7/2021
Rozhodnutie
Národnej banky Slovenska
z 9. novembra 2021,

ktorým sa mení a dopĺňa rozhodnutie Národnej banky Slovenska č. 7/2015 o podmienkach otvorenia a vedenia PM účtu v TARGET2-SK v znení neskorších predpisov

Národná banka Slovenska podľa § 6 ods. 2 písm. g) zákona Národnej rady Slovenskej republiky č. 566/1992 Zb. o Národnej banke Slovenska v znení neskorších predpisov a podľa § 45 ods. 1 zákona č. 492/2009 Z. z. o platobných službách a o zmene a doplnení niektorých zákonov rozhodla:

Čl. I

Rozhodnutie Národnej banky Slovenska č. 7/2015 z 9. júna 2015 o podmienkach otvorenia a vedenia PM účtu v TARGET2-SK v znení rozhodnutia NBS č. 9/2016, rozhodnutia NBS č. 13/2017, rozhodnutia NBS č. 11/2018 a rozhodnutia NBS č. 21/2019 sa mení a dopĺňa takto:

1. V § 2 odsek 41 znie:
„(41) Príkazom sa rozumie príkaz na úhradu, príkaz na prevod likvidity, príkaz na inkaso, príkaz na prevod likvidity z PM účtu na T2S DCA účet, príkaz na prevod likvidity z T2S DCA účtu na PM účet, príkaz na prevod likvidity z T2S DCA účtu na T2S DCA účet, príkaz na prevod likvidity z PM účtu na TIPS DCA účet, príkaz na prevod likvidity z TIPS DCA účtu na PM účet, príkaz na prevod likvidity z technického účtu TIPS AS na TIPS DCA účet, príkaz na prevod likvidity z TIPS DCA účtu na technický účet TIPS AS, príkaz na okamžitú platbu alebo kladná odpoveď na storno.“.

2. Poznámka pod čiarou k odkazu 8 znie:
„[8]) Nariadenie Komisie (ES) č. 1126/2008 z 3. novembra 2008, ktorým sa v súlade s nariadením Európskeho parlamentu a Rady (ES) č. 1606/2002 prijímajú určité medzinárodné účtovné štandardy (Ú. v. EÚ L 320, 29.11.2008) v platnom znení.“.

3. V § 2 sa vypúšťa odsek 69.

Doterajšie odseky 70 až 78 sa označujú ako odseky 69 až 77.

4. V § 2 odsek 72 znie:
„(72) Príkazom na okamžitú platbu sa v súlade so systémom okamžitých úhrad SEPA (ďalej len „systém SCT Inst“) Európskej platobnej rady rozumie platobný pokyn, ktorý možno vykonať 24 hodín denne v ktorýkoľvek kalendárny deň v roku s okamžitým alebo takmer okamžitým spracovaním a oznámením platiteľovi a ktorý zahŕňa
a) príkazy na okamžitú platbu z TIPS DCA účtu na TIPS DCA účet,
b) príkazy na okamžitú platbu z TIPS DCA účtu na technický účet TIPS AS,
c) príkazy na okamžitú platbu z technického účtu TIPS AS na TIPS DCA účet,
d) príkazy na okamžitú platbu z technického účtu TIPS AS na technický účet TIPS AS.“.

5. § 2 sa dopĺňa odsekmi 78 až 82, ktoré znejú:

„(78) Systémom SCT Inst Európskej platobnej rady alebo systémom SCT Inst sa rozumie automatizovaný systém otvorených štandardov, ktorý stanovuje súbor medzibankových pravidiel, ktoré majú dodržiavať účastníci systému SCT Inst a ktorý umožňuje poskytovateľom platobných služieb v SEPA ponúkať automatizovaný produkt okamžitých úhrad v eurách v rámci SEPA.

(79) Technickým účtom TIPS AS sa rozumie účet, ktorého majiteľom je pridružený systém alebo centrálna banka, ktorá ho vedie v mene pridruženého systému v systéme centrálnej banky, ktorý je súčasťou TARGET2 a pridružený systém ho používa na účely vyrovnania okamžitých platieb vo svojich účtovných knihách.

(80) Príkazom na prevod likvidity z TIPS DCA účtu na technický účet TIPS AS sa rozumie pokyn na prevod určitej sumy peňažných prostriedkov z TIPS DCA účtu na technický účet TIPS AS s cieľom zvýšiť krytie pozície majiteľa TIPS DCA alebo pozície iného účastníka pridruženého systému v účtovných knihách pridruženého systému.

(81) Príkazom na prevod likvidity z technického účtu TIPS AS na TIPS DCA účet sa rozumie pokyn na prevod určitej sumy peňažných prostriedkov z technického účtu TIPS AS na TIPS DCA účet s cieľom znížiť krytie pozície majiteľa TIPS DCA účtu alebo pozície iného účastníka pridruženého systému v účtovných knihách pridruženého systému.

