Europos Sąjungos
oficialusis leidinys

LT
L serija

2024/2690

2024 10 18

KOMISIJOS ĮGYVENDINIMO REGLAMENTAS (ES) 2024/2690

2024 m. spalio 17 d.

kuriuo nustatomos Direktyvos (ES) 2022/2555 taikymo taisyklės, susijusios su kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais ir išsamesniu atvejų, kuriais incidentas laikomas dideliu, apibūdinimu, skirtais DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams

(Tekstas svarbus EEE)

EUROPOS KOMISIJA,

atsižvelgdama į Sutartį dėl Europos Sąjungos veikimo,

atsižvelgdama į 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyvą (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148, (TIS 2 direktyvą) ([1]), ypač į jos 21 straipsnio 5 dalies pirmą pastraipą ir 23 straipsnio 11 dalies antrą pastraipą,

kadangi:

(1) šiuo reglamentu siekiama nustatyti Direktyvos (ES) 2022/2555 21 straipsnio 2 dalyje nurodytų priemonių techninius ir metodinius reikalavimus ir pateikti išsamesnį atvejų, kuriais incidentas pagal Direktyvos (ES) 2022/2555 23 straipsnio 3 dalį turėtų būti laikomas dideliu, apibūdinimą, skirtus į Direktyvos (ES) 2022/2555 3 straipsnio aprėptį patenkantiems DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams (atitinkamiems subjektams);

(2) atsižvelgiant į tarpvalstybinį patikimumo užtikrinimo paslaugų teikėjų veiklos pobūdį ir siekiant užtikrinti, kad jiems būtų taikoma nuosekli sistema, šiame reglamente turėtų būti ne tik nustatyti jiems skirti kibernetinio saugumo rizikos valdymo priemonių techniniai ir metodiniai reikalavimai, bet ir pateiktas jiems skirtas išsamesnis atvejų, kuriais incidentas turi būti laikomas dideliu, apibūdinimas;

(3) vadovaujantis Direktyvos (ES) 2022/2555 21 straipsnio 5 dalies trečia pastraipa, šio reglamento priede nustatyti kibernetinio saugumo rizikos valdymo priemonių techniniai ir metodiniai reikalavimai yra pagrįsti su tinklų ir informacinių sistemų saugumu susijusiais Europos bei tarptautiniais standartais, kaip antai ISO/IEC 27001, ISO/IEC 27002 ir ETSI EN 319401, ir techninėmis specifikacijomis, kaip antai CEN/TS 18026:2024;

(4) įgyvendinant ir taikant šio reglamento priede nustatytus kibernetinio saugumo rizikos valdymo priemonių techninius ir metodinius reikalavimus, reikėtų pagal proporcingumo principą deramai atsižvelgti į nevienodą atitinkamiems subjektams kylančią riziką, pavyzdžiui, į atitinkamo subjekto svarbą, į tai, kokia rizika jam kyla, į jo dydį ir struktūrą, taip pat į incidentų tikimybę ir sunkumą, be kita ko, jų socialinį ir ekonominį poveikį, kai laikomasi šio reglamento priede nustatytų kibernetinio saugumo rizikos valdymo priemonių techninių ir metodinių reikalavimų;

([1]) OL L 333, 2022 12 27, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj.

(5) tais atvejais, kai atitinkami subjektai dėl savo dydžio kai kurių kibernetinio saugumo rizikos valdymo priemonių techninių ir metodinių reikalavimų įgyvendinti negali, jie pagal proporcingumo principą turėtų turėti galimybę imtis kitų kompensacinių priemonių, tinkamų tų reikalavimų tikslui pasiekti. Pavyzdžiui, savo viduje apibrėžiant su tinklų ir informacinių sistemų saugumu susijusias funkcijas, pareigas ir organus, labai mažiems atitinkamiems subjektams gali būti sunku nustatyti aiškiai atskirtas prieštaringas pareigas ir atsakomybės sritis. Tokie subjektai turėtų galėti svarstyti galimybę imtis kompensacinių priemonių, tokių kaip tikslinė priežiūra, vykdoma subjekto vadovybės, arba intensyvesnė stebėsena ir registravimas;

(6) tam tikrus šio reglamento priede nustatytus techninius ir metodinius reikalavimus atitinkami subjektai turėtų taikyti, kai tikslinga, kai taikytina ir tiek, kiek įmanoma. Tais atvejais, kai atitinkamas subjektas mano, kad taikyti tam tikrus šio reglamento priede nustatytus techninius ir metodinius reikalavimus jo atveju nėra tikslinga, taikytina ar įmanoma, jis turėtų dokumentuose suprantamai užfiksuoti su tuo susijusius savo argumentus. Vykdydamos priežiūrą, nacionalinės kompetentingos institucijos gali atsižvelgti į tai, kiek laiko atitinkamiems subjektams reikia kibernetinio saugumo rizikos valdymo priemonių techniniams ir metodiniams reikalavimams įgyvendinti;

(7) ENISA arba pagal Direktyvą (ES) 2022/2555 kompetentingos nacionalinės institucijos gali teikti gaires, padedančias atitinkamiems subjektams nustatyti, analizuoti ir vertinti riziką siekiant įgyvendinti techninius ir metodinius reikalavimus, susijusius su tinkamos rizikos valdymo sistemos sukūrimu ir išlaikymu. Tokios gairės visų pirma gali apimti nacionalinių ir sektorinių rizikos vertinimų ir su tam tikros rūšies subjektais susijusių rizikos vertinimų gaires. Jose taip pat gali būti numatytos atitinkamų subjektų lygmens rizikos valdymo sistemos kūrimo priemonės ar modeliai. Padėti atitinkamiems subjektams įrodyti atitiktį šiam reglamentui gali ir valstybių narių nacionalinėje teisėje numatytos sistemos, gairės ar kiti mechanizmai, taip pat atitinkami europiniai ir tarptautiniai standartai. Be to, ENISA arba pagal Direktyvą (ES) 2022/2555 kompetentingos nacionalinės institucijos gali padėti atitinkamiems subjektams surasti ir įgyvendinti tinkamus rizikos, nustatytos atliekant tuos rizikos vertinimus, valdymo sprendimus. Tokios gairės neturėtų daryti poveikio atitinkamų subjektų pareigai nustatyti ir dokumentuoti tinklų ir informacinių sistemų saugumui kylančią riziką ir atitinkamų subjektų pareigai įgyvendinti šio reglamento priede nustatytus kibernetinio saugumo rizikos valdymo priemonių techninius ir metodinius reikalavimus, atsižvelgiant į savo poreikius ir išteklius;

(8) tinklo saugumo priemonės, susijusios su i) perėjimu prie naujausios kartos tinklo lygmens ryšių protokolų, ii) tarptautiniu mastu sutartų ir sąveikių šiuolaikinių e. pašto ryšio standartų diegimu ir iii) DNS saugumo, interneto maršruto parinkimo saugumo ir maršruto parinkimo higienos užtikrinimo geriausios praktikos taikymu, kelia specifinių sunkumų, susijusių su geriausių esamų standartų ir diegimo metodų nustatymu. Kad būtų kuo greičiau užtikrintas aukštas bendras visų tinklų kibernetinio saugumo lygis, Komisija, padedama Europos Sąjungos kibernetinio saugumo agentūros (ENISA) ir bendradarbiaudama su kompetentingomis institucijomis, pramonės, be kita ko, telekomunikacijų sektoriaus, atstovais ir kitais suinteresuotaisiais subjektais, turėtų padėti sukurti įvairių suinteresuotųjų subjektų forumą, turintį nustatyti tuos geriausius esamus standartus ir diegimo metodus. Tų įvairių suinteresuotųjų subjektų teikiamos gairės neturėtų daryti poveikio atitinkamų subjektų pareigai įgyvendinti šio reglamento priede nustatytus kibernetinio saugumo rizikos valdymo priemonių techninius ir metodinius reikalavimus;

(9) vadovaujantis Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a punktu, esminiai ir svarbūs subjektai turėtų taikyti ne tik rizikos analizės, bet ir informacinių sistemų saugumo politiką. Tuo tikslu atitinkami subjektai turėtų nustatyti tinklų ir informacinių sistemų saugumo politiką ir su konkrečiais klausimais, pavyzdžiui, prieigos kontrole, susijusią politiką, kuri turėtų derėti su tinklų ir informacinių sistemų saugumo politika. Tinklų ir informacinių sistemų saugumo politika turėtų būti išdėstyta atitinkamo subjekto valdymo organų patvirtintame aukščiausio lygio dokumente, išreiškiančiame to subjekto bendrą požiūrį į savo tinklų ir informacinių sistemų saugumą. Su konkrečiais klausimais susijusią politiką turėtų patvirtinti tinkamo lygmens valdymo organai. Politikoje turėtų būti nustatyti rodikliai ir priemonės, skirti jos įgyvendinimui ir esamam atitinkamo subjekto tinklų ir informacinių sistemų saugumo brandos lygiui stebėti, visų pirma tam, kad valdymo organams būtų lengviau prižiūrėti kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą;

(10) taikant šio reglamento priede nustatytus techninius ir metodinius reikalavimus, terminas „naudotojas“ turėtų apimti visus juridinius ir fizinius asmenis, turinčius prieigą prie subjekto tinklų ir informacinių sistemų;

(11) siekdami nustatyti ir mažinti tinklų ir informacinių sistemų saugumui kylančią riziką, atitinkami subjektai turėtų sukurti ir išlaikyti tinkamą rizikos valdymo sistemą. Taikydami rizikos valdymo sistemą, atitinkami subjektai turėtų parengti ir įgyvendinti rizikos priežiūros planą ir stebėti jo vykdymą. Šiame plane atitinkami subjektai gali nustatyti ir pagal svarbą išrikiuoti rizikos priežiūros būdus ir priemones. Rizikos priežiūros būdai visų pirma apima rizikos vengimą, mažinimą arba išimtiniais atvejais prisiėmimą. Renkantis rizikos priežiūros būdus, reikėtų atsižvelgti į atitinkamo subjekto atlikto rizikos vertinimo rezultatus ir to subjekto tinklų ir informacinių sistemų saugumo politiką. Siekdami įgyvendinti pasirinktus rizikos priežiūros būdus, atitinkami subjektai turėtų imtis tinkamų rizikos priežiūros priemonių;

(12) kad aptiktų įvykius, vos neįvykusius incidentus ir incidentus, atitinkami subjektai turėtų stebėti savo tinklų ir informacines sistemas ir imtis įvykių, vos neįvykusių incidentų ir incidentų vertinimo veiksmų. Tos priemonės turėtų sudaryti sąlygas laiku aptikti tinklo atakas, remiantis įeinančio ir išeinančio srauto anomalijomis, ir paslaugos trikdymo atakas;

(13) atitinkami subjektai raginami, nagrinėdami poveikį veiklai, atlikti nuodugnią analizę, kuria atitinkamais atvejais būtų nustatytas ilgiausias priimtinas neveikimo laikas ir tikslai, susiję su veikimo atkūrimo laiku, priimtinu prarasti duomenų kiekiu ir paslaugų teikimu;

(14) kad sumažintų riziką, susijusią su savo tiekimo grandine ir savo ryšiais su tiekėjais, atitinkami subjektai turėtų nustatyti tiekimo grandinės saugumo politiką, reglamentuojančią jų ryšius su tiesioginiais tiekėjais ir paslaugų teikėjais. Šie subjektai sutartyse su savo tiesioginiais tiekėjais ar paslaugų teikėjais turėtų nustatyti tinkamas su saugumu susijusias sąlygas, pavyzdžiui, reikalauti, kai tikslinga, pagal Direktyvos (ES) 2022/2555 21 straipsnio 2 dalį arba panašius teisinius reikalavimus taikyti kibernetinio saugumo rizikos valdymo priemones;

(15) atitinkami subjektai turėtų, remdamiesi specialia politika ir procedūromis, reguliariai atlikti saugumo testavimą, skirtą patikrinti, ar kibernetinio saugumo rizikos valdymo priemonės yra įgyvendinamos ir veikia tinkamai. Šis saugumo testavimas, kuriuo gali būti tikrinamos konkrečios tinklų ir informacinės sistemos arba visas atitinkamas subjektas, gali apimti automatinį arba rankinį testavimą, skverbimosi testavimą, pažeidžiamumų skenavimą, statinį ir dinaminį taikomųjų programų saugumo testavimą, konfigūracijų testavimą arba saugumo auditus. Savo tinklų ir informacinių sistemų saugumą atitinkami subjektai gali testuoti, kai šios sistemos kuriamos, po infrastruktūros ar taikomųjų programų naujovinimo ar pakeitimų, kuriuos jie laiko reikšmingais, arba po techninės priežiūros veiksmų. Per saugumo testavimą nustatytais faktais atitinkami subjektai turėtų remtis plėtodami savo kibernetinio saugumo rizikos valdymo priemonių veiksmingumo vertinimo politiką bei procedūras; be to, jais turėtų būti remiamasi per nepriklausomas jų tinklų ir informacinių sistemų saugumo politikos peržiūras;

(16) kad išvengtų didelių sutrikimų ir žalos, kuriuos gali sukelti pasinaudojimas neištaisytais tinklų ir informacinių sistemų pažeidžiamumais, atitinkami subjektai turėtų nustatyti ir taikyti tinkamas saugumo pataisų valdymo procedūras, suderintas su jų pakeitimų valdymo, pažeidžiamumų valdymo, rizikos valdymo ir kitomis atitinkamomis procedūromis. Atitinkami subjektai turėtų imtis jų ištekliams proporcingų priemonių, padedančių užtikrinti, kad dėl saugumo pataisų neatsirastų papildomų pažeidžiamumo ar nestabilumo problemų. Atitinkami subjektai raginami apie planuojamus pataisų diegimo laikotarpius, kuriais paslauga bus neprieinama, iš anksto tinkamai informuoti klientus;

(17) atitinkami subjektai turėtų valdyti riziką, susijusią su IRT produktų ar IRT paslaugų įsigijimu iš tiekėjų ar paslaugų teikėjų, ir turėtų gauti patikinimą, kad ketinamų įsigyti IRT produktų ar IRT paslaugų kibernetinis saugumas siekia tam tikrą lygį, pavyzdžiui, tie IRT produktai ar IRT paslaugos turėtų turėti Europos kibernetinio saugumo sertifikatus ir ES atitikties pareiškimus, išduotus pagal Europos kibernetinio saugumo sertifikavimo schemą, priimtą pagal Europos Parlamento ir Tarybos reglamento (ES) 2019/881 ([2]) 49 straipsnį. Nustatydami ketinamiems įsigyti IRT produktams taikytinus saugumo reikalavimus, atitinkami subjektai turėtų atsižvelgti į Europos Parlamento ir Tarybos reglamente dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų skaitmeninių elementų turintiems produktams, nustatytus pagrindinius kibernetinio saugumo reikalavimus;

(18) atitinkami subjektai turėtų diegti tinklo saugumo sprendimus, padedančius užtikrinti apsaugą nuo kibernetinių grėsmių ir išvengti duomenų saugumo pažeidimų bei apriboti jų mastą. Įprasti tinklo saugumo sprendimai yra, be kita ko, užkardų naudojimas atitinkamų subjektų vidaus tinklams apsaugoti, jungimosi prie paslaugų ir naudojimosi jomis apribojimas iki atvejų, kuriais to būtinai reikia, virtualiųjų privačiųjų tinklų naudojimas nuotolinei prieigai ir galimybės prisijungti paslaugų teikėjams suteikimas tik po to, kai paprašoma leidimo, ir tik nustatytam, pavyzdžiui, techninės priežiūros operacijos trukmei lygiam, laikui;

