NIS2 direktyva: kaip ruoštis pokyčiams jau šiandien?

Evaldas Valūnas
Kibernetinės saugos produktų ir paslaugų vadovas, Atea UAB

NIS/NIS2 kas tai ?

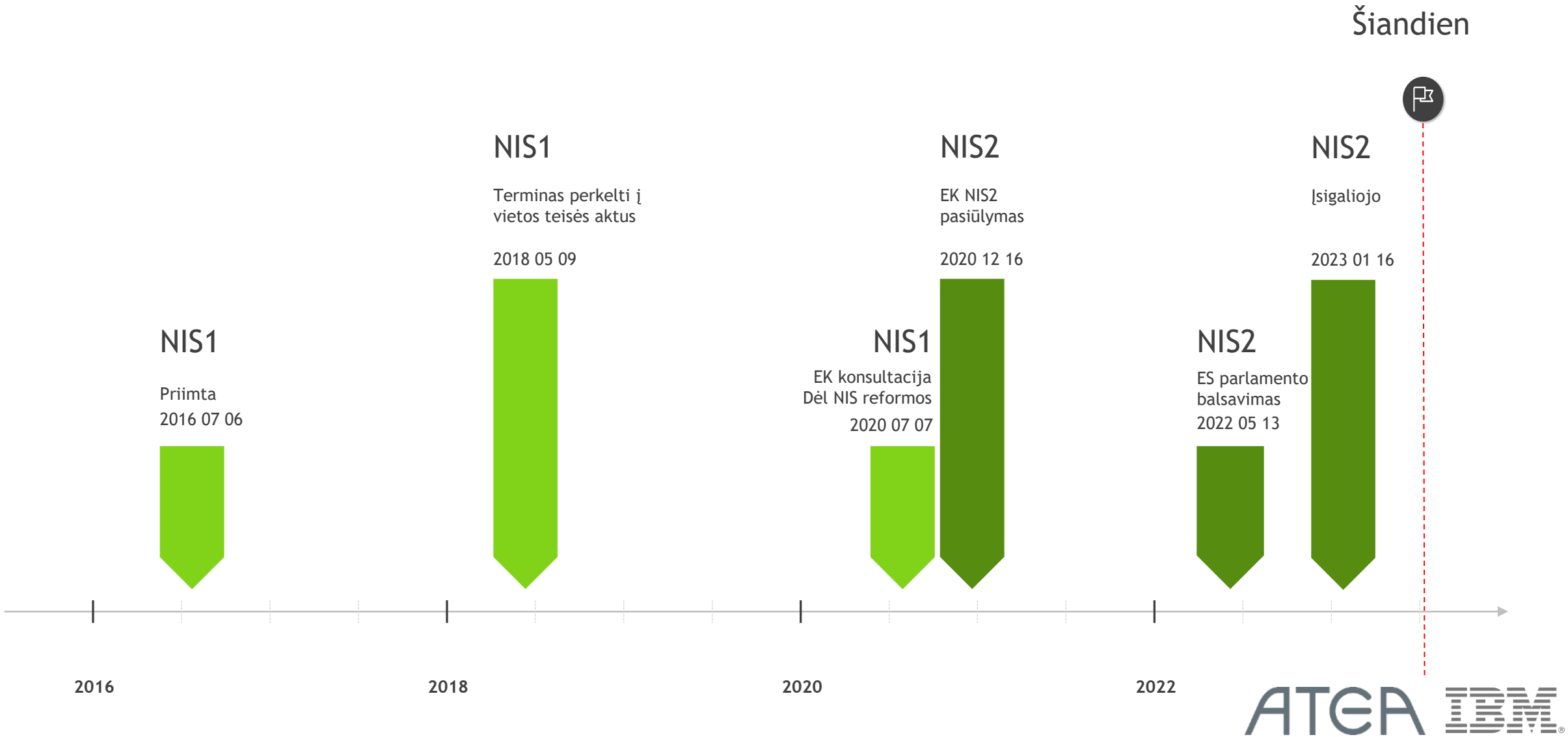
Direktyvos

EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2016/1148 ... dėl priemonių aukštam bendram **Tinklų ir Informacinių Sistemų** saugumo lygiui visoje Sąjungoje užtikrinti (TIS direktyva)

