NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

TREČIŲJŲ ŠALIŲ VALDYMO REKOMENDACIJOS

RUGPJŪTIS

2025

Bendrai finansuoja Europos Sąjungos

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.

Turinys

REKOMENDACIJŲ TIKSLAS

Suteikti organizacijoms gaires, padedančias valdyti tinklų ir informacinių sistemų saugumą (TIS), kai informacijos ir ryšių technologijų (IRT) paslaugas teikia trečiosios šalys.

Trečiosios šalys gali būti:

partneriai | **tiekėjai** | **pardavėjai** | **kitos bendrovės**

perkančiajai organizacijai teikiančios prekes, IRT paslaugas ar jų palaikymą.

Šiame informaciniame leidinyje yra apžvelgiamos perkančiajai organizacijai aktualios rizikos, būdingos pasitelkiant trečiąsias šalis, bei galimos jų valdymo priemonės.

Auditorija

Gairės yra orientuotos į kibernetinio saugumo subjektus, tačiau pritaikomos ir kitoms organizacijoms, valdančioms tiekimo grandinę. Žemiau yra išskiriamos ir pareigybės, kurioms yra aktualus veiklos su trečiosiomis šalimis grėsmių valdymas:

- **Vyriausias informacijos saugumo vadovas (*angl. CISO*)** koordinuoja trečiųjų šalių rizikų vertinimą ir saugos politiką;
- **Pirkimų skyrius** užtikrina, kad sutartyse būtų įtrauktos informacijos saugumo nuostatos;

- **IT saugos komanda**
  atlieka techninius trečiųjų šalių vertinimus ir nuolatinį stebėjimą;

- **Duomenų apsaugos pareigūnas (*angl. DPO*)**
  rūpinasi, kad duomenų valdytojai laikytųsi BDAR reikalavimų;

- **Saugos įgaliotinis**
  užtikrina, kad rizikos, būdingos pasitelkiant trečiąsias šalis, yra tinkamai valdomos.

Iššūkiai, kylantys pasitelkiant trečiąsias šalis

Remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) parengta metine ataskaita, organizacijos pažeidžiamumai per tiekimo grandinę ir trečiąsias šalis, įskaitant ir paslaugų tiekėjus trečiosioms šalims (subtiekėjus), yra įvardijama kaip aktualiausia kibernetinio saugumo grėsmė iki 2030 m.

Net ir tada, kai organizacija pakankamai gerai saugo savo IRT infrastruktūrą – tiekimo grandinėje esantys išoriniai partneriai ir jų IRT infrastruktūroje galimos saugumo spragos tampa silpniausia grandimi, į kurią dažniausiai ir taikosi kibernetiniai nusikaltėliai.

1 Grėsmės, būdingos pasitelkiant trečiąsias šalis

Pasitelkiant trečiųjų šalių teikiamas IRT paslaugas organizacijai iškyla papildomos grėsmės, ir ji tampa pažeidžiama per tiekimo grandinę. Šiame skyriuje yra apibūdintos pagrindinės grėsmės, susijusios su tiekimo grandine.

Trūkumai trečiosios šalies informacijos saugumo valdyme ar jos neveiksnumas

Nesuderinami informacijos saugumo standartai

Trečiosios šalys ar jų subtiekėjai gali neatitikti perkančiosios organizacijos informacijos saugumo politikos ar turėti žemesnius kibernetinio saugumo standartus nei to reikalauja valdomo IRT veiklos proceso ar informacinio turto kritiškumas. Trečiosioms šalims veikiant kitose jurisdikcijose gali būti taikomi kiti duomenų apsaugos ir saugumo reglamentai, o tai gali kelti papildomas teisines ir informacijos saugumo grėsmes bei silpninti perkančiosios organizacijos informacijos saugumą.

Neefektyvi incidentų valdymo procedūra

Trečiosios šalys gali neturėti efektyvios ar tinkamos incidentų valdymo procedūros, o pasekmė būtų – neužtikrintas operatyvus kibernetinių incidentų valdymas ir laiku neinformuota perkančioji organizacija ar kibernetinio saugumo subjektas. Papildomai gali kilti ir komunikacijos bei veiklos koordinavimo nesklandumų incidentų valdymo metu.