(19) siekdami apsaugoti savo tinklus ir informacines sistemas nuo neleistinos ir kenkimo programinės įrangos, atitinkami subjektai turėtų įdiegti kontrolės priemones, neleidžiančias naudoti neleistinos programinės įrangos arba aptikti jos naudojimo atvejus, ir, kai tikslinga, naudoti aptikimo ir reagavimo programinę įrangą. Atitinkami subjektai taip pat turėtų apsvarstyti galimybę įdiegti priemones, padedančias kuo labiau sumažinti išpuolių perimetrą, sumažinti pažeidžiamumų, kuriais gali pasinaudoti išpuolių vykdytojai, kontroliuoti taikomųjų programų vykdymą galiniuose įrenginiuose, taip pat diegti e. pašto ar interneto taikomųjų programų filtrus, mažinančius riziką susidurti su kenkėjišku turiniu;

(20) vadovaujantis Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies g punktu, valstybės narės turi užtikrinti, kad esminiai ir svarbūs subjektai taikytų pagrindinius kibernetinės higienos principus ir organizuotų kibernetinio saugumo mokymus. Pagrindiniai kibernetinės higienos principai gali apimti nulinio pasitikėjimo principus, programinės įrangos naujinimą, įrenginių konfigūravimą, tinklo segmentavimą, tapatumo ir prieigos valdymą arba naudotojų informuotumo didinimą, darbuotojams skirtų mokymų organizavimą ir informuotumo apie kibernetines grėsmes, duomenų viliojimą ar socialinę inžineriją didinimą. Kibernetinės higienos principai yra viena iš šio reglamento priede nustatytų kibernetinio saugumo rizikos valdymo priemonių techninių ir metodinių reikalavimų sudedamųjų dalių. Atitinkamų subjektų svarstymai dėl pagrindinių kibernetinės higienos principų, skirtų naudotojams, turėtų apimti tokius principus kaip tuščio darbo stalo ir ekrano politika, daugiaelemenčio ir kitų tapatumo nustatymo priemonių naudojimas, saugus e. pašto naudojimas ir naršymas internete, apsauga nuo duomenų viliojimo ir socialinės inžinerijos, saugūs nuotolinio darbo metodai;

(21) siekdami užkirsti kelią neteisėtai prieigai prie jų turto, atitinkami subjektai turėtų nustatyti ir įgyvendinti su šiuo klausimu susijusią politiką, reglamentuojančią prieigą pagal asmenis ir pagal tinklų ir informacines sistemas, kaip antai taikomąsias programas;

(22) siekdami užtikrinti, kad darbuotojai negalėtų, pavyzdžiui, pakenkti ir padaryti žalos netinkamai naudodamiesi prieigos teisėmis paties subjekto viduje, atitinkami subjektai turėtų apsvarstyti galimybę taikyti tinkamas darbuotojų patikimumo valdymo priemones ir didinti darbuotojų informuotumą apie tokią riziką. Atitinkami subjektai turėtų nustatyti drausminę procedūrą, taikytiną jų tinklų ir informacinių sistemų saugumo politikos pažeidimų atvejais, apie ją informuoti ir ją išlaikyti; ši procedūra galėtų būti integruota į kitas atitinkamų subjektų nustatytas drausmines procedūras. Užtikrinti atitinkamų subjektų žmogiškųjų išteklių patikimumą turėtų padėti atitinkamų subjektų darbuotojų ir, kai taikytina, tiesioginių tiekėjų ir paslaugų teikėjų patikimumo patikrinimai, galintys apimti tokias priemones kaip patikrinimas, ar asmuo neteistas arba kokias pareigas jis anksčiau ėjo, priklausomai nuo to, kas aktualu atsižvelgiant į asmens pareigas atitinkamame subjekte, ir laikantis atitinkamo subjekto tinklų ir informacinių sistemų saugumo politikos;

([2]) 2019 m. balandžio 17 d. Europos Parlamento ir Tarybos reglamentas (ES) 2019/881 dėl ENISA (Europos Sąjungos kibernetinio saugumo agentūros) ir informacinių ir ryšių technologijų kibernetinio saugumo sertifikavimo, kuriuo panaikinamas Reglamentas (ES) Nr. 526/2013, (Kibernetinio saugumo aktas) (OL L 151, 2019 6 7, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

(23) subjektai turėtų apsvarstyti galimybę taikyti jų kibernetinį saugumą galinčias padidinti daugiaelemenčio tapatumo nustatymo priemones, ypač jei naudotojai prie tinklų ir informacinių sistemų jungiasi nuotoliniu būdu arba jei jie turi prieigą prie neskelbtinos informacijos ar privilegijuotų paskyrų ir sistemų administravimo paskyrų. Daugiaelemenčio tapatumo nustatymo priemonės gali būti derinamos su kitais metodais, kad tam tikromis aplinkybėmis, remiantis iš anksto nustatytomis taisyklėmis ir požymiais, pavyzdžiui, kai jungiamasi neįprastu laiku, esant neįprastoje vietoje arba naudojantis neįprastu įrenginiu, būtų reikalaujama naudoti papildomus elementus;

(24) siekdami valdyti ir saugoti jiems vertingą turtą atitinkami subjektai turėtų užtikrinti patikimą jo valdymą, kuris taip pat turėtų padėti atlikti rizikos analizę ir valdyti veiklos tęstinumą. Atitinkami subjektai turėtų valdyti ir materialųjį, ir nematerialųjį turtą, sudaryti jo inventorių, priskirti jį prie apibrėžtų slaptumo lygmenų, jį tvarkyti bei stebėti ir imtis veiksmų jam apsaugoti visu jo gyvavimo ciklu;

(25) turto valdymas turėtų apimti jo klasifikavimą pagal jo rūšį, jautrumą, rizikos lygį ir saugumo reikalavimus ir tinkamų kontrolės bei kitų priemonių taikymą siekiant užtikrinti turto prieinamumą, vientisumą, konfidencialumą ir autentiškumą. Turto klasifikavimas pagal rizikos lygį turėtų suteikti atitinkamiems subjektams galimybę taikyti tinkamas turtui apsaugoti skirtas saugumo ir kontrolės priemones, tokias kaip šifravimas, prieigos kontrolė (įskaitant perimetro ir fizinės bei loginės prieigos kontrolę), atsarginių kopijų darymas, veiksmų registravimas, stebėjimas, saugojimas ir sunaikinimas. Atlikdami poveikio veiklai analizę, atitinkami subjektai klasifikavimo lygmenį gali nustatyti atsižvelgdami į tai, kokių padarinių jiems sukeltų žala turtui. Visi turtą tvarkantys subjektų darbuotojai turėtų būti susipažinę su turto tvarkymo politika ir instrukcijomis;

(26) turto inventoriaus detalumas turėtų atitikti atitinkamų subjektų poreikius. Išsamiame turto inventoriuje apie kiekvieną turto objektą galėtų būti pateikiama bent ši informacija: unikalus jo identifikatorius, jo savininkas, aprašymas, buvimo vieta, rūšis, jame tvarkomos informacijos rūšis ir kategorija, naujausio jo naujinimo ar taisymo data, jo kategorija rizikos vertinimo požiūriu ir jo gyvavimo ciklo pabaiga. Nustatydami turto objekto savininką, atitinkami subjektai turėtų nustatyti ir asmenį, atsakingą už to turto objekto apsaugą;

(27) nustatant ir organizuojant su kibernetiniu saugumu susijusias funkcijas, pareigas ir organus, atitinkamuose subjektuose turėtų būti sukurta nuosekli kibernetinio saugumo valdymo ir užtikrinimo struktūra ir užtikrinta veiksminga komunikacija incidentų atveju. Apibrėždami konkrečias funkcijas ir joms priskirtas pareigas, atitinkami subjektai turėtų apsvarstyti galimybę nustatyti tokias funkcijas kaip vyriausiasis informacijos saugumo pareigūnas, informacijos saugumo pareigūnas, incidentų valdymo pareigūnas, auditorius ar panašias atitinkamas funkcijas. Funkcijas ir pareigas atitinkami subjektai gali pavesti išorės subjektams, kaip antai IRT paslaugas teikiančioms trečiosioms šalims;

(28) vadovaujantis Direktyvos (ES) 2022/2555 21 straipsnio 2 dalimi, kibernetinio saugumo rizikos valdymo priemonės turi būti grindžiamos visus pavojus apimančiu požiūriu, kurio tikslas – apsaugoti tinklų ir informacines sistemas bei jų fizinę aplinką nuo tokių įvykių kaip vagystė, gaisras, potvynis, telekomunikacijų ar elektros energijos tiekimo triktys arba nuo neteisėtos fizinės prieigos prie esminio ar svarbaus subjekto informacijos ir informacijos tvarkymo įrenginių, žalos jiems ir jų sutrikdymo, kurie galėtų kelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tinklų ir informacines sistemas teikiamų ar prieinamų paslaugų prieinamumui, autentiškumui, vientisumui arba konfidencialumui. Todėl kibernetinio saugumo rizikos valdymo priemonių techniniais ir metodiniais reikalavimais taip pat turėtų būti užtikrinamas tinklų ir informacinių sistemų fizinis ir aplinkos saugumas, t. y. jie turėtų apimti priemones, padedančias apsaugoti tokias sistemas nuo sistemos gedimų, žmogiškųjų klaidų, piktavališkų veiksmų ar gamtos reiškinių. Kitos fizinės ir aplinkos grėsmės gali būti, pavyzdžiui, žemės drebėjimai, sprogimai, sabotažas, vidaus subjektų keliama grėsmė, pilietiniai neramumai, nuodingosios atliekos ir į aplinką išmetami teršalai. Užtikrinimas, kad, nutrūkus arba sutrikus pagrindinių komunalinių paslaugų tiekimui, tinklų ir informacinės sistemos nebūtų prarastos, sugadintos ar pažeistos ir nenustotų veikti, turėtų padėti atitinkamiems subjektams užtikrinti veiklos tęstinumą. Be to, apsauga nuo fizinių ir aplinkos grėsmių turėtų prisidėti prie atitinkamų subjektų tinklų ir informacinių sistemų techninės priežiūros saugumo;

(29) atitinkami subjektai turėtų rengti ir įgyvendinti apsaugos nuo fizinių ir aplinkos grėsmių priemones, nustatyti su fizinėmis ir aplinkos grėsmėmis susijusias mažiausias ir didžiausias kontrolines vertes ir stebėti aplinkos parametrus. Pavyzdžiui, jie turėtų apsvarstyti galimybę įdiegti sistemas, padedančias vietose, kuriose yra tinklų ir informacinės sistemos, anksti aptikti potvynius. Rūpindamiesi apsauga nuo gaisro, atitinkami subjektai turėtų apsvarstyti galimybę duomenų centrą įrengti atskirame gaisriniame skyriuje, naudoti ugniai atsparias medžiagas ir temperatūrai bei drėgniui stebėti skirtus jutiklius ir pastatą sujungti su gaisro signalizavimo sistema, siunčiančia automatinius pranešimus vietos priešgaisrinei tarnybai, ir ankstyvo gaisro aptikimo bei gesinimo sistemomis. Atitinkami subjektai taip pat turėtų reguliariai vykdyti gaisrinės saugos pratybas ir gaisrinės saugos patikrinimus. Be to, kad užtikrintų maitinimą, atitinkami subjektai turėtų apsvarstyti galimybę pasirūpinti apsauga nuo viršįtampio ir susijusiu avariniu maitinimu pagal atitinkamus standartus. Tinklų ir informacinės sistemos gali tapti neprieinamos ir dėl perkaitimo, todėl atitinkami subjektai, ypač duomenų centrų paslaugų teikėjai, turėtų apsvarstyti galimybę įdiegti tinkamas, nuolat veikiančias ir viena kitą dubliuojančias oro kondicionavimo sistemas;

(30) šiame reglamente turi būti pateiktas išsamesnis atvejų, kuriais incidentas taikant Direktyvos (ES) 2022/2555 23 straipsnio 3 dalį turėtų būti laikomas dideliu, apibūdinimas. Kriterijai turėtų būti tokie, kad atitinkami subjektai galėtų nustatyti, ar incidentas yra didelis, kad apie jį praneštų pagal Direktyvą (ES) 2022/2555. Be to, nedarant poveikio Direktyvos (ES) 2022/2555 5 straipsniui, šiame reglamente nustatyti kriterijai turėtų būti laikomi išsamiais. Šiame reglamente nurodomi tiek horizontalieji, tiek su konkrečių rūšių subjektais susiję atvejai, kuriais incidentas turėtų būti laikomas dideliu;

(31) vadovaujantis Direktyvos (ES) 2022/2555 23 straipsnio 4 dalimi, turėtų būti reikalaujama, kad atitinkami subjektai praneštų apie didelius incidentus per toje dalyje nustatytus terminus. Tie pranešimo terminai pradedami skaičiuoti nuo momento, kurį subjektas sužino apie tuos didelius incidentus. Taigi atitinkamas subjektas privalo pranešti apie incidentus, dėl kurių, remiantis jo pradiniu vertinimu, jis gali patirti didelių paslaugų teikimo sutrikimų arba finansinių nuostolių arba kurie gali paveikti kitus fizinius ar juridinius asmenis sukeldami didelę turtinę arba neturtinę žalą. Todėl, kai atitinkamas subjektas nustato įtartiną įvykį arba kai apie galimą incidentą jam praneša trečiasis asmuo, kaip antai fizinis asmuo, klientas, subjektas, institucija, žiniasklaidos organizacija ar kitas šaltinis, jis turėtų laiku įvertinti įtartiną įvykį, kad nustatytų, ar tai incidentas ir, jei taip, koks yra jo pobūdis ir sunkumas. Todėl laikoma, kad apie didelį incidentą atitinkamas subjektas sužino tada, kai atlikęs tą pradinį vertinimą tampa pakankamai tikras, kad įvyko didelis incidentas;

(32) siekdami nustatyti, ar incidentas didelis, atitinkami subjektai, kai aktualu, turėtų suskaičiuoti, kiek naudotojų jis paveiks, atsižvelgdami į verslo ir galutinius klientus, su kuriais jie yra užmezgę sutartinius santykius, ir į fizinius bei juridinius asmenis, susijusius su verslo klientais. Tais atvejais, kai atitinkamas subjektas suskaičiuoti paveiktų naudotojų negali, bendram incidento paveiktų naudotojų skaičiui nustatyti turėtų būti naudojamas atitinkamo subjekto įvertis, kiek daugiausiai gali būti paveiktų naudotojų. Su patikimumo užtikrinimo paslauga susijusio incidento dydis turėtų būti nustatomas remiantis ne vien naudotojų, bet ir pasikliaujančiųjų šalių skaičiumi, nes su patikimumo užtikrinimo paslauga susijęs didelis incidentas lygiai taip pat gali sutrikdyti ir pastarųjų veiklą bei joms padaryti turtinės arba neturtinės žalos. Todėl patikimumo užtikrinimo paslaugų teikėjai, nustatydami, ar incidentas didelis, turėtų, kai taikytina, atsižvelgti ir į pasikliaujančiųjų šalių skaičių. Šiuo tikslu pasikliaujančiosiomis šalimis turėtų būti laikomi patikimumo užtikrinimo paslauga pasikliaujantys fiziniai ar juridiniai asmenys;

(33) techninės priežiūros operacijos, per kurias paslaugos tampa tik iš dalies prieinamos arba neprieinamos, neturėtų būti laikomos dideliais incidentais, jei tos paslaugos tokiomis tampa pagal techninės priežiūros operacijos planą. Be to, dideliais incidentais neturėtų būti laikomi atvejai, kai paslauga neprieinama tampa dėl planinių pertrūkių, pavyzdžiui, kai jos teikimas pertraukiamas arba ji neprieinama tampa pagal iš anksto sudarytą susitarimą;

