NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

REKOMENDACIJOS KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMUI IR ATITIKTIES VERTINIMUI

LAPKRITIS
2025

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.

Turinys

NKSC REKOMENDACIJA

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMUI IR ATITIKTIES VERTINIMUI

Rekomendacijų tikslas

Šių rekomendacijų tikslas – padėti kibernetinio saugumo subjektams ir kitoms organizacijoms (toliau – organizacijos) nustatyti, stebėti ir valdyti įdiegtos informacijos saugumo valdymo sistemos ir jos atitikties kibernetinio saugumo įstatymo reikalavimams veiksmingumo rodiklius.

Auditorija

Šios rekomendacijos yra skirtos KSS, vidutinių ir mažų įmonių (MVĮ) bei organizacijų IT saugos specialistams ir darbuotojams.

Esama situacija ir pagrindiniai iššūkiai

Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos (toliau – NKSC) pastebi, kad kibernetinio saugumo reikalavimų įgyvendinimas yra atliekamas formaliai, neatsižvelgiant į praktinį kibernetinio saugumo priemonių efektyvumą.

Tai dažnai lemia formaliai atliekamas rizikų vertinimas, neatsižvelgiant į rekomenduojamus tarptautinius standartus ar gerą praktiką. Įprastai rizikos yra nustatomos paviršutiniškai, remiantis bendromis prielaidomis, o išvesti rizikų vertinimo rezultatai nėra integruojami į bendrą sprendimų priėmimą dėl informacijos saugumo valdymo sistemos (toliau - ISVS) veiksmingumo gerinimo, taip pat ir atitinkamų informacijos saugumo priemonių diegimo ar prioritetų nustatymo.

Dažnai formalus požiūris į rizikų valdymą nulemia ir netikslų ISVS veiksmingumo matavimo sistemos (rodiklių) nustatymą, įgyvendinama matavimo sistema be aiškaus tikslo ar nuoseklios duomenų rinkimo bei analizės tvarkos. ISVS veiksmingumo ir atitikties rodikliai dažnai renkami epizodiškai, neapimant visų organizacijos padalinių ar procesų. Dėl to suvestinės būna paviršutiniškos ir neatspindi tikrosios ISVS atitikties situacijos, o vadovybė neturi pakankamai pagrįstos informacijos sprendimų priėmimui. Tokia situacija lemia pažeidžiamumų ir neatitikimų nepastebėjimą, per didelės rizikos prisiėmimą bei apsunkina sureagavimą laiku į besikeičiančias kibernetines grėsmes.

Atsižvelgęs į šiuos organizacijoms kylančius iššūkius, NKSC šiose rekomendacijose teikia gerąją praktiką ir nustato esmines veiklas, reikalingas įgyvendinant nuoseklų informacijos saugumo sistemos valdymo vertinimą ir atitiktį.

Matavimo sistemos (rodiklių) nustatymo principai

Remiantis tarptautiniu ISO / IEC 27004:2016 standartu, užtikrinant patikimą ir nuoseklų ISVS veiksmingumo vertinimą, organizacijos turėtų vadovautis atskaitomybės vadovybei, skaidrumo, periodinio stebėjimo ir įrodymais grįsto tobulinimo principais.

Skaidrumas ir tikslumas

Norint gauti patikimus matavimo sistemos (rodiklių) rezultatus, būtina užtikrinti, kad jie būtų palyginami (angl. *comparable*) ir atkartojami (angl. *reproducible*). Tam, kad rodiklių rezultatus būtų galima palyginti tarpusavyje, svarbu užtikrinti, jog ISVS apimtis ir kontekstas kiekvieno vertinimo metu būtų nepakitęs. Rodiklių atkartojamumas, tai yra jų apskaičiavimo metodika turėtų būti pastovi, pavyzdžiui, subjektyvūs vertinimai (anketos) turėtų būti vertinamos aiškiai apibrėžtais ir nekintančiais kriterijais. Tokiu būdu siekiama išlaikyti objektyvius matavimo metodus ir patikimus rezultatus. Tikslūs ir skaidrūs matavimo metodai, net ir kintant duomenų šaltiniams, padeda užtikrinti pastovumą ir tiksliau identifikuoti neteisingai įdiegtas ar neveiksmingas informacijos saugumo priemones ISVS apimtyje. Pavyzdžiui, galima matuoti nepašalintų pažeidžiamumų bendrą svarbą. Šis rodiklis apskaičiuojamas atsižvelgiant į pažeidžiamumų kritiškumą (pvz., naudojant *Common vulnerability scoring system* (CVSS) balą) ir paveiktų sistemų skaičių ar jų kritiškumo lygį. Tai užtikrina, kad ir kur yra randamas pažeidžiamumas, jo apskaičiavimo metodas nekis, o bendras rastų pažeidžiamumų rezultatas, naudojant pastovią apskaičiavimo metodiką, nustatys realų organizacijos rizikos lygį.

Užtikrinkite, kad visus parengtus matavimo rezultatus ir rodiklių suvestines, prieš pateikiant vadovybei, peržiūrėtų ir patvirtintų bent du atsakingi asmenys. Ši praktika dažnai vadinama „keturių akių principu“. Ji padeda užtikrinti duomenų tikslumą, tinkamą skaičiavimo metodiką, objektyvumą ir sumažina galimų klaidų tikimybę.

