VALSTYBĖS KONTROLĖ
VALSTYBINIS AUDITAS

KIBERNETINIO SAUGUMO UŽTIKRINIMAS

2022 m. spalio 27 d.

Nr. VAE-10

SANTRAUKA

Audito svarba

Ypatingos svarbos informacinė infrastruktūra, valstybės informacinių išteklių elektroninė informacija ir jų pagrindu veikiančios sistemos ir paslaugos yra gyvybiškai svarbios Lietuvos Respublikai. Dėl didėjančio paslaugų ir procesų skaitmenizavimo, COVID-19 pandemijos, geopolitinių iššūkių ir įtampų auga kibernetinių ir hibridinių atakų grėsmė, didėja jų socialinis ir ekonominis poveikis. Nacionalinio kibernetinio saugumo centro duomenimis [1], per 3 pastaruosius metus užregistruota 11 659 kibernetinių incidentų: 2019 m. – 3 241, 2020 m. – 4 330, 2021 m. – 4 088. Dėl didelio kibernetinių incidentų skaičiaus, jų modernėjimo, galimos rizikos patirti reikšmingus kibernetinių atakų ir incidentų padarinius, vis svarbiau užtikrinti kibernetinį saugumą nacionaliniu lygmeniu.

Kibernetinio saugumo užtikrinimas grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos ypatingos svarbos informacinės infrastruktūros, ryšių ir informacinių sistemų saugumui, rizikos vertinimu. Rizikos valdymas sudaro pagrindą veiksmingos saugumo reikalavimų valdymo sistemos sukūrimui, diegimui, palaikymui ir tobulinimui. Saugumo valdymo sistema apima institucijų, organizacijų tinklų ir informacinių sistemų saugumo reikalavimų (priemonių, taisyklių ir procedūrų) nustatymą ir vykdymą, stebėseną ir peržiūrą (atitikties vertinimą), kibernetinių incidentų prevenciją, aptikimą, reagavimą į juos, atsigavimą, atsako į kibernetinius incidentus galimybių, jų išvengimo priemonių vertinimą, saugumo technologijų valdymą, darbuotojų mokymą, informuotumo programas.

Suprasdami, kad kibernetinio saugumo rizikos valdymas, kibernetinių incidentų valdymas, prevencinė veikla, įskaitant kibernetinio saugumo pratybas ir mokymus, yra svarbūs veiksmingos saugumo valdymo sistemos elementai (veiksniai), lemiantys kibernetinio saugumo užtikrinimą, nusprendėme atlikti valstybinį auditą.

[1] Prieiga per internetą: https://www.nksc.lt/aktualu.html (Nacionalinio kibernetinio saugumo būklės ataskaitos, žiūrėta 2022-07-08).

Audito tikslas ir apimtis

Audito tikslas – įvertinti, ar užtikrinamas kibernetinis saugumas.

Pagrindiniai audito klausimai:

- ar užtikrinamas kibernetinio saugumo rizikos valdymas nacionaliniu lygiu;
- ar kibernetinio saugumo teisinis reguliavimas ir atitikties teisės aktų nustatytiems reikalavimams vertinimo sistema veiksminga;
- ar užtikrinamas kibernetinių incidentų valdymas;
- ar užtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas.

Audituojamieji subjektai:

- Krašto apsaugos ministerija, nes formuoja kibernetinio saugumo politiką, organizuoja, kontroliuoja ir koordinuoja jos įgyvendinimą[2];
- Nacionalinis kibernetinio saugumo centras, nes įgyvendina kibernetinio saugumo politiką ir yra atsakingas už kibernetinių incidentų stebėseną ir rizikos kibernetinėje erdvėje analizę nacionaliniu lygmeniu, kibernetinio saugumo reikalavimų įgyvendinimo stebėseną, kibernetinio saugumo subjektų saugumo būklės įvertinimą[3].