(34) incidento, paveikiančio paslaugos prieinamumą, trukmė turėtų būti skaičiuojama nuo tada, kai tinkamas tokios paslaugos veikimas sutrinka, iki tada, kai jis atkuriamas. Tais atvejais, kai atitinkamas subjektas sutrikimo pradžios momento nustatyti negali, incidento trukmė turėtų būti skaičiuojama nuo ankstesnio iš šių momentų: incidento nustatymo momento arba incidento užregistravimo tinklo ar sistemos žurnaluose arba kituose duomenų šaltiniuose momento;

(35) visiško paslaugos neprieinamumo trukmė turėtų būti skaičiuojama nuo momento, kurį paslauga tampa visiškai neprieinama naudotojams, iki momento, kurį įprasta veikla ar operacijos atkuriamos iki tokio paslaugų lygio, koks buvo užtikrinamas iki incidento. Tais atvejais, kai atitinkamas subjektas negali nustatyti, kada paslauga tapo visiškai neprieinama, neprieinamumo trukmė turėtų būti skaičiuojama nuo momento, kurį tas subjektas nustatė, kad paslauga neprieinama;

(36) nustatydami incidento sukeltus tiesioginius finansinius nuostolius, atitinkami subjektai turėtų atsižvelgti į visus dėl jo patirtus finansinius nuostolius, tokius kaip programinės įrangos, aparatinės įrangos ar infrastruktūros keitimo ar perkėlimo išlaidos, išlaidos darbuotojams, įskaitant išlaidas, susijusias su darbuotojų keitimu ar perkėlimu, papildomų darbuotojų įdarbinimu, atlyginimu už viršvalandžius ir prarastų arba pablogėjusių įgūdžių atgavimu, mokesčiai, mokėtini dėl sutartinių įsipareigojimų nevykdymo, žalos atlyginimo ir kompensacijų klientams išlaidos, nuostoliai dėl negautų pajamų, su vidaus ir išorės komunikacija susijusios išlaidos, konsultavimosi išlaidos, įskaitant išlaidas, susijusias su teisinėmis konsultacijomis, teismo ekspertizės paslaugomis ir teisinės gynybos paslaugomis, ir kitos su incidentu susijusios išlaidos. Tačiau incidento sukeltais finansiniais nuostoliais neturėtų būti laikomos administracinės baudos ir kasdienei veiklai vykdyti būtinos išlaidos, be kita ko, infrastruktūros, įrenginių, aparatinės įrangos ir programinės įrangos bendrosios techninės priežiūros išlaidos, darbuotojų įgūdžių atnaujinimo išlaidos, vidaus ar išorės išlaidos veiklai po incidento pagerinti, įskaitant naujovinimų, patobulinimų ir rizikos vertinimo iniciatyvų išlaidas, ir draudimo įmokos. Finansinių nuostolių sumas atitinkami subjektai turėtų apskaičiuoti remdamiesi turimais duomenimis, o tais atvejais, kai faktinių finansinių nuostolių sumų nustatyti neįmanoma, subjektai turėtų apskaičiuoti tų sumų įverčius;

(37) atitinkami subjektai taip pat turėtų privalėti pranešti apie incidentus, dėl kurių mirė arba gali mirti arba didelę žalą sveikatai patyrė arba gali patirti fiziniai asmenys, nes tokie incidentai yra itin sunkūs atvejai, kuriais padaroma didelė turtinė ar neturtinė žala. Pavyzdžiui, dėl atitinkamą subjektą paveikusio incidento gali tapti neprieinamos sveikatos priežiūros ar skubiosios pagalbos paslaugos arba būti pažeistas duomenų konfidencialumas ar vientisumas ir taip padarytas poveikis fizinių asmenų sveikatai. Nustatydami, ar incidentas padarė arba gali padaryti didelę žalą fizinio asmens sveikatai, atitinkami subjektai turėtų atsižvelgti į tai, ar jis sukėlė arba gali sukelti sunkių sužalojimų ir sveikatos sutrikimų. Atitinkami subjektai neturėtų būti įpareigoti tuo tikslu rinkti papildomą informaciją, prie kurios jie neturi prieigos;

(38) atitinkamo subjekto teikiama paslauga tik iš dalies prieinama turėtų būti laikoma visų pirma tada, kai ji veikia daug lėčiau, palyginti su vidutine atsako trukme, arba kai veikia ne visos jos funkcijos. Atsako delsai įvertinti, kai įmanoma, turėtų būti taikomi objektyvūs kriterijai, pagrįsti vidutine atitinkamų subjektų teikiamų paslaugų atsako trukme. Paslaugos funkcijų pavyzdžiai – pokalbių funkcija arba vaizdų paieškos funkcija;

(39) sėkminga, kaip įtariama, piktavališka ir neteisėta prieiga prie atitinkamo subjekto tinklų ir informacinių sistemų turėtų būti laikoma dideliu incidentu, jei naudojantis ta prieiga galima smarkiai sutrikdyti veiklą. Pavyzdžiui, jei kibernetinis užpuolikas iš anksto įsiskverbia į atitinkamo subjekto tinklų ir informacines sistemas siekdamas sutrikdyti paslaugų teikimą ateityje, incidentas turėtų būti laikomas dideliu;

(40) tos pačios akivaizdžios pagrindinės priežasties siejami pasikartojantys incidentai, kurie atskirai neatitinka didelio incidento kriterijaus, sudėti kartu turėtų būti laikomi dideliu incidentu, jei sudėti kartu jie atitinka su finansiniais nuostoliais susijusį kriterijų ir jei per šešis mėnesius jie įvyko bent dukart. Tokie pasikartojantys incidentai gali rodyti didelius atitinkamo subjekto kibernetinio saugumo rizikos valdymo procedūrų trūkumus bei spragas ir kibernetinio saugumo brandos lygį. Be to, dėl tokių pasikartojančių incidentų atitinkamas subjektas gali patirti didelių finansinių nuostolių;

(41) vadovaudamasi Direktyvos (ES) 2022/2555 21 straipsnio 5 dalimi ir 23 straipsnio 11 dalimi, Komisija dėl įgyvendinimo akto projekto keitėsi rekomendacijomis ir bendradarbiavo su Bendradarbiavimo grupe ir ENISA;

(42) vadovaujantis Europos Parlamento ir Tarybos reglamento (ES) 2018/1725 ([3]) 42 straipsnio 1 dalimi, buvo konsultuojamasi su Europos duomenų apsaugos priežiūros pareigūnu ir 2024 m. rugsėjo 1 d. jis pateikė nuomonę;

(43) šiame reglamente nustatytos priemonės atitinka pagal Direktyvos (ES) 2022/2555 39 straipsnį įsteigto komiteto nuomonę,

PRIĖMĖ ŠĮ REGLAMENTĄ:

1 straipsnis

Dalykas

Šiuo reglamentu nustatomi Direktyvos (ES) 2022/2555 21 straipsnio 2 dalyje nurodytų priemonių techniniai ir metodiniai reikalavimai ir pateikiamas išsamesnis atvejų, kuriais incidentas pagal Direktyvos (ES) 2022/2555 23 straipsnio 3 dalį turi būti laikomas dideliu, apibūdinimas, skirti DNS paslaugų teikėjams, aukščiausio lygio domenų vardų registrams, debesijos kompiuterijos paslaugų teikėjams, duomenų centrų paslaugų teikėjams, turinio teikimo tinklų teikėjams, valdomų paslaugų teikėjams, valdomų saugumo paslaugų teikėjams, elektroninių prekyviečių, interneto paieškos sistemų ir socialinių tinklų paslaugų platformų teikėjams ir patikimumo užtikrinimo paslaugų teikėjams (atitinkamiems subjektams).

2 straipsnis

Techniniai ir metodiniai reikalavimai

1. Atitinkamiems subjektams skirti Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a–j punktuose nurodytų kibernetinio saugumo rizikos valdymo priemonių techniniai ir metodiniai reikalavimai yra nustatyti šio reglamento priede.

2. Įgyvendindami ir taikydami šio reglamento priede nustatytus kibernetinio saugumo rizikos valdymo priemonių techninius ir metodinius reikalavimus, atitinkami subjektai užtikrina tinklų ir informacinių sistemų saugumo lygį, atitinkantį kylančią riziką. Tuo tikslu jie, laikydamiesi šio reglamento priede nustatytų kibernetinio saugumo rizikos valdymo priemonių techninių ir metodinių reikalavimų, deramai atsižvelgia į jiems kylančios rizikos dydį, savo dydį ir incidentų tikimybę bei sunkumą, be kita ko, jų socialinį ir ekonominį poveikį.

([3]) 2018 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2018/1725 dėl fizinių asmenų apsaugos Sąjungos institucijoms, organams, tarnyboms ir agentūroms tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinamas Reglamentas (EB) Nr. 45/2001 ir Sprendimas Nr. 1247/2002/EB (OL L 295, 2018 11 21, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

Tais atvejais, kai šio reglamento priede numatyta, kad tam tikras kibernetinio saugumo rizikos valdymo priemonės techninis ar metodinis reikalavimas yra taikomas, kai tikslinga, kai taikytina ir tiek, kiek įmanoma, ir kai atitinkamas subjektas mano, kad taikyti tokius techninius ir metodinius reikalavimus jo atveju nėra tikslinga, taikytina ar įmanoma, jis dokumentuose suprantamai užfiksuoja su tuo susijusius savo argumentus.

3 straipsnis

Dideli incidentai

1. Taikant Direktyvos (ES) 2022/2555 23 straipsnio 3 dalį, su atitinkamu subjektu susijęs incidentas laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) dėl incidento atitinkamas subjektas patyrė arba gali patirti tiesioginių finansinių nuostolių, kurių suma viršija mažesniąją iš šių sumų: 500 000 EUR arba 5 % ankstesnių finansinių metų bendros metinės atitinkamo subjekto apyvartos;

b) dėl incidento buvo arba gali būti išgautos atitinkamo subjekto komercinės paslaptys, apibrėžtos Direktyvos (ES) 2016/943 2 straipsnio 1 punkte;

c) dėl incidento mirė arba gali mirti fizinis asmuo;

d) dėl incidento fizinis asmuo patyrė arba gali patirti didelę žalą sveikatai;

e) prie tinklų ir informacinių sistemų įgyta sėkminga, kaip įtariama, piktavališka ir neteisėta prieiga, kuria naudojantis galima smarkiai sutrikdyti veiklą;

f) incidentas atitinka 4 straipsnyje nustatytus kriterijus;

g) incidentas atitinka vieną ar daugiau iš 5–14 straipsniuose nustatytų kriterijų.

2. Planiniai paslaugos teikimo pertrūkiai ir numatyti techninės priežiūros operacijų, atliekamų atitinkamų subjektų arba jų vardu, padariniai dideliais incidentais nelaikomi.

3. 7 straipsnio ir 9–14 straipsnių taikymo tikslais apskaičiuodami incidento paveiktų naudotojų skaičių, atitinkami subjektai atsižvelgia į visus šiuos elementus:

a) skaičių klientų, sudariusių su atitinkamu subjektu sutartį, suteikiančią jiems prieigą prie atitinkamo subjekto tinklų ir informacinių sistemų arba per tas tinklų ir informacines sistemas teikiamų ar prieinamų paslaugų;

b) skaičių fizinių ir juridinių asmenų, susijusių su verslo klientais, besinaudojančiais subjektų tinklų ir informacinėmis sistemomis arba per tas tinklų ir informacines sistemas teikiamomis ar prieinamomis paslaugomis.

4 straipsnis

Pasikartojantys incidentai

Incidentai, kurie atskirai nelaikomi 3 straipsnyje apibūdintais dideliais incidentais, sudėti kartu yra laikomi vienu dideliu incidentu, jei atitinka visus šiuos kriterijus:

a) per šešis mėnesius jie įvyko bent dukart;

b) juos sieja ta pati pagrindinė priežastis;

c) sudėti kartu jie atitinka 3 straipsnio 1 dalies a punkte nustatytą kriterijų.

5 straipsnis

Su DNS paslaugų teikėjais susiję dideli incidentai

Su DNS paslaugų teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) rekursinio arba patikimo domenų vardų keitimo paslauga yra visiškai neprieinama ilgiau kaip 30 minučių;

b) rekursinio arba patikimo domenų vardų keitimo paslaugos atsako į DNS užklausas vidutinė trukmė ilgiau nei vieną valandą viršija 10 sekundžių;

c) kyla pavojus su patikimo domenų vardų keitimo paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui, išskyrus atvejus, kai dėl netinkamos konfigūracijos neteisingi yra mažiau kaip 1 000 DNS paslaugų teikėjo administruojamų domenų vardų, sudarančių ne daugiau kaip 1 % DNS paslaugų teikėjo administruojamų domenų vardų, duomenys.

6 straipsnis

Su aukščiausio lygio domenų vardų registrais susiję dideli incidentai

Su aukščiausio lygio domenų vardų registru susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) patikimo domenų vardų keitimo paslauga yra visiškai neprieinama;

b) patikimo domenų vardų keitimo paslaugos atsako į DNS užklausas vidutinė trukmė ilgiau nei vieną valandą viršija 10 sekundžių;

c) kyla pavojus su aukščiausio lygio domeno techniniu veikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui.

7 straipsnis

Su debesijos kompiuterijos paslaugų teikėjais susiję dideli incidentai

Su debesijos kompiuterijos paslaugų teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) teikiama debesijos kompiuterijos paslauga yra visiškai neprieinama ilgiau kaip 30 minučių;

b) paslaugų teikėjo teikiama debesų kompiuterijos paslauga daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių jos naudotojų ilgiau nei vieną valandą yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su debesų kompiuterijos paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su debesų kompiuterijos paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos debesų kompiuterijos paslaugos naudotojų.

8 straipsnis

Su duomenų centrų paslaugų teikėjais susiję dideli incidentai

Su duomenų centro paslaugų teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) paslaugų teikėjo valdomo duomenų centro paslauga yra visiškai neprieinama;

b) paslaugų teikėjo valdomo duomenų centro paslauga ilgiau nei vieną valandą yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su duomenų centro paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus fizinei prieigai prie paslaugų teikėjo valdomo duomenų centro.

9 straipsnis

Su turinio teikimo tinklų teikėjais susiję dideli incidentai

Su turinio teikimo tinklo teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) turinio teikimo tinklas yra visiškai neprieinamas ilgiau kaip 30 minučių;

b) turinio teikimo tinklas daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių jo naudotojų ilgiau nei vieną valandą yra prieinamas tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su turinio teikimo tinklo teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su turinio teikimo tinklo teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių to turinio teikimo tinklo naudotojų.

10 straipsnis

Su valdomų paslaugų teikėjais ar valdomų saugumo paslaugų teikėjais susiję dideli incidentai

Su valdomų paslaugų teikėju ar valdomų saugumo paslaugų teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) valdoma paslauga ar valdoma saugumo paslauga yra visiškai neprieinama ilgiau kaip 30 minučių;

b) valdoma paslauga ar valdoma saugumo paslauga daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių jos naudotojų ilgiau nei vieną valandą yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su valdomos paslaugos ar valdomos saugumo paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su valdomos paslaugos ar valdomos saugumo paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos valdomos paslaugos ar valdomos saugumo paslaugos naudotojų.

11 straipsnis

Su elektroninių prekyviečių teikėjais susiję dideli incidentai

Su elektroninės prekyvietės teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) elektroninė prekyvietė yra visiškai neprieinama daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių jos naudotojų;

b) elektroninė prekyvietė daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos elektroninės prekyvietės naudotojų yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su elektroninės prekyvietės teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su elektroninės prekyvietės teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos elektroninės prekyvietės naudotojų.