(82) Dostupnou stranou sa rozumie subjekt, ktorý

a) je držiteľom BIC,
b) je určený ako dostupná strana majiteľom TIPS DCA účtu alebo pridruženým systémom,
c) je korešpondentom, klientom alebo pobočkou majiteľa TIPS DCA účtu alebo je účastníkom pridruženého systému, alebo korešpondentom, klientom alebo pobočkou účastníka pridruženého systému a
d) je adresovateľný prostredníctvom platformy TIPS a je schopný zadávať príkazy na okamžitú platbu a prijímať príkazy na okamžitú platbu buď prostredníctvom majiteľa TIPS DCA účtu alebo pridruženého systému alebo priamo, ak mu to povolil majiteľ TIPS DCA účtu alebo pridružený systém.“.

6. V § 3 ods. 1 písmeno i) znie:

„i) príkazy na prevod likvidity z TIPS DCA účtu na PM účet a príkazy na prevod likvidity z PM účtu na TIPS DCA účet,“.

7. V § 3 ods. 1 sa za písmeno i) vkladá nové písmeno j), ktoré znie:

„j) príkazy na prevod likvidity z TIPS DCA účtu na technický účet TIPS AS a príkazy na prevod likvidity z technického účtu TIPS AS na TIPS DCA účet a“.

Doterajšie písmeno j) sa označuje ako písmeno k).

8. V § 3 odsek 2 znie:

„(2) TARGET2 umožňuje v rámci PM účtov, T2S DCA účtov a TIPS DCA účtov hrubé vyrovnanie platieb v reálnom čase v eurách s vyrovnaním v peniazoch centrálnej banky. TARGET2 je vytvorený a funguje na základe SSP, cez ktoré sa technicky

rovnakým spôsobom zadávajú a spracúvajú príkazy a nakoniec aj prijímajú platby. Pokiaľ ide o technické vedenie T2S DCA účtov, TARGET2 je po technickej stránke vytvorený a funguje na základe platformy T2S. Pokiaľ ide o technické vedenie TIPS DCA účtov a technických účtov TIPS AS, TARGET2 je po technickej stránke vytvorený a funguje na základe platformy TIPS.“.

9. § 5 vrátane nadpisu znie:

„§ 5
Priamy účastník

(1) Majiteľ PM účtu v TARGET2-SK je priamym účastníkom a musí spĺňať požiadavky podľa § 8 ods. 1 a 3. Musí mať aspoň jeden PM účet v Národnej banke Slovenska. Majiteľ PM účtu, ktorý pristúpil k uplatňovaniu systému SCT Inst podpísaním dohody o uplatňovaní systému okamžitých úhrad SEPA, je a zostane neustále dostupný v rámci platformy TIPS, a to buď ako majiteľ TIPS DCA účtu alebo ako dostupná strana prostredníctvom majiteľa TIPS DCA účtu.

(2) Majiteľ PM účtu môže určiť adresovateľného držiteľa BIC bez ohľadu na miesto jeho sídla. Majiteľ PM účtu môže určiť adresovateľného držiteľa BIC, ktorý pristúpil k uplatňovaniu systému SCT Inst podpísaním dohody o uplatňovaní systému okamžitých úhrad SEPA, iba ak tento subjekt je a zostane dostupný v rámci platformy TIPS, a to buď ako majiteľ TIPS DCA účtu alebo ako dostupná strana prostredníctvom majiteľa TIPS DCA účtu.

(3) Majiteľ PM účtu môže určiť subjekt za nepriameho účastníka v PM za predpokladu, že sú splnené podmienky podľa § 6. Majiteľ PM účtu môže za nepriameho účastníka určiť subjekt, ktorý pristúpil k uplatňovaniu systému SCT Inst podpísaním dohody o uplatňovaní systému okamžitých úhrad SEPA, iba ak tento subjekt je a zostane dostupný v rámci platformy TIPS, a to buď ako majiteľ TIPS DCA účtu v Národnej banke Slovenska alebo ako dostupná strana prostredníctvom majiteľa TIPS DCA účtu.

(4) Multi-adresný prístup prostredníctvom pobočiek možno poskytnúť takto:

a) subjekt podľa § 4 ods. 1 písm. a) alebo b), ktorý bol uznaný za majiteľa PM účtu, môže udeliť prístup k svojmu PM účtu jednej alebo viacerým svojim pobočkám v Európskej únii alebo v Európskom hospodárskom priestore, aby priamo zadávali príkazy alebo prijímali platby, za predpokladu, že Národná banka Slovenska bola zodpovedajúcim spôsobom informovaná,
b) ak bola pobočka banky uznaná za majiteľa PM účtu, ostatné pobočky toho istého právneho subjektu alebo jeho ústredie podľa § 4 ods. 1 písm. a), môžu mať prístup k PM účtu tejto pobočky za predpokladu, že informovali Národnú banku Slovenska.“.

