Dalyvavimo mokėjimo sistemoje
TARGET-LIETUVOS BANKAS
taisyklių
7 priedas

INFORMACIJOS SAUGUMO VALDYMO IR VEIKLOS TĘSTINUMO VALDYMO REIKALAVIMAI

PLS, T2S SLS IR TIPS SLS TURĖTOJAI

Šie reikalavimai dėl informacijos saugumo valdymo arba veiklos tęstinumo valdymo netaikomi PLS, T2S SLS ir TIPS SLS turėtojams.

RLAA SLS TURĖTOJAI IR IS

Šio 7 priedo 1 skirsnyje („Informacijos saugumo valdymas“) nustatyti reikalavimai taikomi visiems RLAA SLS turėtojams ir IS, išskyrus atvejus, kai RLAA SLS turėtojas arba IS įrodo, kad konkretus reikalavimas jai netaikytinas. Nustatydamas reikalavimų taikymo apimtį savo infrastruktūroje, dalyvis turėtų identifikuoti tuos elementus, kurie yra mokėjimo sandorio grandinės (angl. *Payment Transaction Chain*, PTC) dalis. Konkreti mokėjimo sandorio grandinė pradedama įėjimo taške (angl. *Point of Entry*, PoE), t. y. sistemoje, kuri naudojama operacijoms suformuoti (pvz., profesionaliuosiuose kompiuteriuose, tiesioginių paslaugų ir netiesioginių paslaugų taikomosiose programose, tarpinės programinės įrangos sistemose), ir užbaigiama sistemoje, kuri atsakinga už pranešimo išsiuntimą TPT.

Šio 7 priedo 2 skirsnyje („Veiklos tęstinumo valdymas“) išdėstyti reikalavimai taikomi RLAA SLS turėtojams ir IS, kuriuos Eurosistema nurodo kaip itin svarbius sklandžiam TARGET sistemos veikimui, remdamasi periodiškai atnaujinamais ir ECB interneto svetainėje skelbiamais kriterijais.

1. Informacijos saugumo valdymas

1.1 reikalavimas. Informacijos saugumo politika

Vadovybė nustato aiškią politikos kryptį, atitinkančią veiklos tikslus, ir parodo paramą bei įsipareigojimą užtikrinti informacijos saugumą, nustatydama, patvirtindama ir prižiūrėdama informacijos saugumo politiką, kuria siekiama valdyti informacijos saugumą ir kibernetinį atsparumą visoje organizacijoje informacijos saugumo ir kibernetinio atsparumo rizikos nustatymo, vertinimo ir tvarkymo požiūriu. Politikos principai turi apimti bent šiuos skirsnius: tikslai, taikymo sritis (įskaitant tokias sritis kaip organizacija, žmogiškieji ištekliai, turto valdymas ir t. t.), principai ir atsakomybės paskirstymas.

1.2 reikalavimas. Organizacinė vidaus struktūra

Siekiant organizacijoje įgyvendinti informacijos saugumo politiką, sukuriama informacijos saugumo sistema. Vadovybė koordinuoja ir peržiūri sukurtą informacijos saugumo sistemą, kad užtikrintų informacijos saugumo politikos (kaip nurodyta 1.1 reikalavime) įgyvendinimą organizacijoje, įskaitant pakankamų išteklių ir saugumo pareigų skyrimą šiam tikslui.

1.3 reikalavimas. Išorės šalys

Organizacijos informacijos ir informacijos tvarkymo priemonių saugumas neturėtų sumažėti dėl išorės šalies (šalių) ar jų teikiamų produktų ir (arba) paslaugų įdiegimo ir (arba) priklausomybės nuo jų. Bet kokia išorės šalių prieiga prie organizacijos informacijos tvarkymo priemonių kontroliuojama. Kai išorės šalims arba išorės šalių produktams ar paslaugoms reikia prieigos prie organizacijos informacijos tvarkymo priemonių, atliekamas rizikos vertinimas siekiant nustatyti poveikį saugumui ir kontrolės reikalavimus. Dėl kontrolės priemonių susitariama ir jos apibrėžiamos susitarime su kiekviena atitinkama išorės šalimi.

