HNB

GUVERNER

Na temelju članka 2. stavka 2. Odluke o uvjetima za otvaranje i funkcioniranje PM računa u sustavu TARGET2-HR ("Narodne novine", br. 102/2018., 110/2019. i xxx/2021.) i članka 43. stavka 2. točke 11. Zakona o Hrvatskoj narodnoj banci ("Narodne novine", br. 75/2008., 54/2013. i 47/2020.) guverner Hrvatske narodne banke donosi

DODATAK VIII.

ODLUCI O UVJETIMA ZA OTVARANJE I FUNKCIONIRANJE PM RAČUNA U SUSTAVU TARGET2-HR

ZAHTJEVI ZA UPRAVLJANJE INFORMACIJSKOM SIGURNOSTI I NEPREKINUTIM POSLOVANJEM

1. Predmet

Ovim Dodatkom detaljno se uređuju zahtjevi za upravljanje informacijskom sigurnosti i upravljanje neprekinutim poslovanjem.

2. Upravljanje informacijskom sigurnosti

Ti se zahtjevi primjenjuju na svakog sudionika, osim ako sudionik dokaže da se određeni zahtjev na njega ne primjenjuje. Kod određivanja opsega primjene zahtjeva unutar njegove infrastrukture, sudionik bi trebao utvrditi elemente koji su dio lanca platne transakcije. Lanac platne transakcije započinje kod jedinstvene pristupne točke, odnosno sustava uključenog u kreiranje transakcija (npr. radne stanice, aplikacije za službe za izravan rad s klijentima i aplikacije za službe za pozadinske poslove, programska podrška), a završava kod sustava odgovornog za slanje poruke SWIFT-u (npr. SWIFT VPN box) ili Interneta (ovaj potonji se primjenjuje na internetski pristup).

***Zahtjev 1.1*: Politika informacijske sigurnosti**

Rukovodstvo određuje jasan smjer politike u skladu s poslovnim ciljevima i pokazuje potporu i predanost informacijskoj sigurnosti izdavanjem, odobravanjem i održavanjem politike informacijske sigurnosti čiji je cilj upravljanje informacijskom sigurnosti i kibernetičkom otpornosti u cijeloj organizaciji u smislu identifikacije, procjene i postupanja s rizicima informacijske sigurnosti i kibernetičke otpornosti. Politika bi trebala sadržavati barem sljedeće segmente: ciljevi, područje primjene (uključujući područja kao što su organizacija, ljudski resursi, upravljanje imovinom itd.), načela i raspodjela odgovornosti.

***Zahtjev 1.2*: Unutarnja organizacija**

Radi provedbe politike informacijske sigurnosti u organizaciji se uspostavlja okvir za informacijsku sigurnost. Rukovodstvo koordinira i preispituje uspostavu okvira za informacijsku sigurnost kako bi se osigurala provedba politike informacijske sigurnosti (u skladu sa Zahtjevom 1.1.) u cijeloj organizaciji, uključujući raspodjelu dostatnih sredstava i raspodjelu odgovornosti za sigurnost.

***Zahtjev 1.3*: Vanjske strane**

Sigurnost informacija organizacije i njezine opreme za obradu informacija ne bi se smjela umanjiti zbog uvođenja vanjske strane/strana ili proizvoda/usluga koje one pružaju niti bi se smjela umanjiti zbog ovisnosti o njima. Svaki pristup vanjskih strana opremi organizacije za obradu informacija mora biti kontroliran. Kada se od vanjskih strana ili proizvoda/usluga vanjskih strana zahtijeva da pristupe opremi organizacije za obradu informacija, provodi se procjena rizika kako bi se utvrdile posljedice za sigurnost i zahtjevi u pogledu kontrole. Kontrole se dogovaraju i definiraju u sporazumu sa svakom takvom vanjskom stranom.

***Zahtjev 1.4*: Upravljanje imovinom**

Sva informacijska imovina, poslovni procesi i temeljni informacijski sustavi, kao što su operativni sustavi, infrastruktura, poslovne aplikacije, gotovi proizvodi, usluge i aplikacije koje su razvili korisnici, u okviru lanca platnih transakcija moraju se evidentirati i imati vlasnika. Potrebno je raspodijeliti odgovornost za održavanje i provođenje odgovarajućih kontrola u poslovnim procesima i povezanim komponentama informacijske tehnologije za zaštitu informacijske imovine. Napomena: vlasnik prema potrebi može prenijeti ovlast za provedbu posebnih kontrola, ali ostaje odgovoran za pravilnu zaštitu imovine.