Periodinis stebėjimas ir rodiklių atnaujinimas

Organizacijos turi nustatyti konkrečius terminus ir atsakomybes, kada ir kas atliks stebėseną, matavimus, analizę ir vertinimą. Šie terminai priklauso nuo informacijos saugumo valdymo tikslų ir duomenų, reikalingų rodikliams apskaičiuoti / nustatyti, gyvavimo ciklo. Duomenys gali būti renkami dažniau, negu teikiamos ataskaitos suinteresuotoms šalims. Pavyzdžiui, duomenys apie kibernetinio saugumo incidentus gali būti renkami nuolat, tačiau ataskaitos vadovybei gali būti teikiamos apibendrintai tam tikru periodiškumu, išvedant vidutinę ar maksimalią vertinamo periodo rodiklio vertę. Svarbu nustatyti pradinį atskaitos tašką (angl. *baseline*), rodiklio vertę, nusakančią įprastą organizacijos veiklos būseną, kad būtų galima lyginti skirtingu laiku surinktus duomenis ir identifikuoti situacijos gerėjimą ar blogėjimą. Pavyzdžiui, nustatant pradinį atskaitos tašką nepašalintų pažeidžiamumų bendro svorio rodikliui, organizacija, atlikusi vertinimą, gali nustatyti, jog įprastai pažeidžiamumų svoris yra lygus 100 balų. Ši vertė, gauta pradinio vertinimo metu, jei atsižvelgiant į rizikos lygį yra priimtina, tampa atskaitos tašku (angl. *baseline*). Atliekant periodinę stebėseną, naujai gauta rodiklio vertė lyginama su nustatytu pradiniu atskaitos tašku. Jei nauja vertė yra 80 balų, lyginant su pradiniu atskaitos tašku, tai rodo 20 % pagerėjimą ir reiškia, kad įgyvendintos pažeidžiamumų valdymo priemonės buvo veiksmingos. Taip pat rodiklius reikia peržiūrėti ir sistemingai atnaujinti, kai pasikeičia ISVS aplinka, pavyzdžiui, verslo tikslai, teisiniai reikalavimai ar organizacinė struktūra.

Nuolatinis įrodymais pagrįstas tobulinimas

Rodiklių matavimo rezultatai yra pagrindas nuolatiniam ISVS tobulinimui. Organizacija privalo vertinti, ar jų informacijos saugumo programos planai ir veiklos yra sėkmingi, nes vien formalus informacijos saugumo priemonių įdiegimas neužtikrina informacijos saugumo tikslų pasiekimo. Surinkti duomenys analizuojami, siekiant nustatyti atotrūkį tarp siekiamų ir realių rezultatų, o nustatyti trūkumai parodo sritis, kuriose reikia tobulinti ISVS. Be to, pats stebėsenos, matavimo, analizės ir vertinimo procesas turi būti nuolat gerinamas, atsižvelgiant į grįžtamąjį ryšį iš suinteresuotų šalių, tokių kaip aukščiausio lygio vadovybė ar darbuotojai. Aukščiausio lygio vadovybė teikia atsiliepimus apie matavimo rezultatų naudingumą, padedant priimti pagrįstus sprendimus dėl rizikos valdymo, o darbuotojai, kaip esminiai informacijos saugumo procesų naudotojai (pvz., sistemų naudotojai), teikia grįžtamąjį ryšį apie kasdienių procesų efektyvumą. Atitinkamai, organizacijos privalo saugoti rodikliams surinktus ir naudotus duomenis bei informaciją. kaip įrodymą apie stebėsenos ir matavimų rezultatus.

Apibendrinant, sistemingas aukščiau išdėstytų principų taikymas padeda sukurti tvirtą ISVS veiksmingumo ir atitikties vertinimo pagrindą. Jis užtikrina, kad vertinimo procesas būtų ne tik formalus reikalavimų vykdymas, bet ir vertingas įrankis, leidžiantis objektyviai įvertinti esamą informacijos saugumo būklę ir priimti duomenimis grįstus sprendimus. Norint praktiškai įgyvendinti šiuos principus, kitas svarbus žingsnis yra nustatyti konkrečius duomenų šaltinius ISVS veiksmingumui ir atitikčiai matuoti ir iš jų sudaromus pagrindinius matavimo sistemos rodiklius, kurie bus naudojami nuolatiniam stebėjimui ir vertinimui atlikti.

Duomenų šaltinių ir pagrindinių rodiklių nustatymas

Matavimo sistema (rodikliai) yra priemonė, leidžianti organizacijai ne tik stebėti įgyvendinamą informacijos saugumo programą ar informacijos saugumo priemonių veiksmingumą, bet ir užtikrinti, kad ISVS būtų suderinta su organizacijos strateginiais veiklos tikslais ir kibernetinio saugumo reikalavimais.

Pirmasis žingsnis rodiklių nustatymo procese yra aiškiai įvardinti organizacijos informacijos saugumo poreikį. Prieš parenkant matavimo rodiklius, organizacija turi suprasti, kurios informacijos saugumas jai yra svarbus ir kokiu lygiu jis turi būti užtikrintas. Šis poreikis nustatomas atsižvelgiant į šiuos aspektus:

strateginė kryptis ir tikslai – kokios informacijos saugumas yra būtina siekiant užtikrinti stabilią organizacijos veiklą ir strateginių tikslų siekimą;

rizikos valdymo rezultatai – kokios grėsmės yra aktualios valdomai informacijai pagal atliktą rizikų vertinimą;

reguliaciniai ir sutartiniai įsipareigojimai – kokių teisės aktų, reguliacinių reikalavimų ar sutartinių įsipareigojimų laikantis būtina užtikrinti tam tikros informacijos saugumą;

suinteresuotų šalių poreikiai – kokius informacijos saugumo poreikius iškelia vadovybė, klientai, partneriai ar kitos šalys.