Nepatikimi subtiekėjai

Trečiosios šalys gali pasitelkti į tarptautinių sankcijų sąrašus įtrauktus ar nepatikimoje jurisdikcijoje veiklą vykdančius subtiekėjus. Tai gali kelti grėsmę perkančiosios organizacijos reputacijai, duomenų saugumui ar sutartinių įsipareigojimų vykdymui.

Sutartinių įsipareigojimų trūkumai ar jų nesilaikymas

Esant neapibrėžtiems sutartiniams įsipareigojimams trečioji šalis gali nesilaikyti sutarto paslaugų kokybės lygio (angl. SLA – Service Level Agreement), nespręsti incidentų, nesidalinti reikalinga informacija bei vengti taikyti reikalaujamas informacijos saugumo kontrolės priemones.

Sutrikimai trečiosios šalies infrastruktūroje

Įsiskverbimo atakos, nukreiptos į tiekimo grandinę

Piktavaliai gali kompromituoti trečiosios šalies IRT infrastruktūrą per egzistuojančias ir laiku nesutvarkytas spragas ar apeinant nepakankamas informacijos saugumo kontrolės priemones. Piktavaliai į trečiosios šalies ar jos subtiekėjo infrastruktūrą įterpdami kenkėjišką kodą ar užkrėstą bylą gali įgauti netiesioginę ir neautorizuotą prieigą perkančiosios organizacijos infrastruktūroje.

Trikdymo atakos

Trečiosios šalys tiekimo grandinėje gali tapti paslaugų trikdymo atakų taikiniais (angl. DoS – Denial of Service). Tokio tipo atakos prieš trečiosios šalies teikiamas paslaugas gali trikdyti pačios perkančiosios organizacijos vykdomą veiklą.

Žmogiškųjų išteklių stygius ar žinių trūkumas

Trečiosios šalies personalo trūkumas ar didelė jo kaita gali turėti neigiamą poveikį organizacijos paslaugų kokybei ir sutartinių įsipareigojimų vykdymui (SLA).

Paslaugos tęstinumo trikdymas

Trečiųjų šalių riboti ar nepakankami IRT infrastruktūros pajėgumai bei dažni jų sutrikimai gali trikdyti ir perkančiosios organizacijos veiklą.

Duomenų nutekėjimas

Trečiosios šalies darbuotojams gali būti suteikiama teisė prieiti prie perkančiosios organizacijos vidinių TIS ar neviešo informacinio turto, o piktavaliai, sukompromitavę trečiosios šalies darbuotojų paskyras, gali pasinaudoti suteikta prieiga, siekdami nutekinti neviešą informaciją.

2 Taikytinos saugumo kontrolės priemonės

Šios kontrolės priemonės padeda užtikrinti trečiosioms šalims keliamus informacijos saugumo reikalavimus, mažina perkančiajai organizacijai aktualias grėsmes bei stiprina jos atsparumą.

Trečiųjų šalių klasifikavimas ir vertinimas

Identifikavimas ir registravimas

Būtina identifikuoti ir registruoti visas organizacijai paslaugas teikiančias trečiąsias šalis bei jų subtiekėjus, įskaitant trečiosios šalies vykdomus veiklos procesus bei teikiamą informacinį turtą, t. y. programinę įrangą, IT sistemas, infrastruktūrą ar tinklus. Būtina reguliariai ir esant pokyčiams atnaujinti turimus tiekėjų ir jų teikiamų paslaugų registrus. Remiantis Kibernetinio saugumo reikalavimų aprašo 39 punktu, kibernetinio saugumo subjektas turi būti sudaręs tiekėjų sąrašą, jį numatytu periodiškumu peržiūrėti bei atnaujinti. Taip pat šį sąrašą būtina atnaujinti, kai keičiama sutartis ar kai įvyksta reikšmingi pokyčiai bei incidentai, susiję su tiekėjais.