Audito metu informaciją rinkome iš Krašto apsaugos ministerijos, Nacionalinio kibernetinio saugumo centro, atlikome 212 kibernetinio saugumo subjektų[4] apklausą. Bendravome su Valstybinės duomenų apsaugos inspekcijos, Ryšių reguliavimo tarnybos, Informatikos ir ryšių departamento, Lietuvos kriminalinės policijos biuro, Kauno technologijos universiteto atstovais.

Audituojamasis laikotarpis – 2019–2021 m. Siekdami įvertinti tendencijas ir pokyčius, kai kuriais atvejais naudojome ankstesnių (2015–2018 m.) ir 2022 m. duomenis.

Auditas atliktas pagal tarptautinius aukščiausiųjų audito institucijų standartus. Audito apimtis ir taikyti metodai išsamiau aprašyti 2 priede „Audito apimtis ir metodai“ (43 psl.).

Pagrindiniai audito rezultatai

Tobulintina kibernetinio saugumo užtikrinimo sistema, nes: nacionaliniu lygiu neužtikrinamas tinkamas kibernetinio saugumo rizikos ir incidentų valdymas, nesudarytos tinkamos sąlygos vykdyti atitikties saugumo reikalavimams stebėseną, vis dar nekonsoliduotas kibernetinio saugumo ir elektroninės informacijos saugos teisinis reguliavimas, neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas. Veiksmingai veikianti kibernetinio saugumo užtikrinimo sistema padidintų atsparumą kibernetinėms grėsmėms, efektyviai apsaugotų ypatingos svarbos informacinę infrastruktūrą, valstybės informacinius išteklius, sustiprintų atsaką kibernetinėms grėsmėms.

[2] Kibernetinio saugumo įstatymas, 4 str. 2 d.

[3] Ten pat, 4 str. 3 d., 8 str. 2 d.

[4] Valstybės informacinių išteklių valdytojai ir tvarkytojai, nurodyti http://www.registrai.lt/ tinklalapyje, ir ypatingos svarbos informacinės infrastruktūros valdytojai (žiūrėta 2022-08-18).

1. Saugumo valdymo sistema nepakankamai veiksminga

- Informacija apie kibernetinio saugumo subjektų identifikuotas kibernetinio saugumo rizikas nekaupiama bei nacionaliniu lygiu nevaldoma. Daugiau kaip trečdalis (38 proc., 81 iš 212) apklaustų kibernetinio saugumo subjektų neatlieka kibernetinio saugumo rizikos vertinimo, dėl to gali būti nepastebėtos naujos ar besikartojančios grėsmės, darančios įtaką subjektų saugos būklei ir jų veiklai. Kibernetinio saugumo rizikos vertinimo procesas reikalauja specifinių šios srities žinių ir įstaigų rizikos vertinimą atliekantys specialistai kokybiškai įvertinti kibernetinio saugumo rizikų negali, todėl tikslinga turėti rizikos vertinimo gaires. Daugiau nei pusė (56 proc., 74 iš 131) vertinimus atlikusių kibernetinio saugumo subjektų informacijos apie identifikuotas kibernetinio saugumo rizikas Nacionaliniam kibernetinio saugumo centrui nepateikia. Teisės aktuose neįtvirtinta prievolė kibernetinio saugumo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius, ypatingos svarbos informacinės infrastruktūros valdytojams, periodiškai teikti Nacionaliniam kibernetinio saugumo centrui ryšių ir informacinių sistemų rizikos vertinimo ataskaitas. Kadangi nėra identifikuotų nacionalinių kibernetinio saugumo rizikų, nėra sudarytas nacionalinių kibernetinio saugumo rizikos valdymo priemonių planas ir nenustatyta priimtina nacionalinė kibernetinio saugumo rizika, jos tolerancijos ribos, todėl nacionaliniu lygiu nėra koordinuojamas rizikos valdymo procesas, kuriuo būtų užtikrinamas reikiamų apsaugos, prevencijos ir atsako priemonių bei pajėgumų panaudojimas (1.1 poskyris, 13 psl.).