Nustačius informacijos saugumo poreikius ir saugotiną informaciją, toliau **parenkamos tinkamos informacijos saugumo priemonės.** Remiantis International Organization for Standardization (ISO) ir International Electrotechnical Commission (IEC) 27004:2016 tarptautiniu standartu renkantis informacijos saugumo priemones reikėtų atsižvelgti į:

rizikos mažinimo prioritetus;


turimus išteklius (pvz., žmogiškuosius, techninius);


suinteresuotų šalių poreikius;


matavimų kaštų ir naudos santykį.

Remiantis nustatytais informacijos saugumo poreikiais ir pasirinktų priemonių tikslais, parenkami tokie rodikliai bei duomenų šaltiniai, kurie leis sistemiškai stebėti informacijos saugumo priemonių veiksmingumą ir užtikrinti nuolatinį ISVS tobulinimą.

Matavimo sistemos duomenų šaltiniai

Geroji praktika rodo, kad duomenys, reikalingi ISVS veiksmingumo ir atitikties matavimo sistemos rodikliams sukurti, gali būti gaunami iš įvairių šaltinių, įskaitant technines priemones ir individualius procedūrinius žingsnius. Remiantis ISO/IEC 27004:2016 standartu, sistemos, procesai ir veiklos, kurios gali būti stebimos, siekiant surinkti duomenis, apima:

ISVS procesų įgyvendinimą, kai stebimas kiekvieno žingsnio įgyvendinimas, renkami duomenys, kaip laikomasi nustatytų informacijos saugumo valdymo sistemos procedūrų, fiksuojamos neatitiktys;

Incidentų valdymą, kai renkami duomenys apie informacijos saugumo incidentus, jų skaičių, tipus, sprendimo laiką ir poveikį;

Pažeidžiamumų valdymą, kai stebimas naujai aptiktų pažeidžiamumų skaičius, jų kritiškumas ir laikas, per kurį jie yra pašalinami;

Konfigūracijos valdymą, kai vertinama, ar informacinių sistemų konfigūracija atitinka informacijos saugumo standartus, gamintojo bazinę konfigūraciją ir gerąją praktiką ir ar nebuvo atlikta neautorizuotų pakeitimų;

Darbuotojų sąmoningumas – renkama statistika apie darbuotojų dalyvavimą informacijos saugumo mokymuose, testų rezultatus ir sąmoningumo didinimo kampanijų efektyvumą;

Prieigos kontrolę, ugniasienės ir kiti įvykių žurnalų įrašų stebėseną, kai – analizuojami įrašai iš įvairių informacijos saugumo sistemų, siekiant aptikti neįprastą veiklą, bandymus pažeisti nustatytą informacijos saugumo politiką;

Auditą, kai vertinami vidaus ir išorės auditų rezultatai, nustatytos neatitiktys ir rekomendacijų įgyvendinimo eiga;

Rizikos vertinimo ir rizikos valdymo procesus, kai stebima, ar rizikos vertinimas atliekamas periodiškai, ar laiku ir nuosekliai valdomos nustatytos rizikos, ar rizikos valdymo planas yra aktualus;

Trečiųjų šalių rizikos valdymą, kai vertinama, kaip yra laikomasi informacijos saugumo reikalavimų, nustatytų sutartyse su tiekėjais ir partneriais;

Veiklos tęstinumo valdymą, kai – renkami duomenys iš veiklos tęstinumo planų testavimo pratybų ir vertinamas pasirengimas reaguoti į trikdžius;

Fizinės ir aplinkos apsaugos valdymą, kai stebimi fizinės prieigos žurnalai, vaizdo stebėjimo įrašai ir aplinkos parametrų (pvz., temperatūros) duomenys, fiksuojamos neatitiktys;

Informacinių išteklių stebėseną, kai vykdoma nuolatinė informacinių sistemų, tinklo įrenginių ir kitų informacinių išteklių būsenos stebėsena, siekiant užtikrinti jų stabilų veikimą ir saugumą.

Nustačius ISVS stebėsenos apimtį, tikslus ir reikiamus duomenų šaltinius, kitas žingsnis yra konkrečių, pamatuojamų matavimo sistemos rodiklių nustatymas. Rodikliai leidžia kiekybiškai išreikšti surinktą informaciją, įvertinti ISVS ar informacijos saugumo priemonių veiksmingumą ir priimti duomenimis grįstus sprendimus dėl tolimesnių ISVS tobulinimo ir atsparumo gerinimo veiksmų.

Rodiklių nustatymas

Nustatant rodiklius, įskaitant ir jų siektinas bei ribines reikšmes, **rekomenduojama vadovautis SMART principais,** apibrėžiančiais rodiklių aiškumą, objektyvumą ir praktinę vertę, nes šie principai leidžia nustatyti rodiklius, kurie būtų:

- **konkretūs**
  rodiklis turi aiškiai apibrėžti, ką tiksliai norima matuoti;
- **išmatuojami**
  rodiklis turi būti pagrįstas objektyviais, lengvai surenkamais duomenimis;
- **pasiekiami**
  rodiklis turi būti realistiškas, įgyvendinamas pagal turimus išteklius ir aplinkybes;
- **aktualūs**
  rodiklis turi būti tiesiogiai susijęs su svarbiausiais organizacijos ar informacijos saugumo programos tikslais;
- **apibrėžti laike**
  rodiklis turi turėti aiškų matavimo terminą (nuo kada iki kada bus renkamas) arba periodiškumą.

