SECURITY DAYS

TIS2 IŠŠŪKIS – TIEKĖJŲ GRANDINĖS SAUGUMO UŽTIKRINIMAS

Daiva Tamulionienė - Widen Legal
vyresnioji teisininkė

Rugsėjo 5 d. 2024
KIBERNETINIO SAUGUMO KONFERENCIJA
esd.eset.lt

Grandinės saugumas – kodėl svarbu?

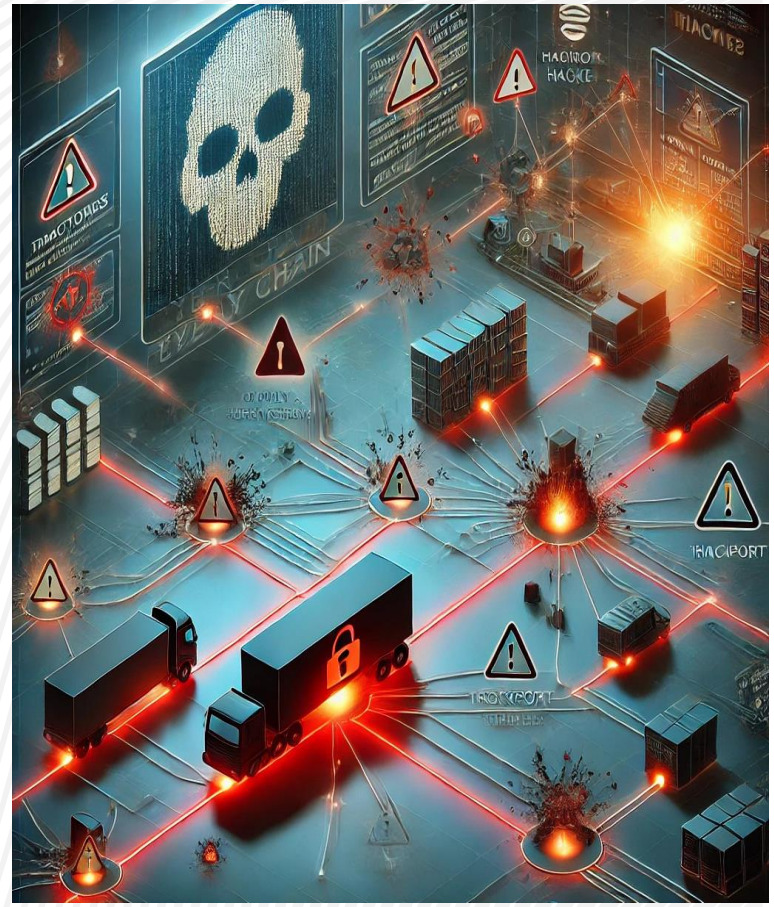
- Siekdami pakenkti tiksliniams klientams, išpuolių vykdytojai sutelkė dėmesį į tiekėjų kodą maždaug **66 % incidentų, apie kuriuos pranešta**
- **Maždaug 58 % analizuotų tiekimo grandinės incidentų klientų turtas daugiausia buvo klientų duomenys,** įskaitant asmeniškai identifikuojamos informacijos (PII) duomenis ir intelektinę nuosavybę
- **66 %** analizuotų išpuolių tiekimo grandinėje **tiekėjai nežinojo arba nepranešė, kaip jiems buvo pakenkta**
- Mažiau nei **9 proc. klientų**, kuriems kilo pavojus dėl atakų tiekimo grandinėje, nežinojo, kaip šie išpuoliai įvyko

Informacijos šaltinis: ENISA paskelbė savo grėsmę tiekimo grandinės išpuoliams. | Shaping Europe's digital future (europa.eu)

WIDEN

„SolarWinds“ kibernetinis incidentas

- 2020 m. į „SolarWinds“ „Orion“ sistemą įdiegta kenkėjiška programinė įranga „Sunburst“, orientuota į šio sistemos atnaujinimus
- Kenkėjiška programinė įranga išplito, kai tūkstančiai „SolarWinds“ klientų įdiegė atnaujinime esantį kenkėjišką kodą, tokiu būdu buvo gauta prieiga prie „SolarWinds“ klientų duomenų
- Pažeidimas paveikė tūkstančius įmonių ir organizacijų, įskaitant svarbiausias JAV vyriausybės agentūras, tokią kaip Energetikos departamentas, Gynybos departamentas ir Finansų departamentas, taip pat privačias korporacijas
- Manoma, kad incidentas paveikė apie **18 000 „SolarWinds“ klientų**, o tam tikros organizacijos prarado itin konfidencialius duomenis



WIDEN

Kokia situacija Lietuvoje?