1.4 reikalavimas. Turto valdymas

Visi informaciniai ištekliai, veiklos procesai ir pagrindinės informacinės sistemos, pavyzdžiui, operacinės sistemos, infrastruktūra, taikomosios verslo programos, standartiniai

produktai, paslaugos ir naudotojų sukurtos taikomosios programos, patenkantys į mokėjimo operacijų grandinės taikymo sritį, apskaitomi ir turi priskirtą savininką. Priskiriama atsakomybė už tinkamą veiklos procesų kontrolę ir susijusių IT komponentų, skirtų informaciniams ištekliams apsaugoti, priežiūrą ir veikimą Pastaba: prireikus savininkas gali pavesti įgyvendinti konkrečias kontrolės priemones, tačiau lieka atsakingas už tinkamą turto apsaugą.

1.5 reikalavimas. Informacinių išteklių klasifikavimas

Informaciniai ištekliai klasifikuojami pagal jų svarbą, kad dalyvis sklandžiai teiktų paslaugas. Klasifikacijoje nurodomas apsaugos, reikalingos naudojant tuos informacinius išteklius atitinkamuose veiklos procesuose, poreikis, prioritetai ir lygis, taip pat atsižvelgiama į pagrindinius IT komponentus. Vadovybės patvirtinta informacinių išteklių klasifikavimo schema naudojama tinkamam apsaugos kontrolės priemonių rinkiniui per visą informacinių išteklių gyvavimo ciklą nustatyti (įskaitant informacinių išteklių pašalinimą ir sunaikinimą) ir norint pranešti apie konkrečių naudojimo priemonių poreikį.

1.6 reikalavimas. Žmogiškųjų išteklių saugumas

Su saugumu susijusios pareigos prieš įdarbinant nurodomos tinkamuose pareigybių aprašymuose ir įdarbinimo sąlygose. Visi kandidatai į darbuotojų pozicijas, rangovai ir trečiųjų šalių naudotojai tinkamai tikrinami, ypač jei užima jautraus pobūdžio darbo vietas. Informacijos tvarkymo priemonių darbuotojai, rangovai ir trečiųjų šalių naudotojai pasirašo susitarimą dėl jų saugumo funkcijų ir atsakomybės. Siekiant kuo labiau sumažinti galimą saugumo riziką, užtikrinamas tinkamas visų darbuotojų, rangovų ir trečiųjų šalių naudotojų informuotumo lygis, jie taip pat šviečiami ir mokomi saugumo procedūrų ir tinkamo informacijos tvarkymo įrangos naudojimo klausimais. Darbuotojų atveju nustatoma oficiali drausminė procedūra saugumo pažeidimams nagrinėti. Turi būti nustatytos pareigos siekiant užtikrinti, kad darbuotojo, rangovo ar trečiosios šalies naudotojo išėjimas iš organizacijos arba jo perkėlimas organizacijoje būtų valdomas ir kad būtų visiškai grąžinta visa įranga ir panaikintos visos prieigos teisės.

1.7 reikalavimas. Fizinis ir aplinkos saugumas

Ypatingos svarbos arba neskelbtinos informacijos tvarkymo priemonės turi būti saugiose teritorijose, apsaugotose įrengiant apibrėžtą saugumo zoną su tinkamomis saugumo užkardomis ir patekimo kontrole. Jos fiziškai apsaugomos nuo neleistinos prieigos, pažeidimo ir įsikišimo. Prieiga suteikiama tik asmenims, kuriems taikomas 1.6 reikalavimas. Nustatomos procedūros ir standartai, skirti fizinėms laikmenoms, kuriose laikomi perkeliami informaciniai ištekliai, apsaugoti.

Įranga turi būti apsaugota nuo fizinių ir aplinkos pavojų. Siekiant sumažinti neteisėtos prieigos prie informacijos riziką ir apsaugoti įrangą ar informaciją nuo praradimo ar sugadinimo, būtina užtikrinti įrangos (įskaitant už objekto ribų naudojamą įrangą) apsaugą, taip pat apsaugą nuo turto paėmimo. Gali prireikti specialių priemonių siekiant apsisaugoti nuo fizinių grėsmių ir apsaugoti pagalbinius įrenginius, pavyzdžiui, elektros energijos tiekimo ir kabelių infrastruktūrą.

1.8 reikalavimas. Operacijų valdymas

Nustatoma atsakomybė ir procedūros, susijusios su informacijos tvarkymo priemonių, apimančių visas pagrindines mokėjimo sandorio grandinės ištisines sistemas, valdymu ir veikimu.