Siekiant sistemiškai įvertinti ISVS veiksmingumą bei informacijos saugumo priemonių veiksmingumą, organizacijos gali pasitelkti kelių kategorijų rodiklius. Pagal tarptautinį ISO/IEC 27004:2016 standartą egzistuoja keletas rodiklių kategorijų, tačiau pagrindiniai ir dažniausiai naudojami rodikliai yra šie:

veiklos rodikliai
(angl. Performance measures)

matuoja, ar veikla, procesas, veiksmas buvo atliktas taip, kaip numatyta ISVS. Rodikliai parodo veiklos įgyvendinimo laipsnį, dažnumą, kiekį, laiką ar kitas kiekybines savybes;

veiksmingumo rodikliai
(angl. Effectiveness measures)

parodo, kokį rezultatą pasiekė ISVS ar įdiegtos informacijos saugumo priemonės, ar jos turėjo poveikį, užtikrinant informacijos saugumą. Jie padeda suprasti, ar priemonės veikia taip, kaip tikėtasi, ir pasiekia norimus informacijos saugumo rezultatus bei tikslus.

Be pagrindinių veiklos ir veiksmingumo rodiklių, išsamesnei analizei ir strateginiam vertinimui taip pat gali būti taikomi šie papildomi rodiklių tipai:

tikslų pasiekimo rodikliai
angl. Key Goal Indicators, KGI)

rodantys, ar pasiekti iš anksto nustatyti informacijos saugumo programos ar organizacijos tikslai;

kritiniai sėkmės veiksniai
(angl. Critical Success Factors, CSF)

esminiai aspektai ar būtinos sąlygos, nuo kurių priklauso informacijos saugumo programos sėkmė.

Remiantis Europos Sąjungos kibernetinio saugumo agentūros (ENISA) tinklų ir informacinių sistemų (toliau - TIS) techninėmis įgyvendinimo gairėmis, toliau pateikiami konkretūs rodiklių, kurie gali būti naudojami ISVS veiksmingumo ir atitikties vertinimui, pavyzdžiai.

Į veiklos rodiklių sąrašą gali įeiti:

Įdiegimo ir palaikymo sąnaudos
(angl. CAPEX/OPEX)

šis rodiklis padeda kiekybiškai įvertinti informacijos saugumo priemonėms įdiegti ir palaikyti skiriamus išteklius, tokius kaip: personalas, techninė įranga, programinė įranga ir paslaugos. Šis rodiklis taip pat parodo, ar ištekliai yra paskirstomi pagal planą;

Darbuotojų, dalyvavusių kibernetinio saugumo mokymuose, skaičius

šiuo rodikliu matuojama, kiek darbuotojų dalyvavo informacijos saugumo mokymuose. Tai yra klasikinis veiklos rodiklis, padedantis įvertinti, ar sąmoningumo didinimo programa vykdoma taip, kaip numatyta.

Veiksmingumo rodiklių sąrašą gali sudaryti:

Aptiktų pažeidžiamumų skaičius ir šalinimo laikas
šie rodikliai yra susiję su pažeidžiamumų valdymo veiksmingumu. Galima matuoti nepašalintų pažeidžiamumų bendrą svarbą, atsižvelgiant į jų kritiškumą ir paveiktų sistemų skaičių. Taip pat galima stebėti, kokiai daliai kritinių sistemų buvo atliktas įsiskverbimo testavimas ar pažeidžiamumų vertinimas. Tai yra veiksmingumo rodikliai, parodantys, kaip sėkmingai organizacija mažina aktualių rizikų poveikį;

Incidentų skaičius ir reagavimo laikas
šie rodikliai parodo incidentų valdymo proceso veiksmingumą. Galima stebėti bendrą incidentų skaičiaus tendenciją per tam tikrą laikotarpį arba matuoti, kiek incidentų nebuvo išspręsta per nustatytą laiką. Tai yra veiksmingumo rodiklis, kuris tiesiogiai atspindi, kaip įdiegtos informacijos saugumo priemonės ir procesai veikia realioje aplinkoje;

Neatitikčių skaičius
šis rodiklis yra susijęs su atitikties stebėsena ir nuolatiniu gerinimu. Jis gali būti išreikštas kaip neįgyvendintų korekcinių veiksmų, kurie dažnai kyla iš nustatytų neatitikčių, santykis. Priklausomai nuo konteksto, tai gali būti veiklos rodiklis, parodantis, ar laikomasi taisymo planų, ar veiksmingumo rodiklis, parodantis bendrą atitikties lygį.

Tikslų pasiekimo rodiklių sąrašą gali sudaryti:

- **Teisės aktų reikalavimų atitiktis**
  šis rodiklis rodo, ar organizacija pasiekė iš anksto nustatytą strateginį tikslą – atitiktį galiojantiems kibernetinio saugumo teisės aktams ir reguliaciniams reikalavimams;
- **Aptiktų pažeidžiamumų skaičius**
  šis rodiklis matuoja bendrą aptiktų pažeidžiamumų skaičių per nustatytą laikotarpį. Šis rodiklis padeda įvertinti, ar pasiektas strateginis tikslas sumažinti organizacijos pažeidžiamumų lygį.

