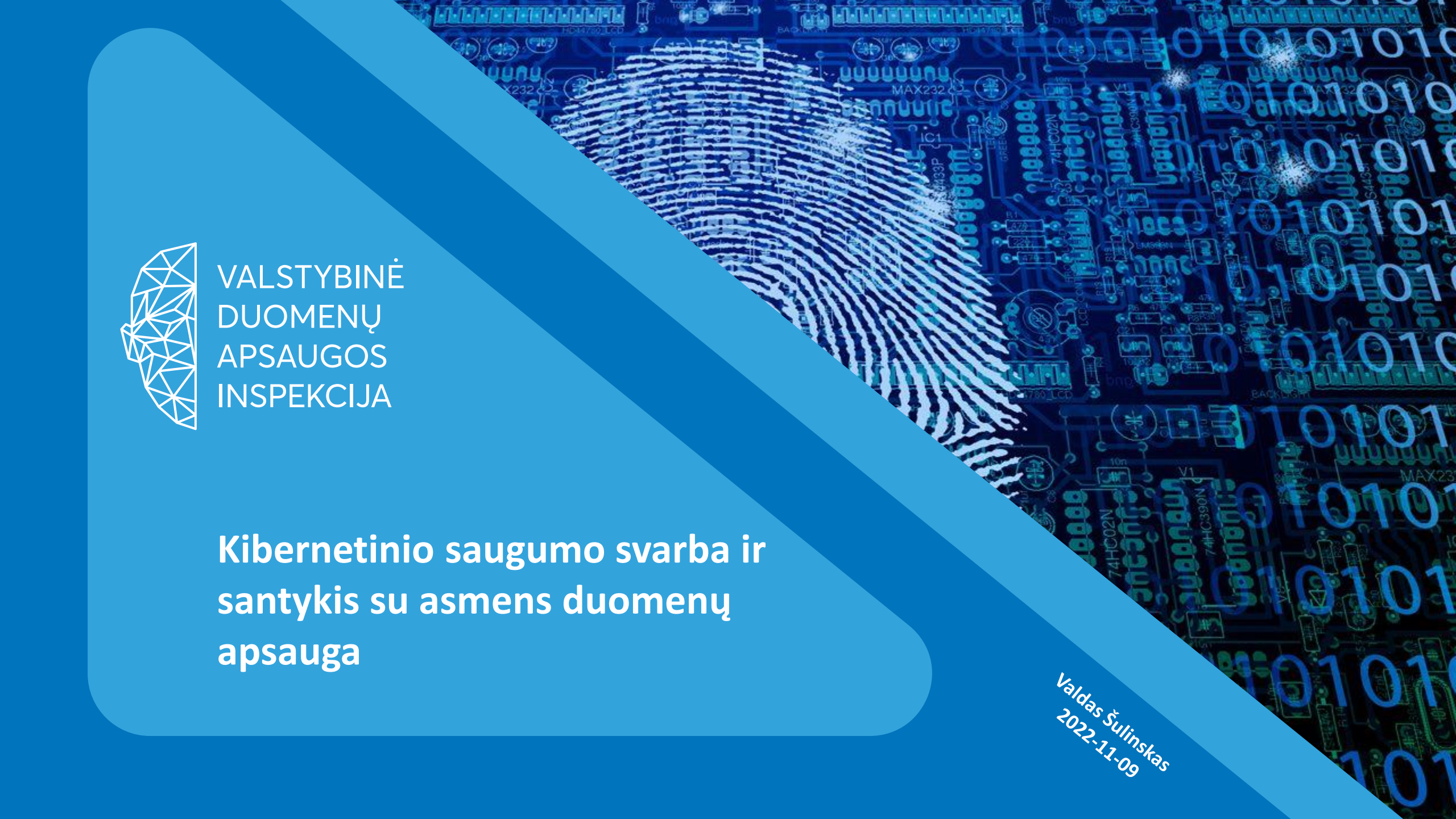


VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

Kibernetinio saugumo svarba ir santykis su asmens duomenų apsauga

Valdas Šulinskas

2022-11-09

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

GRĖSMĖS IR MOTYVACIJA

Šiandieninis pasaulinis kontekstas, ypač Rusijos invazija į Ukrainą, neišvengiamai lemia didelius kibernetinio saugumo grėsmių pokyčius. Daugėja grėsmę keliančių subjektų, daugėja plačiai paplitusių ir didesnį žalingą poveikį turinčių kibernetinių atakų.