12 straipsnis

Su interneto paieškos sistemų teikėjais susiję dideli incidentai

Su interneto paieškos sistemos teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) interneto paieškos sistema yra visiškai neprieinama daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos interneto paieškos sistemos naudotojų;

b) interneto paieškos sistema daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos interneto paieškos sistemos naudotojų yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su interneto paieškos sistemos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su interneto paieškos sistemos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos interneto paieškos sistemos naudotojų.

13 straipsnis

Su socialinių tinklų paslaugų platformų teikėjais susiję dideli incidentai

Su socialinių tinklų paslaugų platformos teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) socialinių tinklų paslaugų platforma yra visiškai neprieinama daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos socialinių tinklų paslaugų platformos naudotojų;

b) socialinių tinklų paslaugų platforma daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos socialinių tinklų paslaugų platformos naudotojų yra prieinama tik iš dalies;

c) dėl, kaip įtariama, piktavališko veiksmo kyla pavojus su socialinių tinklų paslaugų platformos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui;

d) kyla pavojus su socialinių tinklų paslaugų platformos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 5 procentams arba daugiau kaip 1 milijonui (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių tos socialinių tinklų paslaugų platformos naudotojų.

14 straipsnis

Su patikimumo užtikrinimo paslaugų teikėjais susiję dideli incidentai

Su patikimumo užtikrinimo paslaugos teikėju susijęs incidentas pagal 3 straipsnio 1 dalies g punktą laikomas dideliu, jei atitinka vieną ar daugiau iš šių kriterijų:

a) patikimumo užtikrinimo paslauga yra visiškai neprieinama ilgiau kaip 20 minučių;

b) patikimumo užtikrinimo paslauga yra neprieinama naudotojams ar pasikliaujančiosioms šalims ilgiau nei vieną valandą per kalendorinę savaitę;

c) patikimumo užtikrinimo paslauga daugiau kaip 1 procentui arba daugiau kaip 200 000 (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių naudotojų ar pasikliaujančiųjų šalių yra prieinama tik iš dalies;

d) kyla pavojus fizinei prieigai prie tinklų ir informacinių sistemų buvimo vietos, į kurią patekti turi teisę tik patikimi patikimumo užtikrinimo paslaugų teikėjo darbuotojai, arba pavojus tokios fizinės prieigos apsaugai;

e) kyla pavojus su patikimumo užtikrinimo paslaugos teikimu susijusių saugomų, perduodamų ar tvarkomų duomenų vientisumui, konfidencialumui ar autentiškumui ir tai daro poveikį daugiau kaip 0,1 procento arba daugiau kaip 100 (pasirenkamas mažesnis iš šių skaičių) Sąjungoje esančių naudotojų ar pasikliaujančiųjų šalių.

15 straipsnis

Panaikinimas

Komisijos įgyvendinimo reglamentas (ES) 2018/151 ([4]) panaikinamas.

16 straipsnis

Įsigaliojimas ir taikymas

Šis reglamentas įsigalioja dvidešimtą dieną po jo paskelbimo *Europos Sąjungos oficialiajame leidinyje*.

Šis reglamentas privalomas visas ir tiesiogiai taikomas visose valstybėse narėse.

Priimta Briuselyje 2024 m. spalio 17 d.

Komisijos vardu
Pirmininkė
Ursula VON DER LEYEN

([4]) 2018 m. sausio 30 d. Komisijos įgyvendinimo reglamentas (ES) 2018/151, kuriuo nustatomos Europos Parlamento ir Tarybos direktyvos (ES) 2016/1148 taikymo taisyklės, kuriomis patikslinami elementai, į kuriuos turi atsižvelgti skaitmeninių paslaugų teikėjai, kad galėtų valdyti tinklų ir informacinių sistemų saugumui kylančią riziką, ir parametrai, pagal kuriuos nustatoma, ar incidentas daro didelį poveikį (OL L 26, 2018 1 31, p. 48, ELI: http://data.europa.eu/eli/reg_impl/2018/151/oj).

PRIEDAS

Šio reglamento 2 straipsnyje nurodyti techniniai ir metodiniai reikalavimai

1. **Tinklų ir informacinių sistemų saugumo politika (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a punktas)**

1.1. *Tinklų ir informacinių sistemų saugumo politika*

1.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a punkto tikslais tinklų ir informacinių sistemų saugumo politika turi atitikti šiuos reikalavimus:

a) joje nustatomas atitinkamų subjektų požiūris į savo tinklų ir informacinių sistemų saugumo valdymą;

b) ji atitinka atitinkamų subjektų verslo strategiją ir tikslus ir juos papildo;

c) joje nustatomi tinklų ir informacijos saugumo tikslai;

d) ji apima įsipareigojimą nuolat didinti tinklų ir informacinių sistemų saugumą;

e) ji apima įsipareigojimą suteikti jai įgyvendinti reikalingus tinkamus išteklius, įskaitant būtinus darbuotojus, finansinius išteklius, procesus, priemones ir technologijas;

f) apie ją pranešama atitinkamiems darbuotojams ir atitinkamoms suinteresuotosioms išorės šalims ir ji turi būti jų pripažinta;

g) joje nustatomos funkcijos ir pareigos pagal 1.2 punktą;

h) joje pateikiamas saugotinų dokumentų sąrašas ir nurodoma dokumentų saugojimo trukmė;

i) joje pateikiamas su konkrečiomis temomis susijusių politikos sričių sąrašas;

j) joje nustatomi rodikliai ir priemonės, skirti jos įgyvendinimui ir esamam atitinkamų subjektų tinklų ir informacijos saugumo brandos lygiui stebėti;

k) joje nurodoma data, kada ją turi oficialiai patvirtinti atitinkamų subjektų valdymo organai (toliau – valdymo organai).

1.1.2. Valdymo organai bent kasmet, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai, peržiūri tinklų ir informacinių sistemų saugumo politiką ir prireikus ją atnaujina. Peržiūros rezultatai dokumentuojami.

1.2. *Funkcijos, pareigos ir įgaliojimai*

1.2.1. Įgyvendindami 1.1 punkte nurodytą tinklų ir informacinių sistemų saugumo politiką, atitinkami subjektai nustato su tinklų ir informacinių sistemų saugumu susijusias pareigas ir įgaliojimus ir priskiria juos funkcijoms, paskirsto pagal atitinkamų subjektų poreikius ir praneša apie juos valdymo organams.

1.2.2. Atitinkami subjektai reikalauja, kad visi darbuotojai ir visos trečiosios šalys taikytų tinklų ir informacinių sistemų saugumo priemones pagal atitinkamų subjektų nustatytą tinklų ir informacijos saugumo politiką, su konkrečiomis temomis susijusias politikos sritis ir procedūras.

1.2.3. Bent vienas asmuo tiesiogiai atsiskaito valdymo organams tinklų ir informacinių sistemų saugumo klausimais.

1.2.4. Priklausomai nuo atitinkamų subjektų dydžio, tinklų ir informacinių sistemų saugumas užtikrinamas ne tik vykdant esamas funkcijas, bet ir specialias funkcijas ir pareigas.

1.2.5. Kai taikytina, prieštaringos pareigos ir atsakomybės sritys atskiriamos.

1.2.6. Valdymo organai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai, peržiūri funkcijas, pareigas ir įgaliojimus ir prireikus juos atnaujina.

2. **Rizikos valdymo politika (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a punktas)**

2.1. *Rizikos valdymo sistema*

2.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies a punkto tikslais atitinkami subjektai sukuria ir taiko tinkamą rizikos valdymo sistemą, kuria siekiama nustatyti ir šalinti tinklų ir informacinių sistemų saugumui kylančią riziką. Atitinkami subjektai atlieka ir dokumentuoja rizikos vertinimus ir, remdamiesi jų rezultatais, parengia, įgyvendina ir stebi rizikos priežiūros planą. Rizikos vertinimo rezultatus ir liekamąją riziką tvirtina valdymo organai arba, kai taikytina, asmenys, kurie yra atskaitingi ir turi įgaliojimus valdyti riziką, jei atitinkami subjektai užtikrina tinkamą ataskaitų teikimą valdymo organams.

2.1.2. 2.1.1 punkto tikslais atitinkami subjektai sukuria rizikos identifikavimo, analizės, vertinimo ir priežiūros procedūras (toliau – kibernetinio saugumo rizikos valdymo procesas). Atitinkamais atvejais kibernetinio saugumo rizikos valdymo procesas yra neatsiejama atitinkamų subjektų bendro rizikos valdymo proceso dalis. Įgyvendindami kibernetinio saugumo rizikos valdymo procesą, atitinkami subjektai:

a) laikosi rizikos valdymo metodikos;

b) nustato priimtinos rizikos lygį pagal atitinkamų subjektų norimą prisiimti riziką;

c) nustato ir taiko atitinkamus rizikos kriterijus;

d) laikydamiesi visus pavojus apimančio požiūrio, nustato ir dokumentuoja tinklų ir informacinių sistemų saugumui kylančią riziką, visų pirma susijusią su trečiosiomis šalimis, ir riziką, dėl kurios gali sutrikti tinklų ir informacinių sistemų prieinamumas, vientisumas, autentiškumas ir konfidencialumas, be kita ko, nustato kritinį funkcionavimo trikčių tašką;

e) analizuoja tinklų ir informacinių sistemų saugumui kylančią riziką, įskaitant jos grėsmę, tikimybę, poveikį ir lygį, atsižvelgdami į žvalgybos informaciją apie kibernetines grėsmes ir pažeidžiamumą;

f) vertina nustatytą riziką pagal rizikos kriterijus;

g) nustato tinkamas rizikos priežiūros galimybes ir priemones ir jų prioritetus;

h) nuolat stebi rizikos priežiūros priemonių įgyvendinimą;

i) nustato, kas atsakingas už rizikos priežiūros priemonių įgyvendinimą ir kada jos turėtų būti įgyvendinamos;

j) išsamiai dokumentuoja rizikos priežiūros plane pasirinktas rizikos priežiūros priemones ir priežastis, pateisinančias liekamosios rizikos pripažinimą.

2.1.3. Nustatydami tinkamas rizikos priežiūros galimybes ir priemones ir jų prioritetus, atitinkami subjektai atsižvelgia į rizikos vertinimo rezultatus, kibernetinio saugumo rizikos valdymo priemonių veiksmingumo vertinimo procedūros rezultatus, įgyvendinimo išlaidas, palyginti su tikėtina nauda, 12.1 punkte nurodytą turto klasifikavimo kategoriją ir 4.1.3 punkte nurodytą poveikio veiklai analizę.

2.1.4. Atitinkami subjektai planiniu periodiškumu, bet ne rečiau nei kartą per metus, taip pat atsiradus reikšmingiems veiklos pokyčiams, kilus rizikai ar įvykus dideliems incidentams, peržiūri rizikos vertinimo rezultatus ir rizikos priežiūros planą ir prireikus juos atnaujina.

2.2. *Atitikties reikalavimams stebėsena*

2.2.1. Atitinkami subjektai periodiškai peržiūri, kaip laikomasi jų tinklų ir informacinių sistemų saugumo politikos, su konkrečia tema susijusios politikos, taisyklių ir standartų. Valdymo organai reguliariai teikiamomis ataskaitomis informuojami apie tinklų ir informacijos saugumo būklę, nustatytą remiantis atitikties reikalavimams peržiūromis.

2.2.2. Atitinkami subjektai įdiegia veiksmingą atitikties reikalavimams ataskaitų teikimo sistemą, atitinkančią jų struktūras, veiklos aplinką ir grėsmių aplinką. Atitikties reikalavimams ataskaitų teikimo sistema turi būti pajėgi teikti valdymo organams informacija pagrįstą esamos atitinkamų subjektų rizikos valdymo padėties apžvalgą.

2.2.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai, vykdo atitikties reikalavimams stebėseną.

2.3. *Nepriklausoma informacijos ir tinklo saugumo peržiūra*

2.3.1. Atitinkami subjektai nepriklausomai peržiūri savo požiūrį į tinklų ir informacinių sistemų saugumo valdymą ir jo įgyvendinimą, įskaitant žmones, procesus ir technologijas.

2.3.2. Atitinkami subjektai parengia ir taiko nepriklausomų peržiūrų, kurias atlieka tinkamos kompetencijos atlikti auditą turintys asmenys, vykdymo procesus. Kai nepriklausomą peržiūrą atlieka atitinkamo subjekto darbuotojai, peržiūras atliekantys asmenys negali būti pavaldūs peržiūrimos srities darbuotojams. Jei dėl subjekto dydžio tokio pavaldumo neįmanoma atskirti, atitinkami subjektai įdiegia alternatyvias priemones peržiūrų nešališkumui užtikrinti.

2.3.3. Apie nepriklausomų peržiūrų rezultatus, įskaitant pagal 2.2 punktą vykdomos atitikties reikalavimams stebėsenos ir pagal 7 punktą vykdomos stebėsenos bei atliekamo vertinimo rezultatus, pranešama valdymo organams. Imamasi taisomųjų veiksmų arba prisiimama liekamoji rizika pagal atitinkamų subjektų rizikos priimtinumo kriterijus.

2.3.4. Nepriklausomos peržiūros atliekamos planiniais intervalais, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai.

3. **Incidentų valdymas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies b punktas)**

3.1. *Incidentų valdymo politika*

3.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies b punkto tikslais atitinkami subjektai nustato ir įgyvendina incidentų valdymo politiką, kuria nustatomos incidentų aptikimo, analizės, sustabdymo ar reagavimo į juos, veiklos atkūrimo po jų, dokumentavimo ir pranešimo apie juos funkcijos, pareigos ir procedūros.

3.1.2. 3.1.1 punkte nurodyta politika turi derėti su 4.1 punkte nurodytu veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planu. Politika apima:

a) incidentų skirstymo į kategorijas sistemą, atitinkančią įvykių vertinimą ir klasifikavimą, atliekamus pagal 3.4.1 punktą;

b) veiksmingos komunikacijos planus, be kita ko, eskalavimo ir pranešimo;

c) incidentų aptikimo ir tinkamo reagavimo į juos funkcijų priskyrimą kompetentingiems darbuotojams;

d) dokumentus, naudotinus aptinkant incidentus ir reaguojant į juos, pavyzdžiui, reagavimo į incidentus vadovus, eskalavimo schemas, kontaktų sąrašus ir šablonus.

3.1.3. Politikos dokumentuose nustatytos funkcijos, pareigos ir procedūros planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai, testuojamos, peržiūrimos ir prireikus atnaujinamos.

3.2. *Stebėsena ir registravimas*

3.2.1. Atitinkami subjektai nustato procedūras ir naudoja priemones savo tinkluose ir informacinėse sistemose vykdomai veiklai stebėti ir registruoti, siekdami aptikti įvykius, kurie galėtų būti laikomi incidentais, ir atitinkamai reaguoti, kad būtų sumažintas jų poveikis.

3.2.2. Kiek įmanoma, stebėsena turi būti automatizuota ir vykdoma nuolat arba periodiškai, atsižvelgiant į veiklos pajėgumus. Atitinkami subjektai savo stebėsenos veiklą vykdo taip, kad būtų kuo mažiau klaidingų teigiamų ir neigiamų rezultatų.