Kritinių sėkmės veiksnių sąrašą gali sudaryti:

- **Efektyvi darbuotojų sąmoningumo didinimo programa**
  tai kokybinė sąlyga, apibrėžianti būtinybę turėti reguliariai atnaujinamą ir visapusišką darbuotojų mokymų programą. Tai yra kritinė sąlyga, nuo kurios priklauso atsparumas socialinės inžinerijos atakoms ir užtikrinimas bendros saugumo kultūros organizacijoje. Šio veiksnio sėkmė gali būti vertinama pagal tai, koks skaičius darbuotojų dalyvavo mokymuose;
- **Efektyvus incidentų valdymas**
  ši būtina sąlyga nustato organizacijos gebėjimą laiku ir tinkamai reaguoti į kibernetinio saugumo incidentus. Sėkmingas incidentų valdymas yra būtinas, norint sumažinti incidentų poveikį ir užtikrinti veiklos tęstinumą. Šios sąlygos išpildymas gali būti vertinamas pagal reagavimo į incidentus laiką.

Efektyviai parinkti rodikliai padeda organizacijai pasiekti šiuos tikslus:

- Įvertinti ISVS ar informacijos saugumo programos veiksmingumą, pavyzdžiui, ar priemonės padeda mažinti incidentų dažnį ir poveikį?
- Stebėti atitiktį, ar ISVS atitinka kibernetinio saugumo teisės aktų, standartų, DORA reglamento, TIS2 direktyvos ar kitus reikalavimus?
- Analizuoti progresą arba regresą, ar investicijos į informacijos saugumą (finansinės, žmogiškosios, technologinės) lemia apčiuopiamą naudą organizacijai?

Apibendrinant, ISVS ir taikomų informacijos saugumo priemonių tinkamas vertinimas priklauso nuo metodiškai ir tinkamai parinktų, pamatuojamų rodiklių, kurie atitinka organizacijos informacijos saugumo poreikius ir strateginius tikslus. Nustačius veiklos, veiksmingumo ir kitus strateginius rodiklius, itin svarbu užtikrinti, kad jiems matuoti surinkti duomenys ir iš jų gauti rezultatai būtų aiškiai bei suprantamai pateikti atsakingiems asmenims ir vadovybei. Tinkamai ir laiku pateikti duomenys padeda ne tik stebėti esamą saugumo būklę, bet ir laiku priimti duomenimis grįstus ir įrodymais paremtus sprendimus dėl ISVS ar informacijos saugumo priemonių tobulinimo.

Rodiklių atvaizdavimas

Kiekviena organizacija turi pasirinkti jos veiklai ir jos auditorijai tinkamiausius rodiklių atvaizdavimo ir ataskaitų teikimo formatus. Skirtingoms suinteresuotoms šalims gali prireikti skirtingo detalumo ir formato ataskaitų, todėl organizacija turėtų naudoti įvairius ataskaitų teikimo metodus ir formatus. Pavyzdžiui, aukščiausio lygio vadovybei skirti rodikliai gali skirtis nuo tų, kurie teikiami skyrių vadovams.

Ataskaitos gali būti teikiamos, naudojant įvairius metodus bei formatus:

ATASKAITŲ FORMATAI

gali būti parinkti nuo paprastų ir statiškų, pavyzdžiui, tam tikro laikotarpio rodiklių sąrašo, iki sudėtingesnių ataskaitų su grupavimu, apibendrinimais ir dinaminėmis detalizavimo galimybėmis. Ataskaitos yra naudingos, kai reikia pateikti neapdorotus duomenis lengvai skaitomu formatu.

GRAFINIAI ELEMENTAI

rodiklius galima atvaizduoti kaip tekstą, skaičius arba įvairias diagramas (pavaizduotas skrituliais, linijomis, vertikaliomis ar horizontaliomis skiltimis). Taip pat gali būti naudojami dinaminiai matuokliai (angl. *gauges*) su įspėjimais ir papildomais grafiniais elementais.

Užtikrinkite, kad matavimo sistemos rodiklių suvestinės suteiktų objektyvų ISVS veiksmingumo ar informacijos saugumo programos įgyvendinimo vaizdą.

Norint, kad rezultatai būtų teisingi ir patikimi, jie turi būti palyginami ir atkuriami. Surinkti duomenys turi būti analizuojami, atsižvelgiant į nustatytą kiekvieno rodiklio tikslą. Išvados, gautos atlikus analizę, turi būti peržiūrėtos atitinkamų suinteresuotų šalių, kad būtų užtikrinta teisinga duomenų interpretacija. Taip pat, prieš skelbiant informaciją, organizacija turi nustatyti, kaip ir su kuo bus dalijamasi surinktais duomenimis, nes kai kurie su informacijos saugumu susiję duomenys gali būti konfidencialūs.

Pagrindinės stebėsenos veiklos

ISVS ar informacijos saugumo priemonių veiksmingumo vertinimas yra nuolatinis ir daugiasluoksnis procesas, kurį organizacijos privalo vykdyti, siekdamos užtikrinti, kad taikomos priemonės būtų efektyvios, tinkamai palaikomos ir atitiktų kintančius informacijos saugumo poreikius bei tikslus. Siekiant sisteminio vertinimo, organizacijos turi nustatyti ir taikyti aiškią politiką, kuri apibrėžtų, kokios informacijos saugumo priemonės bus stebimos, kokiais metodais ir kaip dažnai bus atliekamas jų vertinimas ir kas bus atsakingas už matavimo rezultatų analizę.