10. V § 12 odsek 2 znie:

„(2) PM účty a ich podúčty sa úročia percentom nula alebo úrokovou sadzbou pre jednodňové sterilizačné operácie podľa toho, ktorá z týchto sadzieb je nižšia a ak sa PM účty a ich podúčty nepoužívajú na udržiavanie povinných minimálnych rezerv alebo prebytočných rezerv. Ak sa PM účty a ich podúčty používajú na udržiavanie povinných minimálnych rezerv alebo prebytočných rezerv, výpočet a platba za udržiavanie povinných

minimálnych rezerv alebo prebytočných rezerv sú upravené vo forme odmeny osobitnými predpismi.[16])“.

Poznámka pod čiarou k odkazu 16 znie:

„[16]) Nariadenie Rady (ES) č. 2531/98 z 23. novembra 1998, ktoré sa týka uplatnenia minimálnych rezerv Európskou centrálnou bankou (Ú. v. ES L 318, 27.11.1998) v platnom znení, nariadenie Európskej centrálnej banky (EÚ) 2021/378 z 22. januára 2021 o uplatňovaní požiadaviek na povinné minimálne rezervy (prepracované znenie) (ECB/2021/1) (Ú. v. EÚ L 73, 3.3.2021) a rozhodnutie Európskej centrálnej banky (EÚ) 2019/1743 z 15. októbra 2019 o úročení prebytočných rezerv a niektorých vkladov (prepracované znenie) (ECB/2019/31) (Ú. v. EÚ L 267, 21.10.2019) v platnom znení.“.

11. V § 29 odsek 5 znie:

„(5) Účastníci poskytnú Národnej banke Slovenska

a) trvalý prístup k svojmu potvrdeniu o splnení požiadaviek nimi zvoleného poskytovateľa sieťových služieb na bezpečnosť koncového bodu,
b) každoročne vyhlásenie o vlastnej certifikácii pre TARGET2, ktoré je v anglickom jazyku uverejnené na internetovej stránke Národnej banky Slovenska a internetovej stránke ECB.“.

12. V § 29 sa za odsek 5 vkladajú nové odseky 6 až 11, ktoré znejú:

„(6) Národná banka Slovenska posúdi vyhlásenie účastníka o vlastnej certifikácii týkajúcej sa úrovne súladu s každou z požiadaviek stanovených v požiadavkách na vlastnú certifikáciu pre TARGET2 podľa prílohy č. 10.

(7) Úroveň súladu účastníka s požiadavkami na vlastnú certifikáciu pre TARGET2 sa kategorizuje vo vzostupnom poradí závažnosti takto: „úplný súlad“, „menej závažný nesúlad“ alebo „závažný nesúlad“. Úplný súlad sa dosiahne, ak účastníci spĺňajú 100 % požiadaviek; k menej závažnému nesúladu dochádza vtedy, keď účastník spĺňa menej ako 100 %, ale nie menej ako 66 % požiadaviek, a k závažnému nesúladu dochádza vtedy, ak účastník spĺňa menej ako 66 % požiadaviek. Ak účastník preukáže, že sa naňho určitá požiadavka nevzťahuje, na účely kategorizácie sa to považuje za splnenie príslušnej požiadavky. Účastník, ktorý nedosahuje „úplný súlad“, predloží akčný plán, v ktorom preukáže, ako zamýšľa dosiahnuť úplný súlad. Národná banka Slovenska informuje príslušné orgány dohľadu o stave plnenia požiadaviek takýmto účastníkom.

(8) Ak účastník odmietne poskytnúť trvalý prístup k svojmu potvrdeniu o splnení požiadaviek ním zvoleného poskytovateľa sieťových služieb na bezpečnosť koncového bodu, alebo neposkytne vlastnú certifikáciu pre TARGET2, úroveň súladu účastníka sa kategorizuje ako „závažný nesúlad“.

(9) Národná banka Slovenska každoročne opätovne posúdi úroveň súladu účastníkov.

(10) Národná banka Slovenska môže účastníkom, ktorých úroveň súladu bola posúdená ako menej závažný nesúlad alebo závažný nesúlad, uložiť tieto nápravné opatrenia vo vzostupnom poradí podľa závažnosti:

a) posilnené monitorovanie: účastník predkladá Národnej banke Slovenska mesačnú správu o pokroku pri riešení nesúladu, ktorú podpisuje riadiaci pracovník účastníka.