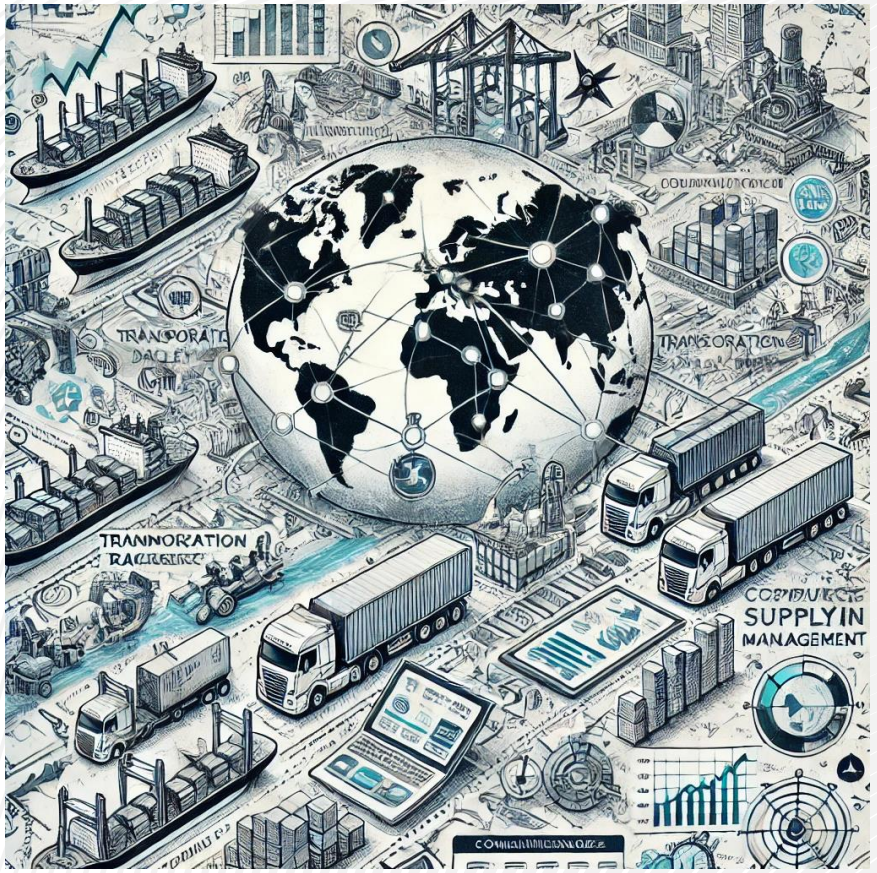
Lietuvoje 2023 m. buvo registruoti incidentai, kai įsilaužus į IRT paslaugas teikiančias įmonės buvo pasiekti tikrieji taikiniai – šių įmonių klientai

https://kam.lt/wp-content/uploads/2024/05/NKSBA2023.pdf

WIDEN

Pagrindiniai iššūkiai

- Tiekėjų patikimumas ir skaidrumas
- Trečiųjų šalių komponentų saugumas
- Kenkėjiškos programinės įrangos ir kibernetinių grėsmių integracija
- Fizinės saugos pažeidžiamumas
- Sudėtingas rizikos valdymas ir atitikimas reguliavimams



WIDEN

Asmens duomenų apsauga tiekimo grandinėje: pagrindinės praktinės problemos

- Asmens duomenų dalijimasis
- Tiekėjų saugumo patikimumas (sutartiniai įsipareigojimai ir trečiųjų šalių auditai)
- Rizikų valdymas tiekimo grandinėje (kibernetinių grėsmių valdymas ir incidentų valdymo planai)
- Reguliaciniai reikalavimai (atitiktis teisės aktams ir pranešimai apie pažeidimus)

WIDEN

Kaip valstybė galėtų padėti užtikrinti trečiųjų šalių valdymą?