Technologijų ir procesų vertinimas

Siekiant tiksliau nustatyti trečiosios šalies veiklai būdingą riziką, būtina įvertinti trečiosios šalies naudojamas technologijas, programinę įrangą, veiklos procesus, informacijos saugumo valdymo tvarką. Vertinant rekomenduojama atsižvelgti į tokius aspektus, kaip: informacinių sistemų atnaujinimo dažnumas, palaikymo lygis, spragų (angl. CVE) valdymas bei šalinimas. Vertinimo kriterijai yra išsamiau aprašyti šių gairių 3.2 punkte.

Informacijos saugumo ir rizikos vertinimas

Privalo būti vertinama kiekvienos perkančiajai organizacijai svarbias paslaugas teikiančios trečiosios šalies atitiktis informacijos saugumo standartams (pvz., ISO/IEC 27001) ir Kibernetinio saugumo įstatymo (toliau – KSĮ) bei jo reikalavimų aprašo (toliau – KSRA) nuostatoms.

Kritiškumo ir rizikos lygio nustatymas

Kiekviena organizacijai paslaugas teikianti trečioji šalis privalo būti vertinama pagal jos teikiamų paslaugų ar vykdomo veiklos proceso svarbumą. Atitinkamai pagal tai, turi būti vertinama ir trečiosios šalies keliama rizika veiklos tęstinumui. Plačiau apie trečiosios šalies svarbumo klasifikavimą ir rizikos vertinimą yra aprašyta šių gairių 3.1 punkte.

Sutarties sąlygų nustatymas

Saugumo standartai

Sutartyse turi būti įtraukti KSĮ ir KSRA reikalavimai bei informacijos saugumo standartai. Trečioji šalis privalo įsipareigoti laikytis sutartyse nustatytų atitikties ir reguliavimo reikalavimų.

Informacijos saugumo būklė ir auditas

Sutartyje reikalinga numatyti, jog pagal perkančiosios organizacijos reikalavimą trečioji šalis privalo teikti informacijos saugumo audito ataskaitas bei, esant poreikiui, leisti perkančiajai organizacijai ar jos pasamdytai kvalifikuotai trečiajai šaliai tokį auditą atlikti. Taip pat sutartyje yra reikalinga numatyti, jog trečioji šalis privalėtų pateikti taikomą informacijos saugumo tvarką bei turimus sertifikatus (pvz., ISO, SOC2 ar kitus).

Paslaugų kokybės reikalavimai

Sutartyje numatyti paslaugų kokybės lygį (SLA). Trečioji šalis turi būti įpareigota informuoti perkančiąją organizaciją apie atsiradusį, įvykusį ar bet kurį perkančiosios organizacijos teikiamoms paslaugoms ar TIS veiklai įtaką darantį incidentą. Privalo būti sutartos procedūros incidentams registruoti ir eskaluoti.

Trečiųjų šalių prieigos valdymas ir stebėsena

Prieigos kontrolė

Trečiosios šalies darbuotojams ir paslaugoms privalo būti taikomas žemiausios privilegijos principas - minimali, terminuota ir tik jų darbo funkcijoms vykdyti reikalinga prieiga prie TIS ir informacinio turto. Perkančiosios organizacijos nevieša informacija privalo būti pasiekiama tik iš vidinio tinklo arba naudojantis VPN (angl. Virtual Private Network). Visi atliekami prisijungimai turi būti registruojami audito įrašuose (pvz., SIEM) ir kontroliuojami tam pritaikytos programinės įrangos (pvz., IAM, PAM). Rekomenduojama taikyti „Zero Trust“ modelį, kur kiekviena prieiga prie perkančiosios organizacijos informacinio turto turėtų būti autentifikuota, autorizuota ir registruojama. Rekomenduojama įpareigoti trečiąsias šalis naudoti sudėtingus slaptažodžius ir daugiapakopę autentifikaciją (angl. MFA Multi-factor authentication).

