

# Cyber Security

## Lesson 9

---



# Labs



## Assignments

### CompTIA Security+ praktinis testas #2

Points

22 points possible

Due April 18, 2025 5:00 AM

#### Instructions

Antrasis CompTIA Security+ praktinis testas.

- TESTO klausimai yra sudaryti anglų kalba.
- TESTO klausimų skaičius: 22vnt.
- **TESTO laikymo trukme: 60min.**

**Testą būtina atlikti iki 2025-04-18 d. 17.00 val.**

**TESTAS išlaikomas sėkmingai, jei iš 22vnt. testo klausimų į bent 12vnt. atsakoma TEISINGAI.**

Atsakymai bus paskelbti: TEORINĖS PASKAITOS #10. metu.

#### Student work



CompTIA Security+ praktinis testas #2 (25 03 26 Kiber NF OV)



---

In the previous lesson...

---

# Legal aspects of cyber security

---



# GDPR (BDAR)

---



BENDRASIS  
DUOMENŲ  
APSAUGOS  
REGLAMENTAS



LIETUVOS RESPUBLIKOS  
ASMENS DUOMENŲ TEISINĖS APSAUGOS  
ĮSTATYMAS

# GDPR (BDAR)

## Bigger Responsibility, Bigger Repercussions





# Scope of the GDPR

---

Any / all information relating to an identified or identifiable individual e.g.

- Information held in manual form or printed out;
- Emails, databases, spreadsheets etc.;
- Photographs on web sites, marketing photographs, ID Cards and Passes;
- CCTV images (both central CCTV system and any localised systems / webcams);
- Web pages;
- Information which may be associated with online identifiers provided by devices, applications, tools and protocols, such as internet protocol addresses, cookie identifiers or other identifiers.

---

# Lesson 9

---



# Legal aspects of cyber security (Continue)

---



# Kas tai yra TIS2 (NIS2)?



TIS2 - Antroji ES tinklų ir informacinių sistemų saugumo direktyva  
NIS2 – The second Network and Information Security Directive



LIETUVOS  
RESPUBLIKOS  
KRAŠTO APSAUGOS  
MINISTERIJA

2024 m. spalio 18 d. įsigaliojo atnaujintas Kibernetinio saugumo įstatymas (TIS2/NIS2).

# KĄ JUMS REIŠKIA ANTROJI TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO DIREKTYVA?

## Kritinės svarbos sektoriai



Energetika

Transportas

Bankų paslaugos

IKT paslaugų valdymas

Geriamojo vandens tiekėjai



Nuotekų valymo įmonės

Sveikatos priežiūros  
paslaugų tiekėjai

Skaitmeninė infrastruktūra

Viešasis administravimas



Finansų rinkos infrastruktūra

Kosminių technologijų paslaugos

## Svarbūs sektoriai



Pašto ir kurjerių paslaugos

Atliekų tvarkymas

Cheminių medžiagų  
gamyba ir tiekimas

Maisto produktų  
gamyba ir tiekimas



Gamyba (elektronikos ir kt.)

Skaitmeninių paslaugų tiekimas

Tyrimai



# Ar mūsų įmonei bus taikoma TIS2?

## TAIKOMA **esminiui subjektui**, jei:

- Įmonėje dirba 250+ darbuotojų *ir*
- Metinės pajamos 50+ mln. EUR *arba*
- Balanse nurodyto turto vertė 43+ mln. EUR.

## TAIKOMA **svarbiam subjektui**, jei:

- Įmonėje dirba 50+ darbuotojų *ir*
- Metinės pajamos 10+ mln. EUR *arba*
- Balanse nurodyto turto vertė 10+ mln. EUR.

## TAIKOMA IŠIMTIS, jei:

- Įmonė valdo kritinę infrastruktūrą.
- Vienintelis paslaugos tiekėjas.

# TIS2/NIS2 Sankcijos

TIS2 direktyvoje reikalaujama, kad valstybės narės numatytų tam tikro dydžio administracines baudas, visų pirma ne mažesnes kaip:

- 10 000 000 EUR arba
- 2 % visos praėjusių finansinių metų pasaulinės metinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.



Digital Security  
Progress. Protected.



# TIS2/NIS2 Sankcijos

**Kalbant apie svarbius subjektus:**

- **7 000 000 EUR baudą arba**
- **ne mažesnę kaip 1,4 % visos praėjusių finansinių metų pasaulinės metinės apyvartos, atsižvelgiant į tai, kuri suma yra didesnė.**



Digital Security  
Progress. Protected.