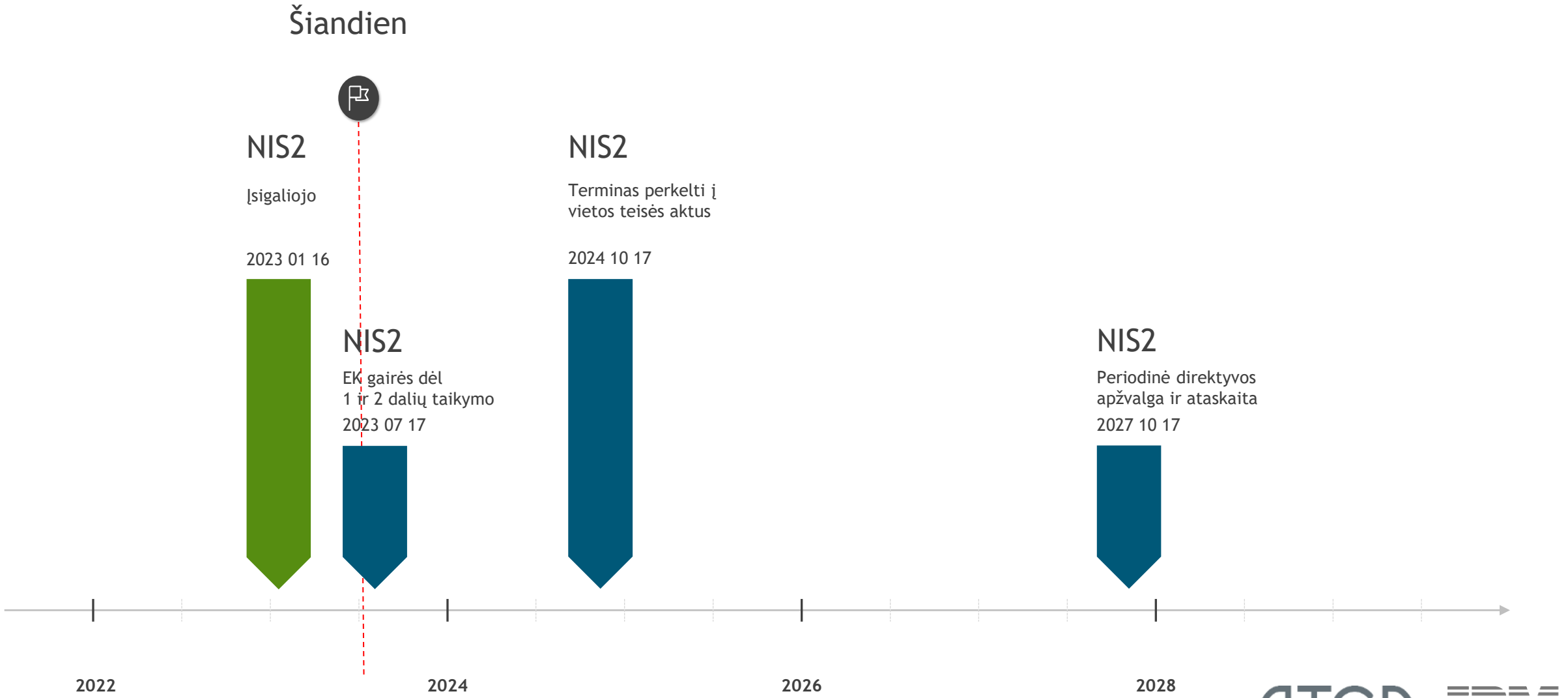
EUROPOS PARLAMENTO IR TARYBOS DIREKTYVA (ES) 2022/2555 ... dėl priemonių aukštam bendram **kibernetinio saugumo lygiui** visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas ... ir panaikinama Direktyva (ES) 2016/1148 (TIS 2 direktyva)


NIS ▶ NIS2

NIS istorija



NIS istorija



NIS2 paskirtis

Tikslai

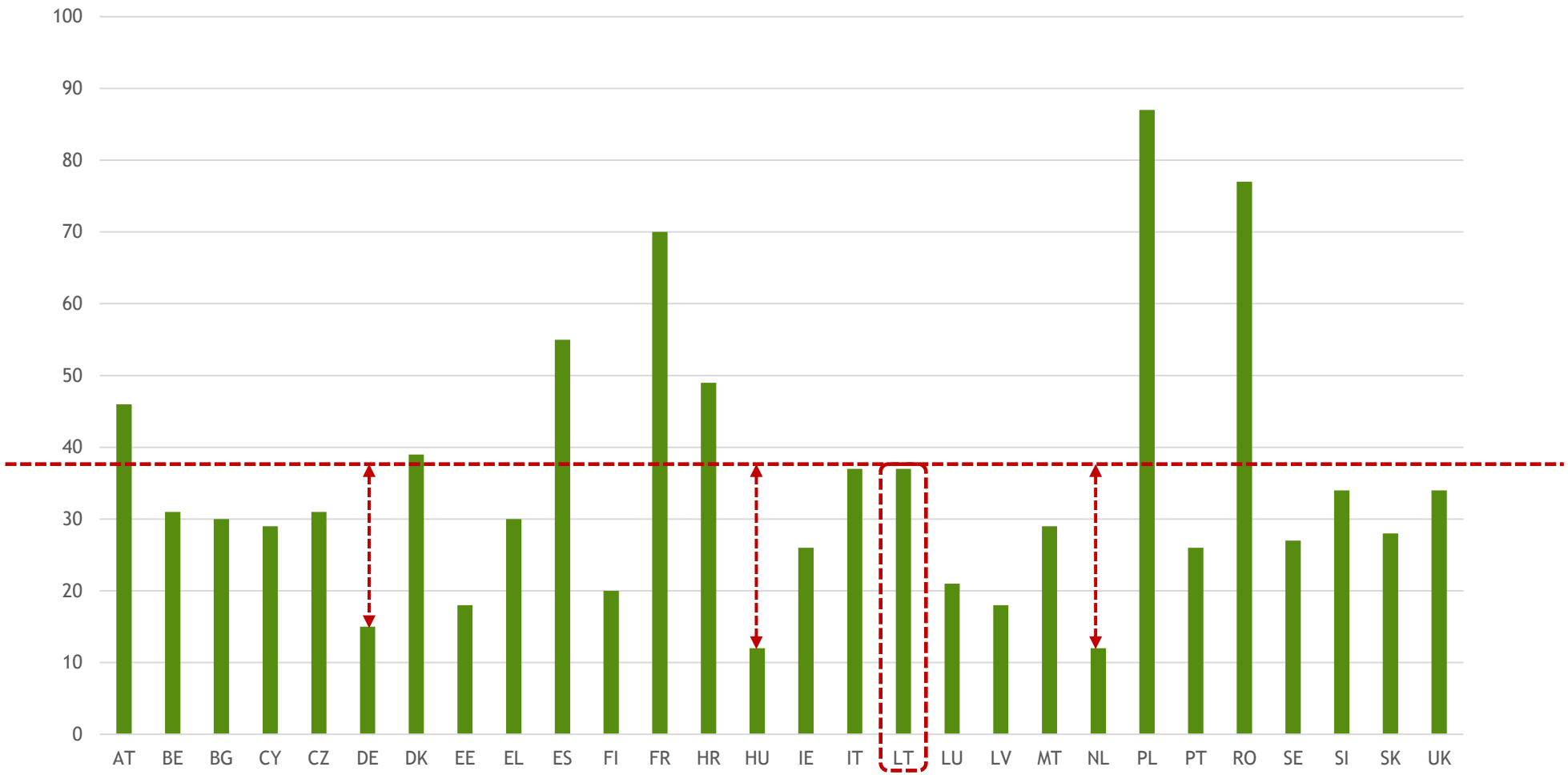
Padidinti Europos Sąjungoje veikiančių įmonių visuose atitinkamuose sektoriuose kibernetinio atsparumo lygį

