



**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

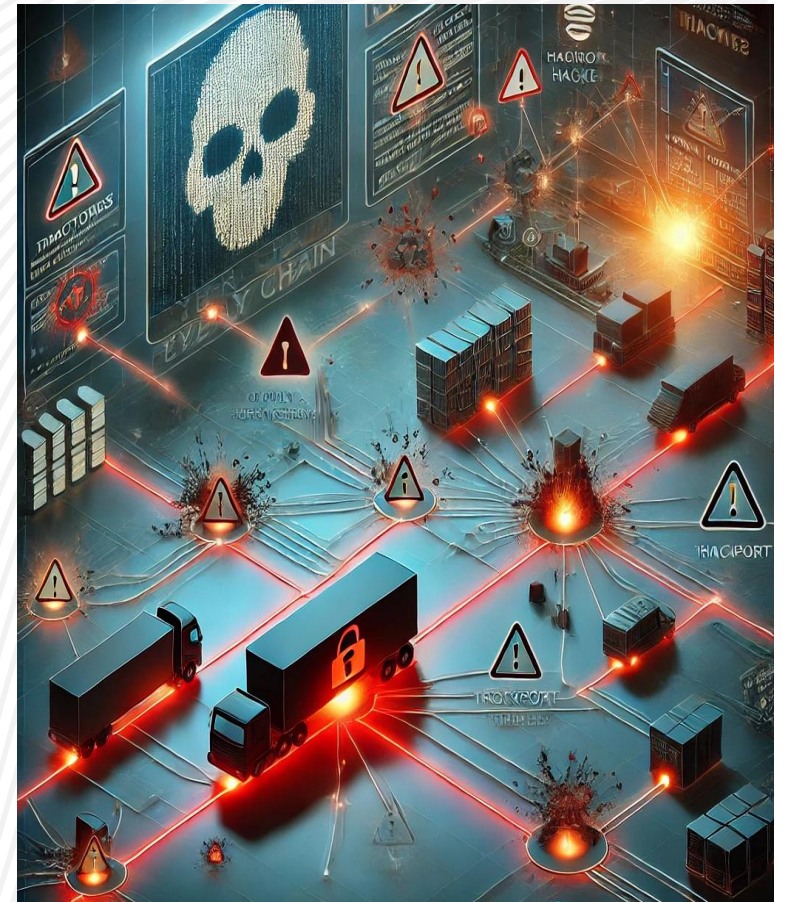
Informacijos šaltinis: [ENISA paskelbė savo grėsmę tiekimo grandinės išpuoliams. | Shaping Europe's digital future \(europa.eu\)](#)



W I D E N

„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



W I D E N

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>



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



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)

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 žemėlapi. 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.