Grėsmių subjektų rūšys:

- **valstybės remiami įsilaužėliai (angl. State-sponsored actors)**
  motyvacija: šnipinėjimas ir destrukcija.
- **kibernetiniai nusikaltėliai (angl. Cybercrime actors)**
  motyvacija: finansinė nauda ir pripažinimas.
- **samdomi įsilaužėliai (angl. Hacker-for-hire actors)**
  motyvacija: finansinė nauda ir pasitenkinimas.
- **įsilaužimo aktyvistai (angl. Hacktivists.)**
  motyvacija: politinės ir socialinės idėjos.

Kibernetinis saugumo užtikrinimas **nėra baigtinis procesas,** jokia įmonė **negali tikėtis visiško atsparumo** kibernetinėms grėsmėms.

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

„Threat Landscape“ ataskaita (2021 m. liepa – 2022 m. liepa)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

PAGRINDINĖS GRĖSMĖS

- **Išpirkos reikalaujančios programos (angl. Ransomware):** 60 proc. nukentėjusių organizacijų galėjo sumokėti išpirką.
- **Kenkėjiškos programos (angl. Malware):** Užfiksuoti 66 nulinės dienos (angl. zero-day) pažeidžiamumai.
- **Socialinė inžinerija (angl. Social engineering):** Socialinės inžinerijos pagalba atliekamos apgaulės ir sukčiavimai tebėra populiarūs, pastebimos naujos jų formos.
- **Grėsmės duomenims (angl. Threats against data):** Grėsmės didėja proporcingai sukuriamų duomenų kiekiui.
- **Grėsmės prieinamumui (angl. Threats against availability):** Atsisakymo teikti paslaugas (DDoS) atakos, interneto infrastruktūros sunaikinimas, interneto srauto sutrikimai.
- **Dezinformacija (angl. Disinformation – misinformation):** Dirbtinio intelekto įgalinta dezinformacija ir klastotės, „dezinformacija kaip paslauga“.
- **Tiekimo grandinės atakos (angl. Supply chain targeting):** Trečiųjų šalių incidentų žymus padidėjimas.

enisa

EUROPEAN UNION AGENCY FOR CYBERSECURITY

„Threat Landscape“ ataskaita (2021 m. liepa – 2022 m. liepa)

https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

DUOMENŲ SAUGUMAS – KUO REMTIS

Organizacijos turi užtikrinti, kad asmens duomenys būtų tvarkomi saugiai. Jos turi imtis būtinų techninių ir organizacinių priemonių tinkamam (aukštam) informacijos saugumo lygiui užtikrinti.

Tačiau, nors organizacinių ir techninių saugumo ir kontrolės priemonių pavyzdžiai BDAR yra nurodomi, pačiame BDAR nėra nepateikiama išsamių gairių, kaip tai pasiekti.

Asmens duomenų saugumui užtikrinti reikalingas **saugumo lygis bei saugumo ir kontrolės priemonės yra nustatomos remiantis ir atliekant rizikos vertinimą**. BDAR yra grindžiamas rizikos vertinimu ir valdymu, tai leidžia pasiekti duomenų apsaugos tikslų, kai vyrauja kintamumas ir neapibrėžtumas.

Saugumo priemonės turi būti proporcingos ir adekvačios, įvertinant jų įgyvendinimo sąnaudas bei atitinkančios techninių galimybių išsivystymo lygį (angl. state-of-the-art). **„State-of-the-art“** - tai pažangiausios ir veiksmingiausios saugumo priemonės, kurios tuo metu yra pripažintos ir pasiekiamos rinkoje.