Sumažinti atsparumo nenuoseklumą visoje vidaus rinkoje, sektoriuose, kuriems jau taikoma direktyva

NIS poveikio tyrimas

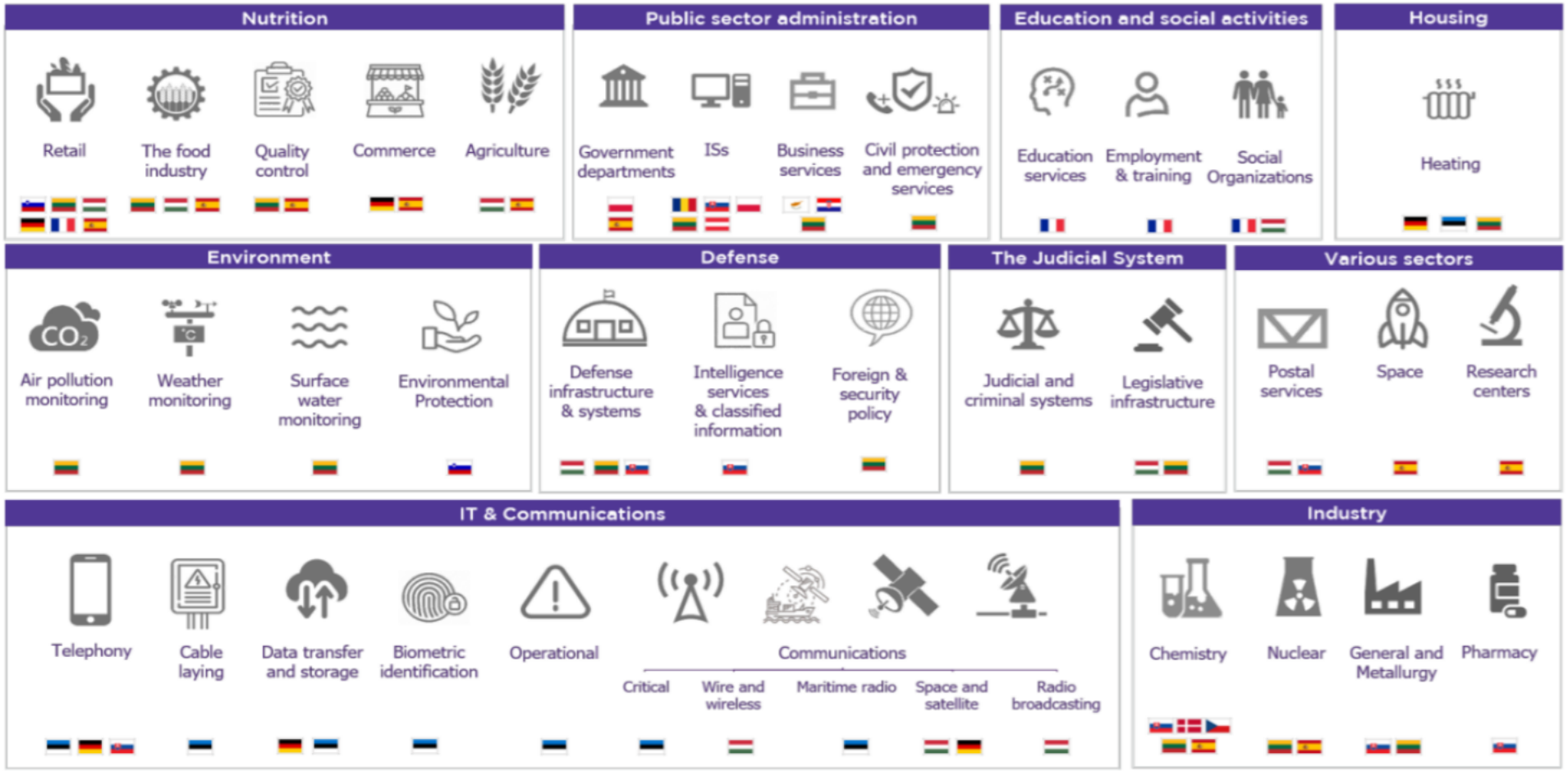
ATEA IBM

Valstybių narių nustatytų Esminių Paslaugų Tiekėjų (EPT) skaičius



Šaltinis: REPORT FROM THE COMMISSION TO THE EUROPEAN PARLIAMENT AND THE COUNCIL
assessing the consistency of the approaches taken by Member States in the identification of operators of essential services in accordance with Article 23(1) of Directive 2016/1148/EU

Papildomi sektoriai ir sub-sektoriai identifikuoti valstybių narių



Šaltinis: Proposal for a Directive of the European Parliament and of the Council on measures for a high common level of cybersecurity across the Union, repealing Directive (EU) 2016/1148 | europa.eu

Scenarijų analizė

- „Status Quo“
- Neženklūs pokyčiai, esamų teisės aktų apimtyje