Pagrindiniai patarimai

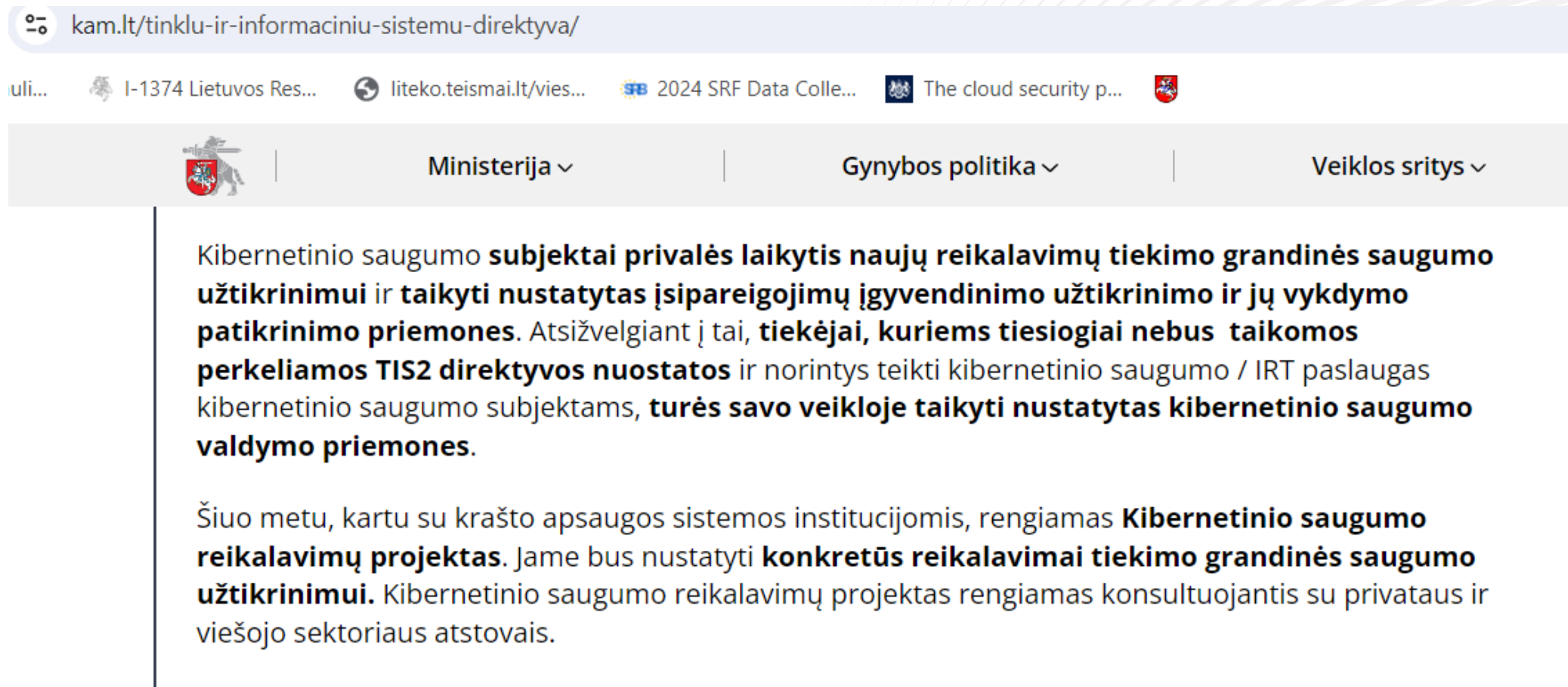
Atitiktis dokumentuose (informacijos saugumo politikoje ar konkretaus dalyko politikoje) dokumentuoti procesą rizikos valdyti

Paslaugų/ produktų pirkimo dokumentuose iš anksto numatyti, kokius reikalavimus turi atitikti pirkimo objektas

Sudarytose sutartyse su tiekėjais numatyti tiekėjo įsipareigojimą laikytis joje įvardintų konkrečių reikalavimų

PRIEŽIŪRA

Ko tikėtis iš valstybės?



The screenshot shows a web browser window with the address bar containing 'kam.lt/tinklu-ir-informaciniu-sistemu-direktyva/'. Below the address bar, there are several open tabs: 'uli...', 'I-1374 Lietuvos Res...', 'liteko.teismai.lt/vies...', '2024 SRF Data Colle...', and 'The cloud security p...'. The website header features the Lithuanian coat of arms, the word 'Ministerija' with a dropdown arrow, 'Gynybos politika' with a dropdown arrow, and 'Veiklos sritys' with a dropdown arrow. The main content area contains a text block with the following text:

Kibernetinio saugumo **subjektai privalės laikytis naujų reikalavimų tiekimo grandinės saugumo užtikrinimui ir taikyti nustatytas įsipareigojimų įgyvendinimo užtikrinimo ir jų vykdymo patikrinimo priemones.** Atsižvelgiant į tai, **tiekėjai, kuriems tiesiogiai nebus taikomos perkeliamos TIS2 direktyvos nuostatos** ir norintys teikti kibernetinio saugumo / IRT paslaugas kibernetinio saugumo subjektams, **turės savo veikloje taikyti nustatytas kibernetinio saugumo valdymo priemones.**

Šiuo metu, kartu su krašto apsaugos sistemos institucijomis, rengiamas **Kibernetinio saugumo reikalavimų projektas.** Jame bus nustatyti **konkretūs reikalavimai tiekimo grandinės saugumo užtikrinimui.** Kibernetinio saugumo reikalavimų projektas rengiamas konsultuojantis su privataus ir viešojo sektoriaus atstovais.



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

Skaidres bei dokumentų šablonus draudžiama platinti, kopijuoti ar kitaip atgaminti bei naudoti.