***Zahtjev 1.5*: Razvrstavanje informacijske imovine**

Informacijska imovina razvrstava se prema svojoj kritičnosti u pogledu nesmetanog pružanja usluge od strane sudionika. U razvrstavanju se navode potrebe, prioriteti i stupanj zaštite potreban pri postupanju s informacijskom imovinom u odgovarajućim poslovnim procesima, te se također uzimaju u obzir temeljne komponente informacijske tehnologije. Sustav razvrstavanja informacijske imovine koji je odobrilo rukovodstvo koristi se za utvrđivanje odgovarajućeg skupa zaštitnih kontrola tijekom životnog ciklusa informacijske imovine (uključujući uklanjanje i uništenje informacijske imovine) i za obavješćivanje o potrebi za posebnim mjerama za postupanje s njima.

***Zahtjev 1.6*: Sigurnost u pogledu ljudskih resursa**

Prije zapošljavanja se u odgovarajućim opisima radnih mjesta te u uvjetima za zapošljavanje utvrđuje odgovornost za sigurnost. Svi kandidati za zapošljavanje, izvođači radova i korisnici treće strane prolaze odgovarajuću provjeru, posebno za osjetljiva radna mjesta. Zaposlenici, izvođači radova i treće strane koji su korisnici opreme za obradu informacija potpisuju sporazum o svojim ulogama i odgovornostima u vezi sa sigurnosti. Za korisnike zaposlenike, izvođače radova i treće strane osigurava se odgovarajuća razina svijesti te im se osigurava obrazovanje i osposobljavanje o

sigurnosnim postupcima i ispravnoj upotrebi opreme za obradu informacija kako bi se mogući sigurnosni rizici sveli na najmanju moguću mjeru. Za zaposlenike se uspostavlja formalni disciplinski postupak za postupanje u vezi s povredama sigurnosnih pravila. Potrebno je uspostaviti odgovornosti kako bi se osiguralo da se upravlja odlaskom zaposlenika, izvođača radova ili korisnika koji su treće strane iz organizacije ili njihova premejštaja unutar organizacije te za provedbu vraćanja sve opreme i oduzimanje svih prava pristupa.

***Zahtjev 1.7*: Fizička sigurnost i sigurnost okoliša**

Oprema za obradu kritičnih ili osjetljivih informacija mora biti smještena u sigurnim prostorima, zaštićena definiranim sigurnosnim okvirima, s odgovarajućim sigurnosnim preprekama i kontrolama ulaska. Mora biti fizički zaštićena od neovlaštenog pristupa, oštećenja i ometanja. Pristup se odobrava samo pojedincima koji su obuhvaćeni područjem primjene zahtjeva 1.6. Potrebno je uspostaviti postupke i standarde za zaštitu fizičkih nositelja podataka koji sadržavaju informacijsku imovinu u prijevozu.

Oprema mora biti zaštićena od fizičkih prijetnji i prijetnji iz okoliša. Potrebna je zaštita opreme (uključujući opremu koja se upotrebljava izvan lokacije) i zaštita od odstranjivanja imovine kako bi se smanjio rizik od neovlaštenog pristupa informacijama i kako bi se informacije ili oprema zaštitile od gubitka ili oštećenja. Za zaštitu od fizičkih prijetnji i za zaštitu pomoćne opreme kao što je infrastruktura za opskrbu električnom energijom i kabelska infrastruktura potrebne su posebne mjere.

***Zahtjev 1.8*: Upravljanje operativnim poslovanjem**

Potrebno je utvrditi odgovornost i postupke za upravljanje i rad opreme za obradu informacija koji moraju obuhvatiti sve osnovne sustave od početka do kraja u lancu platnih transakcija.

Pri operativnim postupcima, uključujući tehničko upravljanje informacijskim sustavima, provodi se razdvajanje dužnosti, prema potrebi, kako bi se smanjio rizik od nemarne ili namjerne zlouporabe sustava. Ako se razdvajanje dužnosti ne može provesti zbog dokumentiranih objektivnih razloga, nakon formalne analize rizika provode se kompenzacijske kontrole. Kontrole se uspostavljaju kako bi se spriječilo i otkrilo uvođenje zlonamjernih kodova za sustave u lancu platnih transakcija. Uspostavljaju se i kontrole (uključujući osvješćivanje korisnika) kako bi se spriječili, otkrili i uklonili zlonamjerni kodovi. Upotrebljavaju se samo mobilni kodovi iz pouzdanih izvora (npr. potpisane komponente Microsoft COM i Java Applets). Konfiguraciju preglednika (npr. upotrebu produžetka i priključaka) potrebno je dosljedno nadzirati.