Pagrindinės stebėsenos veiklos apima šias sritis:

- atitikties stebėsena;
- priemonių veiksmingumo vertinimas;
- kibernetinio saugumo auditas;
- atskaitomybė.

Atitikties stebėsena. Atsižvelgiant į individualius organizacijos informacijos saugumo poreikius ir siekiant užtikrinti, kad organizacijos taikoma ISVS atitiktų kibernetinio saugumo reikalavimus, organizacijos privalo vykdyti reguliarų vidinį atitikties vertinimą, kuris turi būti atliekamas periodiškai, ne rečiau kaip kartą per 12 mėn. Organizacijos turi nustatyti atitikties apimtį ir terminus bei reguliariai vykdyti progreso matavimą, analizę ir vertinimą.

Visi stebėsenos ir matavimų rezultatai privalo būti tinkamai dokumentuojami ir saugomi kaip įrodymai. Šie rezultatai turi būti pateikiami suinteresuotoms šalims, ypač vadovybei, parengiant atitikties vertinimo ataskaitas.

Nustačius neatitiktis, būtina parengti jų šalinimo planą, kuriame būtų įvardinti paskirti atsakingi vykdytojai, numatyti reikalingi ištekliai ir nustatyti konkretūs įgyvendinimo terminai. Nustatytos neatitiktys ir atotrūkiai tarp siekiamų ir realių rezultatų gali rodyti poreikį tobulinti ISVS, įskaitant jos apimtį, politikas, tikslus, priemones ir procesus. Norint įvertinti, ar organizacija veiksmingai ir pagal planą šalina nustatytus trūkumus, galima stebėti neįgyvendintų korekcinių veiksmų santykį ir lyginti jį su ankstesniais laikotarpiais, siekiant nustatyti, ar tendencija yra gerėjanti.

Priemonių veiksmingumo vertinimas. Organizacijos turi nustatyti aiškius informacijos saugumo priemonių veiksmingumo rodiklius bei pradinius atskaitos taškus (angl. *baseline*), kad galėtų stebėti pokyčius ir vertinti pažangą laikui bėgant. Renkant duomenis nustatytu periodiškumu, svarbu naudoti įvairius šaltinius: technines sistemas (pvz., įvykių žurnalus), darbuotojų mokymų registrus, incidentų ataskaitas ar kitas aktualias duomenų bazes.

Atsižvelgiant į aktualias rizikas ir strateginius tikslus, organizacija turi aiškiai nustatyti, kurios informacijos saugumo priemonės bus stebimos ir vertinamos. Matavimus galima taikyti bet kuriems ISVS procesams, veikloms ar priemonėms. Svarbu įvertinti, kaip priemonė modifikuoja riziką – pavyzdžiui, kiek sumažėja rizikos įvykio tikimybė ar galimas jos poveikis, arba kiek laiko užtrunka aptikti įvykį po jo atsiradimo.

Surinkti duomenys analizuojami lyginant juos su iškeltais tikslais (pavyzdžiui, sumažinti rizikos tikimybę) ir pradiniu atskaitos tašku, siekiant įvertinti, ar priemonės duoda norimą rezultatą. Pavyzdžiui, galima stebėti, ar po papildomų darbuotojų mokymų sumažėjo socialinės inžinerijos incidentų skaičius, ar sumažėjo nepašalintų pažeidžiamumų kiekis, ar sutrumpėjo reagavimo į incidentus laiko vidurkis. Taip pat galima vertinti konkrečių priemonių veiksmingumą: apsaugos nuo kenkėjiškos programinės įrangos efektyvumą – pagal incidentų, susijusių su kenkėjiškomis programomis, skaičių ar sistemų su neatnaujintais antivirusiniais parašais procentą; tinklo saugumą – pagal nenaudojamų ugniasienės taisyklių skaičių. Remiantis ISO/IEC 27004:2016 standartu, stebėsenos, matavimo, analizės ir vertinimo procesai gali būti atliekami ir rankinėmis, ir automatizuotomis priemonėmis. Nepaisant to, rekomenduojama, kad duomenų rinkimas, analizė ir ataskaitų teikimas turėtų būti automatizuotas visur, kur įmanoma, siekiant sumažinti sąnaudas, pastangas ir žmogiškosios klaidos tikimybę.

Atsižvelgiant į organizacijos rizikos vertinimo rezultatus, gali būti taikomi ir kiti papildomi informacijos saugumo priemonių veiksmingumo vertinimo metodai. ENISA techninėse įgyvendinimo gairėse nurodomi kiti galimi informacijos saugumo priemonių vertinimo būdai, tokie kaip:

- **Išeities kodo peržiūra.**
  Vienas iš metodų, skirtų kibernetinio saugumo priemonių veiksmingumui vertinti. Sprendimas taikyti šį metodą turėtų būti pagrįstas rizikos valdymo principais. Jei rizikos vertinimas rodo didelę riziką, susijusią su programinės įrangos išeities kodu, tuomet šios srities stebėsena ir vertinimas tampa būtinas.

Pažeidžiamumų vertinimas.