Informacinio turto ar IRT paslaugų stebėsena

Rekomenduojama vykdyti pastovią trečiosios šalies teikiamo informacinio turto ir IRT paslaugų stebėseną, įskaitant ir atliekamų veiksmų žurnalinių įrašų (angl. log) registravimą, stebėjimą ir anomalijų identifikavimą. Šiai kontrolei vykdyti gali būti pasitelkiami ir papildomi įrankiai (pvz., SecurityScorecard, BitSight).

Automatizuotas programinio kodo tikrinimas

Atsižvelgiant į trečiosios šalies kritiškumą, aktualias rizikas ir ekonominį naudingumą, rekomenduojama bent kartą per metus atlikti trečiosios šalies kodo saugumo analizę, naudojant statinį (angl. SAST – Static Application Security Testing) arba dinaminį (angl. DAST – Dynamic Application Security Testing) programinės įrangos saugumo testavimą. Siekiant valdyti trečiosios šalies programinės įrangos priklausomybes ir su tuo susijusias saugumo rizikas, reguliariai atnaujinti SBOM (angl. Software Bill of Materials) registrą, identifikuoti naudojamas naujas bibliotekas ir technologijas. Esant poreikiui, reikalauti pateikti tokių saugumo testavimų ataskaitas, parengtas kvalifikuotų paslaugų tiekėjų.

Įsilaužimų aptikimo ir kontrolės mechanizmų diegimas

Įdiegti mechanizmus tinklo, operacijų ir anomalios veiklos stebėjimui bei užkardymui, tokius kaip: SIEM (angl. Security Information and Event Management), EDR (angl. Endpoint Detection and Response), IDS/IPS (angl. Intrusion Detection / Prevention System) ar kitus.

Incidentų ir veiklos tęstinumo valdymas

Veiklos tęstinumo ir atkūrimo planas

Trečioji šalis privalo turėti parengtą veiksmų planą didelio poveikio incidentų ir veiklos sutrikdymo scenarijų atveju, užtikrinantį operatyvų paslaugų atstatymą ir alternatyvius sprendimus kritinėms paslaugoms teikti bei veiklos tęstinumui užtikrinti.

Incidentų simuliavimas ir testavimas

Rekomenduojama ne rečiau, kaip kartą per metus testuoti reagavimo į incidentus procedūras, įskaitant atsarginių kopijų atkūrimo ir veiklos tęstinumo planą. Atsižvelgiant į trečiosios šalies kritiškumą ir rizikų vertinimą, gali būti svarstoma atlikti „Red Teaming“ testavimą, modeliuojant atakas prieš trečiųjų šalių TIS, pavyzdžiui, trečiosios šalies paskyros perėmimą bei įsiskverbimą į trečiosios šalies infrastruktūrą.

Incidentų tyrimas

Su trečiąja šalimi turi būti suderintos incidentų valdymo ir tyrimo procedūros, apimančios incidentus abiejų šalių infrastruktūrose. Siekiant, kad incidentai būtų kuo greičiau pašalinti, trečioji šalis privalo bendradarbiauti ir dalintis būtina informacija su perkančiąja organizacija ir kitomis institucijomis (pvz., Nacionalinis kibernetinio saugumo centras (NKSC), Policijos departamentas (PD), Valstybinė duomenų apsaugos inspekcija (VDAI)) kaip tą numato KSĮ ir Nacionalinis kibernetinių incidentų valdymo planas.

3 Trečiosios šalies pasitelkimo etapai

Siekiant apsaugoti perkančiosios organizacijos TIS bei užtikrinti jų kibernetinį saugumą yra būtina nustatyti trečiųjų šalių valdymo gaires. Tam būtina parengti tiekimo grandinės saugumo valdymo tvarką, kurioje būtų aiškiai įvardinti trečiosios šalies valdymo principai, atsakomybės ribos ir trečiųjų šalių gyvavimo ciklas – nuo jų atrankos iki sutarties nutraukimo.

Planavimas ir politika

Perkančiosios organizacijos ar kibernetinio saugumo subjekto vadovas arba jo įgaliotas asmuo tiekimo grandinės saugumo valdymo tvarkoje turi numatyti kibernetinio ir informacijos saugumo standartus bei reikalavimus, rizikos vertinimo metodiką, apimančias ir vidaus, ir išorės veiksnius, nustatyti organizacijos ir trečiosios šalies vaidmenis bei atsakomybių ribas.