Rukovodstvo će provesti politiku sigurnosnog kopiranja i obnavljanja podataka; te politike obnavljanja moraju uključivati plan obnavljanja koji se redovno preispituje najmanje jednom godišnje.

Potrebno je nadzirati sustave koji su kritični za sigurnost plaćanja i evidentirati događaje koji su važni za informacijsku sigurnost. Kako bi se osiguralo utvrđivanje problema u informacijskom sustavu

koristi se evidencija operatera. Evidencija operatera redovito se preispituje na temelju uzorka u pogledu kritičnosti operacija. Koristi se praćenje sustava za provjeru učinkovitosti kontrola koje su utvrđene kao kritične za sigurnost plaćanja i za provjeru usklađenosti s modelom politike pristupa.

Razmjene informacija između organizacija temelje se na politici formalne razmjene koja se provodi u skladu sa sporazumima o razmjeni između uključenih strana i u skladu je sa svim relevantnim zakonodavstvom. Sofverske komponente treće strane koje se koriste u razmjeni informacija sa sustavom TARGET2 (kao što je softver primljen od ponuditelja usluga (*Service Bureau)* u 2. scenariju odjeljka o području primjene dokumenta za uređivanje samocertifikacije sustava TARGET2) moraju se koristiti u skladu s formalnim sporazumom s trećom stranom.

***Zahtjev 1.9*: Kontrola pristupa**

Pristup informacijskoj imovini opravdava se na temelju poslovnih zahtjeva (potreba pristupa podatcima[1]) i u skladu s uspostavljenim okvirom korporativnih politika (uključujući politiku informacijske sigurnosti). Potrebno je definirati jasna pravila kontrole pristupa na temelju načela najmanje povlastice[2] kako bi se u velikoj mjeri poštovale potrebe odgovarajućih poslovnih i informatičkih procesa. Prema potrebi, logička kontrola pristupa (npr. za upravljanje sigurnosnim kopijama) trebala bi biti u skladu s kontrolom fizičkog pristupa, osim ako su uspostavljene odgovarajuće zamjenske kontrole (npr. enkripcija, anonimizacija osobnih podataka).

Potrebno je uspostaviti formalne i dokumentirane postupke za kontrolu dodjele prava pristupa informacijskim sustavima i uslugama koji su obuhvaćeni područjem primjene lanca platnih transakcija. Postupci obuhvaćaju sve faze životnog ciklusa pristupa korisnika, od početne registracije novih korisnika do konačne odjave korisnika kojima više nije potreban pristup.

Posebna pozornost posvećuje se, prema potrebi, dodjeli prava pristupa takve kritičnosti da bi zlouporaba tih prava pristupa mogla dovesti do ozbiljnog nepovoljnog učinka na poslovanje sudionika (npr. prava pristupa koja dozvoljavaju upravljanje sustavom, poništavanje kontrola sustava, izravan pristup poslovnim podacima).

Uspostavljaju se odgovarajuće kontrole za identifikaciju, autentikaciju i ovlašćivanje korisnika na određenim točkama mreže organizacije, npr. za lokalni pristup i pristup s udaljenosti sustavima u lancu platnih transakcija. Osobni računi se ne smiju dijeliti kako bi se osiguralo preuzimanje odgovornosti.

---

1 Načelo nužnosti pristupa informacijama odnosi se na utvrđivanje skupa informacija kojima pojedinac treba pristupiti kako bi mogao obavljati svoje dužnosti.

2 Načelo najmanje povlastice odnosi se na prilagodbu pristupnog profila ispitanika IT sustavu kako bi odgovarao odgovarajućoj poslovnoj ulozi.

Za lozinke se utvrđuju pravila i provode se posebne kontrole kako bi se osiguralo da se lozinke ne mogu lako pogoditi, npr. pravila o složenosti i vremenskom ograničenju valjanosti. Uspostavlja se siguran protokol za vraćanje lozinke i/ili ponovno postavljanje lozinke.