Priemonių veiksmingumo vertinimo metodas, kurio taikymo apimtis ir nauda priklauso nuo organizacijos rizikos vertinimo. Šis metodas padeda įvertinti, kaip sėkmingai organizacija mažina savo rizikos lygį. Vertinant pažeidžiamumų valdymo efektyvumą, galima taikyti šiuos rodiklius:

- **matuoti,** kurioms kritinėms sistemoms buvo atliktas įsiskverbimo testavimas (angl. *penetration testing*) ar pažeidžiamumų vertinimas;
- **stebėti** bendrą „pažeidžiamumų vaizdą“ (angl. *vulnerability landscape*), apskaičiuojant nepašalintų pažeidžiamumų svarbą. Šio rodiklio skaičiavimas priklauso nuo pažeidžiamumų kritiškumo ir paveiktų sistemų skaičiaus.

Analizės rezultatai periodiškai pateikiami vadovybei ir naudojami sprendžiant dėl tolesnių veiksmų ar informacijos saugumo priemonių koregavimo. Rodikliai bei stebėjimo procesas turi būti nuolat peržiūrimi ir atnaujinami pagal organizacijos tikslus, pasikeitusią riziką ar aplinkos veiksnius. Toks nuoseklus veiksmingumo stebėjimas padeda užtikrinti, kad informacijos saugumo priemonės būtų ne tik įdiegtos, bet ir faktiškai veiktų bei stiprintų organizacijos atsparumą grėsmėms.

Kibernetinio saugumo auditas. Tai yra nepriklausoma veikla, skirta įvertinti, ar organizacijos ISVS atitinka nustatytus teisinius reikalavimus ar standartus. Šis procesas yra esminė informacijos saugumo priemonių veiksmingumo vertinimo dalis, padedanti vadovybei gauti objektyvų ir nešališką vaizdą apie informacijos saugumo būklę organizacijoje. Kibernetinio saugumo auditas dažniausiai apima vieną arba kelias esmines sritis:

- **ISVS teisinių reikalavimų atitiktis,** pasirinktinai įtraukiant informacijos saugumo priemonių veiksmingumo vertinimą;
- **ISVS įgyvendinimo atitiktis** organizacijos vidaus tvarkoms. Pavyzdžiui, jei politika reikalauja reguliariai peržiūrėti prieigos teises, tai audito metu būtų prašoma pateikti įrodymus, jog atsakingi asmenys atitinkamai ir matavo bei stebėjo kritinių sistemų prieigos paskyras ir jų teises.

Organizacijos, besivadovaujančios Kibernetinio saugumo įstatymo įgyvendinimo reikalavimų nuostatomis, privalo reguliariai, ne rečiau kaip kartą per 3 metus, atlikti kibernetinio saugumo auditą. Auditas yra vienas iš ISVS vertinimo procesų, kurio vykdymą galima ir reikia matuoti. Pavyzdžiui, rekomenduojama vertinti audito programos įgyvendinimo užbaigtumą, lyginant atlikto audito apimtį su planuota audito apimtimi, o tai leidžia vadovybei stebėti, ar audito veiklos vykdomos pagal planą ir apima visas svarbias ISVS sritis.

Nustačius neatitiktis audito metu, organizacija privalo parengti jų šalinimo planą, kuriame būtų aiškiai paskirti atsakingi vykdytojai, numatyti reikalingi ištekliai ir nustatyti įgyvendinimo terminai. Nustatytos neatitiktys dažniausiai virsta korekciniais veiksmais, todėl siūloma matuoti jų įgyvendinimo našumą. Galima stebėti neįgyvendintų korekcinių veiksmų santykį ir šio rodiklio tendencijas per tam tikrą laikotarpį, siekiant įvertinti, ar organizacija efektyviai ir laiku šalina nustatytus trūkumus. Analizuojant surinktus duomenis, galima nustatyti atotrūkį tarp siekiamų ir realių atitikties rezultatų, kuris gali rodyti poreikį tobulinti ISVS.

Atskaitomybė. Siekiant užtikrinti organizacijos veiklos tikslų siekimą bei veiksmingą ISVS, vadovybei turi būti laiku teikiami ir pranešami ISVS stebėsenos bei matavimų rezultatai. Laiku pateiktos rezultatų suvestinės leidžia vadovybei objektyviai įvertinti esamą organizacijos informacijos saugumo būklę ir priimti atitinkamus duomenimis grįstus bei įrodymais paremtus sprendimus dėl ISVS tobulinimo, išteklių paskirstymo ar tolimesnių organizacijos veiksmų. Organizacija taip pat privalo saugoti surinktus matavimų rezultatus kaip įrodymus, kad vadovybė laiku gavo ataskaitas apie informacijos saugumo būklę, priemonių įgyvendinimą ar esamo(-ų) ISVS veiksmingumą.

Atitinkamai, siekiant užtikrinti, kad organizacija atitinka Kibernetinio saugumo įstatymo įgyvendinimo reikalavimus, KSS privalo reguliariai teikti informaciją ir NKSC. Esminiai KSS turi ne rečiau kaip kartą per metus pateikti atitikties vertinimą, užpildydami specialų klausimyną **Kibernetinio saugumo informacinėje sistemoje (KSIS).** Be to, organizacijos privalo pateikti rizikos vertinimo ataskaitos ir rizikos valdymo plano patvirtinimo duomenis į KSIS ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo organizacijoje.

