanu provjeru autentičnosti (kao što je provjera autentičnosti koja se zasniva na korišćenju dva faktora);
6) se aktivnosti korisnika, a naročito sve aktivnosti privilegovanih korisničkih naloga, evidentiraju u sistemskim i operativnim zapisima i da se ti zapisi izrađuju, prate i čuvaju u skladu sa utvrđenom kritičnošću resursa informacionog sistema iz člana 10 ove odluke, u svrhu blagovremenog otkrivanja neovlašćenih pristupa i radnji na informacionom sistemu, rekonstruisanja događaja i utvrđivanja odgovornosti;
7) se prava pristupa blagovremeno odobravaju, povlače ili mijenjaju u skladu sa formalno definisanim procesom (engl. *approval workflow*) u koji su uključena lica koja su u skladu sa članom 10 stav 3 ove odluke utvrđena kao odgovorna za resurse kojima se pristupa;
8) se u slučaju prestanka radnog odnosa prava pristupa povlače bez odlaganja;
9) se preispitivanje dodijeljenih prava pristupa vrši najmanje jednom godišnje kako bi se obezbijedilo da korisnici tih prava ne posjeduju prevelike privilegije, i da su povučene kada im više nijesu potrebne;
10) se primjenjuju metode autentifikacije koje su u dovoljnoj mjeri robusne, i koje na adekvatan i efikasan način obezbjeđuju poštovanje politika i procedura kontrole pristupa;
11) je kompleksnost metoda za provjeru autentičnosti proporcionalna kritičnosti IT sistema, servisa i informacija kojima se pristupa što, najmanje, podrazumijeva korišćenje složenih lozinki ili kompleksinijih metoda za provjeru autentičnosti, u skladu sa procjenom rizika;
12) su prava pristupa koje IT sistemi i aplikacije koriste za elektronski pristup podacima i IT sistemima ograničena na minimalni nivo neophodan za pružanje odgovarajuće usluge ili IT servisa.

(2) Pristupom na daljinu se, u smislu ovog člana, smatra pristup koji omogućava korišćenje prava pristupa resursima informacionog sistema sa udaljene lokacije putem telekomunikacionih linija nad kojima pružalac platnih usluga nema potpunu kontrolu, odnosno nadzor.

(3) Privilegovanim pristupom se, u smislu ovog člana, smatra pristup resursima informacionog sistema koji omogućava korisnicima znatno veća prava, kao i zaobilaženje ugrađenih logičkih kontrola (na primjer, administrator mrežne opreme, baze podataka, sistemskog softvera, aplikativnog softvera i sl.).

(4) Provjerom autentičnosti se, u smislu ovog člana, smatra proces potvrde identiteta korisnika, sistema ili procesa od strane sistema.

(5) Pružalac platnih usluga je dužan da detaljno dokumentuje vrstu, sadržaj, period čuvanja, način zaštite, frekvenciju analize i način nadzora operativnih i sistemskih zapisa koji se izrađuju u skladu sa stavom 1 ovog člana.

Fizička sigurnost

Član 15

(1) Pružalac platnih usluga je dužan da internim aktima definiše i primijeni kontrole fizičke sigurnosti u cilju zaštite prostorija, računarskih centara i osjetljivih područja od neovlašćenog pristupa i opasnosti povezanih sa okolinom (statički elektricitet, visoka temperatura, požar, poplava, itd).

(2) Fizički pristup IT sistemima se mora pratiti i omogućiti samo ovlašćenim licima koja su za to adekvatno obučena, a u skladu sa njihovim zadacima i zaduženjima, i redovno preispitivati kako bi se, bez odlaganja, obezbijedilo povlačenje prava pristupa kada za njima prestane potreba.

(3) Adekvatne fizičke mjere zaštite od opasnosti povezanih sa okolinom moraju biti uspostavljene na način koji je proporcionalan važnosti zgrada i prostorija, kao i kritičnosti IT sistema koji se nalaze u njima ili operacija koje se u njima obavljaju.

(4) Pružalac platnih usluga je dužan da periodično provjerava ispravnost fizičkih mjera zaštite implementiranih u skladu sa ovim članom.