- Sisteminiai ir struktūriniai pokyčiai, naujų teisės aktų priėmimas

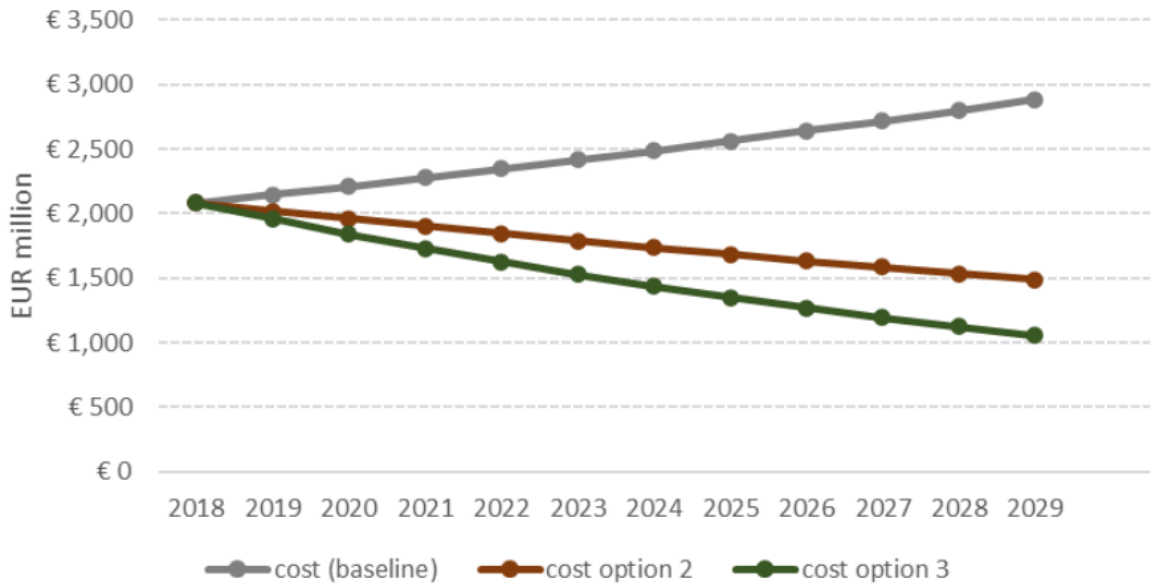
Impacts	Option 0: Baseline – Keep Status Quo	Option 2: Limited changes to the NIS Directive	Option 3: Systemic and structural changes and the adoption of a new legal act
Effectiveness	0	✓✓	✓✓✓
Economic/ Efficiency	0	✓	✓✓✓
Environmental	0	✓	✓
Social	0	✓	✓
Coherence (synergies with other relevant legislation)	0	✓✓	✓✓
Stakeholders' support	0	✓	✓
Proportionality	0	✗	✓✓
Total	0	✓✓✓✓✓✓✓✓ ✗	✓✓✓✓✓✓✓✓✓✓ ✓✓✓

Šaltinis: Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | europa.eu

Ekonominio poveikio analizė

- „Status Quo“
- Neženklūs pokyčiai, esamų teisės aktų apimtyje
- Sisteminiai ir struktūriniai pokyčiai, naujų teisės aktų priėmimas

Figure 1.1 The costs of cyber-incidents across scenarios in EUR million (2018-2029)