ISO 27000 serijos informacijos saugumo standartai

ENISA (duomenų apsaugos) gairės ir rekomendacijos,

VDAI (ir kitų ES priežiūros institucijų) gairės ir rekomendacijos

NIST (informacinių technologijų) standartai

NKSC (LT), CISA (USA) ir NCSC (GB) rekomendacijos

Geroji praktika ir Gamintojų priežiūros rekomendacijos

VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

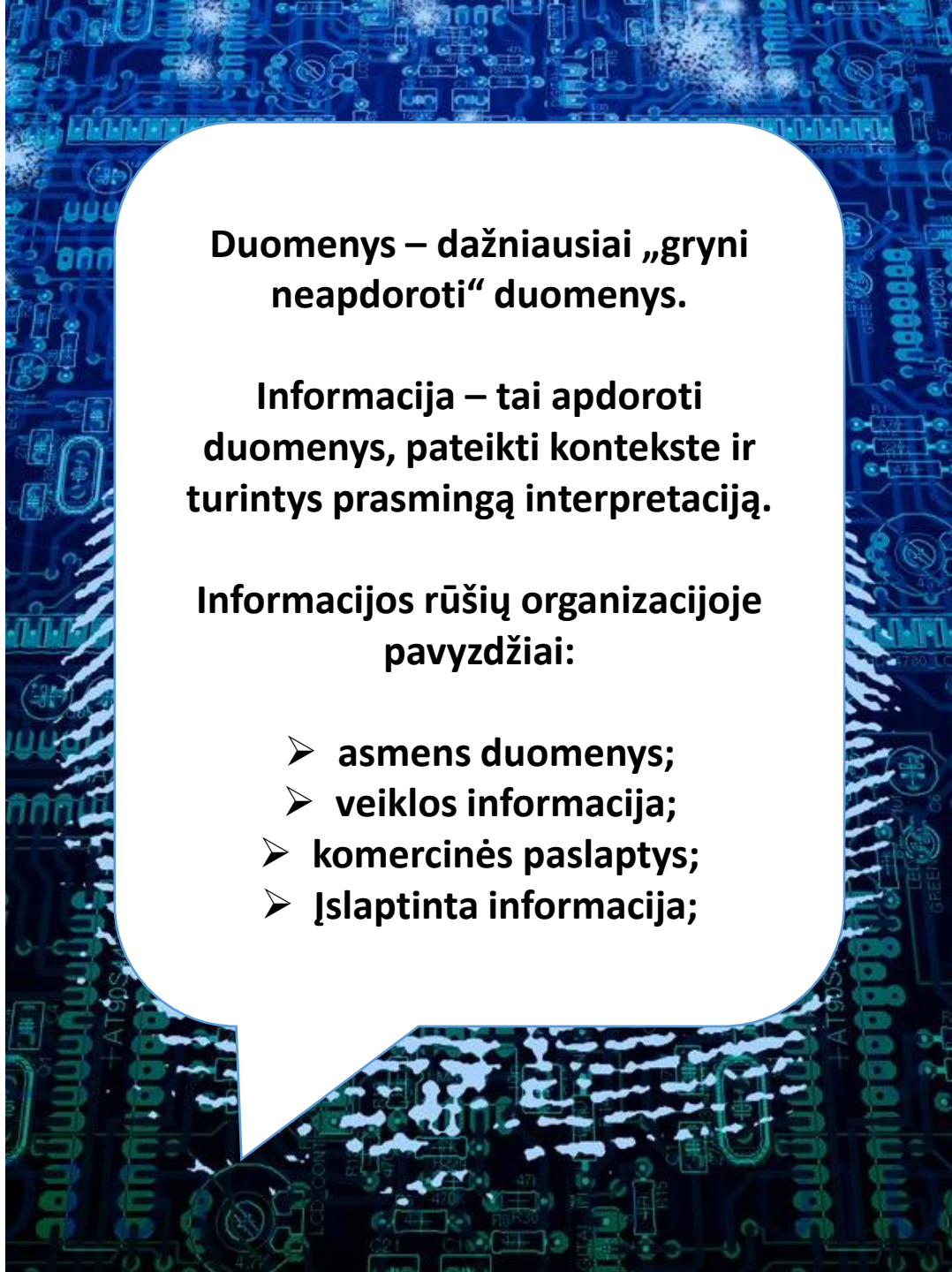
SĄVOKOS IR TERMINAI

Asmens duomenys– bet kokia **informacija** apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti (duomenų subjektas) ...

Kibernetinis saugumas – tai veiksmai, kurių imamasi norint apsaugoti kibernetinę aplinką ir užtikrinti informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos **prieinamumą, vientisumą bei konfidencialumą**.