3.2.3. Atitinkami subjektai tvarko, dokumentuoja ir peržiūri registracijos žurnalus pagal 3.2.1 punkte nurodytas procedūras. Atitinkami subjektai, remdamiesi pagal 2.1 punktą atlikto rizikos vertinimo rezultatais, sudaro turto, kurio naudojimas registruojamas, sąrašą. Kai tikslinga, registracijos žurnaluose pateikiama informacija apie:

a) siunčiamąjį ir gaunamąjį tinklo srautus;

b) atitinkamų subjektų tinklų ir informacinių sistemų naudotojų sukūrimą, pakeitimą ar pašalinimą ir leidimų pratęsimą;

c) prieigą prie sistemų ir taikomųjų programų;

d) su tapatumo nustatymu susijusius įvykius;

e) visą privilegijuotą prieigą prie sistemų ir taikomųjų programų ir administratoriaus paskyrų vykdomą veiklą;

f) prieigą prie ypatingos svarbos konfigūracijos ir atsarginių rinkmenų arba jų pakeitimus;

g) įvykių registracijos įrašus ir saugumo priemonių, pvz., antivirusinių programų, įsibrovimo aptikimo sistemų ar užkardų, registracijos įrašus;

h) sistemos išteklių naudojimą ir jų veiksmingumą;

i) fizinę prieigą prie infrastruktūros;

j) prieigą prie jų tinklo įrangos ir prietaisų ir jų naudojimą;

k) įvairių registracijos žurnalų registracijos aktyvinimą, sustabdymą ir pristabdymą;

l) su aplinka susijusius įvykius.

3.2.4. Registracijos žurnalai periodiškai peržiūrimi siekiant nustatyti, ar nėra kokių nors neįprastų ar nepageidaujamų tendencijų. Kai tikslinga, atitinkami subjektai nustato atitinkamas pavojaus signalo slenkstines vertes. Jei nustatytos pavojaus signalo slenkstinės vertės viršijamos, pavojaus signalas, jei reikia, įjungiamas automatiškai. Atitinkami subjektai užtikrina, kad įsijungus pavojaus signalui būtų inicijuotas kvalifikuotas ir tinkamas reagavimas.

3.2.5. Atitinkami subjektai tvarko registracijos žurnalus ir kuria jų atsargines kopijas iš anksto nustatytos trukmės laikotarpį ir saugo juos nuo neteisėtos prieigos ar pakeitimų.

3.2.6. Kiek įmanoma, atitinkami subjektai užtikrina, kad visose sistemose būtų sinchronizuoti laiko šaltiniai, kad žurnalus būtų galima susieti sistemose įvykių vertinimo tikslais. Atitinkami subjektai sudaro ir tvarko visų registruojamų turto objektų sąrašą ir užtikrina, kad stebėsenos ir registravimo sistemos turėtų atsarginius pajėgumus. Stebėsenos ir registravimo sistemų prieinamumas stebimas nepriklausomai nuo jų stebimų sistemų.

3.2.7. Procedūros ir registruojamų turto objektų sąrašas periodiškai ir po didelių incidentų peržiūrimi ir prireikus atnaujinami.

3.3. *Pranešimas apie įvykius*

3.3.1. Atitinkami subjektai įdiegia paprastą mechanizmą, kad jų darbuotojai, tiekėjai ir klientai galėtų pranešti apie įtartinus įvykius.

3.3.2. Atitinkami subjektai, kai tikslinga, praneša apie pranešimo apie įvykius mechanizmą savo tiekėjams ir klientams ir nuolat moko savo darbuotojus, kaip naudotis mechanizmu.

3.4. *Įvykių vertinimas ir klasifikavimas*

3.4.1. Atitinkami subjektai įvertina įtartinus įvykius siekdami išsiaiškinti, ar jie yra incidentai, ir, jei taip, nustato jų pobūdį ir sunkumą.

3.4.2. 3.4.1 punkto tikslais atitinkami subjektai veikia taip:

a) atlieka vertinimą, grindžiamą iš anksto nustatytais kriterijais ir rikiavimu, kad būtų galima nustatyti incidentų apribojimo ir likvidavimo prioritetus;

b) kas ketvirtį įvertina, ar yra pasikartojančių incidentų, nurodytų šio reglamento 4 straipsnyje;

c) peržiūri atitinkamus registracijos žurnalus įvykių vertinimo ir klasifikavimo tikslais;

d) įdiegia žurnalų susiejimo ir analizės procesą ir

e) iš naujo įvertina ir suklasifikuoja įvykius, jei gaunama naujos informacijos arba kai atliekama anksčiau turėtos informacijos analizė.

3.5. *Reagavimas į incidentus*

3.5.1. Atitinkami subjektai laiku reaguoja į incidentus laikydamiesi dokumentais įformintų procedūrų.

3.5.2. Reagavimo į incidentus procedūras sudaro šie etapai:

a) incidento sustabdymą siekiant užkirsti kelią jo padariniams plisti;

b) likvidavimą, kad incidentas nesitęstų arba nepasikartotų,

c) veiklos atkūrimą po incidento, kai būtina.

3.5.3. Atitinkami subjektai parengia komunikacijos planus ir procedūras:

a) su reagavimo į kompiuterių saugumo incidentus tarnybomis (CSIRT) arba, kai taikytina, su kompetentingomis institucijomis, susijusiomis su pranešimu apie incidentus,

b) skirtus subjekto darbuotojų tarpusavio komunikacijai ir komunikacijai su atitinkamais suinteresuotaisiais subjektais, nepriklausančiais atitinkamam subjektui.

3.5.4. Atitinkami subjektai registruoja reagavimo į incidentus veiklą pagal 3.2.1 punkte nurodytas procedūras, taip pat registruoja įrodymus.

3.5.5. Atitinkami subjektai planiniu periodiškumu testuoja savo reagavimo į incidentus procedūras.

3.6. *Peržiūros po incidento*

3.6.1. Kai tinkama, atitinkami subjektai, atkūrę veiklą po incidento, atlieka peržiūras po incidento. Atliekant peržiūras po incidento, kai įmanoma, nustatoma pagrindinė incidento priežastis ir dokumentuojama įgyta patirtis, siekiant sumažinti būsimų incidentų skaičių ir padarinius.

3.6.2. Atitinkami subjektai užtikrina, kad peržiūros po incidento padėtų pagerinti jų požiūrį į tinklų ir informacijos saugumą, rizikos priežiūros priemones ir incidentų valdymo, aptikimo ir reagavimo į juos procedūras.

3.6.3. Atitinkami subjektai planiniu periodiškumu tikrina, ar įvykus incidentams buvo atliktos peržiūros po incidento.

4. **Veiklos tęstinumas ir krizių valdymas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies c punktas)**

4.1. *Veiklos tęstinumo ir jos atkūrimo po ekstremaliųjų įvykių planas*

4.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies c punkto tikslais atitinkami subjektai parengia ir tvarko veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planą, taikomą įvykus incidentams.

4.1.2. Atitinkamų subjektų veikla atkuriama pagal veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planą. Planas grindžiamas pagal 2.1 punktą atlikto rizikos vertinimo rezultatais ir, kai tikslinga, jame pateikiama ši informacija:

a) tikslas, taikymo sritis ir adresatai;

b) funkcijos ir pareigos;

c) pagrindiniai kontaktai ir (vidaus bei išorės) komunikacijos kanalai;

d) plano vykdymo ir vykdymo nutraukimo sąlygos;

e) veiklos atkūrimo tvarka;

f) konkrečių operacijų atkūrimo planai, įskaitant atkūrimo tikslus;

g) reikalingi ištekliai, įskaitant atsargines kopijas ir atsarginius pajėgumus;

h) veiklos atkūrimas ir atnaujinimas po laikinųjų priemonių taikymo.

4.1.3. Atitinkami subjektai atlieka poveikio veiklai analizę, kad įvertintų galimą didelių jų veiklos sutrikdymų poveikį, ir, remdamiesi poveikio veiklai analizės rezultatais, nustato tinklų ir informacinių sistemų veikimo tęstinumo reikalavimus.

4.1.4. Veiklos tęstinumo planas ir veiklos atkūrimo po ekstremaliųjų įvykių planas testuojami, peržiūrimi ir prireikus atnaujinami planiniais intervalais, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai. Atitinkami subjektai užtikrina, kad į planus būtų įtraukta patirtis, įgyta atliekant tokius testus.

4.2. *Atsarginių kopijų ir atsarginių pajėgumų valdymas*

4.2.1. Atitinkami subjektai saugo atsargines duomenų kopijas ir suteikia pakankamai turimų išteklių, įskaitant įrenginius, tinklų ir informacines sistemas ir darbuotojus, kad būtų užtikrinti pakankami atsarginiai pajėgumai.

4.2.2. Remdamiesi pagal 2.1 punktą atlikto rizikos vertinimo rezultatais ir veiklos tęstinumo planu, atitinkami subjektai parengia atsarginių kopijų kūrimo planus, kurie apima:

a) veiklos atkūrimo laiką;

b) užtikrinimą, kad atsarginės kopijos būtų išsamios ir tikslios, įskaitant konfigūracijos duomenis ir duomenis, saugomus debesijos paslaugų aplinkoje;

c) atsarginių kopijų laikymą (prijungtoje arba atjungtoje aplinkoje) saugioje vietoje arba vietose, kurios nėra tame pačiame tinkle kaip sistema ir yra pakankamai toli, kad joms nebūtų padaryta žalos, jei pagrindinėje vietoje įvyktų ekstremalusis įvykis;

d) tinkamas fizinės ir loginės prieigos prie atsarginių kopijų kontrolės priemones, atitinkančias turto klasifikavimo lygmenį;

e) duomenų atkūrimą iš atsarginių kopijų;

f) saugojimo laikotarpius, nustatytus remiantis veiklos ir reglamentavimo reikalavimais.

4.2.3. Atitinkami subjektai periodiškai tikrina atsarginių kopijų vientisumą.

4.2.4. Remdamiesi pagal 2.1 punktą atlikto rizikos vertinimo rezultatais ir veiklos tęstinumo planu, atitinkami subjektai užtikrina, kad būtų pakankamai išteklių, užtikrindami bent dalinius šių elementų atsarginius pajėgumus:

a) tinklų ir informacinių sistemų;

b) turto, įskaitant priemones, įrangą ir atsargas;

c) darbuotojų, turinčių reikiamą atsakomybę, įgaliojimus ir kompetenciją;

d) tinkamų ryšių kanalų.

4.2.5. Kai tinkama, atitinkami subjektai užtikrina, kad išteklių, įskaitant įrenginius, sistemas ir darbuotojus, stebėsena ir koregavimas būtų tinkamai pagrįsti reikalavimais dėl atsarginių kopijų ir atsarginių pajėgumų.

4.2.6. Atitinkami subjektai periodiškai testuoja veiklos atkūrimą iš atsarginių kopijų ir naudojant atsarginius pajėgumus, siekdami užtikrinti, kad veiklos atkūrimo sąlygomis jais būtų galima pasikliauti, ir testavimas apimtų kopijas, procesus ir žinias, kad būtų užtikrintas veiksmingas veiklos atkūrimas. Atitinkami subjektai dokumentuoja testų rezultatus ir prireikus imasi taisomųjų veiksmų.

4.3. *Krizių valdymas*

4.3.1. Atitinkami subjektai įdiegia krizių valdymo procesą.

4.3.2. Atitinkami subjektai užtikrina, kad krizių valdymo procesas apimtų bent šiuos elementus:

a) darbuotojų ir, kai tinkama, tiekėjų ir paslaugų teikėjų funkcijas ir pareigas, nurodant funkcijų paskirstymą krizinėse situacijose, įskaitant konkrečius veiksmus, kurių reikia imtis;

b) tinkamas atitinkamų subjektų ir atitinkamų kompetentingų institucijų ryšių palaikymo priemones;

c) tinkamų priemonių taikymą siekiant užtikrinti tinklų ir informacinių sistemų saugumą krizinėse situacijose.

B punkto tikslais informacijos srautas tarp atitinkamų subjektų ir atitinkamų kompetentingų institucijų apima tiek privalomus pranešimus, kaip antai pranešimus apie incidentus ir susijusius terminus, tiek neprivalomus pranešimus.

4.3.3. Atitinkami subjektai įgyvendina iš CSIRT arba, kai taikytina, kompetentingų institucijų gautos informacijos apie incidentus, pažeidžiamumą, grėsmes ar galimas poveikio mažinimo priemones tvarkymo ir panaudojimo procesą.

4.3.4. Atitinkami subjektai periodiškai arba įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai testuoja, peržiūri ir prireikus atnaujina krizių valdymo planą.

5. **Tiekimo grandinės saugumas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies d punktas)**

5.1. *Tiekimo grandinės saugumo politika*

5.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies d punkto tikslais atitinkami subjektai nustato, įgyvendina ir taiko tiekimo grandinės saugumo politiką, kuria reglamentuojami santykiai su jų tiesioginiais tiekėjais ir paslaugų teikėjais, kad būtų sumažinta identifikuota rizika tinklų ir informacinių sistemų saugumui. Tiekimo grandinės saugumo politikos dokumente atitinkami subjektai identifikuoja savo vaidmenį tiekimo grandinėje ir apie jį praneša savo tiesioginiams tiekėjams ir paslaugų teikėjams.

5.1.2. Vykdydami 5.1.1 punkte nurodytą tiekimo grandinės saugumo politiką, atitinkami subjektai nustato tiekėjų ir paslaugų teikėjų atrankos ir sutarčių sudarymo kriterijus. Tie kriterijai apima:

a) tiekėjų ir paslaugų teikėjų kibernetinio saugumo praktiką, įskaitant jų saugumo plėtojimo procedūras;

b) tiekėjų ir paslaugų teikėjų gebėjimą laikytis atitinkamų subjektų nustatytų kibernetinio saugumo specifikacijų;

c) bendrą IRT produktų ir IRT paslaugų kokybę bei atsparumą ir į juos įtrauktas kibernetinio saugumo rizikos valdymo priemones, įskaitant IRT produktų ir IRT paslaugų riziką ir klasifikavimo lygmenį;

d) atitinkamų subjektų gebėjimą įvairinti tiekimo šaltinius ir, kai taikytina, apriboti susaistymą su pardavėju.

5.1.3. Nustatydami savo tiekimo grandinės saugumo politiką, atitinkami subjektai, kai taikytina, atsižvelgia į pagal Direktyvos (ES) 2022/2555 22 straipsnio 1 dalį atliktų koordinuotų ypatingos svarbos tiekimo grandinių saugumo rizikos vertinimų rezultatus.

5.1.4. Remdamiesi tiekimo grandinės saugumo politika ir atsižvelgdami į pagal šio priedo 2.1 punktą atlikto rizikos vertinimo rezultatus, atitinkami subjektai užtikrina, kad atitinkamais atvejais jų sutartyse su tiekėjais ir paslaugų teikėjais būtų nurodyta, kai tinkama, sudarant susitarimus dėl paslaugų lygio, ši informacija:

a) tiekėjams ar paslaugų teikėjams taikomi kibernetinio saugumo reikalavimai, įskaitant 6.1 punkte nustatytus reikalavimus dėl IRT paslaugų ar IRT produktų įsigijimo saugumo;

b) reikalavimai, susiję su informuotumu, įgūdžiais, mokymu ir, kai tinkama, kvalifikacijos pažymėjimais, kurių reikalaujama iš tiekėjų ar paslaugų teikėjų darbuotojų;

c) reikalavimai, susiję su tiekėjų ir paslaugų teikėjų darbuotojų asmens patikrinimu;

d) tiekėjų ir paslaugų teikėjų pareiga nepagrįstai nedelsiant pranešti atitinkamiems subjektams apie incidentus, keliančius riziką tų subjektų tinklų ir informacinių sistemų saugumui;

e) teisė į auditą arba teisė gauti audito ataskaitas;

f) tiekėjų ir paslaugų teikėjų pareiga šalinti pažeidžiamumą, keliantį pavojų atitinkamų subjektų tinklų ir informacinių sistemų saugumui;

g) reikalavimai, susiję su subranga, ir, kai atitinkami subjektai leidžia sudaryti subrangos sutartis, kibernetinio saugumo reikalavimai subrangovams, nustatyti remiantis a punkte nurodytais kibernetinio saugumo reikalavimais;

h) tiekėjų ir paslaugų teikėjų pareigos nutraukiant sutartį, pavyzdžiui, dėl informacijos, kurią tiekėjai ir paslaugų teikėjai gauna vykdydami savo užduotis, atgaminimo ir disponavimo ja.