Sigurnost IT operacija

Član 16

(1) Pružalac platnih usluga je dužan da internim aktima definiše i primijeni pravila za sprečavanje pojave sigurnosnih problema u IT sistemima i IT servisima i za svođenje na najmanju mjeru negativnih uticaja koje bi ovi problemi mogli imati na pružanje IT servisa, a koja treba da obezbijede najmanje sljedeće:

1) da se vrši identifikacija i procjena tehničkih ranjivosti i da se one otklanjanju ažuriranjem softverskih komponenti (uključujući firmver i softver koji pružalac platnih usluga obezbjeđuje svojim internim i spoljnim korisnicima) primjenom kritičnih zakrpa ili kompenzacionih kontrola;
2) primjenu sigurnosno ojačane konfiguracije na svim mrežnim komponentama;

3) segmentaciju mreže kao i primjenu sistema za sprečavanje gubitka podataka i kriptovanje mrežnog saobraćaja u skladu sa klasifikacijom podataka;
4) zaštitu krajnjih mrežnih tačaka, što uključuje servere, radne stanice i prenosive uređaje;
5) da se prije odobravanja pristupa korporativnoj mreži određenim uređajima provjerava da li isti ispunjavaju definisane sigurnosne standarde pružaoca platnih usluga;
6) primjenu mehanizama za provjeru integriteta softvera, firmvera i podataka;
7) kriptovanje podataka u stanju mirovanja i tranzitu u skladu sa njihovom klasifikacijom.

(2) Pružalac platnih usluga je dužan da u kontinuitetu razmatra da li promjene u postojećem operativnom okruženju utiču na efikasnost postojećih mjera sigurnosti, zahtijevaju njihovo prilagođavanje ili uvođenje dodatnih mjera u cilju ublažavanja povezanih rizika.

(3) Promjene iz stava 2 ovog člana moraju se sprovoditi u skladu sa formalno definisanim procesom upravljanja promjenama iz člana 28 ove odluke.

Praćenje informacione sigurnosti

Član 17

(1) Pružalac platnih usluga je dužan da internim aktima definiše i primijeni pravila za kontinuirano praćenje informacione sigurnosti i otkrivanje neuobičajenih događaja koji mogu uticati na informacionu sigurnost pružaoca platnih usluga, kao i da na odgovarajući način odgovori na te događaje.

(2) U okviru procesa kontinuiranog praćenja informacione sigurnosti, pružalac platnih usluga je dužan da implementira efikasne mjere za otkrivanje fizičkih i logičkih upada i narušavanja povjerljivosti, integriteta i dostupnosti informacija.

(3) Proces kontinuiranog praćenja informacione sigurnosti obuhvata:
1) relevantne interne i spoljne činioce, uključujući poslovne i IT funkcije;
2) transakcije u cilju otkrivanja zloupotrebe pristupa od strane zaposlenih, treće strane ili drugih subjekata;
3) potencijalne interne i spoljne prijetnje.

(4) Pružalac platnih usluga je dužan da uspostavi i kontinuirano primjenjuje kontrole za otkrivanje događaja kao što su neželjeni odliv informacija, prisustvo malicioznog softvera i korišćenje softvera koji sadrži tehničke ranjivosti o kojima su informacije javno dostupne.

(5) Organizacioni dio i/ili lica odgovorna za praćenje informacione sigurnosti pružaoca platnih usluga dužni su da kontinuirano prate sigurnosne i operativne prijetnje koje bi mogle značajno da utiču na sposobnost pružaoca platnih usluga da pruža usluge, i da prate razvoj tehnologija i sigurnosnih trendova kako bi bili svjesni potencijalnih rizika.

(6) Organizacioni dio i/ili lica odgovorna za praćenje informacione sigurnosti pružaoca platnih usluga dužni su da blagovremeno izvještavaju nadležne organe pružaoca platnih usluga o redovnim i vanrednim aktivnostima sprovedenim u cilju praćenja

informacione sigurnosti, a naročito o otkrivenim događajima koji su uticali ili mogu uticati na informacionu sigurnost pružaoca platnih usluga.

Testiranje informacione sigurnosti

Član 18

(1) Pružalac platnih usluga je dužan da internim aktima definiše i primijeni pravila za testiranje informacione sigurnosti u cilju potvrde pouzdanosti i djelotvornosti implementiranih mjera informacione sigurnosti.

(2) Pravilima za testiranje informacione sigurnosti iz stava 1 ovog člana pružalac platnih usluga mora obezbijediti da testiranja:

1) sprovode lica koja nijesu uključena u razvoj mjera informacione sigurnosti i koja posjeduju dovoljno znanja, vještina i iskustva u vezi sa testiranjem tih mjera;
2) u skladu sa procjenom nivoa rizika, uključuju penetracione testove i skeniranja IT sistema u cilju pronalaženja ranjivosti.