Informacijos saugumas – tai visuma organizacinių, teisinių ir techninių priemonių, kuriomis užtikrinamas veiklos procesų, tvarkomos informacijos ar naudojamų technologijų **atsparumas** kibernetinėms atakoms ar kitiems saugumo incidentams.

Kibernetinis **atsparumas** – gebėjimas adaptuotis prie kintančių sąlygų, atlaikyti destrukcinius veiksmus juos absorbuojant ar atmetant bei greitai po jų atsistatyti. Dėmesys atsparumui stiprina bendrą kibernetinio ir duomenų saugumo lygį.



Duomenys – dažniausiai „gryni neapdoroti“ duomenys.

Informacija – tai apdoroti duomenys, pateikti kontekste ir turintys prasmingą interpretaciją.

Informacijos rūšių organizacijoje pavyzdžiai:

- **asmens duomenys;**
- **veiklos informacija;**
- **komercinės paslaptys;**
- **Įslaptinta informacija;**

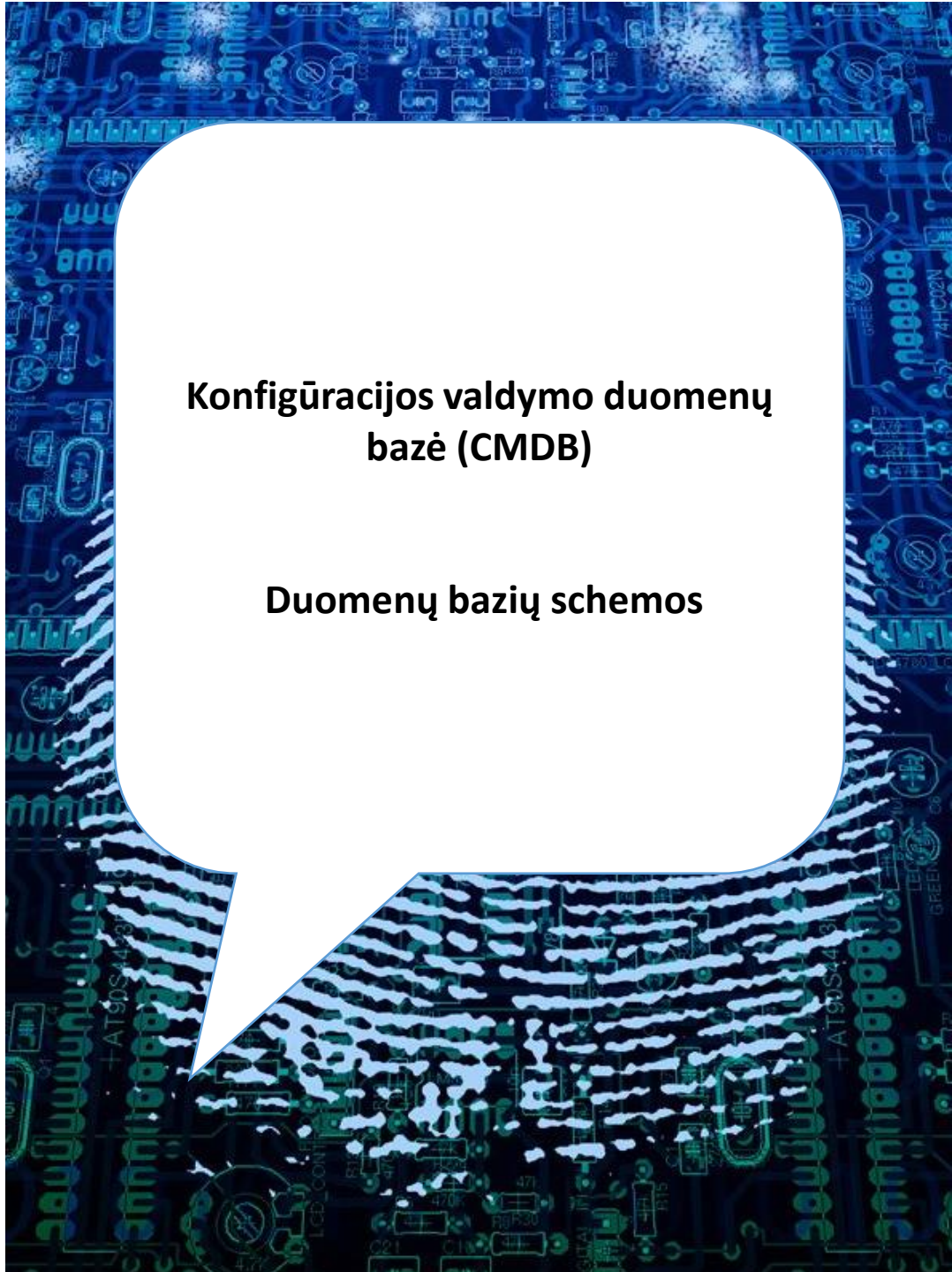
VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ŽINOKITE SAVO SAUGUMO APLINKĄ