- 2019–2021 m. beveik pusė (45 proc., 80 iš 176) valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų nė karto neatliko informacinių technologijų saugos atitikties vertinimo ir taip neįsitikino savo informacijos saugumo valdymo sistemos būkle, kad, prireikus, laiku galėtų imtis veiksmų ją tobulinti. Kasmet informacinių technologijų saugos atitikties vertinimų skaičius auga, tačiau 2021 m. nepateikta net 81 proc. valstybės informacinių išteklių informacinių technologijų saugos atitikties vertinimo ataskaitų. Didelė dalis (41 proc., 39 iš 96) informacinių technologijų saugos atitikties vertinimus atlikusių valstybės informacinių išteklių valdytojų ir (arba) tvarkytojų duomenų Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemai neteikė. Tai mažina galimybes centralizuotai valdyti informaciją apie informacinių technologijų saugos neatitiktis ir nacionaliniu lygiu užtikrinti reikalavimų laikymosi priežiūrą. Valstybės kontrolė 2018 m. nustatė trūkumų[5], nors rekomendacijos priemonė turėjo būti įgyvendinta iki 2019-06-01, tačiau problemos iki šios dienos nėra išspręstos, nes pagal esamą programinį kodą nėra galimybės atlikti Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistemos funkcinio praplėtimo, todėl ilgus metus problemos, kurių nepavyksta išspręsti, neigiamai veikia šį tvarumą, sudaro sąlygas pažeidžiamumams atsirasti (1.2 poskyris, 15 psl.).

- Krašto apsaugos ministerijai 2015 m. perėmus kibernetinio saugumo ir 2018 m. valstybės informacinių išteklių (elektroninės informacijos saugos) politikos formavimo funkcijas nebuvo konsoliduota šių sričių teisinė bazė. Valstybės kontrolė 2015 m. pateikė rekomendaciją[6] peržiūrėti ir suderinti (konsoliduoti) kibernetinio saugumo ir

[5] Valstybės informacinių išteklių atitikties informacijos saugos reikalavimams stebėsenos sistema sukurta valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenai palengvinti ir jos funkcionalumas nėra pakankamai panaudojamas.

[6] Prieiga per internetą: https://www.valstybeskontrole.lt/LT/Product/23587/kibernetinio-saugumo-aplinka-lietuvoje (žiūrėta 2022-08-18).

elektroninės informacijos saugos reikalavimus. Krašto apsaugos ir Vidaus reikalų ministerijos ją įsipareigojo įgyvendinti iki 2016 m. IV ketv., tačiau iki šiol vieningos saugumo reikalavimų sistemos projektas neparengtas. Tam tikri skirtinguose teisės aktuose išdėstyti reikalavimai kibernetiniam saugumui ir elektroninės informacijos saugai užtikrinti yra tapatūs, o tai apsunkina saugumo reikalavimų įgyvendinimą kibernetinio saugumo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius (1.3 poskyris, 17 psl.).