Účastníkovi sa za každý dotknutý účet dodatočne uloží mesačný sankčný poplatok, ktorý sa rovná jeho mesačnému poplatku stanovenému v prvom bode odseku 1 prílohy č. 6 bez transakčných poplatkov. Toto nápravné opatrenie sa môže uložiť v prípade, že úroveň súladu účastníka bola dvakrát po sebe posúdená ako menej závažný nesúlad alebo bola posúdená ako závažný nesúlad,

b) pozastavenie účasti: účasť účastníka v TARGET2-SK môže byť pozastavená podľa § 35 ods. 2 písm. b) a c). Odchylne od § 35 sa na takéto pozastavenie účasti účastníka vzťahuje výpovedná doba 3 mesiace. Účastníkovi sa za každý pozastavený účet uloží mesačný sankčný poplatok vo výške, ktorá predstavuje dvojnásobok jeho mesačného poplatku stanoveného v prvom bode odseku 1 prílohy č. 6 bez transakčných poplatkov. Toto nápravné opatrenie sa môže uložiť v prípade, že úroveň súladu účastníka bola dvakrát po sebe posúdená ako závažný nesúlad,

c) ukončenie účasti: účasť účastníka v TARGET2-SK môže byť ukončená podľa § 35 ods. 2 písm. b) a c). Odchylne od § 35 sa na takéto ukončenie účasti účastníka vzťahuje výpovedná doba 3 mesiace. Účastníkovi sa uloží dodatočný sankčný poplatok vo výške 1 000 eur za každý zrušený účet. Toto nápravné opatrenie môže byť uložené, ak účastník do troch mesiacov od pozastavenia jeho účasti neučinil nápravu, ktorú Národná banka Slovenska považuje za dostatočnú.

(11) Účastníci, ktorí využívajú prístup prostredníctvom internetu, poskytnú Národnej banke Slovenska ich vlastné osvedčenie pre TARGET2.“.

Doterajší odsek 6 sa označuje ako odsek 12.

13. V § 29 ods. 12 sa slová „v odsekoch 1 až 5“ nahrádzajú slovami „v odsekoch 1 až 11“.

14. V § 40 odsek 1 znie:

„(1) Účastníci sú povinní dodržiavať právne predpisy, ktoré upravujú ochranu údajov, a tieto povinnosti si plnia a sú schopní preukázať ich plnenie dotknutým príslušným orgánom. Účastníci sú povinní dodržiavať právne predpisy, ktoré upravujú predchádzanie praniu špinavých peňazí, financovanie terorizmu, činnosti v jadrovej oblasti citlivé z hľadiska šírenia jadrových zbraní a vývoja nosičov jadrových zbraní, a tieto povinnosti si plnia, najmä pokiaľ ide o implementáciu zodpovedajúcich opatrení týkajúcich sa platieb zaúčtovaných na ťarchu alebo pripísaných v prospech ich PM účtov. Účastníci sa oboznámia s politikou obnovenia údajov poskytovateľa sieťových služieb predtým, ako uzavrú zmluvný vzťah s poskytovateľom sieťových služieb. Pred uzavretím zmluvného vzťahu s poskytovateľom internetových služieb sa účastníci, ktorí využívajú prístup prostredníctvom internetu, oboznámia s politikou obnovenia údajov poskytovateľa internetových služieb.“.

15. Za § 45 sa vkladá § 45a, ktorý vrátane nadpisu znie:

„§ 45a
Prechodné ustanovenia

(1) Po uvedení systému TARGET do prevádzky a po ukončení prevádzky systému TARGET2 sa zostatky na PM účtoch v systéme TARGET2 prevedú na príslušné nástupnícke účty majiteľa účtu v systéme TARGET.

(2) Požiadavka, aby majitelia PM účtov, nepriami účastníci a adresovateľní držitelia BIC, ktorí uplatňujú systém SCT Inst boli dostupní v rámci platformy TIPS podľa § 5, sa uplatňuje od 25. februára 2022.“.

16. V prílohe č. 1 ôsmom bode ods. 4 písm. b) sa vypúšťajú slová „a JavaScript“.

17. V prílohe č. 4 šiestom bode v písm. h) sa slová „dodatočný zábezpeka“ nahrádzajú slovami „akceptovateľné aktíva ako kolaterál“.

18. Rozhodnutie NBS sa dopĺňa prílohou č. 10, ktorá vrátane nadpisu znie:

„Príloha č. 10 k rozhodnutiu NBS č. 7/2015

POŽIADAVKY NA RIADENIE BEZPEČNOSTI INFORMÁCIÍ A RIADENIE KONTINUITY ČINNOSTÍ

Riadenie bezpečnosti informácií
Tieto požiadavky sa vzťahujú na každého účastníka, pokiaľ účastník nepreukáže, že sa naňho určitá požiadavka nevzťahuje. Pri stanovovaní rozsahu uplatňovania požiadaviek v rámci svojej infraštruktúry by mal účastník identifikovať prvky, ktoré sú súčasťou celého reťazca platobných transakcií. Reťazec platobných transakcií začína na prístupovom mieste, t. j. v systéme, ktorý sa podieľa na vytváraní transakcií (napr. pracovné stanice, aplikácie front-office a back-office, middleware), a končí v systéme zodpovednom za odosielanie správy do SWIFT (napr. SWIFT VPN Box) alebo do internetu (v tomto prípade ide o internetový prístup).