(3) Pružalac platnih usluga je dužan da periodično ponavlja testiranje mjera informacione sigurnosti, i to najmanje jednom godišnje za sve kritične IT sisteme, odnosno najmanje jednom u tri godine za IT sisteme koji se ne smatraju kritičnim.

(4) Pružalac platnih usluga je dužan da vrši i vanredna testiranja mjera informacione sigurnosti u slučaju:

1) promjene infrastrukture i značajnih procesa i procedura;
2) promjena nastalih zbog značajnih operativnih ili sigurnosnih incidenata;
3) uvođenja novih ili značajne izmjene postojećih kritičnih aplikacija dostupnih na internetu.

(5) Pružalac platnih usluga je dužan da pravilima za testiranje informacione sigurnosti obuhvati sigurnosne mjere relevantne za:

1) platne terminale i uređaje koji se upotrebljavaju za pružanje platnih usluga;
2) platne terminale i uređaje koji se upotrebljavaju za provjeru autentičnosti korisnika platnih usluga;
3) uređaje i softver za generisanje/prijem kodova za provjeru autentičnosti, koje korisnicima platnih usluga obezbjeđuje pružalac platnih usluga.

(6) Pružalac platnih usluga je dužan da u skladu sa rezultatima sprovedenih testiranja iz ovog člana prilagodi mjere informacione sigurnosti, a u slučaju kritičnih IT sistema da to uradi bez odlaganja.

(7) Rezultati redovnih i vanrednih testiranja informacione sigurnosti pružaoca platnih usluga dio su sveobuhvatne procjene operativnih i sigurnosnih rizika povezanih sa platnim uslugama, a koju pružalac platnih usluga dostavlja Centralnoj banci u skladu sa zakonom.

Obuka i podizanje svijesti o informacionoj sigurnosti

Član 19

(1) Pružalac platnih usluga je dužan da donese, sprovodi i redovno ažurira program podizanja svijesti o informacionoj sigurnosti u skladu sa aktuelnim trendovima.

(2) Pružalac platnih usluga je dužan da obezbijedi da se, u skladu sa programom iz stava 1 ovog člana, svi zaposleni i druga lica angažovana kod pružaoca platnih usluga periodično, a najmanje jednom godišnje, obučavaju kako bi se obezbijedilo da su osposobljeni za izvršavanje svojih dužnosti i odgovornosti u skladu sa politikom i pravilima informacione sigurnosti u cilju smanjenja ljudskih grešaka, krađa, prevara, zloupotreba ili gubitaka, i da znaju kako da postupe u situacijama koje predstavljaju rizik po informacionu sigurnost pružaoca platnih usluga.

Upravljanje IT operacijama

Član 20

(1) Pružalac platnih usluga je dužan da upravlja svojim IT operacijama u skladu sa definisanim procesima opisanim u jasnim, potpunim i detaljnim procedurama.

(2) Pružalac platnih usluga dužan je da obezbijedi da je izvršavanje IT operacija usklađeno sa njegovim poslovnim zahtjevima, kao i da održava i, kada je to moguće, unaprjeđuje efikasnost IT sistema i operacija, uključujući i razmatranje načina na koji bi se na najmanju moguću mjeru svele potencijalne greške koje proizilaze iz ručnog obavljanja zadataka.

(3) Pružalac platnih usluga je dužan da vodi i redovno ažurira popis softverskih i hardverskih komponenti informacionog sistema koji sadrži osnovne informacije o njihovoj konfiguraciji i omogućava brzu identifikaciju komponenti, njihove lokacije, sigurnosne klasifikacije i vlasništva.

(4) Pružalac platnih usluga je dužan da uredno vodi dokumentaciju u kojoj je opisana međuzavisnost i povezanost različitih softverskih i hardverskih komponenti informacionog sistema, kako bi se omogućilo adekvatno upravljanje konfiguracijama i promjenama i brz odgovor na sigurnosne i operativne incidente uključujući i sajber napade.

(5) Pružalac platnih usluga je dužan da uredno vodi evidenciju o svim spoljašnjim mrežnim tačkama konekcije kroz koje treća lica eventualno mogu neovlašćeno pristupiti internom dijelu informacionog sistema pružaoca platnih usluga, kao i o svim uređajima koji imaju pristup internetu.

Upravljanje hardverskom i softverskom imovinom

Član 21

(1) Pružalac platnih usluga je dužan da upravlja hardverskom i softverskom imovinom tokom njenog životnog ciklusa, od nabavke ili razvoja do povlačenja iz upotrebe, kako bi se obezbijedilo da ta imovina u kontinuitetu ispunjava zahtjeve poslovanja i upravljanja rizicima.