Kiek tai susiję su veiklos procedūromis, įskaitant IT sistemų techninį administravimą, kai tinkama, įgyvendinamas pareigų atskyrimas, siekiant sumažinti aplaidaus ar tyčinio netinkamo sistemos naudojimo riziką. Tais atvejais, kai pareigų atskyrimas negali būti įgyvendintas dėl dokumentais pagrįstų objektyvių priežasčių, atlikus oficialią rizikos analizę, įgyvendinama kompensacinė kontrolė. Nustatomos kontrolės priemonės, kuriomis siekiama užkirsti kelią kenkėjiško kodo įvedimui mokėjimo sandorio grandinėje ir jį aptikti. Taip pat nustatomos kontrolės priemonės (įskaitant naudotojų informuotumą), kuriomis siekiama užkirsti kelią kenkėjiškiems kodams, juos aptikti ir pašalinti. Judriojo ryšio kodas naudojamas tik iš patikimų šaltinių (pvz., pasirašytų *Microsoft* COM komponentų ir *Java Applets*). Turi būti griežtai kontroliuojama naršyklės konfigūracija (pvz., plėtinių ir papildinių naudojimas).

Vadovybė įgyvendina duomenų atsarginių kopijų saugojimo ir atkūrimo politiką. Ši atkūrimo politika apima atkūrimo proceso planą, kuris reguliariai patikrinamas bent kartą per metus.

Itin svarbios mokėjimų saugumui sistemos stebimos ir registruojami su informacijos saugumu susiję įvykiai. Naudojami operatoriaus žurnalai, siekiant užtikrinti, kad būtų nustatytos informacinės sistemos problemos. Operatoriaus žurnalai reguliariai peržiūrimi pasirinktinai, atsižvelgiant į operacijų svarbą. Sistemos stebėsena atliekama tikrinant kontrolės priemonių, kurios pripažintos itin svarbiomis mokėjimų saugumui, veiksmingumą ir tikrinant atitiktį prieigos politikos modeliui.

Organizacijos keičiasi informacija vadovaudamosi oficialia keitimosi informacija politika, ja keičiamasi pagal dalyvaujančių šalių sudarytus keitimosi susitarimus ir laikantis visų atitinkamų teisės aktų. Trečiųjų šalių programinės įrangos komponentai, naudojami keičiantis informacija su TARGET (pvz., programinė įranga, gauta iš paslaugų biuro), turi būti naudojami pagal oficialų susitarimą su trečiąja šalimi.

1.9 reikalavimas. Prieigos kontrolė

Prieiga prie informacinių išteklių pagrindžiama verslo reikalavimais (būtinumo žinoti principu[1]) ir vadovaujantis nustatyta įmonių politikos sistema (įskaitant informacijos saugumo politiką). Aiškios prieigos kontrolės taisyklės nustatomos remiantis mažiausios privilegijos principu[2], kad būtų tiksliai atspindėti atitinkamų verslo ir IT procesų poreikiai. Atitinkamais atvejais (pvz., atsarginių kopijų valdymo) loginės prieigos kontrolė turėtų būti suderinta su fizinės prieigos kontrole, išskyrus atvejus, kai taikomos tinkamos kompensacinės kontrolės priemonės (pvz., šifravimas, asmens duomenų anonimizavimas).

Nustatomos oficialios dokumentais įformintos procedūros, skirtos kontroliuoti, kaip suteikiamos prieigos prie informacinių sistemų ir paslaugų, patenkančių į mokėjimo operacijos grandinės taikymo sritį, teisės. Procedūros taikomos visiems naudotojo prieigos gyvavimo ciklo etapams nuo pradinės naujų naudotojų registracijos iki galutinio naudotojų, kuriems prieiga nebereikalinga, išregistravimo.

Tam tikrais atvejais ypatingas dėmesys skiriamas suteikiant tokios svarbos prieigos teises, kai nepagrįstas naudojimasis tomis prieigos teisėmis gali turėti didelį neigiamą poveikį dalyvio veiklai (pvz., prieigos teisėms, leidžiančioms administruoti sistemą, perskirstyti sistemos kontrolės priemones, gauti tiesioginę prieigą prie verslo duomenų).

Įdiegiamos tinkamos kontrolės priemonės, skirtos naudotojams identifikuoti, autentiškumui nustatyti ir autorizuoti konkrečiuose organizacijos tinklo taškuose, pvz., vietinei ir nuotolinei prieigai prie mokėjimo operacijų grandinės sistemų. Siekiant užtikrinti atskaitomybę, asmeninėmis paskyromis nesidalijama.