5.1.5. Atitinkami subjektai atsižvelgia į 5.1.2 ir 5.1.3 punktuose nurodytus elementus atrinkdami naujus tiekėjus ir paslaugų teikėjus ir vykdydami 6.1 punkte nurodytą viešojo pirkimo procesą.

5.1.6. Atitinkami subjektai peržiūri tiekimo grandinės saugumo politiką ir stebi tiekėjų ir paslaugų teikėjų kibernetinio saugumo praktikos pokyčius, juos vertina ir prireikus dėl jų imasi veiksmų planiniu periodiškumu, taip pat atsiradus reikšmingiems veiklos pokyčiams, kilus rizikai ar įvykus dideliems incidentams, susijusiems su IRT paslaugų teikimu arba darantiems poveikį iš tiekėjų ir paslaugų teikėjų gautų IRT produktų saugumui.

5.1.7. 5.1.6 punkto tikslais atitinkami subjektai:

a) kai taikytina, periodiškai apžvelgia susitarimų dėl paslaugų lygio įgyvendinimo ataskaitas;

b) peržiūri incidentus, susijusius su iš tiekėjų ir paslaugų teikėjų gautais IRT produktais ir paslaugomis;

c) įvertina neplaninių peržiūrų poreikį ir išsamiai dokumentuoja nustatytus faktus;

d) analizuoja riziką, kylančią dėl pokyčių, susijusių su iš tiekėjų ir paslaugų teikėjų gautais IRT produktais ir paslaugomis, ir prireikus laiku imasi rizikos mažinimo priemonių.

5.2. *Tiekėjų ir paslaugų teikėjų sąrašas*

Atitinkami subjektai tvarko ir nuolat atnaujina savo tiesioginių tiekėjų ir paslaugų teikėjų registrą, į kurį, be kita ko, įtraukiama ši informacija:

a) kiekvieno tiesioginio tiekėjo ir paslaugų teikėjo kontaktiniai asmenys;

b) IRT produktų, paslaugų ir procesų, kuriuos tiesioginis tiekėjas ar paslaugų teikėjas teikia atitinkamam subjektui, sąrašas.

6. **Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies e punktas)**

6.1. *IRT paslaugų ir produktų įsigijimo saugumas*

6.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies e punkto tikslais atitinkami subjektai, remdamiesi pagal 2.1 punktą atliktu rizikos vertinimu, nustato ir įgyvendina procesus, kuriais siekiama valdyti riziką, kylančią dėl IRT paslaugų ar IRT produktų, skirtų komponentams, kurie yra itin svarbūs atitinkamų subjektų tinklų ir informacinių sistemų saugumui, įsigijimo iš tiekėjų ar paslaugų teikėjų per visą jų gyvavimo ciklą.

6.1.2. 6.1.1 punkto tikslais jame nurodyti procesai apima:

a) saugumo reikalavimus, taikomus įsigytinoms IRT paslaugoms ar IRT produktams;

b) reikalavimus dėl saugumo naujinių diegimo per visą IRT paslaugų ar IRT produktų naudojimo trukmę arba pakeitimo pasibaigus paramos laikotarpiui;

c) aprašomojo pobūdžio informaciją apie aparatinės ir programinės įrangos komponentus, naudojamus teikiant IRT paslaugas ar IRT produktuose;

d) aprašomojo pobūdžio informaciją apie įdiegtas IRT paslaugų ar IRT produktų kibernetinio saugumo funkcijas ir jų saugiam veikimui reikalingą konfigūraciją;

e) užtikrinimą, kad IRT paslaugos ar IRT produktai atitinka a punkte nurodytus saugumo reikalavimus;

f) teikiamų IRT paslaugų ar IRT produktų atitikties nustatytiems saugumo reikalavimams patvirtinimo metodus, taip pat patvirtinimo rezultatų dokumentavimą.

6.1.3. Atitinkami subjektai procesus ir procedūras peržiūri planiniu periodiškumu, taip pat įvykus dideliems incidentams, ir prireikus atnaujina.

6.2. *Saugaus plėtojimo gyvavimo ciklas*

6.2.1. Prieš pradėdami kurti tinklų ir informacinę sistemą, įskaitant programinę įrangą, atitinkami subjektai nustato saugaus tinklų ir informacinių sistemų plėtojimo taisykles ir jas taiko kurdami vidines tinklų ir informacines sistemas arba užsakydami tinklų ir informacinių sistemų plėtojimo paslaugas. Taisyklės taikomos visiems plėtojimo etapams, įskaitant specifikacijos rengimą, projektavimą, kūrimą, diegimą ir testavimą.

6.2.2. 6.2.1 punkto tikslais atitinkami subjektai:

a) atlieka saugumo reikalavimų analizę bet kurio plėtojimo ar įsigijimo projekto, kurį vykdo atitinkami subjektai arba kuris vykdomas tų subjektų vardu, specifikacijos rengimo ir projektavimo etapais;

b) taiko saugių sistemų projektavimo ir saugaus programavimo principus visai informacinių sistemų plėtojimo veiklai, pvz., skatina integruotąjį kibernetinį saugumą, nulinio pasitikėjimo architektūrą;

c) nustato saugumo reikalavimus, susijusius su plėtojimo aplinka;

d) nustato ir įdiegia saugumo testavimo procesus plėtojimo ciklo metu;

e) tinkamai parenka, saugo ir tvarko saugumo testų informaciją;

f) apvalo ir anonimizuoja testų duomenis, remdamiesi pagal 2.1 punktą atliktu rizikos vertinimu.

6.2.3. Užsakomosioms tinklų ir informacinių sistemų plėtojimo paslaugoms atitinkami subjektai taip pat taiko 5 ir 6.1 punktuose nurodytą politiką ir procedūras.

6.2.4. Atitinkami subjektai savo saugios plėtros taisykles planiniu periodiškumu peržiūri ir prireikus atnaujina.

6.3. *Konfigūracijos valdymas*

6.3.1. Atitinkami subjektai imasi tinkamų priemonių, kad nustatytų, dokumentuotų, įdiegtų ir stebėtų konfigūracijas, įskaitant aparatinės įrangos, programinės įrangos, paslaugų ir tinklų saugumo konfigūracijas.

6.3.2. 6.3.1 punkto tikslais atitinkami subjektai:

a) nustato ir užtikrina savo aparatinės įrangos, programinės įrangos, paslaugų ir tinklų saugumą jų konfigūracijose;

b) nustato ir įdiegia procesus ir priemones, kad būtų užtikrintas nustatytų saugių aparatinės įrangos, programinės įrangos, paslaugų ir tinklų konfigūracijų taikymas įrengtose naujose sistemose ir veikiančiose sistemose visą jų naudojimo trukmę.

6.3.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, konfigūracijas peržiūri ir prireikus atnaujina.

6.4. *Pakeitimų valdymas, remontas ir techninė priežiūra*

6.4.1. Atitinkami subjektai taiko pakeitimų valdymo procedūras, siekdami kontroliuoti tinklų ir informacinių sistemų pakeitimus. Kai taikytina, procedūros turi atitikti bendrąją atitinkamų subjektų pakeitimų valdymo politiką.

6.4.2. 6.4.1 punkte nurodytos procedūros taikomos bet kokios veikiančios programinės ir aparatinės įrangos laidoms, modifikacijoms ir skubiems pakeitimams, taip pat konfigūracijos pakeitimams. Procedūromis užtikrinama, kad tie pakeitimai prieš juos įdiegiant būtų dokumentuoti ir, remiantis pagal 2.1 punktą atliktu rizikos vertinimu, būtų atliktas jų testavimas ir vertinimas atsižvelgiant į galimą poveikį.

6.4.3. Jei dėl ekstremaliosios situacijos nebuvo galima laikytis įprastų pakeitimų valdymo procedūrų, atitinkami subjektai dokumentuoja pakeitimo rezultatą ir paaiškinimą, kodėl procedūrų nebuvo galima laikytis.

6.4.4. Atitinkami subjektai procedūras planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, peržiūri ir prireikus atnaujina.

6.5. *Saugumo testavimas*

6.5.1. Atitinkami subjektai nustato, įdiegia ir taiko saugumo testavimo politiką ir procedūras.

6.5.2. Atitinkami subjektai:

a) remdamiesi pagal 2.1 punktą atliktu rizikos vertinimu, nustato saugumo testų poreikį, apimtį, atlikimo dažnumą ir rūšį;

b) atlieka saugumo testus pagal dokumentuotą testavimo metodiką, apimančią komponentus, kurie rizikos analizėje nustatyti kaip svarbūs saugiam veikimui;

c) dokumentais patvirtina testų rūšį, apimtį, atlikimo laiką ir rezultatus, įskaitant kiekvieno nustatyto fakto kritiškumą ir jo poveikio mažinimo veiksmų vertinimą;

d) nustatę kritinius faktus, taiko poveikio mažinimo veiksmus.

6.5.3. Atitinkami subjektai savo saugumo testavimo politiką planiniu periodiškumu peržiūri ir prireikus atnaujina.

6.6. *Saugumo pataisų valdymas*

6.6.1. Atitinkami subjektai nustato ir taiko procedūras, kurios atitinka 6.4.1 punkte nurodytas pakeitimų valdymo procedūras, taip pat pažeidžiamumo valdymo, rizikos valdymo ir kitas aktualias valdymo procedūras, ir kuriomis užtikrinama, kad:

a) saugumo pataisos būtų pradėtos taikyti per pagrįstą laikotarpį nuo tada, kai jos tampa prieinamos;

b) prieš pradedant taikyti saugumo pataisas darbinėse sistemose būtų atliktas jų testavimas;

c) saugumo pataisos būtų gaunamos iš patikimų šaltinių ir būtų patikrintas jų vientisumas;

d) tais atvejais, kai pataisos nėra arba ji netaikoma pagal 6.6.2 punktą, būtų įdiegtos papildomos priemonės ir prisiimta liekamoji rizika.

6.6.2. Nukrypstant nuo 6.6.1 punkto a papunkčio, atitinkami subjektai gali nuspręsti netaikyti saugumo pataisų, kai saugumo pataisų taikymo trūkumai yra didesni už naudą kibernetiniam saugumui. Atitinkami subjektai tinkamai dokumentuoja ir pagrindžia tokio sprendimo priežastis.

6.7. *Tinklo saugumas*

6.7.1. Atitinkami subjektai imasi tinkamų priemonių, kad apsaugotų savo tinklų ir informacines sistemas nuo kibernetinių grėsmių.

6.7.2. 6.7.1 punkto tikslais atitinkami subjektai:

a) suprantamai dokumentuoja naujausią tinklo architektūrą;

b) nustato ir taiko kontrolės priemones, skirtas atitinkamų subjektų vidaus tinklo sritims apsaugoti nuo neteisėtos prieigos;

c) konfigūruoja kontrolės priemones taip, kad būtų užkirstas kelias prieigai ir tinklo ryšiams, kurie nėra būtini atitinkamų subjektų veiklai;

d) nustato ir taiko nuotolinės prieigos prie tinklų ir informacinių sistemų, įskaitant paslaugų teikėjų prieigą, kontrolės priemones;

e) sistemų, naudojamų saugumo politikos įgyvendinimui administruoti, nenaudoja kitais tikslais;

f) aiškiai uždraudžia arba atjungia nereikalingas jungtis ir paslaugas;

g) kai tinkama, suteikia prieigą prie atitinkamų subjektų tinklų ir informacinių sistemų tik tų subjektų patvirtintiems įrenginiams;

h) leidžia paslaugų teikėjams jungtis tik pateikus prašymą suteikti leidimą ir tik nustatytą laikotarpį, pvz., kol vyksta techninės priežiūros operacija;

i) atskirų sistemų tarpusavio ryšį užmezga tik patikimais kanalais, kurie nuo kitų ryšių kanalų atskiriami naudojant loginį, kriptografinį ar fizinį atskyrimą, ir užtikrina jų galutinių taškų identifikavimą bei kanalų duomenų apsaugą nuo pakeitimo ar atskleidimo;

j) priima įgyvendinimo planą, kaip visapusiškai, saugiai, tinkamai ir laipsniškai pereiti prie naujausios kartos tinklo lygmens ryšių protokolų, ir nustato priemones tokiam perėjimui paspartinti;

k) priima tarptautiniu mastu sutartų ir sąveikių šiuolaikinių e. pašto ryšių standartų diegimo įgyvendinimo planą, kad būtų užtikrintas saugus e. pašto ryšys ir taip sumažintas pažeidžiamumas dėl su e. paštu susijusių grėsmių, ir nustato priemones tokiam diegimui paspartinti;

l) taiko geriausią domenų vardų sistemos (DNS) saugumo, interneto maršruto parinkimo saugumo ir iš tinklo siunčiamo ir į jį gaunamo srauto maršruto parinkimo higienos praktiką.

6.7.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, šias priemones peržiūri ir prireikus atnaujina.

6.8. *Tinklo segmentavimas*

6.8.1. Atitinkami subjektai suskirsto sistemas į tinklus arba zonas, remdamiesi 2.1 punkte nurodyto rizikos vertinimo rezultatais. Jie atskiria savo sistemas ir tinklus nuo trečiųjų šalių sistemų ir tinklų.

6.8.2. Tuo tikslu atitinkami subjektai:

a) įvertina funkcinį, loginį ir fizinį ryšį, įskaitant vietą, tarp patikimų sistemų ir paslaugų;

b) suteikia prieigą prie tinklo ar zonos, remdamiesi tinklo ar zonos saugumo reikalavimais;

c) užtikrina, kad sistemos, kurios yra itin svarbios atitinkamų subjektų veiklai arba saugai, būtų saugiose zonose;

d) įdiegia savo ryšių tinkluose periferijos zoną, kad būtų užtikrintas iš jų tinklų užmezgamo ar į juos inicijuojamo ryšio saugumas;

e) prieigą prie zonų ir jų viduje, taip pat jų tarpusavio ryšį ir ryšį jų viduje, apriboja tik atitinkamų subjektų veiklai arba saugai užtikrinti būtina prieiga ir ryšiu;

f) atskiria specialų tinklų ir informacinių sistemų administravimo tinklą nuo atitinkamų subjektų veiklos tinklo;

g) atskiria tinklo administravimo kanalus nuo kito tinklo srauto;

h) atskiria atitinkamų subjektų paslaugų darbines sistemas nuo sistemų, naudojamų vykdant plėtojimo ir testavimo veiklą, įskaitant atsarginių kopijų kūrimą.

6.8.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, tinklo segmentavimą peržiūri ir prireikus atnaujina.

6.9. *Apsauga nuo kenkimo ir neleistinos programinės įrangos*

6.9.1. Atitinkami subjektai apsaugo savo tinklų ir informacines sistemas nuo kenkimo ir neleistinos programinės įrangos.

6.9.2. Tuo tikslu atitinkami subjektai visų pirma įdiegia priemones, kuriomis aptinkamas ir blokuojamas kenkimo ar neleistinos programinės įrangos naudojimas. Atitinkami subjektai, kai tikslinga, užtikrina, kad, remiantis pagal 2.1 punktą atliktu rizikos vertinimu ir sutartiniais susitarimais su paslaugų teikėjais, jų tinklų ir informacinėse sistemose būtų įdiegta ir reguliariai atnaujinama aptikimo ir reagavimo programinė įranga.