# NIS2 (TIS2)

---



- Didinti kibernetinio atsparumo lygį.
- Laiku sureaguoti į incidentus bei juos suvaldyti.
- Pagerinti informacijos mainų saugą tarp įmonės ir trečiųjų šalių.
- Atsižvelgti į kibernetinio saugumo higieną.

# Pagrindiniai TIS2 ramščiai

---



ES valstybių narių  
atsakomybė



Įmonių  
atsakomybė



Bendradarbiavimas  
ir keitimasis  
informacija

# Kas yra NIS2 direktyva ir jos pagrindiniai tikslai. Esminiai skirtumai nuo NIS1 direktyvos

---

1. Daugiau sektorių
2. Daugiau įmonių
3. Dvi kategorijos subjektų: esminiai ir svarbūs
4. Detalesnės nuostatos dėl pranešimo apie incidentus proceso, pranešimų turinio ir terminų
5. Periodinės audito pareigos
6. NIS2 sugriežtina įmonėms taikomus saugumo reikalavimus, nustatydamą rizikos valdymo metodą ir minimalų pagrindinių saugumo elementų sąrašą.
7. NIS2 sprendžiami tiekimo grandinių saugumo ir santykių su tiekėjais klausimai, reikalaujant, kad atskiros įmonės spręstų kibernetinio saugumo rizikos klausimus tiekimo grandinėse ir santykiuose su tiekėjais

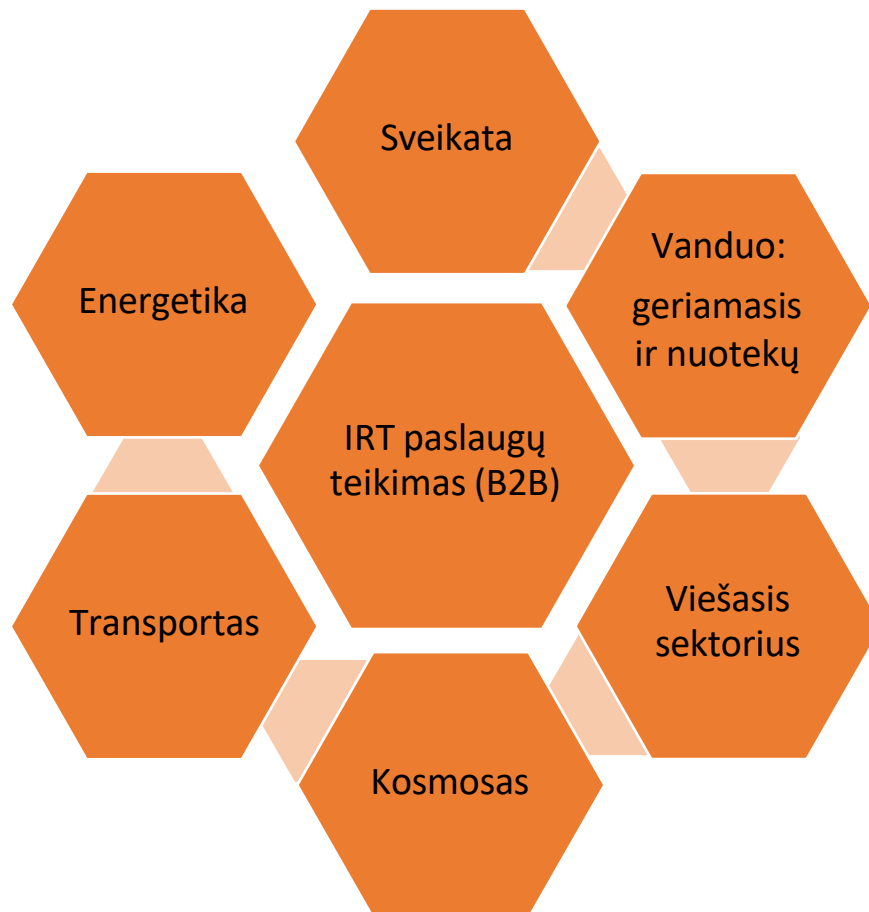
# Kas yra NIS2 direktyva ir jos pagrindiniai tikslai. Esminiai skirtumai nuo NIS1 direktyvos