Požiadavka 1.1: Politika bezpečnosti informácií
Manažment stanoví jasné smerovanie politiky v súlade s obchodnými cieľmi a preukáže podporu a odhodlanie v oblasti bezpečnosti informácií prostredníctvom vydávania, schvaľovania a udržiavania politiky bezpečnosti informácií zameranej na riadenie bezpečnosti informácií a kybernetickej odolnosti v celej organizácii, pokiaľ ide o identifikáciu, posudzovanie a riešenie rizík v oblasti bezpečnosti informácií a kybernetickej odolnosti. Táto politika by mala obsahovať aspoň tieto časti: ciele, rozsah pôsobnosti (vrátane oblastí, ako sú organizácia, ľudské zdroje, správa aktív atď.), zásady a rozdelenie zodpovedností.

Požiadavka 1.2: Vnútorná organizácia
Zavedie sa rámec pre bezpečnosť informácií na vykonávanie politiky bezpečnosti informácií v rámci organizácie. Manažment koordinuje a preskúmava zavedenie rámca pre bezpečnosť informácií s cieľom zabezpečiť vykonávanie politiky bezpečnosti informácií (v zmysle požiadavky 1.1) v celej organizácii vrátane poskytnutia dostatočných zdrojov a pridelenia povinností týkajúcich sa bezpečnosti na tento účel.

Požiadavka 1.3: Externé subjekty
Bezpečnosť údajov organizácie a jej zariadení na spracovanie údajov by sa nemala znížiť zapojením externých subjektov alebo zavedením produktov alebo služieb, ktoré tieto subjekty poskytujú alebo závislosťou na nich. Prístup externých subjektov k zariadeniam organizácie na spracovanie údajov podlieha kontrole. Ak sa od externých subjektov alebo ich produktov alebo služieb vyžaduje prístup k zariadeniam organizácie na spracovanie

údajov, vykoná sa posúdenie rizika s cieľom určiť dopad na bezpečnosť a požiadavky na kontrolu. Kontroly sa dohodnú a vymedzia v dohode s každým dotknutým externým subjektom.

Požiadavka 1.4: Správa aktív
Všetky informačné aktíva, obchodné postupy a príslušné informačné systémy ako sú operačné systémy, infraštruktúry, obchodné aplikácie, bežne dostupné produkty, služby a aplikácie vyvinuté užívateľmi v rámci reťazca platobných transakcií sa musia zaevidovať a musia mať určeného vlastníka. Je potrebné stanoviť zodpovednosť za údržbu a prevádzku primeraných kontrolných mechanizmov v obchodných postupoch a súvisiacich zložiek informačných technológií na účely ochrany informačných aktív. Poznámka: vlastník môže podľa potreby delegovať vykonávanie určitých kontrol, ale naďalej zodpovedá za náležitú ochranu aktív.

Požiadavka 1.5: Klasifikácia informačných aktív
Informačné aktíva sa klasifikujú z hľadiska ich kritického významu pre bezproblémové poskytovanie služby účastníkom. V rámci klasifikácie sa uvádza potreba, priority a stupeň ochrany požadované pri zaobchádzaní s informačným aktívom v rámci príslušných obchodných postupov a zohľadnia sa aj príslušné prvky IT. Systém klasifikácie informačných aktív schválený manažmentom sa používa na vymedzenie vhodného súboru ochranných kontrolných mechanizmov počas celého životného cyklu informačných aktív (vrátane odstránenia a zničenia informačných aktív) a na oznámenie potreby osobitných opatrení týkajúcich sa zaobchádzania s nim.

Požiadavka 1.6: Bezpečnosť ľudských zdrojov
Povinnosti týkajúce sa bezpečnosti sú pred nástupom do zamestnania upravené v zodpovedajúcich popisoch pracovnej náplne a v pracovných podmienkach. Všetci uchádzači o zamestnanie, dodávatelia a užívatelia, ktorí sú tretími osobami, sa primerane preveria, najmä pokiaľ ide o citlivé pracovné činnosti. Zamestnanci, dodávatelia a užívatelia zariadení na spracovanie údajov, ktorí sú tretími osobami, podpíšu dohodu o svojich úlohách a povinnostiach v oblasti bezpečnosti. Zabezpečí sa primeraná úroveň informovanosti všetkých zamestnancov, dodávateľov a užívateľov, ktorí sú tretími osobami, a zabezpečí sa ich vzdelávanie a odborná príprava v oblasti bezpečnostných postupov a správneho používania zariadení na spracovanie údajov s cieľom minimalizovať možné bezpečnostné riziká. Pre zamestnancov sa zavedie formálny disciplinárny postup na riešenie prípadov narušenia bezpečnosti. Zavedú sa povinnosti, ktorými sa zabezpečí riadny odchod zamestnanca, dodávateľa alebo užívateľa, ktorý je treťou osobou, z organizácie alebo jeho presun v rámci organizácie, ako aj vrátenie všetkého vybavenia a zrušenie všetkých prístupových práv.