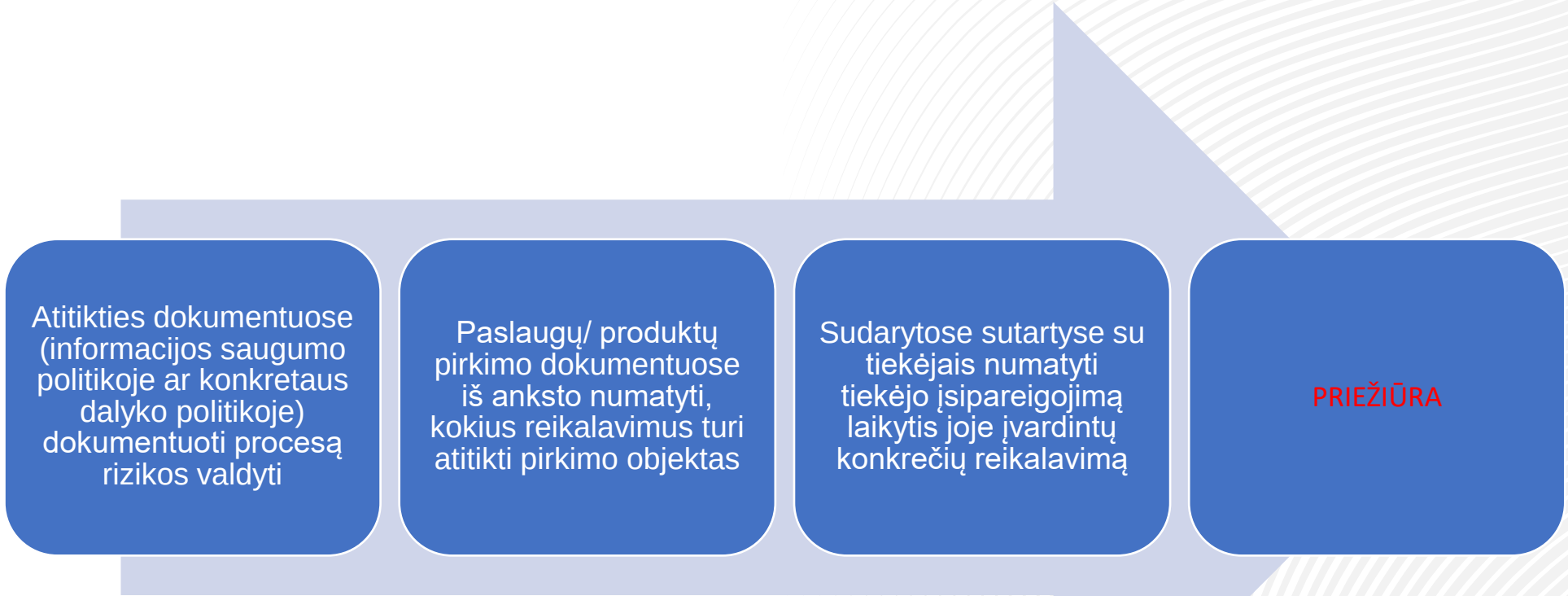
Lietuvoje šiuo metu nėra aiškių reguliavimo struktūrų ir procedūrų, kurios leistų efektyviai valdyti trečiųjų šalių kibernetinį saugumą

Rekomendacijos sprendimams Lietuvoje:

- Struktūruoti kibernetinio saugumo santykius su tiekėjais. Pavyzdžiui, remdamasi Danijos pavyzdžiu Lietuva galėtų parengti kibernetinių saugumo santykių su tiekėjais valdymo gaires arba numatyti proceso etapus.
- Atlikti trečiųjų šalių vertinimus ir suteikti įvairaus tipo sertifikatus. Pavyzdžiui, pasinaudodama Austrijos pavyzdžiu Lietuva galėtų sukurti „Cyber Trust"[29] sertifikavimo lygius, kurie padėtų įvertinti tiekimo grandinės dalyvių kibernetinio saugumo būklę. Tai galėtų padėti organizacijoms lengviau pasirinkti saugius ir patikimus tiekėjus.
- Sudaryti tiekimo grandinės žemėlapį. Pavyzdžiui, remdamasi Didžiosios Britanijos pavyzdžiu Lietuva galėtų taikyti tiekimo grandinės žemėlapio sudarymo principą, kad identifikuotų potencialias rizikas ir sužinotų, kaip organizacijos procesus gali paveikti jų valdymo trečiosioms šalims.
- Sukurti standartus. Pavyzdžiui, remtis Prancūzijos modeliu ir skatinti organizacijas atitikti kibernetinio saugumo standartus.
- Palengvinti viešųjų pirkimų procesą. Pavyzdžiui, sukurti skirtingas preliminarias sutartis (sutarčių šablonus) su paslaugų teikėjais.
- Dalytis informacija. Pavyzdžiui, remiantis ENISA pavyzdžiu skatinti tiekėjus informuoti ir viešai skelbti apie informaciją apie kibernetinius incidentus, susijusius su tiekimo grandinės atakomis.