---

8. Griežtesnės priežiūros priemonės nacionalinėms institucijoms
9. Griežtesni vykdymo užtikrinimo reikalavimai
10. Siekiama suderinti sankcijų režimus visose valstybėse narėse
11. Didėja baudos
12. **Stiprinamas operatyvinis bendradarbiavimas CSIRT** (reagavimo į kompiuterinius saugumo incidentus tarnybų tinklas) tinkle
13. **Isteigiamas Europos kibernetinių krizių ryšių palaikymo organizacijų tinklas** (EU-CyCLONe), siekiant remti koordinuotą didelio masto kibernetinio saugumo incidentų ir krizių valdymą
14. NIS2 nustatoma pagrindinė **sistema su atsakingais pagrindiniais subjektais dėl koordinuoto pažeidžiamumo atskleidimo**, susijusio su naujai nustatyta pažeidžiamumu visoje ES, ir sukurama viešai žinomų IRT produktų ir IRT paslaugų pažeidžiamumo duomenų bazė, kurią turi valdyti ir prižiūrėti ES kibernetinio saugumo agentūra (ENISA)
15. Stiprinamas Bendradarbiavimo grupės vaidmuo priimant strateginius politikos sprendimus ir stiprinamas valstybių narių institucijų keitimasis informacija ir bendradarbiavimas

# SEKTORIAI: ypatingos svarbos sektoriai

---

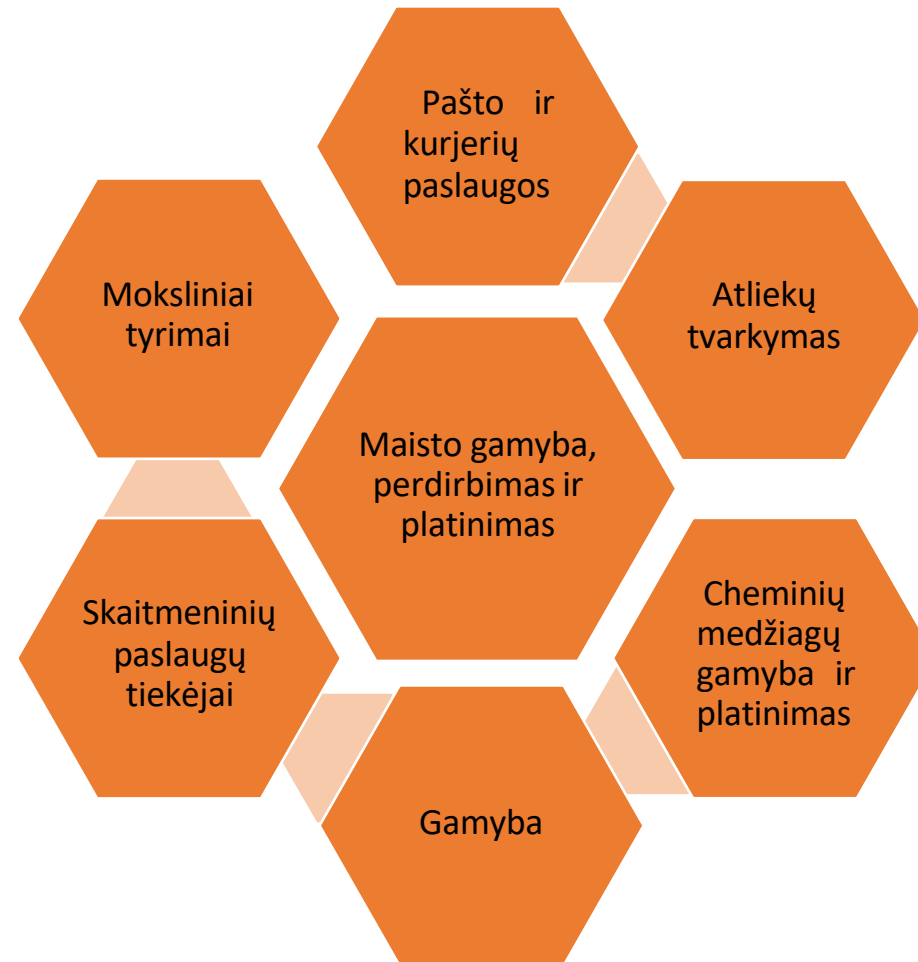


Bankininkystė:  
*lex specialis DORA*

Finansų rinkų infrastruktūros  
objektai:  
*lex specialis DORA*

# SEKTORIAI: itin svarbūs sektoriai

---





# NIS2 santykis su kitomis įstatyminėmis priemonėmis, kurių poveikis yra laikomas lygiaverčiu NIS

---

Įstatymo 1 str. 3 d.