(2) U okviru upravljanja imovinom iz stava 1 ovog člana, pružalac platnih usluga je dužan da obezbijedi adekvatno održavanje hardverske i softverske imovine u skladu sa preporukama proizvođača, i da umanji rizike koji proizilaze iz upotrebe imovine koja je zastarjela ili više nema podršku proizvođača.

(3) Pružalac platnih usluga je dužan da uspostavi i osmisli IT sisteme i IT servise na način koji je usklađen sa rezultatima analize uticaja na poslovanje iz člana 30 ove odluke, a kojim se obezbjeđuje dupliranje određenih kritičnih komponenti kako bi se spriječili prekidi izazvani događajima koji utiču na te komponente.

Sistemski i operativni zapisi

Član 22

(1) Pružalac platnih usluga je dužan da izrađuje, prati i obezbijedi čuvanje sistemskih i operativnih zapisa sa kritičnih IT sistema u cilju otkrivanja, analize i ispravljanja grešaka.

(2) Pružalac platnih usluga je dužan da detaljno dokumentuje vrstu, sadržaj, period čuvanja, način zaštite, učestalost analize i način nadzora operativnih i sistemskih zapisa koji se izrađuju u skladu sa stavom 1 ovog člana.

Planiranje i praćenje performansi i kapaciteta

Član 23

Pružalac platnih usluga je dužan da uspostavi proces planiranja i praćenja performansi i kapaciteta IT sistema u cilju blagovremenog sprečavanja, otkrivanja i otklanjanja značajnih problema u radu ovih sistema i nedostatka njihovog kapaciteta.

Rezervne kopije podataka

Član 24

(1) Pružalac platnih usluga je dužan da uspostavi proces upravljanja rezervnim kopijama podataka koji obuhvata postupke izrade, smještanja i testiranja rezervnih kopija podataka i restauracije podataka sa rezervnih kopija kako bi se obezbijedila dostupnost podataka u slučaju potrebe.

(2) Proces iz stava 1 ovog člana mora biti uspostavljen u skladu sa zahtjevima po pitanju oporavka, odnosno ponovnog uspostavljanja poslovanja i utvrđenom kritičnošću poslovnih procesa, podataka, IT sistema i IT servisa, kao i sprovedenom procjenom rizika.

(3) Rezervne kopije podataka moraju biti redovno ažurirane, zaštićene i smještene na primjeren način, na jednoj ili više bezbjednih lokacija, od kojih najmanje jedna mora biti dovoljno udaljena od lokacije na kojoj se nalaze izvorni podaci, kako rezervne kopije podataka ne bi bile izložene istim rizicima kojima su izloženi izvorni podaci.

(4) Pružalac platnih usluga je dužan da internim aktom utvrdi vrstu, obim, način i učestalost izrade rezervnih kopija podataka, način testiranja i način i učestalost odlaganja na udaljenu lokaciju, period čuvanja rezervnih kopija podataka, kao i način vođenja evidencije o njima.

Upravljanje incidentima i problemima

Član 25

(1) Pružalac platnih usluga je dužan da uspostavi proces upravljanja incidentima i problemima kako bi se smanjio uticaj štetnih događaja i omogućio brz i efikasan odgovor na njih, a naročito u slučaju značajnih operativnih i sigurnosnih incidenata.

(2) Pružalac platnih usluga je dužan da utvrdi kriterijume i limite na osnovu kojih će određivati da li neki događaj predstavlja operativni ili sigurnosni incident, kao i indikatore ranog upozorenja koji će omogućiti rano otkrivanje tih incidenata.

(3) Proces upravljanja incidentima i problemima obuhvata:

1) postupke za utvrđivanje, praćenje, evidentiranje, kategorizaciju i klasifikaciju incidenata po prioritetima, u skladu sa negativnim uticajem koji imaju ili mogu imati na poslovanje;
2) uloge i odgovornosti za različite incidentne situacije i kategorije incidenata;
3) postupke brzog odgovora na incidente kojima će se ublažiti negativni uticaji incidenta i obezbijediti da usluga ponovo bude operativna i sigurna;
4) postupke za utvrđivanje, analiziranje i otklanjanje osnovnih uzroka nastanka jednog ili više incidenata, kako bi se spriječilo ponavljanje istih incidenata;
5) efikasne postupke interne komunikacije, uključujući komunikaciju u vezi sa prijavljivanjem i eskalacijom incidenata na viši nivo upravljanja, kao i žalbe korisnika platnih usluga po pitanju sigurnosti, kojima se obezbjeđuje da:
   - su rukovodioci svih relevantnih organizacionih jedinica blagovremeno obaviješteni o svim incidentima koji potencijalno mogu imati visok negativni uticaj na kritične IT sisteme i servise;
   - se nadležni organi pružaoca platnih usluga, putem vanrednih izvještaja o značajnim incidentima, obavještavaju najmanje o negativnom učinku značajnih incidenata, odgovoru na te incidente i dodatnim aktivnostima koje je potrebno preduzeti zbog nastanka tih incidenata;
6) efikasne postupke spoljne komunikacije u vezi sa kritičnim poslovnim funkcijama i procesima, kojima se obezbjeđuje:
   - saradnja sa relevantnim akterima u cilju efikasnog odgovora na incidente i oporavka od tih incidenata;
   - blagovremeno i adekvatno informisanje klijenata i drugih strana u skladu sa propisima.