Perkančioji organizacija turi taikyti rizika grįstą požiūrį (pvz., galima remtis ISO/IEC 27001 standartu) trečiųjų šalių teikiamų paslaugų valdymui, vertindama kiekvieną susitarimą pagal paslaugų dydį, rizikos lygį ir paslaugų, veiklų bei operacijų sudėtingumą ir kritiškumą. Organizacija privalo klasifikuoti trečiąsias šalis pagal jų vaidmenis ir teikiamų paslaugų svarbą verslo operacijoms:

Kritinė trečioji šalis

Nekritinė trečioji šalis

Trečiosios šalies atitikties Kibernetinio saugumo įstatymo (KSĮ) ir Kibernetinio saugumo įstatymo įgyvendinimo reikalavimų aprašo (KSRA) reikalavimams vertinimas turi būti dalis rizikos vertinimo proceso. Visos IRT paslaugos, kurios yra kritinės veiklos tęstinumui užtikrinti, turi būti identifikuotos, klasifikuotos ir apsaugotos, taikant specifinius sutartinius įsipareigojimus su trečiosiomis šalimis ir jų subtiekėjais.

Trečiosios šalies vertinimas ir pasirinkimas

Renkantis trečiąją šalį, perkančioji organizacija turi vertinti jos gebėjimą teikti reikiamas IRT paslaugas bei atitiktį perkančiosios organizacijos informacijos saugumo reikalavimams, įskaitant KSĮ bei KSRA reikalavimus. Kibernetinio saugumo subjektas, nustatydamas tiekimo grandinės saugumo valdymo tvarką, **turi numatyti TIS tiekėjų atrankos kriterijus, apimančius:**

Saugumo standartų suderinamumą.

Trečiosios šalies gebėjimas atitikti perkančiosios organizacijos saugumo reikalavimus, įskaitant duomenų konfidencialumą, vientisumą ir prieinamumą, bei galimybes bendradarbiauti auditų metu ir reaguojant į incidentus.

Saugumo reikalavimų atitiktį.

Trečiosios šalies atitiktis nustatytoms KSĮ ir KSRA nuostatoms.

Teikiamų paslaugų kokybės lygį.

Trečiosios šalies teikiamų paslaugų kokybės reikalavimus TIS produktams, paslaugoms (pvz., paslaugų pasiekiamumo apimtį, atkūrimo greitį ir kitas).

Prieigų valdymo galimybes.

Trečiosios šalies prieigų valdymo galimybes, įskaitant prieigų laikotarpio ribojimą.

Technologinės pažangos stebėjimą.

Gebėjimą stebėti technologinę pažangą, nustatyti pažangiausią IRT saugumo praktiką ir prireikus ją įgyvendinti.

Subtiekėjų pasitelkimą.

Įsitikinkite, ar trečioji šalis atskleidžia bet kokį esamą ar planuojamą subtiekėjų pasitelkimą kritinėms ar svarbioms IRT paslaugoms teikti

Atnaujinimus ir palaikymą.

Įsitikinkite, kad trečioji šalis teikia programinės įrangos palaikymą bei vykdo reguliarius saugumo atnaujinimus.

Patikimumą.

Įvertinkite, ar trečioji šalis turi gerą reputaciją, pakankamą kompetenciją, išteklius, reikiamą organizacinę struktūrą, vidaus kontrolę ir, jei taikoma, ar turi reikiamus leidimus teikti sprendimą.

Paslaugos tiekimą.

Įvertinkite, ar trečioji šalis yra įsikūrusi Europos Sąjungoje, Europos ekonominėje erdvėje ar NATO šalyje ir ar tvarko bei saugo duomenis pagal Europos Sąjungoje galiojančius reikalavimus. Jei ne, įvertinkite, ar šalis, kurioje trečioji šalis vykdo veiklą, jūsų organizacijai nesukelia papildomos operacinės ar reputacinės rizikos, ar jums nekyla ribojančių priemonių, pavyzdžiui, sankcijų, galinčių turėti įtakos jūsų organizacijos gebėjimui teikti paslaugas arba jas gauti.