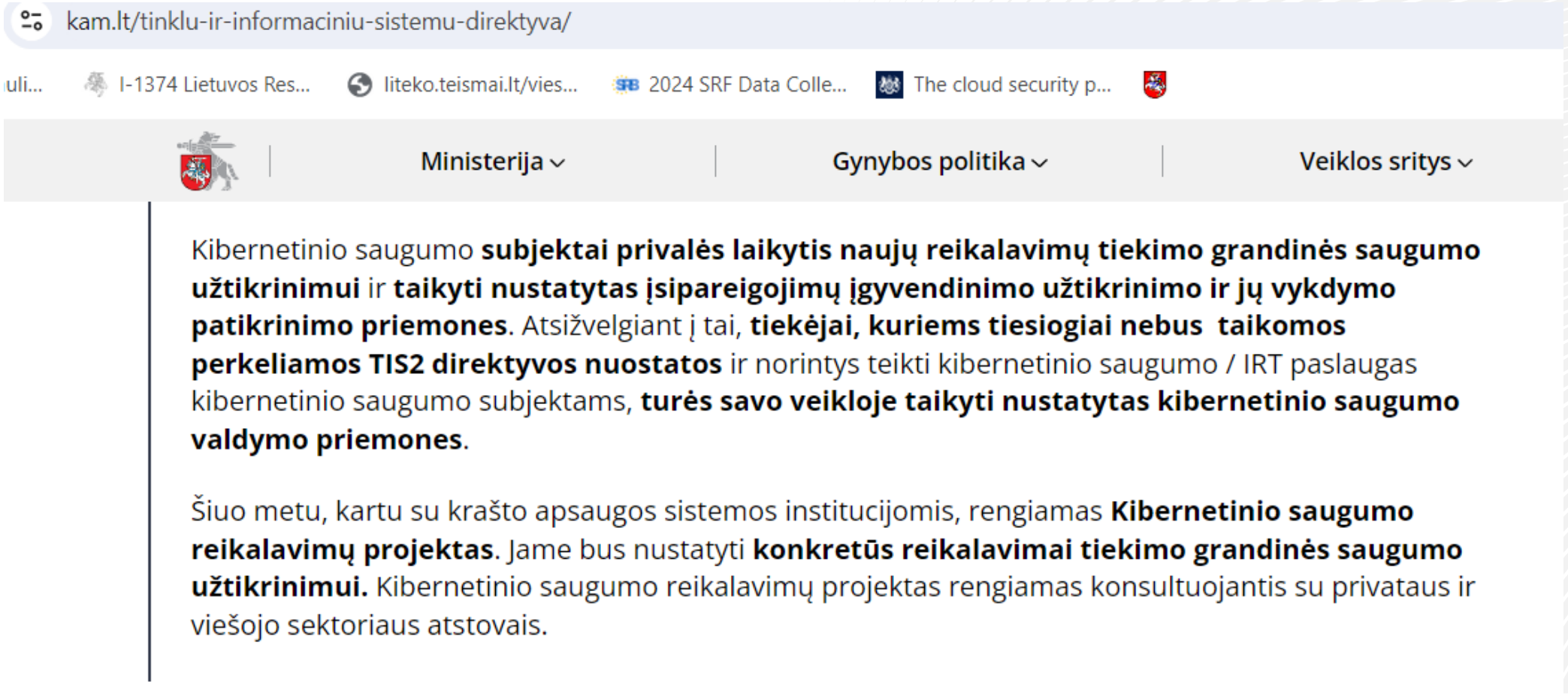
WIDEN

Pagrindiniai patarimai



WIDEN

Ko tikėtis iš valstybės?



WIDEN

DAIVA TAMULIONIENĖ

- WIDEN legal vyresnioji teisininkė
- daiva.tamulioniene@widen.legal
- Konstitucijos pr. 7, verslo centras „Europa“, 24 aukštas, LT-09308, Vilnius
- +370 5 24 876 70
- lithuania@widen.legal
- widen.legal

WIDEN