Upravljanje IT projektima

Član 26

(1) Pružalac platnih usluga je dužan da uspostavi proces upravljanja IT projektima koji na adekvatan način podržava sprovođenje strategije razvoja informacionog sistema iz člana 7 ove odluke.

(2) Pružalac platnih usluga je dužan da donese i primijeni politiku upravljanja IT projektima koja najmanje obuhvata:

1) ciljeve projekta;
2) uloge i odgovornosti;
3) procjenu rizika projekta;
4) plan, vremenski okvir i aktivnosti projekta;

5) ključne etape projekta (engl. *milestones*);
6) zahtjeve po pitanju upravljanja promjenama.

(3) Uloge i odgovornosti iz stava 2 tačka 2 ovog člana je potrebno definisati na način da zahtjeve po pitanju informacione sigurnosti analizira i odobrava organizacioni dio i/ili lice koje je nezavisno od organizacionog dijela i/ili lica zaduženog za razvoj IT sistema.

(4) Pružalac platnih usluga je dužan da internim aktima za upravljanje IS rizicima iz člana 8 ove odluke na adekvatan način obuhvati i rizike povezane sa IT projektima.

(5) Pružalac platnih usluga je dužan da na adekvatan način upravlja rizicima koji proizilaze iz portfolija IT projekata (upravljanje projektnim programom), naročito uzimajući u obzir rizike koji mogu proizaći iz međuzavisnosti različitih projekata i zavisnosti više različitih projekata od istih resursa i/ili ekspertiza.

(6) Pružalac platnih usluga je dužan da obezbijedi da su sva poslovna područja i funkcije na koje IT projekat utiče zastupljena u projektnom timu koji raspolaže sa znanjem potrebnim za sigurnu i uspješnu realizaciju projekta.

(7) Pružalac platnih usluga je dužan da uspostavi izvještavanje nadležnih organa pružaoca platnih usluga o redovnim i vanrednim aktivnostima u vezi sa upravljanjem IT projektima, na pojedinačnoj i zbirnoj osnovi u zavisnosti od važnosti i veličine IT projekta, a naročito o pokretanju projekta, statusu njegove realizacije i povezanim rizicima.

Nabavka i razvoj IT sistema

Član 27

(1) Pružalac platnih usluga je dužan da internim aktima, korišćenjem pristupa zasnovanog na procjeni rizika, definiše i primijeni pravila za upravljanje nabavkom, razvojem i održavanjem IT sistema, koja najmanje obezbjeđuju da su:
1) funkcionalni i nefunkcionalni zahtjevi, uključujući i zahtjeve po pitanju informacione sigurnosti, jasno definisani i odobreni od nadležnih lica prije nabavke ili razvoja IT sistema;
2) uspostavljene mjere za ublažavanje rizika od nenamjernih izmjena IT sistema i namjernog manipulisanja tim sistemima u toku njihovog razvoja i/ili stavljanja u produkcioni rad;
3) nabavljeni i razvijeni IT sistemi testirani i odobreni primjenom adekvatne metodologije, prije njihove prve upotrebe u produkciji.

(2) Pružalac platnih usluga je dužan da metodologijom za testiranje i odobravanje korišćenja IT sistema obezbijedi da:
1) je prilikom testiranja uzeta u obzir utvrđena kritičnost poslovnih procesa i ostalih relevantnih resursa informacionog sistema;
2) se testiranjem potvrđuje pouzdanost novog IT sistema, odnosno da taj sistem funkcioniše na predviđeni način;
3) se testiranje vrši na testnom okruženju koje na odgovarajući način odražava produkciono okruženje;

4) se provjerava implementacija mjera informacione sigurnosti kako bi se identifikovale moguće sigurnosne slabosti, odstupanja od propisanih pravila ili incidenti.