Atsakomybę ir priežiūrą.

Įvertinkite, ar trečioji šalis laikosi sutartinių įsipareigojimų, leidžia jums veiksmingai atlikti auditą, įskaitant patikrinimus, bei veikia etiškai ir socialiai atsakingai, gerbia žmogaus teises, laikosi aplinkosaugos principų ir užtikrina tinkamas darbo sąlygas savo darbuotojams.

Norint įvertinti trečiosios šalies atitiktį KSĮ ir KSRA, perkančioji organizacija turi nustatyti jai tinkamus patikros metodus, leidžiančius užtikrinti reikiamą paslaugos patikimumo lygį. Patikrai vykdyti perkančioji organizacija gali remtis nepriklausomomis išorės ar vidaus audito ataskaitomis, vieša informacija, sertifikatais ir kita informacija, pateikiama trečiosios šalies.

Sutarties sąlygų nustatymas

Remdamasi atliktu rizikos vertinimu, rizikos valdymo planu, taikoma informacijos saugumo tvarka bei KSĮ ir KSRA reikalavimais perkančioji organizacija sutartyse privalo nustatyti informacijos saugumo reikalavimus trečiajai šaliai. **Sutartiniai reikalavimai turėtų apimti:**

Atitiktį reikalavimams.
Trečiosios šalies atitiktį KSRA nuostatoms.

Personalo mokymus.
Trečiosios šalies personalui reikalingus įgūdžius ir (ar) mokymus, ir (ar) sertifikatus, ir (ar) kvalifikaciją.

Incidentų valdymą.
Trečiosios šalies pareigą, kai tik sužino apie incidentą, pranešti perkančiajai organizacijai apie visus didelius ir (ar) vos neįvykusius incidentus, susijusius su perkančiosios organizacijos TIS, ir pareigą pateikti perkančiajai organizacijai kibernetinio incidento tyrimo ataskaitą.

Atitikties vertinimą.
Teisę perkančiajai organizacijai arba jos įgaliotiems paslaugų tiekėjams atlikti trečiosios šalies atitikties KSĮ auditą (įskaitant neplaninį) ir trečiosios šalies pareigą sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui.

Spragų valdymą.
Pareigą užtikrinti spragų, keliančių riziką perkančiosios organizacijos TIS, valdymą.

Konfidencialumą.
Konfidencialumo ir duomenų neatskleidimo įsipareigojimus.

Paslaugų kokybę.
Paslaugų teikimo lygmenis SLA.

Prieigos valdymą.
Apibrėžti trečiosios šalies prieigos (loginės ir fizinės) prie TIS lygius ir sąlygas.

Reikalavimus patalpoms.
Numatyti reikalavimus, keliamus trečiosios šalies patalpoms, įrangai, TIS priežiūrai, informacijos perdavimui tinklais.

Teises ir pareigas.
Numatyti trečiosios šalies ir perkančiosios šalies teises ir pareigas.

Sutartyse taip pat yra rekomenduojama numatyti vaidmenų ir atsakomybės pasidalijimą saugumo, atitikties reikalavimų ir patikrinimo kontekste. Atitinkamai turi būti numatyta ir komunikacijos tarp perkančiosios organizacijos ir trečiosios šalies procedūra, apimanti:

Reguliarius susitikimus ir jų formatą (nuotolinis, fizinis), kurių metu aptariama paslaugų teikimo būsena, kylantys klausimai bei galimi pakeitimai. Rekomenduojama šiuos susitikimus vykdyti ne rečiau kaip kartą per mėnesį. Susitikimų dažnumas turėtų priklausyti nuo trečiosios šalies teikiamų paslaugų kritiškumo.

Kasdienę komunikaciją ir jos būdus krizės ar avarinių situacijų atvejais, užtikrinant, kad saugumo incidentai būtų laiku aptarti ir sprendžiami.

Pokyčius, pvz., saugumo priemonių, atsižvelgiant į tuo metu aktualias grėsmes, ar TIS infrastruktūros pokyčius.