„Šio įstatymo 14 straipsnio, 15 straipsnio ir 18 straipsnio 1 dalies 1 ir (ar) 2 punktų nuostatos netaikomos kibernetinio saugumo subjektams, jeigu jiems taikomuose Europos Sąjungos teisės aktuose yra keliami reikalavimai **įgyvendinti kibernetinio saugumo rizikos valdymo priemonės, pranešti apie didelius kibernetinius incidentus** ar **skirti už kibernetinį saugumą atsakingus asmenis** ir jeigu šių reikalavimų poveikis yra bent lygiavertis šio įstatymo 14 straipsnyje ar jo pagrindu priimtuose įgyvendinamuosiuose teisės aktuose, 15 straipsnio 1–4 dalyse, 18 straipsnio 1 dalies 1 punkte ir 4 dalyje ir (ar) 18 straipsnio 1 dalies 2 punkte ir 5 dalyje nustatytų reikalavimų poveikiui.“

# NIS2 įgyvendinimas

---

- ✓ **Įstatymas įsigalios 2024 m. spalio 18 d.**
- ✓ Vyriausybė, KAM, NKSC iki **2024 m. spalio 17 d.** priima Įstatymo **įgyvendinamuosius teisės aktus**.
- ✓ NKSC iki **2025 m. balandžio 17 d. identifikuoja KSS** ir įtraukia juos į Kibernetinio saugumo informacinę sistemą (KSIS)
- ✓ **Subjektai, kurie iki Įstatymo įsigaliojimo** buvo įtraukti į Vyriausybės patvirtintą **ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą**, iki **2025 m. balandžio 17 d.** privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio Įstatymo įsigaliojimo galiojusiems Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkto redakcijoje nurodytiems organizaciniais ir techniniais KS reikalavimams, taikomiems KSS.
- ✓ **Subjektai, kurie iki Įstatymo įsigaliojimo** buvo įtraukti į Vyriausybės patvirtintą **ypatingos svarbos informacinės infrastruktūros ir jos valdytojų sąrašą, įtraukti į KSS registrą**, privalo toliau užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį iki šio Įstatymo įsigaliojimo galiojusiems KSS 11 straipsnio 1 dalies 1 punkto redakcijoje nurodytiems organizaciniais ir techniniais kibernetinio saugumo reikalavimams, taikomiems KSS, tol, kol atsiras pareiga užtikrinti jų valdomų tinklų ir informacinių sistemų atitiktį Įstatymu patvirtintos Kibernetinio saugumo įstatymo redakcijos 14 straipsnio 1 dalyje nurodytoms kibernetinio saugumo rizikos valdymo priemonėms.

# NIS2 įgyvendinimas

---

- ✓ Nauji reikalavimai **saugos įgaliotiniams** įsigalioja **2 metai po Įstatymo įsigaliojimo**.
- ✓ NKSC, nustatęs iki Įstatymo įsigaliojimo galiojusioje Kibernetinio saugumo įstatymo 11 straipsnio 1 dalies 1 punkto redakcijoje nurodytų organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų KSS, pažeidimų, taiko iki Įstatymo įsigaliojimo galiojusias Lietuvos Respublikos administracinių nusižengimų kodekso 480 straipsnio 4 ir 5 dalies nuostatas.
- ✓ Iki Įstatymo įsigaliojimo galiojusios Kibernetinio saugumo įstatymo redakcijos pagrindu pradėtos procedūros tęsiamos ir baigiamos vadovaujantis teisės normomis, galiojusiomis iki Įstatymo įsigaliojimo.

# Subjektai pagal Direktyvą

---

## Išimtys:

1. Patenka į nurodytus sektorius, nesvarbu dydis:
  - 1.1. paslaugas teikia:
    - i) viešųjų elektroninių ryšių tinklų arba viešai prieinamų elektroninių ryšių paslaugų teikėjai;
    - ii) patikimumo užtikrinimo paslaugų teikėjai;
    - iii) aukščiausio lygio domenų vardų registrai ir domenų vardų sistemos paslaugų teikėjai;
  - 1.2. subjektas yra **vienintelis paslaugos**, kuri yra būtina siekiant užtikrinti ypatingos svarbos **visuomeninės ar ekonominės veiklos vykdymą**, teikėjas valstybėje narėje;
  - 1.3. paslaugos, kurią teikia subjektas, **sutrikimas** galėtų daryti **didelį poveikį viešajam saugumui, visuomenės saugumui arba visuomenės sveikatai**;
  - 1.4. paslaugos, kurią teikia subjektas, **sutrikimas** galėtų kelti didelę **sisteminę riziką** visų **pirma sektoriuose, kuriuose toks sutrikimas galėtų daryti tarpvalstybinį poveikį**;
  - 1.5. subjektas yra **ypatingos svarbos atsižvelgiant į jo konkrečią svarbą konkrečiam sektoriui ar paslaugos rūšiai** arba kitiems tarpusavyje priklausomiems sektoriams valstybėje narėje **nacionaliniu ar regioniniu lygmeniu**;
  - 1.6. valdžios viešojo administravimo subjektas:
    - i) centrinės;
    - ii) regioninio lygmens, kuris, atlikus riziką grindžiamą vertinimą, teikia paslaugas, kurių sutrikimas galėtų daryti **didelį poveikį ypatingos svarbos visuomenei ar ekonominei veiklai**, viešojo administravimo subjektas.
- 2. asmuo pagal Direktyvą (ES) 2022/2557 pripažintas **ypatingos svarbos subjektu**.
- 3. subjektams, teikiantiems **domenų vardų registravimo paslaugas**.