6.10. *Pažeidžiamumo valdymas ir atskleidimas*

6.10.1. Atitinkami subjektai gauna informaciją apie savo tinklų ir informacinių sistemų techninį pažeidžiamumą, įvertina tokio pažeidžiamumo poveikį ir imasi tinkamų priemonių jam valdyti.

6.10.2. 6.10.1 punkto tikslais atitinkami subjektai:

a) stebi informaciją apie pažeidžiamą, naudodamiesi atitinkamais kanalais, pavyzdžiui, CSIRT ir kompetentingų institucijų pranešimais arba tiekėjų ar paslaugų teikėjų teikiama informacija;

b) planiniais intervalais atlieka, kai tikslinga, pažeidžiamumo skenavimą ir registruoja skenavimo rezultatų įrodymus;

c) nepagrįstai nedelsdami pašalina pažeidžiamumą, kurį atitinkami subjektai nustatė kaip itin svarbų jų veiklai;

d) užtikrina, kad jų pažeidžiamumo valdymas būtų suderinamas su jų pakeitimų, saugumo pataisų ir incidentų valdymo procedūromis;

e) nustato pažeidžiamumo atskleidimo procedūrą pagal taikomą nacionalinę suderintą pažeidžiamumo atskleidimo politiką.

6.10.3. Kai tai pateisinama dėl galimo pažeidžiamumo poveikio, atitinkami subjektai parengia ir įgyvendina pažeidžiamumo mažinimo planą. Kitais atvejais atitinkami subjektai dokumentuoja ir pagrindžia priežastį, dėl kurios pažeidžiamumo ištaisyti nereikia.

6.10.4. Atitinkami subjektai informacijai apie pažeidžiamumą stebėti naudojamus kanalus planiniu periodiškumu peržiūri ir prireikus atnaujina.

7. **Politika ir procedūros, skirtos kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies f punktas)**

7.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies f punkto tikslais atitinkami subjektai nustato, įdiegia ir taiko politiką ir procedūras, pagal kurias vertinama, ar kibernetinio saugumo rizikos valdymo priemonės, kurių ėmėsi atitinkamas subjektas, yra veiksmingai įgyvendinamos ir palaikomos.

7.2. Taikant 7.1 punkte nurodytą politiką ir procedūras atsižvelgiama į pagal 2.1 punktą atlikto rizikos vertinimo rezultatus ir ankstesnius didelius incidentus. Atitinkami subjektai nustato:

a) kokios kibernetinio saugumo rizikos valdymo priemonės turi būti stebimos ir vertinamos, įskaitant procesus ir kontrolės priemones;

b) stebėjimo, matavimo, analizės ir vertinimo metodus, priklausomai nuo to, kas taikytina, kuriais užtikrinama, kad rezultatai būtų patikimi;

c) kada turi būti atliekama stebėsena ir matavimas;

d) kas atsakingas už kibernetinio saugumo rizikos valdymo priemonių veiksmingumo stebėseną ir matavimą;

e) kada turi būti analizuojami ir vertinami stebėsenos ir matavimo rezultatai;

f) kas turi atlikti šių rezultatų analizę ir vertinimą.

7.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai, politiką ir procedūras peržiūri ir prireikus atnaujina.

8. **Pagrindiniai kibernetinės higienos principai ir kibernetinio saugumo mokymai (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies g punktas)**

8.1. *Informuotumo didinimas ir pagrindiniai kibernetinės higienos principai*

8.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies g punkto tikslais atitinkami subjektai užtikrina, kad jų darbuotojai, įskaitant valdymo organų narius, taip pat tiesioginiai tiekėjai ir paslaugų teikėjai žinotų apie riziką, būtų informuoti apie kibernetinio saugumo svarbą ir taikytų kibernetinės higienos principus.

8.1.2. 8.1.1 punkto tikslais atitinkami subjektai savo darbuotojams, įskaitant valdymo organų narius, taip pat, kai tinkama, tiesioginiams tiekėjams ir paslaugų teikėjams pagal 5.1.4 punktą siūlo informuotumo didinimo programą, kuri:

a) turi būti įgyvendinama pagal tvarkaraštį, kad veikla būtų kartojama ir apimtų naujus darbuotojus;

b) turi būti parengta laikantis tinklų ir informacijos saugumo politikos, su konkrečia tema susijusios politikos ir atitinkamų procedūrų, susijusių su tinklų ir informacijos saugumu;

c) turi apimti atitinkamas kibernetines grėsmes, taikomas kibernetinio saugumo rizikos valdymo priemones, kontaktinius asmenis ir išteklius, skirtus papildomai informacijai ir konsultacijoms kibernetinio saugumo klausimais teikti, taip pat naudotojų kibernetinės higienos principus.

8.1.3. Kai tinkama, išbandomas informuotumo didinimo programos veiksmingumas. Informuotumo didinimo programa atnaujinama ir teikiama planiniais laikotarpiais, atsižvelgiant į kibernetinės higienos principų pokyčius, esamą grėsmių aplinką ir atitinkamiems subjektams kylančią riziką.

8.2. *Saugumo mokymai*

8.2.1. Atitinkami subjektai identifikuoja darbuotojus, kurių funkcijoms vykdyti reikia su saugumu susijusių įgūdžių ir kompetencijos, ir užtikrina, kad jie būtų reguliariai mokomi tinklų ir informacinių sistemų saugumo klausimais.

8.2.2. Atitinkami subjektai parengia, įgyvendina ir taiko mokymo programą, atitinkančią tinklų ir informacijos saugumo politiką, su konkrečiomis temomis susijusią politiką ir kitas aktualias tinklų ir informacijos saugumo procedūras, kurioje pagal atitinkamus kriterijus būtų nustatyti su tam tikromis funkcijomis ir pareigomis susiję mokymo poreikiai.

8.2.3. 8.2.1 punkte nurodyti mokymai turi būti aktualūs darbuotojo funkcijai ir turi būti vertinamas jų veiksmingumas. Rengiant mokymus atsižvelgiama į taikomas saugumo priemones ir jie apima:

a) nurodymus dėl tinklų ir informacinių sistemų, įskaitant mobiliuosius prietaisus, saugios konfigūracijos ir veikimo;

b) informavimą apie žinomas kibernetines grėsmes;

c) mokymus apie elgesį įvykus su saugumu susijusiems įvykiams.

8.2.4. Atitinkami subjektai rengia mokymus darbuotojams, kurie perkeliami į naujas pareigas ar kuriems priskiriamos naujos funkcijos, kurioms atlikti reikia su saugumu susijusių įgūdžių ir žinių.

8.2.5. Programa atnaujinama ir vykdoma periodiškai, atsižvelgiant į taikytiną politiką ir taisykles, priskirtas funkcijas, pareigas, taip pat į žinomas kibernetines grėsmes ir technologinę plėtrą.

9. **Kriptografija (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies h punktas)**

9.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies h punkto tikslais atitinkami subjektai nustato, įgyvendina ir taiko su kriptografija susijusią politiką ir procedūras, kad būtų užtikrintas tinkamas ir veiksmingas kriptografijos naudojimas siekiant apsaugoti informacijos konfidencialumą, autentiškumą ir vientisumą, atsižvelgiant į atitinkamų subjektų turto klasifikavimą ir pagal 2.1 punktą atlikto rizikos vertinimo rezultatus.

9.2. 9.1 punkte nurodyta politika ir procedūromis nustatoma:

a) kriptografinių priemonių, reikalingų atitinkamų subjektų turtui apsaugoti, įskaitant laikomus ir perduodamus duomenis, rūšis, saugumas ir kokybė, atsižvelgiant į atitinkamų subjektų turto klasifikavimą;

b) remiantis a punktu – protokolai, kuriuos reikia priimti, ar tokių protokolų šeimos, taip pat kriptografiniai algoritmai, šifravimo stiprumas, kriptografiniai sprendimai ir naudojimo praktika, kuriuos būtina patvirtinti ir kuriuos subjektai turi naudoti, laikydamiesi, kai tinkama, kriptografinio budrumo principų;

c) atitinkamų subjektų požiūris į raktų valdymą, įskaitant, kai tinkama, metodus, skirtus:

i) įvairiems kriptografinių sistemų ir taikomųjų programų raktams generuoti;

ii) viešojo rakto sertifikatams išduoti ir gauti;

iii) raktams paskirstyti numatytiems subjektams, įskaitant tai, kaip gavus raktus juos įjungti;

iv) raktams saugoti, įskaitant tai, kaip įgaliotieji naudotojai gauna prieigą prie raktų;

v) raktams keisti ir atnaujinti, įskaitant taisykles, kada ir kaip keisti raktus;

vi) atskleistiems raktams tvarkyti;

vii) raktams atšaukti, įskaitant tai, kaip raktus panaikinti arba išjungti;

viii) pamestiems arba sugadintiems raktams atkurti;

ix) raktų atsarginėms kopijoms daryti arba raktams archyvuoti;

x) raktams sunaikinti;

xi) pagrindinei su valdymu susijusiais veiklai registruoti ir jos auditams atlikti;

xii) raktų įjungimo ir išjungimo datoms nustatyti, užtikrinant, kad raktus būtų galima naudoti tik nustatytą laikotarpį pagal organizacijos raktų valdymo taisykles.

9.3. Atitinkami subjektai planiniu periodiškumu savo politiką ir procedūras peržiūri ir prireikus atnaujina, atsižvelgdami į naujausias kriptografijos technologijas.

10. **Žmogiškųjų išteklių saugumas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punktas)**

10.1. *Žmogiškųjų išteklių saugumas*

10.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punkto tikslais atitinkami subjektai užtikrina, kad jų darbuotojai ir tiesioginiai tiekėjai bei paslaugų teikėjai, kai taikytina, suprastų ir įsipareigotų vykdyti siūlomoms paslaugoms ir darbui aktualias su saugumu susijusias savo pareigas, laikantis atitinkamų subjektų tinklų ir informacinių sistemų saugumo politikos.

10.1.2. 10.1.1 punkte nurodytas reikalavimas apima:

a) mechanizmus, kuriais užtikrinama, kad visi darbuotojai, tiesioginiai tiekėjai ir paslaugų teikėjai, kai taikytina, suprastų standartinius kibernetinės higienos principus, kuriuos atitinkami subjektai taiko pagal 8.1 punktą, ir jų laikytųsi;

b) mechanizmus, kuriais užtikrinama, kad visi naudotojai, turintys administracinę ar privilegijuotą prieigą, suprastų savo funkcijas, pareigas ir įgaliojimus ir vykdytų savo veiklą jų laikydamiesi;

c) mechanizmus, kuriais užtikrinama, kad valdymo organų nariai suprastų su informacinių sistemų saugumu susijusias savo funkcijas, pareigas ir įgaliojimus ir vykdytų veiklą jų laikydamiesi;

d) darbuotojų, kvalifikuotų vykdyti atitinkamas funkcijas, įdarbinimo mechanizmai, pavyzdžiui, rekomendacijų ir kredencialų patikrinimas, patikimumo patikrinimo procedūra, sertifikatų tikrumo patvirtinimas arba testai raštu.

10.1.3. Atitinkami subjektai planiniu periodiškumu ir bent kartą per metus peržiūri darbuotojų paskyrimą vykdyti konkrečias funkcijas, kaip nurodyta 1.2 punkte, taip pat su tuo susijusius savo įsipareigojimus skirti žmogiškųjų išteklių. Prireikus jie atnaujina priskyrimą.

10.2. *Asmens patikrinimas*

10.2.1. Atitinkami subjektai tiek, kiek įmanoma, užtikrina, kad būtų atliekamas jų darbuotojų ir, kai taikytina, tiesioginių tiekėjų ir paslaugų teikėjų darbuotojų asmens patikrinimas pagal 5.1.4 punktą, jei to reikia dėl jų funkcijų, pareigų ir įgaliojimų.

10.2.2. 10.2.1 punkto tikslais atitinkami subjektai:

a) nustato kriterijus, pagal kuriuos nustatoma, kokias funkcijas, pareigas ir įgaliojimus vykdo tik asmenys, kurių asmens patikrinimas buvo atliktas;

b) užtikrina, kad prieš šiems asmenims pradedant vykdyti šias funkcijas, pareigas ir įgaliojimus būtų atliktas 10.2.1 punkte nurodytas jų asmens patikrinimas, atsižvelgiant į taikytinus įstatymus, kitus teisės aktus ir etiką proporcingai veiklos reikalavimams, turto klasifikavimą, kaip nurodyta 12.1 punkte, tinklų ir informacines sistemas, prie kurių bus jungiamasi, ir numatomą riziką.

10.2.3. Atitinkami subjektai planiniu periodiškumu peržiūri politiką ir prireikus ją atnaujina.

10.3. *Įdarbinimo procedūrų nutraukimas arba pakeitimas*

10.3.1. Atitinkami subjektai užtikrina, kad su tinklų ir informacinių sistemų saugumu susijusi atsakomybė ir pareigos, kurios lieka galioti nutraukus arba pakeitus jų darbuotojų darbo sutartį, būtų apibrėžtos sutartyje ir vykdomos.

10.3.2. 10.3.1 punkto tikslais atitinkami subjektai į asmens įdarbinimo, darbo sutarties ar susitarimo sąlygas įtraukia atsakomybę ir pareigas, kurios vis dar galioja nutraukus darbo santykius ar sutartį, pavyzdžiui, konfidencialumo sąlygas.

10.4. *Drausminė procedūra*

10.4.1. Atitinkami subjektai nustato drausminę procedūrą tinklų ir informacinių sistemų saugumo politikos pažeidimams nagrinėti, apie ją pranešą ir ją taiko. Šia procedūra atsižvelgiama į aktualius teisinius, įstatyminius, sutartinius ir veiklos reikalavimus.

10.4.2. Atitinkami subjektai planiniu periodiškumu, taip pat atsiradus teisiniams ar reikšmingiems veiklos pokyčiams arba kilus rizikai, peržiūri drausminę procedūrą ir prireikus ją atnaujina.

11. **Prieigos kontrolė (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i ir j punktai)**

11.1. *Prieigos kontrolės politika*

11.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punkto tikslais atitinkami subjektai nustato, dokumentuoja ir įgyvendina loginės ir fizinės prieigos prie jų tinklų ir informacinių sistemų kontrolės politiką, grindžiamą veiklos reikalavimais, taip pat tinklų ir informacinių sistemų saugumo reikalavimais.

11.1.2. 11.1.1 punkte nurodyta politika:

a) sprendžiami klausimai, susiję su asmenims, įskaitant darbuotojus, lankytojus ir išorės subjektus, pavyzdžiui, tiekėjus ir paslaugų teikėjus, suteikiama prieiga;

b) sprendžiami klausimai, susiję su tinklų ir informacinėms sistemoms suteikiama prieiga;

c) užtikrinama, kad prieiga būtų suteikiama tik tiems naudotojams, kurių tapatumas buvo tinkamai nustatytas.

11.1.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, peržiūri šią politiką ir prireikus ją atnaujina.

11.2. *Prieigos teisių valdymas*

11.2.1. Atitinkami subjektai suteikia, keičia, panaikina ir dokumentuoja prieigos prie tinklų ir informacinių sistemų teises pagal 11.1 punkte nurodytą prieigos kontrolės politiką.

11.2.2. Atitinkami subjektai:

a) suteikia ir panaikina prieigos teises, remdamiesi būtinybės žinoti, minimaliosios prieigos teisės ir pareigų atskyrimo principais;

b) užtikrina, kad nutraukus darbo sutartį arba pakeitus darbo vietą prieigos teisės būtų atitinkamai pakeistos;

c) užtikrina, kad prieigos prie tinklų ir informacinių sistemų leidimą suteiktų atitinkami asmenys;

d) užtikrina, kad prieigos teisės būtų tinkamai taikomos trečiųjų šalių, pavyzdžiui, lankytojų, tiekėjų ir paslaugų teikėjų, prieigai, visų pirma apribodami prieigos teisių taikymo sritį ir trukmę;

e) tvarko suteiktų prieigos teisių registrą;

f) taiko prieigos teisių valdymo registravimą.