Reikalavimai trečiosioms šalims ir jų paslaugų teikimui turi būti išmatuojami, aiškūs ir apibrėžti laike, tokiu būdu juos bus lengviau kontroliuoti ir stebėti visą sutarties gyvavimo laikotarpį. Esant poreikiui, rekomenduojama konsultacijai kreiptis ir į Nacionalinį kibernetinio saugumo centrą (NKSC).

Trečiosios šalies ir jos subtiekėjų kontrolė

Rekomenduojama, kad perkančioji organizacija sutartyse su trečiosiomis šalimis numatytų priemones ir pagrindinius rodiklius, leidžiančius nuolat stebėti trečiųjų šalių teikiamų paslaugų kokybę ir susijusią veiklą. **Kontrolė turėtų apimti šias ataskaitas:**

Periodinės

Trečiosios šalys turėtų reguliariai pateikti perkančiajai organizacijai atitinkamas ataskaitas apie savo veiklą, susijusią su perkančiajai organizacijai teikiamomis paslaugomis, įskaitant incidentų ataskaitas, paslaugų teikimo ataskaitas, ataskaitas apie IRT saugumą ir ataskaitas apie veiklos tęstinumo priemones bei testavimus.

Atitikties

Periodines vidaus ar išorės audito ataskaitas, kurios patvirtina, jog trečiosios šalies veikla atitinka perkančiosios organizacijos TIS ir rizikos valdymo reikalavimus.

Rodiklių

Pagrindinius kokybinius ir kiekybinius veiklos rodiklius, apimančius paslaugos teikimo lygio vertinimą, pasitenkinimo tyrimą, paslaugos efektyvumą, klaidų dažnį, nepasiekiamumą, auditus, vertinimus ir nepriklausomas peržiūras.

Incidentų

Įvykusių saugumo ar kitų incidentų tyrimo ataskaitas.

Rekomenduojama visas trečiųjų šalių ataskaitas ir vertinimus saugoti ir naudoti rizikos vertinimams atlikti. Siekiant išvengti sutartinių įsipareigojimų nevykdymo rizikų, perkančiajai organizacijai yra rekomenduojama sutartyse su trečiosiomis šalimis iš anksto nustatyti sutarties įgyvendinimo kontrolės priemones. Šios priemonės galėtų apimti:

a) iš anksto sutartas baudas;
b) kainos už paslaugas koregavimą;
c) taisomųjų veiksmų planus, siekiant atkurti paslaugų patikimumą ir atitiktį.

Suaktyvinus tokias priemones perkančiajai organizacijai yra rekomenduojama vykdyti nuolatinį stebėjimą, siekiant užtikrinti, kad korekciniai veiksmai būtų įvykdyti, efektyvūs ir atlikti per nustatytą terminą.

Sutarties nutraukimo sąlygos

Perkančiosios organizacijos kibernetinio ir informacijos saugumo lygis turi būti užtikrintas viso sutarties nutraukimo proceso metu, nepriklausomai nuo to, ar teikiamos IRT paslaugos perduodamos naujai trečiajai šaliai, ar perimamos perkančiosios organizacijos.

Vykdant sutarties nutraukimo procesą yra rekomenduojama fiksuoti visus trečiosios šalies ir perkančiosios organizacijos sutartinių įsipareigojimų užbaigimo veiksmus, įskaitant išmoktas pamokas.

Trečiosios šalies paslaugų teikimo pabaigoje yra būtina užtikrinti, kad visi perkančiosios organizacijos duomenys ir kitas informacinis turtas būtų saugiai trečiosios šalies grąžintas arba sunaikintas, pateikiant sunaikinimo įrodymus. Sutarties nutraukimo proceso metu turi būti peržiūrimos ir panaikinamos visos trečiosios šalies prieigos prie perkančiosios organizacijos TIS. Siekiant įsitikinti, kad nebuvo atlikta jokia įtartina veikla, perkančioji organizacija privalo atlikti paskutinių trečiosios šalies veiksmų audito žurnalinių įrašų analizę ir juos saugoti ne mažiau kaip 90 kalendorinių dienų.