Požiadavka 1.7: Fyzická a environmentálna bezpečnosť
Zariadenia na spracovanie kritických alebo citlivých informácií sa umiestnia v bezpečných priestoroch chránených vymedzenými bezpečnostnými zónami s primeranými bezpečnostnými prekážkami a vstupnými kontrolami. Musia byť fyzicky chránené pred neoprávneným prístupom, poškodením a zásahom. Prístup sa umožní len jednotlivcom, na ktorých sa vzťahuje požiadavka 1.6. Zavedú sa postupy a normy na ochranu fyzických médií obsahujúcich informačné aktíva počas tranzitu.
Vybavenie musí byť chránené pred fyzickými a environmentálnymi hrozbami. Ochrana vybavenia (vrátane vybavenia používaného mimo priestorov organizácie) a ochrana pred

odcudzením majetku je potrebná na zníženie rizika neoprávneného prístupu k informáciám a na ochranu vybavenia alebo informácií pred stratou alebo poškodením. Na ochranu pred fyzickými hrozbami a na zabezpečenie podporných zariadení, ako je infraštruktúra elektrického napájania a káblových rozvodov, môžu byť potrebné osobitné opatrenia.

Požiadavka 1.8: Manažment prevádzky
Zavedú sa zodpovednosti a postupy pre riadenie a prevádzku zariadení na spracovanie údajov, ktoré sa budú vzťahovať na všetky základné systémy v rámci celého reťazca platobných transakcií.
Pokiaľ ide o prevádzkové postupy vrátane technickej správy informačných systémov, v prípade potreby sa uskutoční oddelenie funkcií s cieľom znížiť riziko zneužitia systému z nedbanlivosti alebo jeho úmyselného zneužitia. Ak nie je možné uskutočniť oddelenie funkcií z preukázaných objektívnych dôvodov, kompenzačné kontroly sa uskutočnia na základe formálnej analýzy rizík. Zavedú sa kontroly s cieľom zabrániť zavedeniu škodlivých kódov do systémov v reťazci platobných transakcií a odhaľovať ich. Zavedú sa aj kontroly (vrátane informovanosti užívateľov) s cieľom zabrániť zavedeniu škodlivých kódov, odhaľovať a odstraňovať ich. Mobilný kód sa môže použiť len z dôveryhodných zdrojov (napr. podpísané komponenty Microsoft COM a Java Applets). Konfigurácia prehliadača (napr. používanie rozšírení a zásuvných modulov) sa prísne kontroluje.
Manažment zavedie postupy pre zálohovanie a obnovu údajov; postupy pre obnovu údajov musia zahŕňať plán obnovy, ktorý sa pravidelne aspoň raz za rok testuje.
Systémy, ktoré sú kritické pre bezpečnosť platieb, sa monitorujú a zaznamenávajú sa udalosti súvisiace s bezpečnosťou informácií. Na zabezpečenie identifikácie problémov informačného systému sa použijú logy prevádzkovateľa. Logy prevádzkovateľa sa pravidelne preskúmavajú na základe vzoriek, a to podľa kritického charakteru operácií. Monitorovanie systému sa používa na overenie účinnosti kontrol, ktoré sú identifikované ako kritické z hľadiska bezpečnosti platieb, a na overenie súladu s modelom politiky prístupu.
Výmena informácií medzi organizáciami sa zakladá na oficiálnej politike výmeny informácií vykonávanej v súlade s dohodami o výmene medzi zúčastnenými stranami a je v súlade s príslušnými právnymi predpismi. Softvérové komponenty tretích osôb používané pri výmene informácií s TARGET2 (ako napr. softvér prijatý od Service Bureau v zmysle dokumentu o vlastnej certifikácii pre TARGET2, ktorý Národná banka Slovenska poskytne účastníkovi) sa musia používať na základe formálnej dohody s treťou osobou.

Požiadavka 1.9: Kontrola prístupu
Prístup k informačným aktívam musí byť odôvodnený na základe obchodných požiadaviek (opodstatnená potreba) a v súlade so zavedeným rámcom podnikových politík (vrátane politiky bezpečnosti informácií). Jasné pravidlá kontroly prístupu účastník vymedzí na základe zásady minimálnych práv, aby sa dôkladne zohľadnili potreby príslušných obchodných postupov a postupov v oblasti informačných technológií. V prípade potreby (napr. v prípade správy zálohovania) by mala byť kontrola logického prístupu v súlade s kontrolou fyzického prístupu, pokiaľ nie sú zavedené primerané kompenzačné kontroly (napr. šifrovanie, anonymizácia osobných údajov).
Zavedú sa formálne a zdokumentované postupy na kontrolu prideľovania prístupových práv k informačným systémom a službám, ktoré patria do rozsahu reťazca platobných transakcií. Tieto postupy sa vzťahujú na všetky štádiá životného cyklu prístupu užívateľa od prvotnej registrácie nových užívateľov až po konečné zrušenie registrácie užívateľov, ktorí už nepotrebujú prístup.