2. Tobulintinas kibernetinių incidentų valdymas

- Kibernetinius incidentus valdančios ir (ar) tiriančios institucijos (Nacionalinis kibernetinio saugumo centras, Valstybinė duomenų apsaugos inspekcija, Lietuvos policija) ne visais atvejais keičiasi informacija apie kibernetinius incidentus, kurie joms aktualūs pagal jų veiklos pobūdį, todėl šios institucijos nesudaro prielaidų greitai atpažinti skirtingo pobūdžio kibernetinius incidentus ir perduoti kompetentingoms institucijoms informaciją, kad pastarosios galėtų laiku atlikti nusikalstamų veikų ar pažeidimų užkardymą, dėl to gali nukentėti kibernetinio saugumo subjektai ir visuomenė. Kibernetinio saugumo subjektai ir kibernetinius incidentus valdančios ir (ar) tiriančios institucijos informaciją apie kibernetinius incidentus turi perduoti per Kibernetinio saugumo informacinį tinklą, o jeigu tokios galimybės nėra, kitomis saugiomis informacijos perdavimo priemonėmis, tačiau Nacionalinis kibernetinio saugumo centras informaciją apie kibernetinius incidentus iš subjektų ir institucijų priima tik kitomis saugiomis informacijos perdavimo priemonėmis, bet ne per tinklą. Nustatėme, kad kibernetinio saugumo subjektai pasyviai naudojasi tinklu (per pastaruosius 3 mėn. 59 proc., arba 125 iš 212 subjektų nesinaudojo tinklu), o suinteresuotų šalių nuomone (Informatikos ir ryšių departamento, Ryšių reguliavimo tarnybos, Valstybinės duomenų apsaugos inspekcijos, Krašto apsaugos ministerijos), tinklas šiuo metu veikia neefektyviai ir galėtų būti plačiau pritaikytas naudojimui (2.1 poskyris, 21 psl.).
- Kibernetinio saugumo pratybos, mokymai ir konsultacijos kibernetinio saugumo klausimais vykdomos, bet yra nepakankamai rezultatyvios siekiant stiprinti kibernetinio saugumo subjektų gebėjimus efektyviai atremti kibernetines atakas ir užkirsti joms kelią. Kasmet rengiamos nacionalinės kibernetinio saugumo pratybos, organizuojami kibernetinio saugumo mokymai, teikiamos konsultacijos ir metodinės rekomendacijos, dauguma (73 proc., arba 101 iš 138 pratybose ir 72 proc., arba 73 iš 102 mokymuose dalyvavusiųjų) kibernetinio saugumo subjektų teigiamai jas vertina, tačiau kibernetinio saugumo subjektų įsitraukimas į pratybas ir mokymus yra nepakankamas: per tris pastaruosius metus (2019–2021 m.) net 35 proc. (74 iš 212) subjektų nė karto nedalyvavo pratybose, 52 proc. (110 iš 212) – mokymuose. Kas ketvirtas kibernetinio saugumo subjektas (26 proc., 55 iš 212) neturi kibernetinių incidentų valdymo plano (tvarkos), nėra patvirtintas tipinis kibernetinių incidentų valdymo planas, kuris turėtų būti pavyzdžiu kibernetinio saugumo subjektams. Jei šiems subjektams būtų nustatyta prievolė reguliariai dalyvauti kibernetinio saugumo pratybose ar mokymuose, patvirtintas tipinis kibernetinių incidentų valdymo planas, būtų užtikrintas šių subjektų kibernetinio saugumo kompetencijų ir įgūdžių stiprinimas, jie žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui, veiksmingai jį suvaldyti ir užkirsti kelią galimoms grėsmėms (2.2 poskyris, 23 psl.).

3. Neužtikrinamas nuoseklus kibernetinio saugumo planavimo įgyvendinimas

- Nacionalinės kibernetinio saugumo strategijos įgyvendinimo stebėsena ir kontrolė orientuota į nuolatinį atsiskaitymą už pasiektą pažangą, tačiau 2019–2021 m. strategijos įgyvendinimo rezultatai nebuvo peržiūrimi kasmet: nuo 2021 m. įsigaliojus Strateginio valdymo įstatymui, Krašto apsaugos ministerija nerinko ir nesistemino informacijos apie Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus, Strategijos vykdytojai stebėjo ne visas priemones ir vertinimo kriterijus. Iš 28 Nacionalinės kibernetinio saugumo strategijos įgyvendinimo tarpinstituciniame veiklos plane numatytų priemonių tik 17 buvo visiškai įgyvendintos, 4 – neįgyvendintos, 7 – vykdytos, bet dėl COVID-19 pandemijos ir neįvykusių viešųjų pirkimų procedūrų buvo įgyvendintos ne visa apimtimi arba dėl baigtos priemonių įgyvendinimo stebėsenos nežinoma jų įgyvendinimo būklė. Dėl tų pačių priežasčių 11 (iš 38) strateginių rodiklių reikšmės nėra pasiektos, 5 (iš 38) – reikšmė nežinoma. 2020 m. buvo rengiamas Tarpinstitucinio veiklos plano pakeitimo projektas, tačiau dėl neatitikties Strateginio valdymo įstatymo normoms jis buvo sustabdytas. Nenuoseklus suplanuotų kibernetinio saugumo stiprinimo priemonių įgyvendinimas ir nepakankama stebėsena lėmė tai, kad nacionalinių kibernetinio saugumo planavimo dokumentų nustatyti tikslai ir uždaviniai stiprinant valstybės kibernetinį saugumą ir kibernetinių gynybos pajėgumų plėtrą, skatinant kibernetinio saugumo kultūrą ir inovacijų plėtrą, nėra visiškai pasiekti vertinant 2021 m. Nacionalinės kibernetinio saugumo strategijos įgyvendinimo rezultatus pagal numatytus vertinimo kriterijus. Pažymėtina, kad strateginiame planavime numatyti pokyčiai – iki 2022 IV ketv. Krašto apsaugos ministerija turi parengti Nacionalinę kibernetinio saugumo plėtros programą, kuri apibrėžtų naujas pažangos (kibernetinio saugumo stiprinimo) priemones (3 skyrius, 28 psl.).