Siekiant išvengti netikėto sutarties nutraukimo ar paslaugų sutrikdymo, perkančiajai organizacijai yra rekomenduojama išlaikyti sutarties su trečiąja šalimi kontrolę. Rekomenduojama į sutartinius įsipareigojimus įtraukti sąlygas, kurioms esant, perkančioji organizacija galėtų nutraukti sutartį. **Nutraukti sutartį būtų galima dėl šių sąlygų nevykdymo:**

- dėl reikšmingo trečiosios šalies padaryto galiojančių įstatymų, kitų teisės aktų, taip pat ir KSĮ bei KSRA, ar sutarties sąlygų pažeidimo;
- nustačius aplinkybes, kurios gali reikšmingai pabloginti teikiamų paslaugų vykdymą;
- nustačius reikšmingus trečiosios šalies rizikos valdymo ar atitikties KSĮ ir KSRA trūkumus, ypač tuos, kurie susiję su neviešų duomenų prieinamumu, autentiškumu, vientisumu ar konfidencialumu;
- kai perkančioji organizacija nebegali toliau veiksmingai vertinti trečiosios šalies teikiamų paslaugų kokybės.

Perkančiajai organizacijai yra rekomenduojama parengti ir kiekvienai trečiajai šaliai turėti sutarties nutraukimo planą. Jį periodiškai peržiūrėti ir testuoti, plane turėtų būti numatytos alternatyvos, kaip bus teikiamos paslaugos, ir pereinamojo laikotarpio veiksmai, užtikrinantys saugų perkančiosios organizacijos duomenų perkėlimą ar paslaugų iš trečiosios šalies perėmimą. Net ir po sutarties nutraukimo abi šalys privalo tęsti konfidencialumo įsipareigojimus.

TREČIŲJŲ ŠALIŲ
VALDYMO REKOMENDACIJOS

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Organizacijos pažeidžiamumai per tiekimo grandinę ir trečiąsias šalis yra įvardijama kaip aktualiausia kibernetinio saugumo grėsmė iki 2030 m.

GRĖSMĖS

Pasitelkiant trečiųjų šalių teikiamas IRT paslaugas organizacijai iškyla papildomos grėsmės, ir ji tampa pažeidžiama per tiekimo grandinę.

- **Trūkumai trečiosios šalies informacijos saugumo valdyme ar jos neveiksnumas**
- **Sutrikimai trečiosios šalies infrastruktūroje**

SAUGUMO PRIEMONĖS

Kontrolės priemonės padeda užtikrinti trečiosioms šalims keliamus informacijos saugumo reikalavimus, mažina perkančiajai organizacijai aktualias grėsmes bei stiprina jos atsparumą.

- **Sutarties sąlygų nustatymas**
- **Trečiųjų šalių klasifikavimas ir vertinimas**
- **Trečiųjų šalių prieigos valdymas ir stebėsena**
- **Incidentų ir veiklos tęstinumo valdymas**

TREČIŲJŲ ŠALIŲ PASITELKIMO ETAPAI

Siekiant apsaugoti organizacijos TIS ir užtikrinti kibernetinį saugumą, reikia nustatyti trečiųjų šalių valdymo gaires su aiškiais principais, atsakomybėmis ir gyvavimo ciklu nuo atrankos iki sutarties pabaigos.

- **Planavimas ir politika**
- **Trečiosios šalies vertinimas ir pasirinkimas**
- **Sutarties sąlygų nustatymas**
- **Trečiosios šalies ir jos subtiekėjų kontrolė**
- **Sutarties nutraukimo sąlygos**

Bendrai finansuoja Europos Sąjunga

Bendrai finansuojama Europos Sąjungos lėšomis. Tačiau išsakytos nuomonės ir požiūriai yra tik autoriaus (-ių) ir nebūtinai atspindi Europos Sąjungos ar Europos kibernetinio saugumo kompetencijų centro (ECCC) požiūrį. Europos Sąjunga ir dotaciją teikianti institucija nėra atsakingos už šią informaciją.