(3) Pružalac platnih usluga je dužan da na adekvatan način razdvoji razvojno, testno i produkciono okruženje, kako bi se omogućila segregacija dužnosti, adekvatan razvoj i testiranje.

(4) Pružalac platnih usluga je dužan da ograniči korišćenje produkcionih podataka na razvojnom, testnom i drugim neprodukcionim okruženjima i da obezbijedi integritet i povjerljivost ovih podataka na svim sistemima.

(5) Pravo pristupa produkcionim podacima se smije dodijeliti samo ovlašćenim korisnicima, nezavisno od okruženja na kojem se ti podaci nalaze.

(6) Pružalac platnih usluga je dužan da implementira mjere zaštite kojima se garantuje integritet izvornog programskog koda interno razvijenih IT sistema.

(7) Pružalac platnih usluga je dužan da uspostavi proces dokumentovanja razvoja, implementacije, rada i/ili konfiguracije IT sistema kako bi se smanjio rizik zavisnosti od stručnjaka/eksperata iz te oblasti.

(8) Dokumentacija iz stava 7 ovog člana treba da bude potpuna, tačna i redovno ažurirana i, gdje je primjenljivo, da najmanje obuhvata korisničku i tehničku dokumentaciju i operativne procedure.

(9) Odredbe ovog člana se, u skladu sa procjenom rizika, primjenjuju i na softverska rješenja kojima upravljaju ili ih razvijaju krajni interni korisnici koji nijesu angažovani u organizacionoj jedinici za IT, kao što su aplikacije za tabelarne kalkulacije i ostali alati koji omogućavaju krajnje-korisničko programiranje (engl. e*nd user computing*).

(10) Pružalac platnih usluga je dužan da vodi evidenciju aplikacija koje zadovoljavaju karakteristike navedene u stavu 9 ovog člana ukoliko te aplikacije predstavljaju podršku kritičnim poslovnim funkcijama i procesima.

Upravljanje promjenama

Član 28

(1) Pružalac platnih usluga je dužan da uspostavi proces upravljanja promjenama hardverskih i softverskih komponenti informacionog sistema kojim se obezbjeđuje da se sve promjene procjenjuju, testiraju, odobravaju, sprovode i evidentiraju na kontrolisan način i da se utvrđuju planovi vraćanja na prethodno stanje, kako bi se izbjeglo da promjene dovedu do neočekivanog i neželjenog ponašanja ovog sistema, odnosno naruše njegovu sigurnost ili funkcionalnost.

(2) Pružalac platnih usluga je dužan da obezbijedi da se promjene hardverskih i softverskih komponenti, koje se, u cilju prevazilaženja vanrednih situacija, moraju realizovati što je prije moguće, sprovode u skladu sa procedurama koje pružaju odgovarajuće mjere zaštite.

Upravljanje kontinuitetom poslovanja

Član 29

Pružalac platnih usluga je dužan da uspostavi proces upravljanja kontinuitetom poslovanja kojim se obezbjeđuje kontinuitet pružanja platnih usluga i ograničavaju gubici u slučaju ozbiljnog poremećaja ili prekida u poslovanju.

Analiza uticaja na poslovanje

Član 30

(1) U okviru procesa upravljanja kontinuitetom poslovanja iz člana 29 ove odluke, pružalac platnih usluga je dužan da periodično analizira svoju izloženost ozbiljnim poremećajima i prekidima u poslovanju i da, korišćenjem raspoloživih internih i spoljnih podataka i analize scenarija, kvalitativno i kvantitativno procijeni njihov potencijalni uticaj na poslovanje.

(2) Pružalac platnih usluga je dužan da prilikom vršenja analize uticaja na poslovanje iz stava 1 ovog člana uzme u obzir utvrđenu klasifikaciju i međusobnu povezanost poslovnih funkcija, procesa, informacione imovine, IT sistema, IT servisa, zaposlenih i spoljnih pružalaca usluga iz čl. 9 i 10 ove odluke.

(3) Na osnovu analize uticaja na poslovanje iz stava 1 ovog člana, pružalac platnih usluga formalno utvrđuje:

1) ključne/kritične poslovne aktivnosti, procese, IT sisteme i servise, uključujući i one koji su povjereni trećim stranama;
2) nivoe usluga koje je pružalac platnih usluga dužan da održava ili blagovremeno obnovi;
3) ciljna vremena oporavka (engl. *recovery time objective - RTO*), koja označavaju najduži prihvatljiv vremenski period unutar kojeg se, nakon incidenta, poslovni proces i IT sistemi i servisi koji ga podržavaju moraju oporaviti;
4) ciljne tačke oporavka (engl. *recovery point objective - RPO*), koje označavaju najduži prihvatljiv vremenski period, prije dešavanja incidenta, za koji podaci smiju biti izgubljeni.