# KSS registras

---

- ✓ KSS registro ir duomenų valdytojas – KAM, tvarkytojas - NKSC
- ✓ KSS, KS informacinės sistemos **tvarkytojui** pateikia duomenis
- ✓ Asmenys turi **teisę skusti** sprendimą juos ne/registruoti KS informacinėje sistemoje Lietuvos Respublikos administracinių bylų teisenos įstatymo nustatyta tvarka.

[https://kam.lt/wp-content/uploads/2023/05/NIS2\\_Identifikuojimo-kriterijai.pdf](https://kam.lt/wp-content/uploads/2023/05/NIS2_Identifikuojimo-kriterijai.pdf)

# Auditas

---

1. Atitikties dokumentavimas – patvirtinti kibernetinio saugumo rizikos valdymo priemonės – aukštesniojo lygio vadovybės atsakomybė
2. **KSS Kibernetinio saugumo informacinio tinklo nuostatų nustatyta tvarka privalo pateikti duomenis apie kibernetinio saugumo rizikos valdymo priemonių įgyvendinimą.**
3. Valdymo organų ir darbuotojų dalyvavimas kibernetinių rizikos valdymo priemonių praktikos mokymuose
4. Kibernetinio saugumo rizikos valdymo priemonių, paremtų rizikos požiūriu, įgyvendinimas
5. Pranešimai apie incidentus
6. Auditai



# Auditas

---

1. KSS auditą privalo atlikti ne rečiau kaip kartą per 3 metus
2. pagal NKSC patvirtintą metodiką
3. auditą atlieka:
  - nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugumo atitikties auditoriai,
  - audito įmonės ar
  - kitos institucijos, Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka mokymus išklause ir kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą išlaikę asmenys, kurie atitinka Nacionalinio kibernetinio saugumo centro kibernetinio saugumo auditų atlikimo metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus, (toliau kartu – auditoriai).
- Auditoriams negali būti pavedama vertinti tinklų ir informacinių sistemų, kurias valdo ir (ar) tvarko subjektas, kuriame dirba auditorius, saugos.

# Organizaciniai ir techniniai kibernetinio saugumo reikalavimai

---

- KAM 2024 m. viduryje planavo:
  - ✓ patvirtinti organizacinius ir techninius kibernetinio saugumo reikalavimus, kurie bus pagrįsti tarptautiniu standartu ISO/ IEC 27001:2022 „Informacijos sauga, kibernetinis saugumas ir privatumo apsauga“
  - ✓ Numatyti, kokias politikas ir procedūras reikės turėti siekiant įvertinti kibernetinio saugumo rizikos valdymo priemonių veiksmingumą
- Vyriausybė nustatys minimalų **12 mėn. pereinamąjį laikotarpį** kibernetinio saugumo reikalavimams įgyvendinti skaičiuojant nuo įmonės įtraukimo į KSS registrą

# Ką svarbu žinoti apie ISO 27001 ir NIS2?

---

1. Įgyvendinus ISO 27001 standartą, didžioji dalis NIS2 reikalavimų bus įgyvendinta, tačiau nepilnai (tiekimo grandinės kontrolė/valdymas)
2. Įgyvendinto ISO 27001 standarto taikymo įmonėje apimtis gali būti per siaura, būtina pasitikrinti

# Kibernetinio saugumo rizikos valdymo priemonės pagal Įstatymą (apima)

---

- 1) kibernetinio saugumo rizikos analizės, TIS kibernetinio saugumo politiką;
- 2) už kibernetinį saugumą atsakingų asmenų, ir KSS vadovo ar jo įgalioto asmens pareigas;
- 3) kibernetinių incidentų valdymą;
- 4) veiklos testinimą;
- 5) tiekimo grandinės saugumą, įskaitant su saugumu susijusius aspektus, susijusius su kiekvieno KSS ir jo tiesioginių tiekėjų ar paslaugų teikėjų santykius;
- 6) TIS įsigijimą, plėtojimą ir priežiūros saugumą, įskaitant spragų valdymą ir atskleidimą;
- 7) politiką ir procedūras, skirtas kibernetinio saugumo reikalavimų veiksmingumui įvertinti;
- 8) kibernetinės higienos praktiką ir reguliarius kibernetinio saugumo mokymus;
- 9) kriptografijos ir šifravimo naudojimo politiką ir procedūras;