Razvija se i provodi politika o uporabi kriptografskih kontrola radi zaštite povjerljivosti, autentičnosti i cjelovitosti informacija. Uspostavlja se politika upravljanja ključevima kako bi se podržala upotreba kriptografskih kontrola.

Potrebno je uspostaviti politiku za pregledavanje povjerljivih informacija na zaslonu ili u tiskanom obliku (npr. politika praznog zaslona ili praznog stola) kako bi se smanjio rizik od neovlaštenog pristupa.

Pri radu na daljinu uzimaju se u obzir rizici u vezi s radom u nezaštićenom okruženju te se provode odgovarajuće tehničke i organizacijske kontrole.

***Zahtjev 1.10*: Nabava, razvoj i održavanje informacijskih sustava**

Sigurnosni zahtjevi utvrđuju se i dogovaraju prije razvoja i/ili uvođenja informacijskih sustava.

Kako bi se osigurala pravilna obrada potrebno je u aplikacije, uključujući aplikacije koje su razvili korisnici, ugraditi odgovarajuće kontrole. Te kontrole uključuju validaciju ulaznih podataka, unutarnje obrade i izlaznih podataka. Za sustave koji obrađuju osjetljive, vrijedne ili kritične informacije ili utječu na njih potrebne su dodatne kontrole. Takve se kontrole utvrđuju na temelju sigurnosnih zahtjeva i procjene rizika u skladu s utvrđenim politikama (npr. politika informacijske sigurnosti, politika kriptografskih kontrola).

Prije prihvaćanja i uporabe novih sustava utvrđuju se, dokumentiraju i ispituju njihovi operativni zahtjevi. Što se tiče sigurnosti mreže, trebalo bi provesti odgovarajuće kontrole, uključujući segmentaciju i sigurno upravljanje, na temelju kritičnosti protoka podataka i razine rizika mrežnih područja u organizaciji. Potrebno je uspostaviti posebne kontrole za zaštitu osjetljivih informacija koje se prenose preko javnih mreža.

Pristup sistemskim datotekama i programskom izvornom kodu se kontrolira, a projekti na području informacijske tehnologije i aktivnosti potpore provode se na siguran način. Treba paziti da se izbjegne izlaganje osjetljivih podataka u testnim okruženjima. Projektna i potporna okruženja strogo se nadziru. Uvođenje promjena u produkciju strogo se nadzire. Provodi se procjena rizika značajnih promjena koje će se uvesti u produkciju.

Redovite aktivnosti ispitivanja sigurnosti sustava u produkciji provode se i u skladu s unaprijed definiranim planom koji se temelji na rezultatima procjene rizika, a testiranje sigurnosti uključuje barem procjene ranjivosti. Ocjenjuju se svi nedostaci ustanovljeni tijekom testiranja sigurnosti, a akcijski planovi za uklanjanje svih utvrđenih nedostataka moraju se pravodobno pripremiti i pratiti.

***Zahtjev 1.11*: Informacijska sigurnost u odnosima s dobavljačima**[3]

Kako bi se osigurala zaštita internih informacijskih sustava sudionika, koji su dostupni dobavljačima, potrebno je dokumentirati zahtjeve u pogledu informacijske sigurnosti za ublažavanje rizika povezanih s pristupom dobavljača te se o njima sporazumjeti s dobavljačem.

***Zahtjev 1.12*: Upravljanje incidentima u području informacijske sigurnosti i poboljšanja**

Kako bi se osigurao dosljedan i učinkovit pristup upravljanju incidentima povezanima s informacijskom sigurnosti, uključujući komunikaciju o sigurnosnim događajima i slabostima, uspostavljaju se i testiraju uloge, odgovornosti i postupci na poslovnoj i tehničkoj razini kako bi se osigurao brz, učinkovit te uredan i siguran oporavak od incidenata u vezi s informacijskom sigurnosti, uključujući scenarije povezane s uzrokom povezanim s kibernetičkom sigurnošću (npr. prijevara koju je počinio vanjski napadač ili unutarnji subjekt). Osoblje uključeno u te postupke mora biti odgovarajuće osposobljeno.

***Zahtjev 1.13*: Pregled tehničke usklađenosti**

Unutarnji informacijski sustavi sudionika (npr. sustavi jedinica za pozadinske poslove, unutarnje mreže i povezivost s vanjskim mrežama) redovito se procjenjuje u pogledu usklađenosti s uspostavljenim okvirom politika organizacije (npr. politika informacijske sigurnosti, politika kriptografskog nadzora).