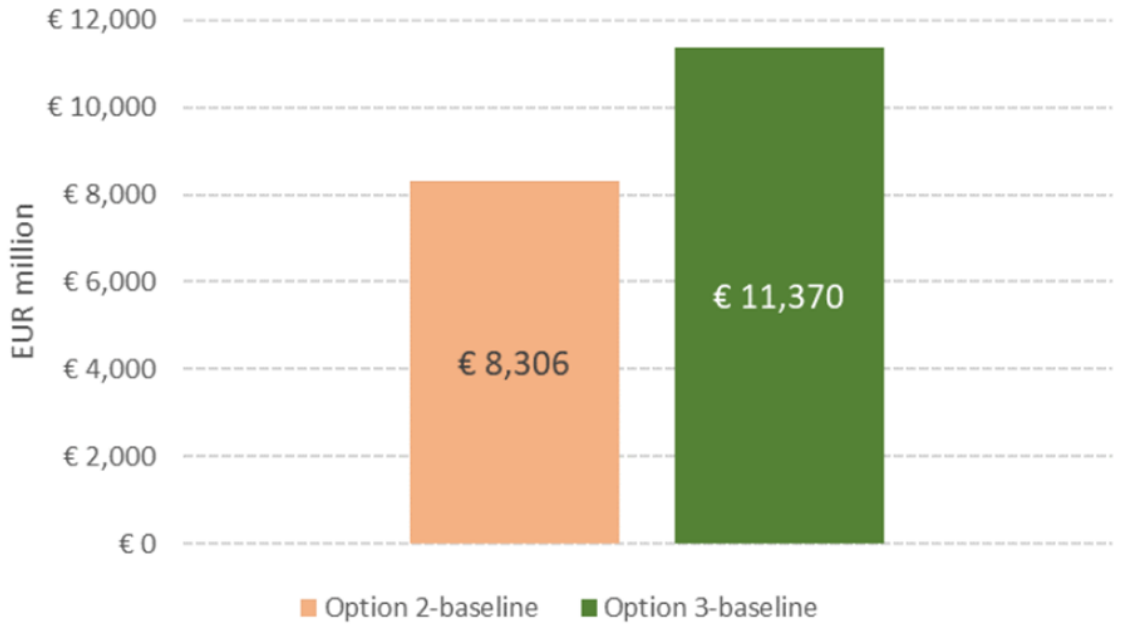


Šaltinis: Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | europa.eu

Ekonominio poveikio analizė

- „Status Quo“
- Neženklūs pokyčiai, esamų teisės aktų apimtyje
- Sisteminiai ir struktūriniai pokyčiai, naujų teisės aktų priėmimas

Figure 1.2 Saving in cyber incident per option compared to the baseline

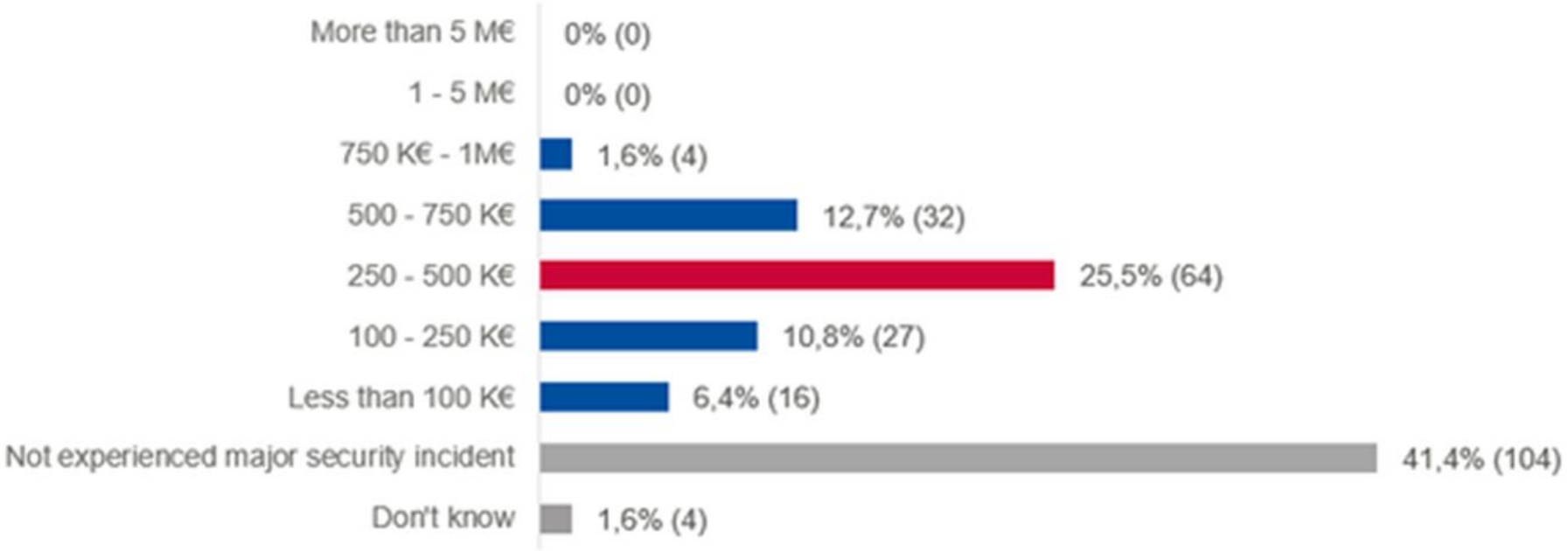


Šaltinis: Impact assessment Proposal for directive on measures for high common level of cybersecurity across the Union | europa.eu