11.2.3. Atitinkami subjektai planiniu periodiškumu peržiūri prieigos teises ir jas keičia, atsižvelgdami į organizacinius pokyčius. Atitinkami subjektai dokumentuoja peržiūros rezultatus, įskaitant būtinus prieigos teisių pakeitimus.

11.3. *Privilegijuotosios paskyros ir sistemos administravimo paskyros*

11.3.1. Atitinkami subjektai, įgyvendindami 11.1 punkte nurodytą prieigos kontrolės politiką, taiko privilegijuotųjų paskyrų ir sistemos administravimo paskyrų valdymo politiką.

11.3.2. 11.3.1 punkte nurodyta politika:

a) sukuriamos griežtos privilegijuotosioms paskyroms ir sistemos administravimo paskyroms taikomos identifikavimo, tapatumo nustatymo, pvz., daugiaelemenčio tapatumo nustatymo, ir leidimų suteikimo procedūros;

b) sukuriamos specialios paskyros, naudotinos tik sistemos administravimo operacijoms, pvz., diegimui, konfigūravimui, valdymui ar techninei priežiūrai atlikti;

c) kuo labiau individualizuojamos ir apribojamos sistemos administravimo teisės;

d) nustatoma, kad sistemos administravimo paskyros naudojamos tik jungiantis prie sistemos administravimo sistemų.

11.3.3. Atitinkami subjektai planiniu periodiškumu peržiūri prieigos prie privilegijuotų paskyrų ir sistemos administravimo paskyrų teises ir jas keičia, remdamiesi organizaciniais pokyčiais, taip pat dokumentuoja peržiūros rezultatus, įskaitant būtinus prieigos teisių pakeitimus.

11.4. *Administravimo sistemos*

11.4.1. Atitinkami subjektai apriboja ir kontroliuoja sistemos administravimo sistemų naudojimą pagal 11.1 punkte nurodytą prieigos kontrolės politiką.

11.4.2. Tuo tikslu atitinkami subjektai:

a) naudoja sistemos administravimo sistemas tik sistemos administravimo tikslais ir neatlieka jose jokių kitų operacijų;

b) logiškai atskiria tokias sistemas nuo taikomosios programinės įrangos, kuri nėra naudojama sistemos administravimo tikslais;

c) apsaugo prieigą prie sistemos administravimo sistemų tapatumo nustatymo ir šifravimo priemonėmis.

11.5. *Identifikavimas*

11.5.1. Atitinkami subjektai valdo visą tinklų ir informacinių sistemų ir jų naudotojų identifikatorių gyvavimo ciklą.

11.5.2. Tuo tikslu atitinkami subjektai:

a) sukuria unikalius tinklų ir informacinių sistemų ir jų naudotojų identifikatorius;

b) susieja naudotojo identifikatorių su vienu asmeniu;

c) užtikrina tinklų ir informacinių sistemų identifikatorių priežiūrą;

d) taiko identifikatorių valdymo registravimą.

11.5.3. Atitinkami subjektai leidžia naudoti identifikatorius, priskirtus keliems asmenims, pavyzdžiui, bendrus identifikatorius, tik jei jie yra būtini dėl verslo ar veiklos priežasčių ir jiems taikoma aiškaus patvirtinimo procedūra bei dokumentavimas. Atitinkami subjektai atsižvelgia į keliems asmenims priskirtus identifikatorius 2.1 punkte nurodytoje kibernetinio saugumo rizikos valdymo sistemoje.

11.5.4. Atitinkami subjektai periodiškai peržiūri tinklų ir informacinių sistemų ir jų naudotojų identifikatorius ir, jei jų nebereikia, nedelsdami juos išjungia.

11.6. *Tapatumo nustatymas*

11.6.1. Atitinkami subjektai įdiegia saugias tapatumo nustatymo procedūras ir technologijas, grindžiamas prieigos apribojimais ir prieigos kontrolės politika.

11.6.2. Tuo tikslu atitinkami subjektai:

a) užtikrina, kad tapatumo patvirtinimo metodo saugumas atitiktų turto, prie kurio bus suteikta prieiga, klasifikavimą;

b) kontroliuoja slaptos tapatumo nustatymo informacijos priskyrimą naudotojams ir jos valdymą, taikydami procedūrą, kuria užtikrinamas informacijos konfidencialumas, be kita ko, konsultuodami darbuotojus dėl tinkamo tapatumo nustatymo informacijos tvarkymo;

c) reikalauja pakeisti tapatumo nustatymo kredencialus iš pradžių, nustatytais laiko intervalais, taip pat įtarus, kad tapatumo nustatymo kredencialai buvo atskleisti;

d) reikalauja iš naujo nustatyti tapatumo nustatymo kredencialus ir blokuoti naudotoją po iš anksto nustatyto skaičiaus nesėkmingų bandymų prisijungti;

e) nutraukia neaktyvius seansus po iš anksto nustatyto neveiklumo laikotarpio ir

f) reikalauja atskirų kredencialų, kad būtų galima naudotis privilegijuota prieiga arba administracinėmis paskyromis.

11.6.3. Atitinkami subjektai naudoja pažangiausius tapatumo nustatymo metodus, atsižvelgdami į susijusią įvertintą riziką ir turto, prie kurio bus suteikta prieiga, klasifikavimą, taip pat unikalią tapatumo nustatymo informaciją.

11.6.4. Atitinkami subjektai planiniu periodiškumu peržiūri tapatumo nustatymo procedūras ir technologijas.

11.7. *Daugiaelementis tapatumo nustatymas*

11.7.1. Atitinkami subjektai užtikrina, kad naudotojų tapatumas būtų nustatomas taikant daugiaelementį tapatumo nustatymą ar nuolatinio tapatumo nustatymo mechanizmus, kad būtų galima prisijungti prie subjektų tinklų ir informacinių sistemų, kai tinkama, atsižvelgiant į turto, prie kurio bus suteikta prieiga, klasifikavimą.

11.7.2. Atitinkami subjektai užtikrina, kad tapatumo nustatymo metodo saugumas atitiktų turto, prie kurio bus suteikta prieiga, klasifikavimą.

12. **Turto valdymas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punktas)**

12.1. *Turto klasifikavimas*

12.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punkto tikslais atitinkami subjektai nustato viso jų tinklų ir informacinių sistemų turto, įskaitant informaciją, klasifikavimo lygmenis, kad būtų užtikrintas reikalaujamas apsaugos lygis.

12.1.2. 12.1.1 punkto tikslais atitinkami subjektai:

a) sukuria turto klasifikavimo lygmenų nustatymo sistemą;

b) visam turtui priskiria klasifikavimo lygmenis, remdamiesi konfidencialumo, vientisumo, autentiškumo ir prieinamumo reikalavimais, kad būtų nurodyta reikalinga apsauga, atsižvelgiant į jų jautrumą, svarbą, riziką ir vertę verslui;

c) suderina turto prieinamumo reikalavimus su jų veiklos tęstinumo ir veiklos atkūrimo po ekstremaliųjų įvykių planuose nustatytais veiklos vykdymo ir jos atkūrimo tikslais.

12.1.3. Atitinkami subjektai periodiškai peržiūri turto klasifikavimo lygmenis ir, kai tinkama, juos atnaujina.

12.2. *Turto tvarkymas*

12.2.1. Atitinkami subjektai nustato, įdiegia ir taiko turto, įskaitant informaciją, tinkamo tvarkymo politiką pagal savo tinklų ir informacijos saugumo politiką ir praneša tą politiką visiems, kurie naudoja arba tvarko turtą.

12.2.2. Ši politika:

a) apima visą turto gyvavimo ciklą, įskaitant įsigijimą, naudojimą, saugojimą, transportavimą ir šalinimą;

b) ja nustatomos saugaus turto naudojimo, laikymo, transportavimo ir negrįžtamo pašalinimo bei sunaikinimo taisyklės.

c) joje numatoma, kad perdavimas vyktų saugiai, atsižvelgiant į perduodamo turto rūšį.

12.2.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, šią politiką peržiūri ir prireikus atnaujina.

12.3. *Keičiamųjų laikmenų politika*

12.3.1. Atitinkami subjektai nustato, įdiegia ir taiko keičiamųjų laikmenų politiką ir ją praneša savo darbuotojams ir trečiosioms šalims, tvarkantiems keičiamąsias laikmenas atitinkamų subjektų patalpose ar kitose vietose, kuriose laikmenos yra prijungtos prie atitinkamų subjektų tinklų ir informacinių sistemų.

12.3.2. Šioje politikoje:

a) numatomas techninis draudimas prijungti keičiamąsias laikmenas, jeigu nėra organizacinių priežasčių jas naudoti;

b) numatomas savaiminio tokiose laikmenose esančių programų vykdymo blokavimas ir galimybė laikmenas skenuoti, siekiant nustatyti, ar jose nėra kenkimo programos kodo, prieš pradedant jas naudoti subjektų sistemose;

c) numatomos nešiojamųjų kaupiklių, kuriuose laikomi perduodami ar saugomi duomenys, kontrolės ir apsaugos priemonės;

d) prireikus numatomos kriptografinių metodų naudojimo siekiant apsaugoti keičiamosiose laikmenose laikomą informaciją priemonės.

12.3.3. Atitinkami subjektai planiniu periodiškumu, taip pat įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams arba kilus rizikai, šią politiką peržiūri ir prireikus atnaujina.

12.4. *Turto inventorius*

12.4.1. Atitinkami subjektai parengia ir tvarko išsamų, tikslų, aktualų ir nuoseklų savo turto inventorių. Jie registruoja inventoriaus įrašų pakeitimus taip, kad juos būtų galima atsekti.

12.4.2. Turto inventoriaus detalumo laipsnis turi atitikti atitinkamų subjektų poreikius. Į inventorių įtraukiama ši informacija:

a) operacijų ir paslaugų sąrašas ir jų aprašymas,

b) tinklų ir informacinių sistemų bei kito susijusio turto, kuriuo palaikoma subjektų veikla ir paslaugos, sąrašas.

12.4.3. Atitinkami subjektai periodiškai peržiūri ir atnaujina inventorių bei savo turtą ir dokumentuoja pokyčių istoriją.

12.5. *Turto atidavimas saugoti, grąžinimas arba sunaikinimas nutraukus darbo sutartį*

Atitinkami subjektai nustato, įdiegia ir taiko procedūras, kuriomis užtikrinama, kad jų darbuotojų naudojamas turtas nutraukus darbo sutartį būtų atiduotas saugoti, grąžintas arba sunaikintas, ir dokumentuoja to turto atidavimą saugoti, grąžinimą ir sunaikinimą. Kai turto atiduoti saugoti, grąžinti ar sunaikinti neįmanoma, atitinkami subjektai užtikrina, kad turtas nebeturėtų prieigos prie atitinkamo subjekto tinklų ir informacinių sistemų pagal 12.2.2 punktą.

13. **Aplinkos ir fizinis saugumas (Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies c, e ir i punktai)**

13.1. *Pagalbiniai inžineriniai tinklai*

13.1.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies c punkto tikslais atitinkami subjektai užtikrina, kad tinklų ir informacinės sistemos nebūtų prarastos, pažeistos ar joms kiltų pavojus arba nutrūktų jų veikimas dėl pagalbinių inžinerinių tinklų gedimo ir jų veikimo sutrikimo.

13.1.2. Tuo tikslu atitinkami subjektai, kai tinkama:

a) apsaugo įrenginius nuo elektros energijos tiekimo trikčių ir kitų sutrikimų, kuriuos sukelia gedimai pagalbiniuose inžineriniuose tinkluose, pvz., elektros tiekimo, telekomunikacijų, vandentiekio, dujų tiekimo, nuotekų, ventiliacijos ir oro kondicionavimo;

b) apsvarsto galimybę naudoti inžinerinių tinklų atsarginius pajėgumus;

c) apsaugo inžinerinius elektros energijos tiekimo ir telekomunikacijų tinklus, kuriais į tinklų ir informacines sistemas perduodami duomenys arba tiekiama elektros energija, nuo perėmimo ir žalos;

d) stebi c punkte nurodytus inžinerinius tinklus ir praneša kompetentingiems vidaus ar išorės darbuotojams apie įvykius, kuriems netaikomos 13.2.2 punkto b papunktyje nurodytos mažiausios ir didžiausios kontrolės slenkstinės vertės ir kurie daro poveikį inžineriniams tinklams;

e) sudaro sutartis dėl avarinio tiekimo, pvz., dėl avariniam energijos tiekimui skirto kuro, su atitinkamomis tarnybomis;

f) užtikrina nuolatinį tinklų ir informacinių sistemų aprūpinimo, būtino siūlomai paslaugai teikti, visų pirma elektros energijos tiekimo, temperatūros ir drėgmės kontrolės, telekomunikacijų ir interneto ryšio, veiksmingumą, stebėseną, techninę priežiūrą ir bandymą.

13.1.3. Atitinkami subjektai periodiškai arba įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai testuoja apsaugos priemones, jas peržiūri ir prireikus atnaujina.

13.2. *Apsauga nuo fizinių ir aplinkos grėsmių*

13.2.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies e punkto tikslais atitinkami subjektai, remdamiesi pagal 2.1 punktą atlikto rizikos vertinimo rezultatais, užkerta kelią įvykių, kuriuos sukelia fizinės ir aplinkos grėsmės, pavyzdžiui, gaivalinės nelaimės ir kitos tyčinės ar netyčinės grėsmės, padariniams arba juos sumažina.

13.2.2. Tuo tikslu atitinkami subjektai, kai tinkama:

a) parengia ir įdiegia apsaugos nuo fizinių ir aplinkos grėsmių priemones;

b) nustato mažiausias ir didžiausias fizinių ir aplinkos grėsmių kontrolės slenkstines vertes;

c) stebi aplinkos parametrus ir praneša kompetentingiems vidaus ar išorės darbuotojams apie įvykius, viršijančius b punkte nurodytas mažiausias ir didžiausias kontrolės slenkstines vertes.

13.2.3. Atitinkami subjektai periodiškai arba įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai testuoja apsaugos nuo fizinių ir aplinkos grėsmių priemones, jas peržiūri ir prireikus atnaujina.

13.3. *Perimetras ir fizinės prieigos kontrolė*

13.3.1. Direktyvos (ES) 2022/2555 21 straipsnio 2 dalies i punkto tikslais atitinkami subjektai užtikrina, kad nebūtų neleistinos fizinės prieigos prie jų tinklų ir informacinių sistemų, joms nebūtų daroma žala ar keliami trikdžiai ir vykdo atitinkamą stebėseną.

13.3.2. Tuo tikslu atitinkami subjektai:

a) remdamiesi pagal 2.1 punktą atliktu rizikos vertinimu, nustato ir naudoja saugumo perimetrus zonoms, kuriose yra tinklų ir informacinės sistemos bei kitas susijęs turtas, apsaugoti;

b) apsaugo a punkte nurodytas zonas, taikydami tinkamas patekimo į jas kontrolės priemones ir patekimo punktus;

c) parengia ir įdiegia biurų, patalpų ir įrangos fizinės apsaugos priemones;

d) nuolat stebi, ar nėra neleistino fizinio patekimo į patalpas.

13.3.3. Atitinkami subjektai periodiškai arba įvykus dideliems incidentams, atsiradus reikšmingiems veiklos pokyčiams ar kilus rizikai testuoja fizinės prieigos kontrolės priemones, jas peržiūri ir prireikus atnaujina.