***Zahtjev 1.14*: Virtualizacija**

Gostujuća virtualna računala moraju biti u skladu sa svim sigurnosnim kontrolama koje su postavljene za fizičku strojnu opremu i sustave (npr. očvrsnuće, evidentiranje). Kontrole koje se odnose na hipervizore moraju uključivati: očvršćivanje hipervizora i operativne sustave domaćina, redovne popravke, jasno odvajanje različitih okruženja (npr. produkcija i razvoj). Centralizirano upravljanje, evidentiranje i praćenje te upravljanje pravima pristupa, posebno za visoko povlaštene račune provodi se na temelju procjene rizika. Gostujući virtualni strojevi kojima upravlja isti hipervizor moraju imati sličan profil rizičnosti.

***Zahtjev 1.15*: Računalstvo u oblaku**

3 Dobavljača u kontekstu ove vježbe treba se shvatiti kao svaku treću stranu (i njezino osoblje) koja je pod ugovorom (sporazumom) s institucijom da pruži uslugu, a u skladu sa sporazumom o uslugama treća strana (i njezino osoblje) ima pristup, na daljinu ili na licu mjesta, informacijama i/ili informacijskim sustavima i/ili opremi za obradu informacija institucije u opsegu područja primjene obuhvaćenom izvršavanjem samocertifikacije u sustavu TARGET2 ili su s njim povezani.

Upotreba javnih i/ili hibridnih rješenja u oblaku u lancu platnih transakcija mora se temeljiti na formalnoj procjeni rizika, uzimajući u obzir tehničke kontrole i ugovorne klauzule povezane s rješenjem računalstva u oblaku.

Ako se upotrebljavaju hibridna rješenja u oblaku, podrazumijeva se da je razina kritičnosti cjelokupnog sustava jednaka najvišoj razini kritičnosti nekog od povezanih sustava. Sve lokalne komponente hibridnih rješenja potrebno je odvojiti od ostalih sustava na lokaciji.

3. Upravljanje neprekinutim poslovanjem

Sljedeći zahtjevi (od 2.1. do 2.6.) odnose se na upravljanje neprekinutim poslovanjem. Svaki sudionik sustava TARGET2 kojeg je Eurosustav razvrstao kao kritičnog za nesmetano funkcioniranje sustava TARGET2 mora imati uspostavljenu strategiju neprekinutog poslovanja koja obuhvaća sljedeće elemente:

Zahtjev 2.1:

Izradit će se planovi neprekinutog poslovanja i uspostaviti postupci za njihovo održavanje.

Zahtjev 2.2:

Zamjenska operativna lokacija bit će dostupna.

Zahtjev 2.3:

Profil rizičnosti zamjenske lokacije razlikovat će se od profila rizičnosti primarne lokacije kako bi se izbjeglo da na obje lokacije istodobno utječe isti događaj. Na primjer, zamjenska lokacija bit će priključena na električnu mrežu i središnju telekomunikacijsku mrežu različitu od one na primarnoj poslovnoj lokaciji.

Zahtjev 2.4:

U slučaju većih poremećaja u radu zbog kojih primarna lokacija nije dostupna i/ili kritično osoblje nije na raspolaganju, kritični sudionik moći će nastaviti s uobičajenim operacijama sa zamjenske lokacije gdje će biti moguće pravilno završiti radni dan i započeti sljedeći radni dan (sljedeće radne dane).

Zahtjev 2.5:

Uspostavit će se postupci kojima se osigurava da se obrada transakcija nastavi sa zamjenske lokacije u razumnom roku nakon početnog prekida usluge i razmjerno kritičnosti poslovanja koje je prekinuto.

Zahtjev 2.6:

Sposobnost suočavanja s prekidima rada ispitat će se najmanje jednom godišnje, a kritično osoblje će biti na dogovarajući način će osposobljeno. Najdulje razdoblje između ispitivanja ne smije biti dulje od jedne godine.

4. Stupanje na snagu i objava

Ovaj Dodatak objavljuje se na mrežnim stranicama Hrvatske narodne banke, a stupa na snagu sljedećeg dana od dana objave.

O. br.: 311-091/11-21/BV

Zagreb, 24. studenoga 2021.

G U V E R N E R

HRVATSKE NARODNE BANKE

Boris Vujčić