NIS investicijų tyrimas

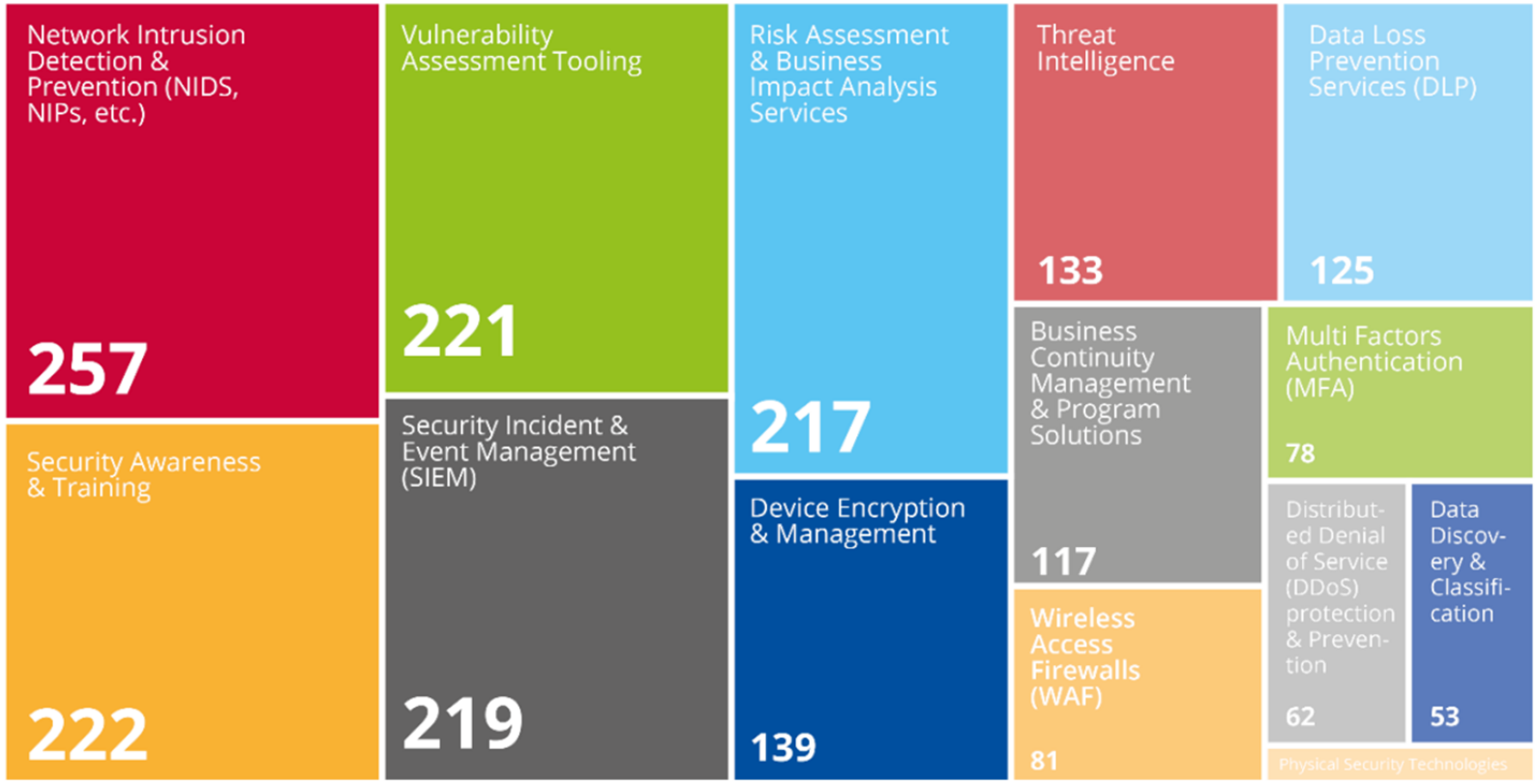
ATEA IBM

Kokia apskaičiuota žala, patirta dėl paskutinio(-ių) didesnio(-ių) saugumo incidento(-ų), kurį(-iuos) patyrė jūsų organizacija?



Šaltinis: https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist

Kokias technologijas ar paslaugas įsigijote NIS direktyvos įgyvendinimui?



n=631
[4 organisations did not procure any technologies]

Šaltinis: https://www.enisa.europa.eu/news/enisa-news/nis-directive-has-positive-effect-though-study-finds-gaps-in-cybersecurity-investment-exist

Reikalingi resursai

- Beveik 50 % ES (EPT/SPT) organizacijų samdė rangovus, kad padėtų jų informacijos saugos darbuotojams
- Beveik 50 % ES (EPT/SPT) organizacijų samdė naujus darbuotojus įgyvendinant direktyvą
- Tipiškame ES EPT/SPT reagavimui į incidentus dirba vidutiniškai du etatai

Šaltinis: NIS Directive has Positive Effect, though Study Finds Gaps in Cybersecurity Investment Exist — ENISA (europa.eu)


NIS2

Sektoriai NIS1

Esminių Paslaugų Tiekėjai

- Energetika (elektra, nafta, dujos)
- Transportas (oro, geležinkelių, vandens, kelių)
- Bankininkystė
- Finansų rinkų infrastruktūra
- Geriamasis vanduo

Skaitmeninių Paslaugų Tiekėjai

- Internetinės prekyvietės
- Internetiniai paieškos varikiai
- Debesijos paslaugos

Šaltinis: NIS direktyva, EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu)