Slaptažodžių taisyklės nustatomos ir jų vykdymas užtikrinamas specialiomis kontrolės priemonėmis, siekiant užtikrinti, kad slaptažodžių nebūtų galima lengvai atspėti, pvz., sudėtingumo taisyklės ir ribotas galiojimo laikas. Nustatomas slaptažodžio saugaus atkūrimo ir (arba) atstatymo protokolas.

Siekiant apsaugoti informacijos konfidencialumą, autentiškumą ir vientisumą, parengiama ir įgyvendinama šifravimo kontrolės priemonių naudojimo politika. Nustatoma rakto valdymo politika, kuri padėtų naudoti kriptografines kontrolės priemones.

Siekiant sumažinti neteisėtos prieigos riziką, nustatoma konfidencialios informacijos ekrane arba spausdintame vaizde peržiūros politika (pvz., tuščias ekranas, tuščio darbo stalo politika).

Dirbant nuotoliniu būdu atsižvelgiama į darbo neapsaugotoje aplinkoje riziką ir taikomos tinkamos techninės ir organizacinės kontrolės priemonės.

1.10 reikalavimas. Informacinių sistemų įsigijimas, kūrimas ir priežiūra

Saugumo reikalavimai nustatomi ir dėl jų susitariama prieš kuriant ir (arba) diegiant informacines sistemas.

Siekiant užtikrinti tinkamą apdorojimą, į taikomąsias programas, įskaitant naudotojų sukurtas taikomąsias programas, įdiegiamos tinkamos kontrolės priemonės. Šios kontrolės priemonės apima pradinių duomenų, vidaus apdorojimo ir išvesties duomenų patvirtinimą. Gali reikėti papildomų kontrolės priemonių sistemoms, kurios apdoroja arba daro poveikį neskelbtinai, vertingai ar

[1] Principas „būtina žinoti“ reiškia informacijos, su kuria asmeniui reikia susipažinti, kad galėtų vykdyti savo pareigas, nustatymą.
[2] Mažiausios privilegijos principas susijęs su subjekto prieigos prie IT sistemos profilio pritaikymu, kad jis atitiktų atitinkamą verslo vaidmenį.

ypatingos svarbos informacijai. Tokios kontrolės priemonės nustatomos remiantis saugumo reikalavimais ir rizikos vertinimu pagal nustatytą politiką (pvz., informacijos saugumo politiką, šifravimo kontrolės politiką).

Naujų sistemų eksploatavimo reikalavimai nustatomi, įtvirtinami dokumentuose ir išbandomi prieš tas sistemas priimant ir naudojant. Tinklo saugumo srityje turėtų būti įgyvendintos tinkamos kontrolės priemonės, įskaitant segmentaciją ir saugų valdymą, atsižvelgiant į duomenų srautų svarbą ir tinklo zonų rizikos lygį organizacijoje. Turi būti taikomos specialios kontrolės priemonės, skirtos viešaisiais tinklais perduodamai neskelbtinai informacijai apsaugoti.

Prieiga prie sistemos rinkmenų ir pirminio programos kodo kontroliuojama, o IT projektai ir pagalbinė veikla vykdomi saugiai. Turi būti pasirūpinta, kad testinėje aplinkoje nebūtų atskleisti jautrūs duomenys. Projektų ir pagalbinė aplinka griežtai kontroliuojama. Pokyčių diegimas gamybinėje aplinkoje griežtai kontroliuojamas. Vertinama pagrindinių gamybinėje aplinkoje diegtinų pokyčių rizika.

Pagal iš anksto nustatytą planą, grindžiamą rizikos vertinimo rezultatais, atliekamas reguliarus naudojamų sistemų saugumo testavimas, o saugumo testavimas apima bent pažeidžiamumo vertinimą. Įvertinami visi saugumo testavimo metu išryškėję trūkumai ir parengiami veiksmų planai nustatytiems trūkumams pašalinti, o vėliau laiku imamasi tolesnių veiksmų.

1.11 reikalavimas. Informacijos saugumas santykiuose su tiekėju

Siekiant užtikrinti dalyvio vidaus informacinių sistemų, prie kurių gali prisijungti tiekėjai, apsaugą, dokumentuojami ir su tiekėju oficialiai suderinami informacijos saugumo reikalavimai, skirti su tiekėjo prieiga susijusiai rizikai mažinti.