Planiranje kontinuiteta poslovanja

Član 31

(1) Pružalac platnih usluga je dužan da na osnovu analize uticaja na poslovanje iz člana 30 ove odluke utvrdi plan kontinuiteta poslovanja (engl. *business continuity plan* - BCP).

(2) Prilikom definisanja plana kontinuiteta poslovanja iz stava 1 ovog člana, pružalac platnih usluga je dužan da koordinira te aktivnosti sa svim relevantnim internim i spoljnim akterima i uzme u obzir zavisnost od trećih strana i usluga koje pružaju.

(3) Prilikom definisanja plana kontinuiteta poslovanja iz stava 1 ovog člana, pružalac platnih usluga je dužan da uzme u obzir rizike koji bi mogli negativno uticati na njegove ciljeve po pitanju očuvanja i, po potrebi, ponovnog uspostavljanja dostupnosti, integriteta i povjerljivosti poslovnih funkcija, podržavajućih procesa, IT sistema, IT servisa i informacione imovine.

(4) Plan kontinuiteta poslovanja iz stava 1 ovog člana mora biti osmišljen na način koji omogućava pružaocu platnih usluga da adekvatno reaguje na moguće scenarije vanrednih situacija i da, nakon prekida, može ponovo uspostaviti obavljanje svojih kritičnih poslovnih aktivnosti u okviru ciljnog vremena oporavka (RTO) i ciljne tačke oporavka (RPO).

(5) Plan kontinuiteta poslovanja iz stava 1 ovog člana mora da sadrži spisak prioriteta po kojima će se postupiti u slučaju da je potrebno oporaviti više poslovnih aktivnosti.

(6) Pružalac platnih usluga je dužan da u planu kontinuiteta poslovanja iz stava 1 ovog člana razmotri niz različitih scenarija kojima bi mogao biti izložen, uključujući i ekstremne ali moguće scenarije, kao i scenario sajber napada, i opiše na koji način se u tim scenarijima obezbjeđuje kontinuitet IT sistema i servisa, kao i informaciona sigurnost pružaoca platnih usluga.

Plan oporavka informacionog sistema

Član 32

(1) Pružalac platnih usluga je dužan da na osnovu analize uticaja na poslovanje iz člana 30 ove odluke i mogućih scenarija iz člana 31 stav 6 ove odluke, razmatranjem kratkoročnih i dugoročnih ciljeva oporavka, utvrdi plan ili planove oporavka informacionog sistema (engl. *disaster recovery plan* - DRP).

(2) Planom oporavka informacionog sistema iz stava 1 ovog člana naročito se utvrđuju:

1) uslovi koji moraju biti ispunjeni za primjenu plana;
2) detaljan opis postupaka kojima se omogućava oporavak i dostupnost najmanje ključnih/kritičnih IT sistema i servisa u skladu sa definisanim zahtjevima;
3) spisak prioriteta po kojima će se postupiti u slučaju da je potrebno oporaviti više IT sistema i/ili servisa;
4) podatke o timovima koji će biti odgovorni za oporavak pojedinih IT sistema ili servisa i članovima tih timova, uključujući i njihove jasno utvrđene dužnosti i odgovornosti;
5) podatke o lokaciji za oporavak informacionog sistema;
6) podatke o ključnim pružaocima usluga.

(3) Plan iz stava 1 ovog člana mora biti usmjeren na oporavak operacija kritičnih poslovnih funkcija, procesa koji se izvršavaju u okviru tih funkcija, informacione imovine i njihovih međuzavisnosti kako bi se izbjegli negativni efekti na funkcionisanje pružalaca platnih usluga i finansijski sistem, uključujući platne sisteme i korisnike platnih usluga, i kako bi se obezbijedilo izvršenje platnih transakcija koje su na čekanju (engl. *pending*).

Testiranje, ažuriranje i dostupnost planova

Član 33

(1) Pružalac platnih usluga je dužan da redovno testira planove iz čl. 31 i 32 ove odluke i o tome sačinjava izvještaje, pri čemu se adekvatnost planova za

ključne/kritične poslovne aktivnosti, procese, IT sisteme i servise, provjerava najmanje jednom godišnje na osnovu ekstremnih, ali mogućih scenarija.