Sektoriai NIS2

Esminių Paslaugų Tiekėjai

- Energetika (elektra, nafta, dujos, vandenilis, centralizuotas šildymas /vėsinimas)
- Transportas (oro, geležinkelių, vandens, kelių)
- Bankininkystė
- Finansų rinkų infrastruktūra
- Geriamasis vanduo
- Nuotekos
- Skaitmeninė infrastruktūra
- IRT paslaugų valdymas
- Viešasis administravimas
- Kosmosas

Svarbių Paslaugų Tiekėjai

- Pašto ir kurjerių paslaugos
- Atliekų tvarkymas
- Cheminių medžiagų gamyba ir platinimas
- Maisto gamyba, perdirbimas ir platinimas
- Gamyba (med. priemonės, elektronika, el. įranga, motorinių transporto priemonių, kita)
- Skaitmeninių paslaugų tiekėjai (paieška, prekyvietės, socialiniai tinklai)
- Moksliniai tyrimai

Šaltinis: NIS2 direktyva, *Publications Office (europa.eu)

Priemonės

Kibernetinio saugumo rizikos valdymo priemonės turi apimti:

a. rizikos analizės ir informacinių sistemų saugumo politiką;
b. incidentų valdymą;
c. veiklos tęstinumą (pvz., Atsarginių kopijų valdymą ir veiklos atkūrimą po ekstremaliųjų įvykių, ir krizių valdymą);
d. tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno subjekto ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykiais;
e. tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant pažeidžiamumo valdymą ir atskleidimą;
f. politiką ir procedūras, skirtas kibernetinio saugumo rizikos valdymo priemonių veiksmingumui įvertinti;
g. pagrindinę kibernetinės higienos praktiką ir kibernetinio saugumo mokymus;
h. kriptografijos ir, kai taikytina, šifravimo naudojimo politiką ir procedūras;
i. žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;
j. kai taikytina, kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą.

Šaltinis: NIS2 direktyva, 21 straipsnis; *Publications Office (europa.eu)

Įmonės(1)

Vidutinės įmonės:

- 50+ darbuotojų
- 10+ mln. Eur apyvarta

Įmonių kategorija	Darbuotojų skaičius: metiniai darbo vienetai (MDV)	Metinė apyvarta	arba	Bendras metinis balansas
Vidutinės	< 250	≤ 50 mln. EUR	arba	≤ 43 mln. EUR
Mažosios	< 50	≤ 10 mln. EUR	arba	≤ 10 mln. EUR
Labai mažos	< 10	≤ 2 mln. EUR	arba	≤ 2 mln. EUR

Šaltinis: MVĮ apibrėžties vartotojo vadovas (europa.eu)

Imonės(2)

Nepaisant subjektų dydžio, ši direktyva taikoma:

- viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai
- subjektas yra vienintelis paslaugos tiekėjas ... valstybėje narėje
- paslaugos, kurią teikia subjektas, sutrikimas galėtų daryti didelį poveikį
- centrinės valdžios administravimo subjektas
- regioninio lygmens, kurių sutrikimas galėtų daryti didelį poveikį ypatingos svarbos visuomeninei ar ekonominei veiklai, viešojo administravimo subjektas

Šaltinis: NIS2 direktyva, *Publications Office (europa.eu)

Baudos

- NIS1

Valstybės narės nustato sankcijų, taikomų pažeidus pagal šią direktyvą priimtas nacionalines nuostatas, taisykles ir būtinų priemonių užtikrinti, kad šios sankcijos būtų įgyvendinamos. Numatytos sankcijos turi būti veiksmingos, proporcingos ir atgrasomos

- NIS2

Esminiams subjektams 10 000 000 EUR arba 2 proc. (kuris didesnis)
Svarbiems subjektams 7 000 000 EUR arba 1,4 proc. (kuris didesnis)

Kiekviena valstybė narė gali nustatyti taisykles dėl to, ar ir kokiu mastu administracinės baudos gali būti skiriamos viešojo administravimo subjektams

Šaltiniai: NIS direktyva, EUR-Lex - 32016L1148 - EN - EUR-Lex (europa.eu); NIS2 direktyva, *Publications Office (europa.eu)

Teisės aktai

- Lietuvos Respublikos kibernetinio saugumo įstatymas Nr. XII-1428
- Nutarimas dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo Nr. 818
- Lietuvos Respublikos administracinių nusižengimų kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo tvarkos įstatymas Nr. XII-1869

Šaltinis: NIS Directive tool — ENISA (europa.eu)

Pozicija

- KAM, bendradarbiaudama su kitomis suinteresuotomis Lietuvos institucijomis ir organizacijomis, derybose išlaikė ambicingus NIS2 direktyvos tikslus dėl taikymo srities išplėtimo, aukštesnio lygio rizikos valdymo ir aiškių kriterijų nustatymo, kartu užtikrinant šių nuostatų proporcingumą
- Šiuo metu atliekamas NIS2 direktyvos nuostatų ir jų atitikties teisės aktams vertinimas, jų aptarimas su susijusiomis Lietuvos institucijomis. Preliminariai nustatyta, kad dėl įsigaliojusios NIS2 direktyvos gali reikėti keisti 11 teisės aktų ir įtraukti kitas institucijas (pagal kompetencijas elektroninių ryšių, asmens duomenų apsaugos, krizių valdymo, finansų sektoriaus srityje ir pan.)

