NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

# Kibernetinis saugumas: kaip valdyti trečiųjų šalių keliamas rizikas? Vieša konsultacija

„Kurk LT“ bendradarbiaujant su „Kibernetinio saugumo ekspertų asociacija“ sukvietė NKSC, NKC, KAM KSITPG, „NOD Baltic| ESET Lietuva“ ir skirtingus ūkio sektorių (finansų, vandens tiekimo paslaugų, energetikos, transporto) ekspertus

2024 02 08 „Scalewolf“ Vilnius

Apskritojo stalo diskusijos tikslas – pristatyti bei pateikti pasiūlymus ir aptarti  kaip valdyti trečiųjų šalių keliamas rizikas.

# 3 Pagrindiniai probleminiai teiginiai

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk nW LT

1. Lietuvoje Kibernetinio saugumo paslaugų tiekėjams (trečiosioms šalims) netaikomi privalomi organizaciniai ar techniniai reikalavimai ( pagal OTR 13 str. išskyrus VII ir YSII valdytojų tiekėjus).
2. Trečiosios šalys nėra įpareigotos informuoti apie kibernetinius incidentus arba pateikti apie juos informaciją.
3. Trečioji šalis neįtraukiama į rizikos kategoriją ir nelaikoma kontroliuojama tiekimo grandinės rizika.

# Diskusijoje pasidalintos pašnekovo mintys apie IT specialistų esamą situaciją

IT specialistų žinių trūkumas, susijęs su nežinojimu apie savo nežinojimą rizikos vertinimo kontekste, kelia reikšmingą iššūkį užtikrinant tinkamą technologinių sistemų saugumą ir veiksmingumą. Tai apima nepakankamą supratimą apie plataus spektro rizikas, įskaitant trečiųjų šalių rizikos valdymą, reglamentavimo bei atitikties reikalavimus, taikytinas rizikos vertinimo metodikas, žmogiškąjį faktorių ir organizacinės kultūros įtaką, kompleksinių sistemų tarpusavio priklausomybes, taip pat nepakankamą incidentų atsako ir atkūrimo planavimą.

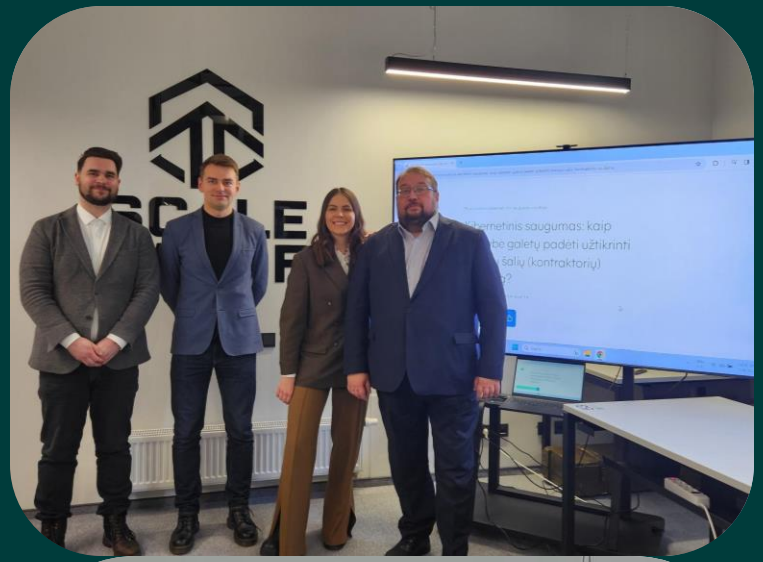
# Diskusijoje iškelti probleminiai klausimai