# Kibernetinio saugumo rizikos valdymo priemonės pagal Įstatymą (apima)

---

10) žmogiškųjų išteklių saugumą, prieigos kontrolės politiką ir turto valdymą;

11) kai taikytina, kelių veiksmų tapatumo nustatymo ar nuolatinio tapatumo nustatymo sprendimų, saugių balso, vaizdo ir teksto ryšių bei saugių avarinių ryšių sistemų subjekto viduje naudojimą;

12) KSS naudotojų, administratorių, tiekėjų, jų subtiekių ir kitų ūkio subjektų teisių ir prieigos prie kibernetinio saugumo subjektų valdomų ir (ar) tvarkomų TIS ir (ar) skaitmeninių duomenų suteikimo ir valdymo politiką;

13) kitus atskiriems sektoriams arba atskiroms kibernetinio saugumo subjektų grupėms taikomus kibernetinio saugumo reikalavimus, nustatytus atsižvelgiant į atskiruose sektoriuose identifikuotas kibernetinio saugumo rizikas.

# Organizacinės priemonės



# Organizacinės priemonės (1/2)

Klientas turi įvertinti turimų/trūkstančių teisinių dokumentų aktualumą:



# Organizacinės priemonės (2/2)

Įmonės darbuotojams organizuoti nuolatinis kibernetinio saugumo mokymus bei vykdykime atsparumo grėsmėms higienos praktiką

**Baziniai  
kibernetinio saugumo  
mokymai visiems!**



## El. pašto apsauga

Nepageidajami  
laiškai, prisegtukų  
politika



## Interneto apsauga

„Wi-Fi“, daiktų  
internetu ir paieškos  
variklio saugumas



## Praktiniai patarimai

Kaip apsisaugoti nuo  
kibernetinių grėsmių  
darbe ir namuose



## Grėsmių apžvalga

Kenkėjiškų programų  
ir sukčiavimo tipai,  
socialinė inžinerija



## Slaptažodžių politika

Slaptažodžių higiena,  
2 veiksnių  
autentifikacija



## Nuotolinis darbas

Saugus prisijungimas  
prie įmonės vidinio  
tinklo

Phishing



Smishing



Vishing



+ Simuliacinė ataka

# Technologinės priemonės

# Technologinės priemonės (1/8)

Klientas ar jūs turėtų atlikti įmonėje valdomo turto (techninės ir programinės įrangos) inventorizaciją



# Technologinės priemonės (2/8)

Klientas ar jūs turėtų centralizuotai valdyti visus įmonės įrenginius bei diegti pažangius saugumo sprendimus



Bazinės  
antivirusinės  
jau negana!

# Technologinės priemonės (3/8)

Klientas ar jūs turėtų centralizuotai valdyti naudojamos programinės įrangos pažeidžiamumų patikrą bei užkardyti aptiktas saugumo klaidas ir atnaujinti pasenusias programas