Šaltinis: Nacionaline-kibernetinio-saugumo-ataskaita-2022.pdf (nksc.lt)

Galimi sprendimai

Kibernetinio saugumo rizikos valdymo priemonės

Rizikos analizės ir informacinių sistemų saugumo politika:

- Randori Recon (ASM)
- IBM Guardium Vulnerability assessment
- IBM Guardium Data Discover and Classification
- IBM QRadar UBA

Pagrindinis duomenų saugumo iššūkis - nustatyti, kas turi prieigą ir ką gali daryti. Įmonėms reikia realiuoju laiku stebėti vietinių ir debesijos duomenų šaltinių veiklą, kad svarbūs duomenys išliktų apsaugoti.

Kibernetinio saugumo rizikos valdymo priemonės

Incidentų valdymas:

- IBM Cloud Pack for Security
- IBM Security QRadar SIEM
- IBM Security QRadar SOAR
- XDR Connect
- IBM X-Force*
  - Pentest
  - Manage SOC
- IBM PL – Cyber Range mobileSOC

Svarbu ne problema, o tai, kaip ją sprendžiate.

* „Enterprise“ dydžio klientams

Kibernetinio saugumo rizikos valdymo priemonės

Veiklos tęstinumas, krizių valdymas:

- IBM QRadar SOAR
  - CSIRT integracija
  - (automatizacija, incidentų raportavimo sistema)
  - SOC >> CSIRT
- IBM Storage (safe guarded copies)
- IBM Cloud - backup
- IBM PL – Cyber Range mSOC

Reaguoti į kibernetinius incidentus yra visos įmonės pareiga.
Paprastai valdydama įvykius ir užduotis, jūsų komanda gali sklandžiai vadovauti tyrimo ir reagavimo veiksmams.

Kibernetinio saugumo rizikos valdymo priemonės

Tiekimo grandinės saugumas:

- IBM X-Force
- IBM Security Supply Chain Cyber Risk Management Services
- IBM Cloud Security - Dev/Sec/Ops
- RedHat (ACS)

Užtikrina didesnį visų tiekimo grandinės veiksmų matomumą.
Suteikia beveik realiuoju laiku operacijų matomumą ir galimybę imtis veiksmų anksčiau.

ATEA IBM

Kibernetinio saugumo rizikos valdymo priemonės

Tinklų ir informacinių sistemų įsigijimas:

- IBM CloudPak for Security
  - Qradar QNI, Forensic
  - IBM QRadar SOAR
  - OT/IoT security
  - IBM QRadar XDR
- MaaS360
- IBM Verify (IAM)
- Randori (ASM)
- ReaQta
- IBM X-Force Red*
- IBM Research - IBM Beyond Presence

* „Enterprise“ dydžio klientams

Kibernetinio saugumo rizikos valdymo priemonės

Politikos ir procedūros, kibernetinio saugumo rizikos valdymo veiksmingumui įvertinti:

- IBM QRadar SOAR
- IBM Open Pages
- IBM Guardium Data Protection
- IBM PL – Cyber Range

Vidaus auditas nuolat stebi vidaus verslo praktikų nuoseklumą, jo tikslas yra užtikrinti organizacijos politikų ir procedūrų laikymąsi ir įspėti vadovybę apie politikų laikymosi spragas.

Kibernetinio saugumo rizikos valdymo priemonės

Kriptografija ir šifravimo naudojimo politikos ir procedūros:

- IBM Security Guardium
  Data Encryption (GDE)
- IBM Cloud - Hyper Protect Crypto Services
  Unified Key Orchestrator (multicloud)

Kriptografija yra viena iš svarbiausių priemonių, kurią įmonės naudoja siekdamos apsaugoti sistemas, kuriose saugomas svarbiausias turtas – duomenys, nesvarbu ar jie yra saugomi ar judantys.

Kibernetinio saugumo rizikos valdymo priemonės

Pagrindinė kibernetinės higienos praktika ir kibernetinio saugumo mokymai:

- IBM PL – Cyber Range
- X-Force - Cyber Range*

"Cyber Range" sprendimas sukuria simuliacijas, kurios padeda organizacijoms atlikti realius pažeidimo scenarijus, padedančius užtikrinti, kad galite reaguoti ir atsigauti po kibernetinių incidentų organizacijos mastu.

* „Enterprise“ dydžio klientams

Kibernetinio saugumo rizikos valdymo priemonės

Kelių veiksnių tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimai:

- IBM Verify
- IBM Trusteer

Sprendimai padeda aptikti sukčiavimą, autentifikuoti naudotojus ir nustatyti tapatybės patikimumą visame daugiakanaliame naudotojų judėjime.

Kibernetinio saugumo rizikos valdymo priemonės

Žmogiškųjų išteklių saugumas, prieigos kontrolės politika ir turto valdymas:

- IBM IAM
- IBM Verify
- IBM Trusteer
- IBM QRadar XDR
- IBM Cognos

Vidaus auditas nuolat stebi vidaus verslo praktikų nuoseklumą, jo tikslas yra užtikrinti organizacijos politikų ir procedūrų laikymąsi ir įspėti vadovybę apie politikų laikymosi spragas.

Klausimai?

Norite sužinoti daugiau apie NIS2?

Bendraukime:

Evaldas.Valunas@atea.lt

+370 682 55171


Kuriame Lietuvą su IT