(2) Pružalac platnih usluga je dužan da testiranjem iz stava 1 ovog člana utvrdi da li može uspješno preći na alternativni način obavljanja kritičnih poslovnih aktivnosti iz okruženja predviđenog za oporavak od katastrofe (engl. *disaster recovery enviroment*), da li može takav režim rada održati dovoljno dug vremenski period i nakon toga ponovo uspostaviti uobičajen rad.

(3) Pružalac platnih usluga je dužan da redovno revidira i ažurira planove iz čl. 31 i 32 ove odluke u skladu sa iskustvima iz prethodno nastalih incidenata, rezultatima testiranja, novim utvrđenim rizicima i prijetnjama, promijenjenim ciljevima i prioritetima oporavka, poslovnim promjenama, uključujući promjene u proizvodima, aktivnostima, procesima i sistemima, promjenama u okruženju i u strategiji poslovanja.

(4) U cilju efikasnog sprovođenja planova iz čl. 31 i 32 ove odluke, pružalac platnih usluga je dužan da obezbijedi da su svi zaposleni upoznati sa svojim ulogama i odgovornostima u slučaju nastupanja vanrednih situacija i da su im ovi planovi lako dostupni u tim situacijama.

Izvještavanje i komunikacija u vanrednim situacijama

Član 34

(1) Pružalac platnih usluga je dužan da obezbijedi izvještavanje nadležnih organa pružaoca platnih usluga o aktivnostima u vezi sa svim relevantnim činjenicama koje se odnose na proces upravljanja kontinuitetom poslovanja, a naročito o testiranju planova iz čl. 31 i 32 ove odluke, analizi nedostataka utvrđenih testiranjem i značajnim promjenama u vezi sa upravljanjem kontinuitetom poslovanja.

(2) Pružalac platnih usluga je dužan da utvrdi mjere u skladu sa kojima će, u slučaju prekida poslovanja ili nastanka druge vanredne situacije, o tome informisati sve relevantne interne i spoljne aktere i održavati komunikaciju sa njima.

Upravljanje odnosom sa korisnicima platnih usluga

Član 35

(1) Pružalac platnih usluga je dužan da uspostavi i sprovodi procese za podizanje svijesti korisnika platnih usluga o sigurnosnim rizicima povezanim sa platnim uslugama usmjeravajući ih i pružajući im pomoć.

(2) Pružalac platnih usluga je dužan da pomoć i smjernice koje nudi korisnicima platnih usluga redovno ažurira u skladu sa novim prijetnjama i ranjivostima, i da o tim promjenama obavještava korisnike platnih usluga.

(3) Pružalac platnih usluga je dužan da omogući korisnicima platnih usluga da onemoguće određene platne funkcionalnosti povezane sa platnom uslugom koju im nudi, ako to dozvoljava funkcionalnost proizvoda.

(4) U slučaju kada je pružalac platnih usluga sa platiocem ugovorio limite potrošnje za platne transakcije koje se izvršavaju određenim platnim instrumentom pružalac platnih

usluga je dužan da omogući platiocu da prilagodi te limite do iznosa najvišeg ugovorenog limita.

(5) Pružalac platnih usluga je dužan da korisnicima platnih usluga ponudi mogućnost prijema upozorenja o iniciranju i/ili neuspješnim pokušajima iniciranja platnih transakcija, kako bi im omogućio da otkriju prevare ili zlonamjerno korišćenje njihovih računa.

(6) Pružalac platnih usluga je dužan da obavještava korisnike platnih usluga o promjenama sigurnosnih procedura koje utiču na te korisnike.

(7) Pružalac platnih usluga je dužan da pruži pomoć korisnicima platnih usluga u vezi sa svim pitanjima, zahtjevima za podršku i prijavama nepravilnosti ili problemima u vezi sigurnosti platnih usluga.

(8) Pružalac platnih usluga je dužan da obavijesti korisnike platnih usluga o načinu dobijanja pomoći iz stava 7 ovog člana.

III. ZAVRŠNA ODREDBA

Stupanje na snagu

Član 36

Ova odluka objaviće se u „Službenom listu Crne Gore“, a stupa na snagu danom stupanja na snagu Zakona o izmjenama i dopunama Zakona o platnom prometu („Službeni list CG“, broj 111/22).

SAVJET CENTRALNE BANKE CRNE GORE

O. br. 0101-3480-3/2023
Podgorica, 28.04.2023. godine

PREDSJEDAVAJUĆI
GUVERNER,

dr Radoje Žugić, s.r.