Rekomendacijos

Krašto apsaugos ministerijai

1. Siekiant užtikrinti kibernetinės apsaugos, prevencijos ir atsako priemonių panaudojimą, turi būti diegiamas ir nacionaliniu mastu koordinuojamas informacinių technologijų saugumo rizikų (įskaitant kibernetines) valdymo procesas, kuris leistų gautą informaciją apie kibernetinio saugumo rizikingumo būklę naudoti priimant strateginius sprendimus dėl kibernetinio saugumo stiprinimo (1-asis pagrindinis audito rezultatas).

2. Siekiant kibernetinio saugumo subjektams efektyviau įgyvendinti teisės aktuose nustatytus saugumo reikalavimus, sukurti bendrą valstybės informacinių išteklių kibernetinio saugumo ir informacinių technologijų saugos atitikties vertinimo metodiką, sudarančią galimybes atlikti išsamų atitikties teisės aktuose nustatytiems reikalavimams vertinimą, leisiančią priežiūrą ir stebėseną atliekančiai institucijai rezultatyviau pateikti duomenimis grįstą faktinės būklės nacionalinio lygiu analizę, įžvalgas, apibendrinimą (1-asis pagrindinis audito rezultatas).

3. Siekiant sudaryti sąlygas, kad visi kibernetinio saugumo subjektai žinotų veiksmus, kurių reikia imtis įvykus kibernetiniam incidentui ar siekiant užkirsti kelią galimoms grėsmėms:

    - patvirtinti priemones, kurios užtikrintų sklandesnį komunikavimą apie kibernetinius incidentus naudojantis kibernetinio saugumo informaciniu tinklu;

- įpareigoti kibernetinio saugumo subjektus (valstybės informacinių išteklių valdytojus ir tvarkytojus, ypatingos svarbos informacinės infrastruktūros valdytojus) dalyvauti nacionalinėse kibernetinio saugumo pratybose ir numatyti Nacionalinio kibernetinio saugumo centro vykdomos švietimo veiklos vertinimo rodiklius bei periodiškai juos stebėti;
- parengti ir patvirtinti detalų tipinį kibernetinių incidentų valdymo planą ir įpareigoti kibernetinio saugumo subjektus, pagal šio standartinio plano pavyzdį, parengti ar atnaujinti savo vidinius kibernetinių incidentų valdymo planus / tvarkas (2-asis pagrindinis audito rezultatas).

Rekomendacijų įgyvendinimo priemonės ir terminai, laukiamas audito poveikis ir pokyčių vertinimo rodikliai pateikti ataskaitos dalyje „Rekomendacijų įgyvendinimo planas“ (34 psl.). Aktuali informacija apie rekomendacijų įgyvendinimo būklę, rezultatus ir įvykusius pokyčius yra skelbiama atviruose duomenyse Valstybės kontrolės interneto svetainėje https://www.valstybeskontrole.lt/LT/AtviriDuomenys.