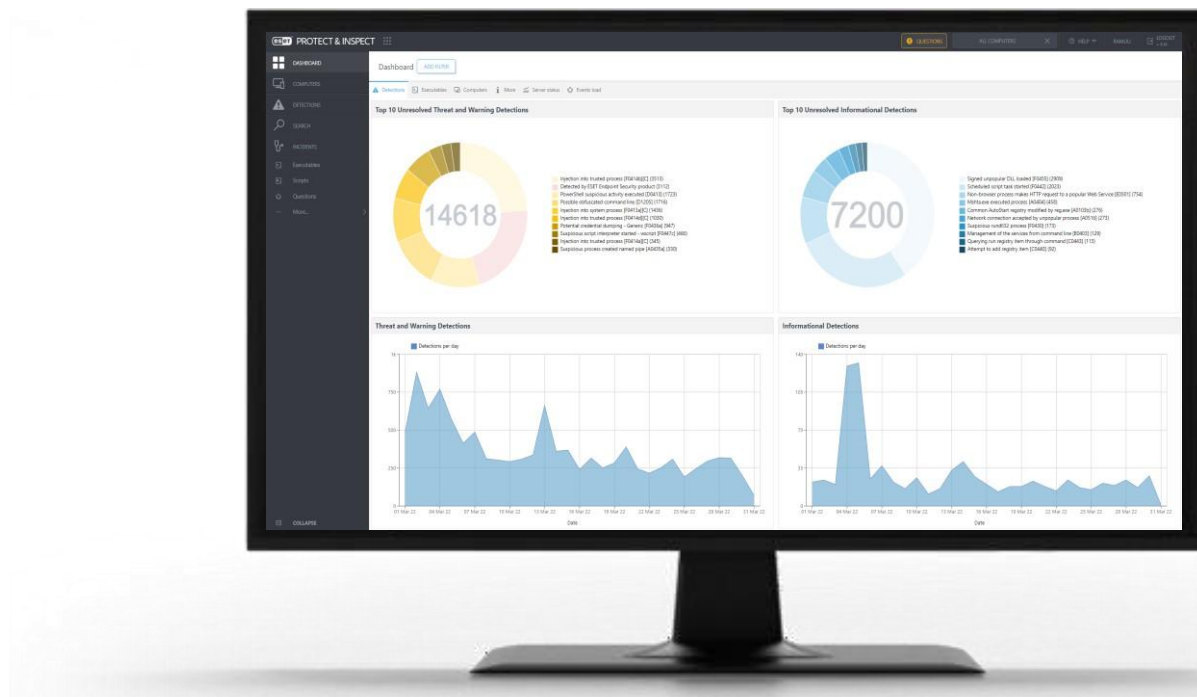


Windows Server

Windows Server  
Update Services  
(WSUS)

# Technologinės priemonės (4/8)

Klientas ar jūs turėtų reguliariai analizuoti ir kaupti įvykius iš įmonės įrenginių (pasitelkiant EDR, XDR ar SIEM įrankius), o aptikus grėsmę - operatyviai sureaguoti ir ją užblokuoti



Jeigu turime ribotą  
laiką ar trūksta  
žinių, rinkimės  
**MDR** ar **SOC**  
paslaugas

## Technologinės priemonės (5/8)

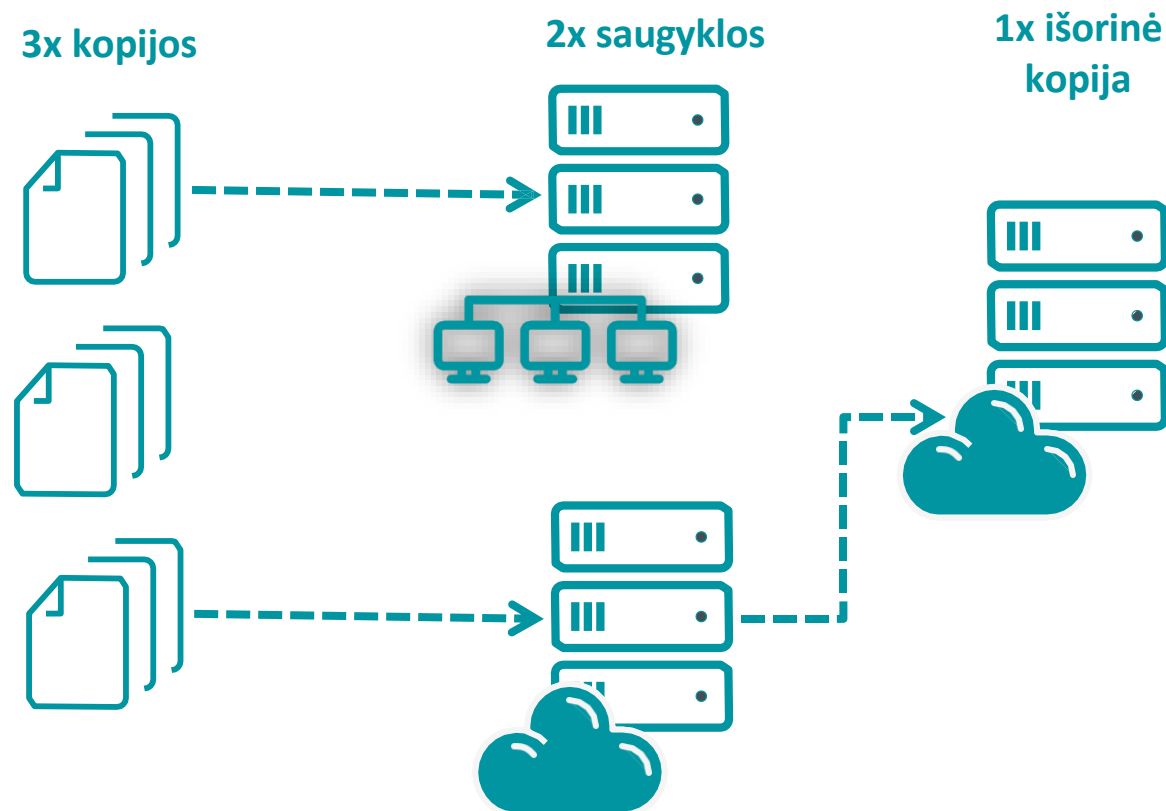
Klientas ar jūs turėtų aktyvuoti/įdiegti dviejų faktorių autentifikaciją tiek jungiantis prie informacinių sistemų, tiek per RDP prie serverių bei įmonės resursų per VPN