Organizacija **negali teigti**, kad ji laikosi BDAR reikalavimų, jei nežino, kur ir kokiose IT/IS sistemose tvarkomi jos valdomi asmens duomenys.

Jei jūsų organizacijoje yra **Konfigūracijos elementų valdymo duomenų bazė (CMDB)**, paprašykite, kad suteiktų jums prieigą (peržiūrai) ir paaiškintų, kaip interpretuoti sukauptą informaciją, sąsajas tarp komponentų ir jų pokyčius laike.

Jei jūsų organizacijoje yra **duomenų bazių administratorius** (DBA), susėskite su juo ir paprašykite, kad jis supažindintų jus su savo prižiūrimomis duomenų bazėmis. Paprašykite DBA pateikti duomenų bazių schemas. Schemos parodo duomenų bazės lenteles ir laukus ir gali būti geras būdas nustatyti galimus asmeninių ir neskelbtinų duomenų šaltinius.



VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

ŽINOKITE SAVO SAUGUMO APLINKĄ

Jei jūsų organizacija yra suderinusi savo veiklą su ITIL metodika, ji turėtų būti pasirengusi **Paslaugų katalogą** (angl. ITIL Service Management Catalogue), kuriame pateikiama informacija apie visas aktualias veiklos paslaugas. Naudinga peržvelgti ir **Paslaugų portfelį**, nes jame bus nurodytos nebenaudojamos paslaugos bei dar tik planuojami projektai.

CMDB, ITIL metodika ir projektų valdymo metodai yra naudingi tada, kai organizacijos turi išvystytus procesus, tačiau jie net ir tada tiek geri, kiek yra gera ir tiksli užfiksuota informacija. Finansų skyrius yra ta vieta, kuri paprastai labai gerai fiksuoja informaciją apie išleistas lėšas. **Finansiniai įrašai** gali padėti atsekti IT paslaugų tiekėjų teikiamas paslaugas ir pokyčius juose.

Jei organizacija turi projektų vadovą, vykdo nemažai projektinės veiklos, visada naudinga atlikti ir organizacijos **Projektų portfelio** peržiūrą (rengiamų, vykdomų ir užbaigtų projektų sąrašas).