Osobitná pozornosť sa v prípade potreby venuje prideľovaniu prístupových práv s takou dôležitosťou, že zneužitie týchto prístupových práv by mohlo viesť k vážnemu nepriaznivému vplyvu na operácie účastníka (napr. prístupové práva umožňujúce správu systému, nerešpektovanie systémových kontrol alebo priamy prístup k obchodným údajom).
Zavedú sa primerané kontrolné mechanizmy na identifikáciu a autentifikáciu užívateľov a autorizáciu užívateľov na určitých miestach siete organizácie, napr. pre miestny a vzdialený prístup do systémov v rámci reťazca platobných transakcií. S cieľom zabezpečiť zodpovednosť sa osobné účty nesmú zdieľať.
Pokiaľ ide o heslá, pravidlá sa stanovia a presadzujú prostredníctvom osobitných kontrolných mechanizmov, aby sa zabezpečilo, že heslá nie je možné ľahko uhádnuť, napr. pravidlá týkajúce sa zložitosti a časovo obmedzená platnosť. Vytvorí sa protokol na bezpečnú obnovu alebo vytvorenie nového hesla.
Vypracuje sa a zavedie sa postup pre používanie kryptografických kontrolných mechanizmov na ochranu dôvernosti, pravosti a integrity informácií. Na podporu používania kryptografických kontrolných mechanizmov sa zavedie stratégia správy kľúčov.
Musia existovať pravidlá pre prehliadanie dôverných informácií na obrazovke alebo v tlačenej podobe (napr. pravidlo čistej obrazovky a čistého stola) s cieľom znížiť riziko neoprávneného prístupu.
Pri práci na diaľku sa zohľadňujú riziká práce v nechránenom prostredí a uplatňujú sa primerané technické a organizačné kontrolné mechanizmy.

Požiadavka 1.10: Získavanie, vývoj a údržba informačných systémov
Požiadavky na bezpečnosť sa stanovia a schvália pred vývojom a/alebo zavedením informačných systémov.
Na zabezpečenie správneho spracovania sa do aplikácií, vrátane aplikácií vyvinutých užívateľmi, zabudujú vhodné kontrolné mechanizmy. Tieto kontrolné mechanizmy zahŕňajú validáciu vstupných údajov, interné spracovanie a výstupné údaje. Dodatočné kontrolné mechanizmy sa môžu vyžadovať v prípade systémov, ktoré spracúvajú citlivé, cenné alebo kritické informácie, alebo majú na ne vplyv. Takéto kontrolné mechanizmy sa stanovia na základe bezpečnostných požiadaviek a posúdenia rizík v súlade so zavedenými politikami (napr. politikou bezpečnosti informácií, politikou kryptografických kontrolných mechanizmov).
Prevádzkové požiadavky nových systémov sa stanovia, zdokumentujú a otestujú pred ich prijatím a použitím. Pokiaľ ide o bezpečnosť sietí, mali by sa na základe kritického charakteru tokov údajov a úrovne rizika sieťových zón v organizácii zaviesť vhodné kontrolné mechanizmy vrátane segmentácie a bezpečného riadenia. Musia existovať osobitné kontrolné mechanizmy na ochranu citlivých informácií, ktoré sa prenášajú prostredníctvom verejných sietí.
Prístup k systémovým súborom a zdrojovému kódu programu sa kontroluje a IT projekty a podporné činnosti sa vykonávajú bezpečným spôsobom. Treba dbať na to, aby sa v testovacom prostredí zabránilo expozícii citlivých údajov. Prostredie projektu a podporné prostredie sa prísne kontrolujú. Zavádzanie zmien v produkčnom prostredí sa prísne kontroluje. Vykoná sa posúdenie rizík výrazných zmien, ktoré sa majú zaviesť v produkčnom prostredí.
Vykonáva sa aj pravidelné testovanie bezpečnosti systémov v produkčnom prostredí podľa vopred stanoveného plánu na základe výsledku posúdenia rizík a testovanie bezpečnosti zahŕňa minimálne posúdenie zraniteľnosti. Posúdia sa všetky nedostatky, ktoré boli zistené

počas testovania bezpečnosti a vypracujú sa a včas realizujú akčné plány na odstránenie zistených nedostatkov.

Požiadavka 1.11: Bezpečnosť informácií vo vzťahoch s dodávateľmi
S cieľom zabezpečiť ochranu interných informačných systémov účastníka, ku ktorým majú prístup dodávatelia, sa požiadavky na bezpečnosť informácií na zmiernenie rizík spojených s prístupom dodávateľa zdokumentujú a formálne dohodnú s dodávateľom.