# Technologinės priemonės (6/8)

Klientas ar jūs turėtų patikrinti, kaip yra vykdomos atsarginės duomenų kopijos  
(būtina užtikrinti veiklos tęstinumą bei duomenų atkūrimą)



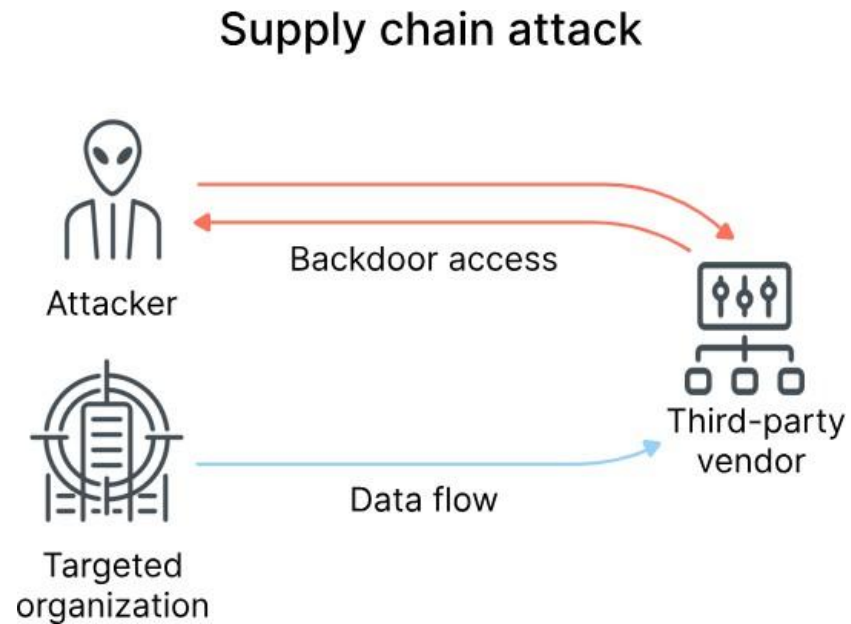
# Technologinės priemonės (7/8)

Darbai bei keitimai su riboto naudojimo informacija klientas ar jūs turėtų taikyti kriptografijos principus bei centralizuotai šifruoti kietuosius diskus



# Technologinės priemonės (8/8)

Klientas ar jūs turėtų riboti ir stebėti prisijungimus prie įmonės resursų iš trečiųjų šalių kompanijų, diegiant privilegijuotos prieigos valdymo sprendimus (PAM\*)



# Kibernetinio saugumo reikalavimų aprašas


---

Kibernetinio saugumo subjektai nustatytus organizacinius kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip per 12 mėnesių nuo jų įtraukimo į Kibernetinio saugumo subjekty registrą.

Kibernetinio saugumo subjektai nustatytus techninius kibernetinio saugumo reikalavimus privalo įgyvendinti ne vėliau kaip per 24 mėnesius nuo jų įtraukimo į Kibernetinio saugumo subjekty registrą.

# Oficiali LR krašto apsaugos ministerijos svetainė

<https://kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/>





LIETUVOS RESPUBLIKOS  
KRAŠTO APSAUGOS MINISTERIJA


f t in y

Paieška...

Q



LT

 |

Ministerija v |

Gynybos politika v |

Veiklos sritys v |

Naujienos v

Pagrindinis / Tinklų ir informacinių sistemų direktyva (TIS 2)

## Tinklų ir informacinių sistemų direktyva (TIS 2)

2022 m. gruodžio 14 d. priimta Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 Dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (toliau – TIS 2 direktyva).

**Lietuva TIS 2 (angl. NIS 2) direktyvą į nacionalinę teisę turės perkelti iki 2024 m. spalio 17 d.**

**TIS 2 direktyva siekiama trijų pagrindinių tikslų:**

- ES mastu padidinti organizacijų, kurios įvairiuose sektoriuose atlieka itin svarbias funkcijas, kibernetinio atsparumo lygį.
- Sumažinti kibernetinio atsparumo neatitikimus tarp sektorių ir sektoriuose, kuriems taikoma TIS 2 direktyva.
- Pagerinti informacijos mainus ir kolektyvinius gebėjimus pasirengti ir reaguoti į incidentus.

### SUSIJUSIOS NAUJIENOS

2024-02-21

Lietuva susigražino pirmininkavimą ES kibernetinėms greitojo reagavimo pajėgoms

2024-02-16

Po patirto incidento LKA imasi papildomų prevencinių priemonių stiprinant kibernetinį saugumą

2024-01-08