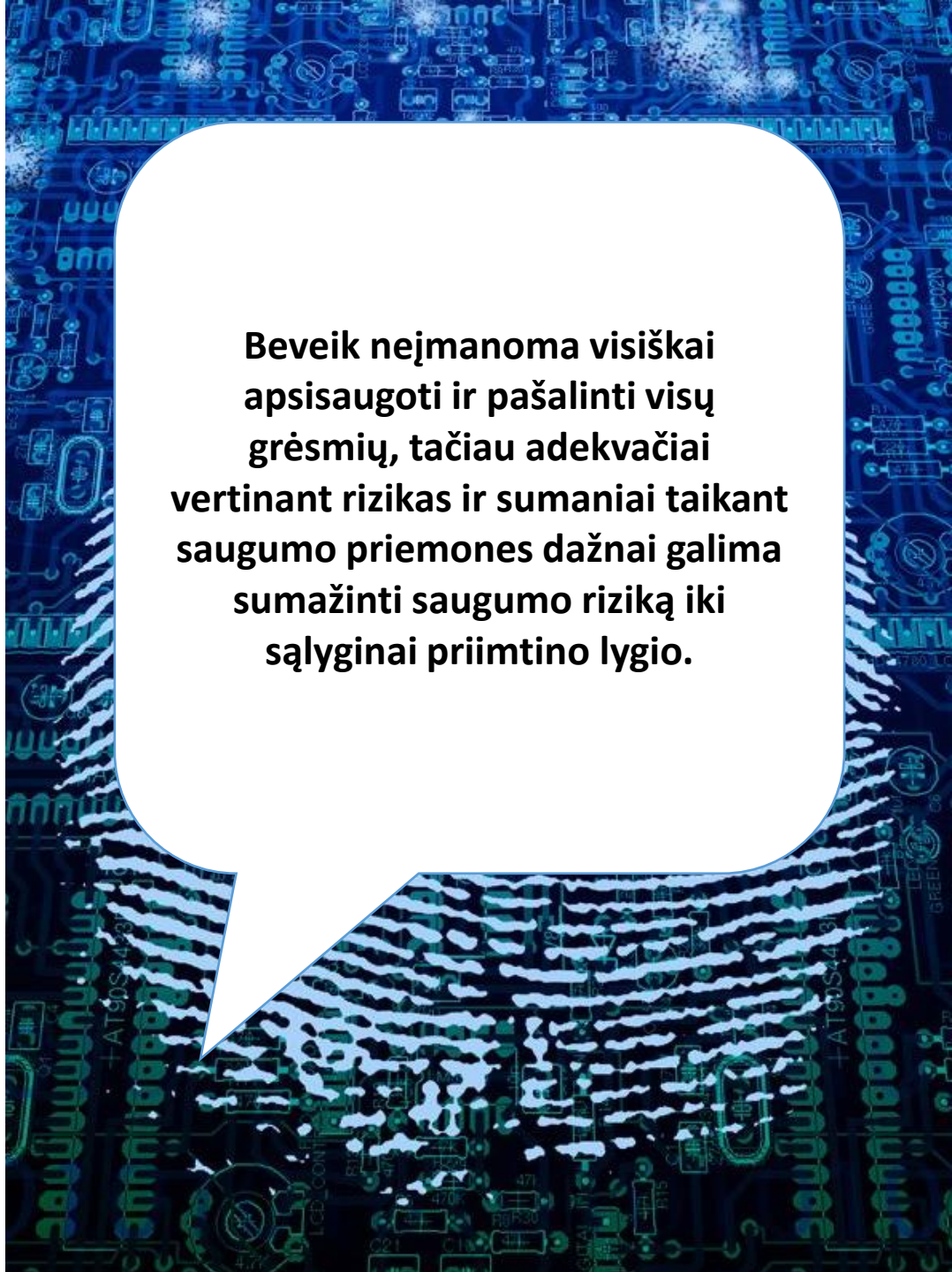
VALSTYBINĖ DUOMENŲ APSAUGOS INSPEKCIJA

PABAIGAI

Kibernetinio saugumo užtikrinimas yra **tęstinis procesas**, reikalaujantis nemažai jūsų resursų, tačiau žvelgiant į jį kaip į organizacijos veiklos sudėtinę dalį, nemažai saugumo priemonių gali būti įgyvendintos sparčiai ir palaipsniui.

Vertindami IT sistemų ir jose tvarkomų duomenų saugumą paklauskite savęs, kas atsitiktų, jeigu negrįžtamai dingtų visi jūsų duomenys. Kurių duomenų praradimas padarytų sunkiai pakeliamą žalą jūsų organizacijai ir sukeltų grėsmę jos veiklos tęstinumui? Kurie žmonės yra esminiai (jūsų organizacijos ar jūsų paslaugų tiekėjo) specialistai, kurie užtikrins tinkamą kibernetinio incidento ir (-ar) duomenų saugumo pažeidimo suvaldymą bei duomenų atstatymą iš rezervinių kopijų.

Pirmiausia apsaugokite savo kritinius duomenis ir sistemas, savo organizacijos „karūnos brangakmenius“. Iš senovės Romos atėjęs principas „skaldyk ir valdyk“ puikiai tinka ir informacijos saugumo valdymo kontekste.



Beveik neįmanoma visiškai apsisaugoti ir pašalinti visų grėsmių, tačiau adekvačiai vertinant rizikas ir sumaniai taikant saugumo priemones dažnai galima sumažinti saugumo riziką iki sąlyginai priimtino lygio.