Požiadavka 1.12: Riadenie incidentov v oblasti bezpečnosti informácií a zlepšenia
Na zabezpečenie konzistentného a účinného prístupu k riadeniu incidentov v oblasti bezpečnosti informácií vrátane komunikácie o bezpečnostných udalostiach a slabých stránkach sa na obchodnej a technickej úrovni zavedú a otestujú úlohy, zodpovednosti a postupy, aby sa zabezpečila rýchla, účinná a usporiadaná a bezpečná náprava incidentov v oblasti bezpečnosti informácií vrátane scenárov súvisiacich s kybernetickou príčinou (napr. podvod, ktorého sa dopustil externý útočník alebo osoba, ktorá má prístup k interným informáciám). Zamestnanci zapojení do týchto postupov musia byť primerane vyškolení.

Požiadavka 1.13: Preskúmanie technického súladu
Interné informačné systémy účastníka (napr. back-office systémy, interné siete a externé sieťové pripojenie) sa pravidelne posudzujú z hľadiska súladu so zavedenými politikami organizácie (napr. politika bezpečnosti informácií, politika kryptografickej ochrany).

Požiadavka 1.14: Virtualizácia
Hosťujúce virtuálne počítače musia byť v súlade so všetkými bezpečnostnými opatreniami, ktoré sú nastavené pre fyzický hardvér a systémy (napr. bezpečnostná konfigurácia, logovanie). Opatrenia týkajúce sa hypervízorov musia zahŕňať: bezpečnostnú konfiguráciu hypervízora a hostiteľského operačného systému, pravidelné nasadzovanie bezpečnostných opráv, dôsledné oddelenie rôznych prostredí (napr. produkčného a vývojového). Centralizované spravovanie, logovanie a monitorovanie, ako aj správa prístupových práv, najmä pre vysoko privilegované účty sa zavedú na základe posúdenia rizík. Hosťujúce virtuálne počítače spravované tým istým hypervízorom musia mať podobný rizikový profil.

Požiadavka 1.15: Využívanie technológie „Cloud computing“
Používanie verejných alebo hybridných cloudových riešení v reťazci platobných transakcií musí byť založené na formálnom posúdení rizík, pričom sa zohľadnia technické kontrolné opatrenia a zmluvné ustanovenia týkajúce sa cloudového riešenia.
Ak sa používajú hybridné cloudové riešenia, vychádza sa z toho, že úroveň kritickosti celkového systému je najvyššou z prepojených systémov. Všetky komponenty hybridných riešení musia byť oddelené od ostatných lokálnych systémov.

Riadenie kontinuity činností (vzťahuje sa len na kritických účastníkov)

Nasledujúce požiadavky (2.1 až 2.6) sa týkajú riadenia kontinuity činností. Každý účastník TARGET2 klasifikovaný Eurosystémom ako kritický pre bezproblémové fungovanie systému TARGET2 musí mať zavedenú stratégiu kontinuity činností, pozostávajúcu z nasledovných opatrení:

Požiadavka 2.1: Musia byť vypracované plány na zabezpečenie kontinuity činností a zavedené postupy na ich udržiavanie.

Požiadavka 2.2: Musí byť k dispozícii náhradné miesto prevádzky.

Požiadavka 2.3: Rizikový profil náhradného miesta prevádzky sa musí odlišovať od rizikového profilu hlavného primárneho miesta prevádzky, aby sa zabránilo tomu, že obe lokality budú súčasne zasiahnuté tou istou udalosťou. Náhradné miesto prevádzky musí byť napríklad napojené na inú elektrickú rozvodnú sieť a centrálny telekomunikačný okruh ako hlavné miesto činnosti.

Požiadavka 2.4: V prípade závažného narušenia prevádzky, ktoré spôsobí nedostupnosť hlavného miesta prevádzky alebo kritických zamestnancov, musí byť kritický účastník schopný obnoviť bežnú prevádzku z náhradného miesta, kde musí byť možné riadne ukončiť pracovný deň a začať nasledujúce pracovné dni.

Požiadavka 2.5: Musia sa zaviesť postupy, ktorými sa zabezpečí, že spracovanie transakcií sa obnoví z náhradného miesta prevádzky v primeranom čase po počiatočnom prerušení služby a úmerne ku kritickému významu činnosti, ktorá bola narušená.

Požiadavka 2.6: Schopnosť vysporiadať sa s narušeniami prevádzky sa musí testovať aspoň raz ročne a kritickí zamestnanci musia byť náležite vyškolení. Maximálna doba medzi testami nesmie presiahnuť jeden rok.“.

Čl. II

Vo Vestníku Národnej banky Slovenska sa vyhlási úplné znenie rozhodnutia Národnej banky Slovenska č. 7/2015 z 9. júna 2015 o podmienkach otvorenia a vedenia PM účtu v TARGET2-SK ako vyplýva zo zmien a doplnení vykonaných rozhodnutím NBS č. 9/2016, rozhodnutím NBS č. 13/2017, rozhodnutím NBS č. 11/2018, rozhodnutím NBS č. 21/2019 a týmto rozhodnutím Národnej banky Slovenska.

Čl. III

Toto rozhodnutie NBS nadobúda účinnosť 21. novembra 2021.

Peter Kažimír v. r.
guvernér

Vydávajúci útvar: odbor platobných systémov