1.12 reikalavimas. Informacijos saugumo incidentų valdymas ir tobulinimas

Siekiant užtikrinti nuoseklų ir veiksmingą požiūrį į informacijos saugumo incidentų valdymą, įskaitant informavimą apie saugumo įvykius ir trūkumus, veiklos ir techniniu lygmenimis nustatomi ir išbandomi vaidmenys, pareigos ir procedūros, siekiant užtikrinti greitą, veiksmingą, tvarkingą ir saugų atsigavimą po informacijos saugumo incidentų, įskaitant scenarijus, susijusius su kibernetine priežastimi (pvz., sukčiavimas, kurį vykdo išorės užpuolikas ar vidaus subjektas). Šiose procedūrose dalyvaujantys darbuotojai turi būti tinkamai apmokyti.

1.13 reikalavimas. Techninės atitikties peržiūra

Reguliariai vertinama, ar dalyvio vidaus informacinės sistemos (pvz., administracinio padalinio sistemos, vidaus tinklai ir išorinio tinklo ryšys) atitinka organizacijos nustatytą politikos sistemą (pvz., informacijos saugumo politiką, kriptografinės kontrolės politiką).

1.14 reikalavimas. Virtualizavimas

Virtualiosios svečių mašinos turi atitikti visas saugumo kontrolės priemones, nustatytas fizinei techninei įrangai ir sistemoms (pvz., apsaugos stiprinimo, registravimo). Su hipervizoriais susijusios kontrolės priemonės turi apimti: hipervizoriaus ir prieglobos operacinės sistemos sustiprinimą, reguliarų taisymą, griežtą skirtingų aplinkų (pvz., gamybinės ir kūrimo) atskyrimą. Centralizuotas valdymas, registravimas ir stebėjimas, taip pat prieigos teisių, ypač labai privilegijuotų paskyrų, valdymas įgyvendinami remiantis rizikos vertinimu. To paties hipervizoriaus valdomos virtualiosios mašinos turi lygiavertį rizikos profilį.

1.15 reikalavimas. Debesų kompiuterija

Viešųjų ir (arba) hibridinių debesijos sprendimų naudojimas mokėjimo sandorio grandinėje turi būti grindžiamas oficialiu rizikos vertinimu, atsižvelgiant į technines kontrolės priemones ir sutarčių sąlygas, susijusias su debesijos sprendimu.

Jei naudojami hibridiniai debesijos sprendimai, laikoma, kad visos sistemos kritiškumo lygis yra aukščiausiasis iš susietųjų sistemų. Visi vietiniai hibridinių sprendimų komponentai turi būti atskirti nuo kitų vietinių sistemų.

2. Veiklos tęstinumo valdymas

Toliau nurodyti reikalavimai susiję su veiklos tęstinumo valdymu. Kiekvienas TARGET dalyvis, kurį Eurosistema priskiria prie ypatingai svarbių sklandžiam TARGET sistemos veikimui, turi veiklos tęstinumo strategiją, kuri atitinka toliau nurodytus reikalavimus.

2.1 reikalavimas

Parengiami veiklos tęstinumo planai ir nustatomos jų priežiūros procedūros.

2.2 reikalavimas

Galima naudotis atsargine veiklos vieta.

2.3 reikalavimas

Atsarginės vietos rizikos profilis skiriasi nuo pirminės vietos rizikos profilio, kad tas pats įvykis tuo pačiu metu nepaveiktų abiejų veiklos vietų. Pavyzdžiui, atsarginė veiklos vieta yra kitame nei pagrindinės veiklos vietos elektros energijos tinkle ir centrinėje telekomunikacijos grandinėje.

2.4 reikalavimas

Įvykus dideliam veiklos sutrikimui, dėl kurio pagrindinė veiklos vieta tampa neprieinama ir (arba) jos ypač svarbūs darbuotojai yra nepasiekiami, ypatingos svarbos dalyvis turi pajėgumų atnaujinti įprastas operacijas iš atsarginės veiklos vietos, kurioje įmanoma tinkamai užbaigti darbo dieną ir pradėti kitą (-as) darbo dieną (-as).

2.5 reikalavimas

Nustatomos procedūros, užtikrinančios, kad operacijų apdorojimas iš atsarginės veiklos vietos būtų atnaujintas per pagrįstą laikotarpį po pradinio paslaugų teikimo sutrikdymo ir atitiktų sutrikusios veiklos svarbą.

2.6 reikalavimas

Pajėgumas įveikti veiklos sutrikimus tikrinamas bent kartą per metus, o ypač svarbūs darbuotojai yra tinkamai apmokyti. Ilgiausias laikotarpis tarp patikrinimų negali viršyti vienų metų.