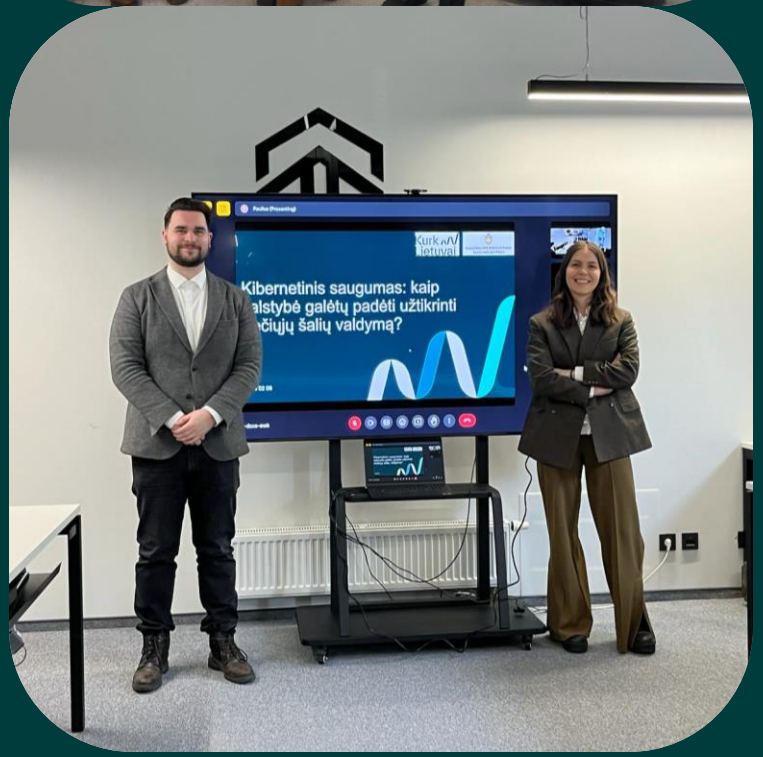
NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk nV LT

1. Kaip organizacijos gali atlikti efektyvų rizikų įsivertinimą, identifikuojant ir įvertinant potencialias grėsmes, kurios gali trukdyti pasiekti jų tikslus ir veiksmingumą?
2. Kokios strategijos ir metodai yra labiausiai tinkami kompleksinėms rizikoms nustatyti ir jų valdymo prioritetams sudaryti, siekiant užtikrinti organizacijos stabilumą ir tvarumą ilgalaikėje perspektyvoje?

# Apskritojo stalo diskusijos pašnekovai






NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

# Diskusijos pašnekovų siūlomi sprendimai

# Deklaracija ir sertifikavimas

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

Siekiant užtikrinti įmonių veiklos tvarumą ir atsparumą išorės rizikoms, yra svarbu, kad įmonių vadovybė ne tik suvoktų, bet ir imtųsi aktyvių veiksmų įtraukiant trečiąsias šalis kaip potencialius rizikos veiksnius.

Tai galima pasiekti dviem pagrindiniais būdais:

- Deklaracijų pateikimu (kaip daro JAV).
- Sertifikavimu.

# Deklaracija

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

Deklaracijų pateikimas reiškia, kad įmonės oficialiai pripažįsta ir deklaruoja savo atsakomybę už trečiųjų šalių sukeltą riziką. Tai apima aiškius įsipareigojimus laikytis tam tikrų standartų ir procedūrų, kurie užtikrina, jog įmonės veikla ir jos partneriai atitinka saugumo principus. Tokios deklaracijos gali apimti tiek vidaus, tiek išorės politikas ir gaires, kurios reglamentuoja įmonės santykius su tiekėjais, partneriais ir kitomis susijusiomis šalimis.

# Sertifikavimas

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk nuo LT

Sertifikavimas yra dar vienas įrankis, rodantis įmonių vadovų sąmoningumą ir įsipareigojimą valdyti trečiųjų šalių keliamas rizikas. Sertifikavimo procesas apima nepriklausomų institucijų atliktą įmonės veiklos vertinimą, siekiant nustatyti, ar ji atitinka tarptautinius standartus ir normas. Sertifikavimas ne tik padeda įmonėms rodyti savo atsakomybę ir skaidrumą, bet ir stiprina pasitikėjimą tarp įmonės, jos partnerių ir klientų.

# Trečiųjų šalių reitingavimo sistema

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

Pirmiausia visos organizacijos pradėtu nuo savęs, sužinotu savo silpnas ir kritines vietas.