NKSC pareikalavus, KSS taip pat privalo pateikti audito ataskaitų, atitikties vertinimo ataskaitų, neatitikčių šalinimo planų, rizikos vertinimo ataskaitų bei rizikos valdymo planų kopijas per 5 darbo dienas. Visi organizacijos vadovo patvirtinti dokumentai, tokie kaip rizikos vertinimo ataskaitos ir rizikos valdymo planai, turi būti saugomi ne trumpiau kaip 3 metus.

Nuolatinis matavimo sistemos veiksmingumo gerinimas

Tobulinant ISVS veiksmingumo ir atitikties matavimo sistemą, pirmiausia atsižvelgiama į organizacijos informacijos saugumo poreikius. Tobulinimas gali apimti ir esamų matavimo sistemos rodiklių ar analizės procesų atnaujinimą, ir visiškai naujų rodiklių nustatymą ar duomenų šaltinių įtraukimą. Naujai identifikuoti arba atnaujinti matavimo sistemos rodikliai turėtų būti detaliai apibūdinti, įvardinant aiškius tikslus, duomenų šaltinius ir rodiklių apskaičiavimo metodiką.

Pats stebėsenos, matavimo, analizės ir vertinimo procesas turi būti aprašytas, nuolat peržiūrimas ir tobulinamas. Nuolatinio matavimo sistemos veiksmingumo gerinimo procesas turi apimti grįžtamojo ryšio iš suinteresuotų šalių rinkimą, duomenų rinkimo ir analizės metodų peržiūrą, remiantis išmoktomis pamokomis, bei rodiklių stebėsenos procedūrų atnaujinimą. Taip užtikrinama, kad matavimo (rodiklių) sistema išlieka aktuali, efektyvi ir atitinka besikeičiančius organizacijos poreikius.

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO IR ATITIKTIES VERTINIMAS

NKSC pastebi, kad kibernetinio saugumo reikalavimai dažnai įgyvendinami formaliai, neįvertinant priemonių efektyvumo, todėl rizikos nustatomos paviršutiniškai, o toks požiūris lemia netikslų informacijos saugumo valdymo sistemos veiksmingumo rodiklių nustatymą.

MATAVIMO SISTEMOS (RODIKLIŲ) NUSTATYMO PRINCIPAI

- **Skaidrumas ir tikslumas**
- **Periodinis stebėjimas ir rodiklių atnaujinimas**
- **Nuolatinis įrodymais pagrįstas tobulinimas**

DUOMENŲ ŠALTINIŲ IR PAGRINDINIŲ RODIKLIŲ NUSTATYMAS

1

Pirmasis žingsnis rodiklių nustatymo procese yra aiškiai įvardinti organizacijos informacijos saugumo poreikį

2

Nustačius informacijos saugumo poreikius ir saugotiną informaciją, toliau parenkamos tinkamos informacijos saugumo priemonės.

3

Parenkami rodikliai ir duomenų šaltiniai, leidžiantys stebėti informacijos saugumo priemonių veiksmingumą ir užtikrinti ISVS tobulinimą.

MATAVIMO SISTEMOS DUOMENŲ ŠALTINIAI

Remiantis ISO/IEC 27004:2016 standartu, sistemos, procesai ir veiklos, kurios gali būti stebimos, siekiant surinkti duomenis, apima:

- **Incidentų valdymą,** kai renkami duomenys apie informacijos saugumo incidentus, jų skaičių, tipus, sprendimo laiką ir poveikį;
- **Pažeidžiamumų valdymą,** kai stebimas naujai aptiktų pažeidžiamumų skaičius, jų kritiškumas ir laikas, per kurį jie yra pašalinami;
- **Prieigos kontrolę, ugniasienės** ir kiti įvykių žurnalų įrašų stebėseną, kai – analizuojami įrašai iš įvairių informacijos saugumo sistemų, siekiant aptikti neįprastą veiklą, bandymus pažeisti nustatytą informacijos saugumo politiką;
- **Trečiųjų šalių rizikos valdymą,** kai vertinama, kaip yra laikomasi informacijos saugumo reikalavimų, nustatytų sutartyse su tiekėjais ir partneriais;
- **Veiklos tęstinumo valdymą**, kai – renkami duomenys iš veiklos tęstinumo planų testavimo pratybų ir vertinamas pasirengimas reaguoti į trikdžius;

RODIKLIŲ NUSTATYMAS

TIPAI

- veiklos rodikliai
- veiksmingumo rodikliai
- tikslų pasiekimo rodikliai
- kritiniai sėkmės veiksniai

SMART

- konkretūs
- išmatuojami
- pasiekiami
- aktualūs
- apibrėžti laike

Užtikrinkite, kad matavimo sistemos rodiklių suvestinės suteiktų objektyvų ISVS veiksmingumo ar informacijos saugumo programos įgyvendinimo vaizdą.

PAGRINDINĖS STEBĖSENOS VEIKLOS

Atitikties stebėsena	Priemonių veiksmingumo vertinimas
Atskaitomybė	Kibernetinio saugumo auditas

Pats stebėsenos, matavimo, analizės ir vertinimo procesas turi būti aprašytas, nuolat peržiūrimas ir tobulinamas. Nuolatinio matavimo sistemos veiksmingumo gerinimo procesas turi apimti grįžtamojo ryšio iš suinteresuotų šalių rinkimą, duomenų rinkimo ir analizės metodų peržiūrą, remiantis išmoktomis pamokomis, bei rodiklių stebėsenos procedūrų atnaujinimą.

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.