Trečiųjų šalių reitingavimo sistema – naudinga organizacijoms, siekiant vertinti ir valdyti rizikas, susijusias su partneriais, tiekėjais ar kitomis suinteresuotosiomis šalimis.
Tikslas įvertinti balais už kiekvieną atliktą veiksmą, pavyzdžiui, atliktas pentest, tęstinumo planas ir t.t.

# Trečiųjų šalių reitingavimo sistemos nauda

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

1. Gali būti itin naudinga organizacijoms, siekiant vertinti ir valdyti rizikas, susijusias su partneriais, tiekėjais ar kitomis suinteresuotosiomis šalimis.
2. Leistų įmonėms sistemingai įvertinti trečiųjų šalių patikimumą.
3. Turėti mažesnę finansinę riziką.
4. Teisinį atitikimą ir kitus svarbius veiksnius.

Padeda nustatyti galimas grėsmes ir imtis prevencinių priemonių prieš pradedant ar tęsiant bendradarbiavimą.

# Trečiųjų šalių darbuotojų auditas

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

Nacionalinio saugumo klausimas, susijęs su trečiųjų šalių darbuotojų patikimumo tikrinimu, yra itin svarbus ir reikalauja kruopštaus ir daugiamatės strategijos taikymo. Siekiant nacionalinio saugumo, būtina imtis visapusiškų priemonių, kad būtų užtikrintas trečiųjų šalių darbuotojų patikimumas. Tai reikalauja ne tik griežtų procedūrų įgyvendinimo, bet ir nuolatinio vertinimo bei prisitaikymo prie kintančių saugumo aplinkybių.

# Sutartys

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk nw LT

Konkurencijos ribojimo rizikos apima veiksmus ar sutartis, kurios gali apriboti konkurenciją rinkoje, darydamos neigiamą poveikį verslui, vartotojams ir ekonomikai apskritai. Šios rizikos yra svarbios tiek verslams, tiek reguliavimo institucijoms, nes jų nustatymas ir valdymas yra būtinas norint užtikrinti sveiką konkurencinę aplinką.

# Vadovautis bei remtis
# Darbos saugos reikalavimų metodika

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Kurk LT

Kiekviena darbo sritis aprašyta su nustatytais aiškiais punktais.

Pvz,

27 straipsnis. Darbuotojų instruktavimas ir mokymas

1. Darbdavys negali reikalauti, kad darbuotojas pradėtų dirbti jam pavestą darbą įmonėje, jeigu jis neinstruktuotas ir (ar) neišmokytas saugiai jį atlikti. Darbuotojas instruktuojamas atsižvelgiant į jo darbo vietą ar atliekamą darbą, jį priimant į darbą, perkeliant į kitą darbą ar darbo vietą, pradėjus naudoti naujas ar modernizuotas darbo priemones, naujas technologijas.

# Ačiū už bendradarbiavimą

Kurk nVLT

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Vilniaus vandenys

KLAIPĖDOS VANDUO

Vilniaus šilumos tinklai

SCALEWOLF

ESET ENJOY SAFER TECHNOLOGY™

NOD BALTIC

ignitis

NKC NACIONALINIS KOORDINAVIMO CENTRAS LIETUVA

Litgrid

LIETUVOS ORO UOSTAI VNO KUN PLQ

LIETUVOS BANKAS

KIBERNETINIO SAUGUMO EKSPERTŲ ASOCIACIJA

Kurk Lietuvai

NACIONALINIS KIBERNETINIO SAUGUMO CENTRAS

Daugiau informacijos rasite „KurkLt“ puslapyje: https://kurklt.lt/projektai/kibernetinis-saugumas-kaip-valstybe-galetu-padeti-uztikrinti-treciuju-saliu-kontraktoriu-valdyma


**Paulius Bagdonas**

„Kurk Lietuvai“ projekto vadovas

paulius.bagdonas@kurklt.lt

**Aurelija Požytė-Grinė**

„Kurk Lietuvai“ projekto vadovė

aurelija.pozyte@kurklt.lt