ESET SECURITY DAYS

ATSTATYMO PLANAS? DAR VIENA POLITIKA STALČIUJE, O GAL GALIMYBĖ AUGTI

Renata Karpavičė, nepriklausoma sukčiavimo prevencijos ir kibernetinio saugumo atitikties konsultantė, lektorė

Atstatymo planas

- [ ] Politika stalčiuje
- [ ] Strateginis pranašumas

Turėti planą ≠ pasiruošus

Reguliacija

- ✅ TIS2 (KSĮ)
- ✅ DORA
- ✅ BDAR
- ✅ KAA (CRA)
- ✅ ...

Reikalavimai

- 🔹 Reikalauja **incidentų valdymo planų**,
- 🔹 Periodinių **atsparumo testavimų**,
- 🔹 Aiškaus **atsakomybės paskirstymo**,
- 🔹 Kai kur – net **asmeninės vadovų atsakomybės**.

Organizacija

- ✋ Kas esate girdėję apie **incidentų valdymo planą**?
- ✋ O apie **verslo tęstinumo arba atstatymo planą**?
- ✋ Kas tokį **rengė**?
- ✋ Ir kas jį **testavo per pastaruosius 12 mėnesių**?

Turėti planą ≠ pasiruošus

60%

60% organizacijų tiki, kad gali atstatyti procesus per kelias valandas po incidento

35%

tik 35% organizacijų gali iš tikrųjų

25%

tik 25% organizacijų yra testavusios atstatymo planą kartą per metus ar rečiau

Šaltinis: The State of Backup and Recovery Report 2025

Incidentų valdymo planas ≠ atstatymo planas

86% kibernetinių incidentų buvo skirti verslo sutrikdymui – *Palo Alto Unit42, 2025*

	Incidentų valdymo planas (IRP)	Atstatymo planas (DRP)	Verslo tęstinumo planas (BCP)
Planai	**IRP**	**DRP**	**BCP**
Fokusas	Reaguoti į saugumo incidentus, juos valdyti ir sušvelninti	IT infrastruktūros, sistemų ir duomenų atkūrimas po incidento	Visos organizacijos kritinių verslo funkcijų tęstinumas
Tikslai	Greitai identifikuoti ir suvaldyti incidentą, mažinti žalą	Atkurti kritines IT sistemas, sumažinti veiklos prastovas	Užtikrinti verslo procesų veiklos tęstinumą kritinėmis situacijomis
Terminai	Trumpalaikis (valandos–dienos), pirmoji reakcija	Vidutinis terminas (dienos–savaitės), atkūrimo laikotarpis	Ilgalaikis (dienos–mėnesiai), bendro veiklos tęstinumo valdymas
Atsakomybė	IT saugumo komanda, incidentų valdytojai, kiti atsakingi asmenys	IT skyrius, infrastruktūros administratoriai, techninė komanda	Aukščiausio lygio vadovybė, procesų savininkai, visos organizacijos komandos

Reguliacija ≠ tik teisininkams

https://ecs-org.eu/activities/nis2-directive-transposition-tracker/

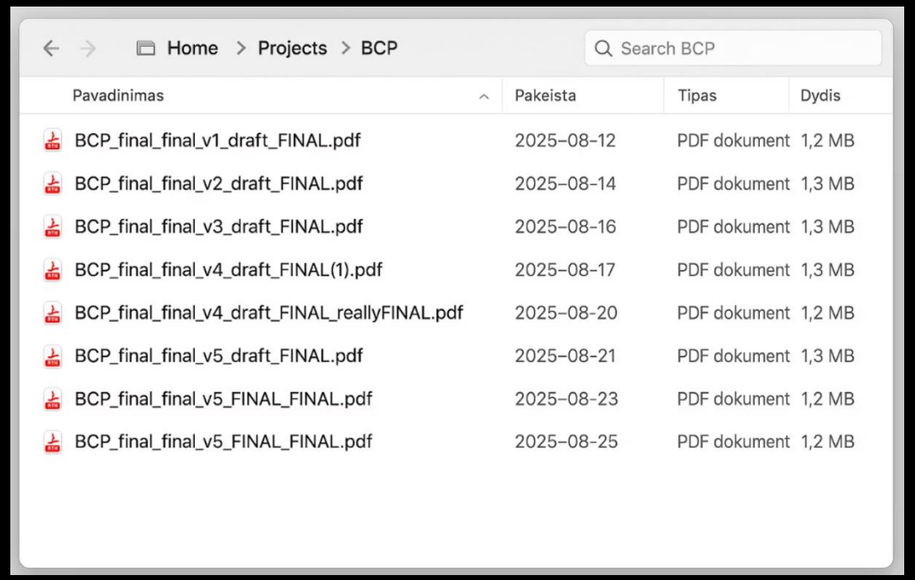
Reguliacija = darbas komandoje

- Ar reguliacija – tik teisininkų funkcija, ar visos organizacijos atsakomybė?
- Ką direktyvos ir reglamentai reiškia verslui?
- Kokie procesai yra kritiniai ir kaip jie apibrėžiami?
- Kiek prastovos laiko organizacija gali atlaikyti?
- Ar atliktas rizikų įsivertinimas?
- Kaip reguliacijos įgyvendinimą paversti organizacijos kultūros dalimi, o ne vienkartiniu projektu?

Reguliacija rodo kryptį. Bet tikras pasirengimas atsiranda tada, kai šie dokumentai tampa ne priedu, o kasdienės praktikos dalimi.

ATITIKTIS ≠ PASIRENGIMAS

☑ Varnelės neapsaugo nuo incidentų



- Kiek laiko vienas ar kitas procesas gali nevykti?
- Kur yra kritinė riba?
- Ar alternatyvios sistemos išbandytos?
- Ar atsarginės kopijos realiai išbandomos ir duomenys tikslūs?
- Ar komandos pasiekiamos? Ar kontaktai atnaujinti?
- Ar žmonės žino, ką daryti – ne tik teoriškai? O jei nėra vadovo?

INCIDENTAS – TIKRAS TESTAS

Turite atstatymo planą.
Bet…

- [ ] Kas jį aktyvuoja?
- [ ] Kur jis laikomas?
- [ ] Kas bendrauja su klientais? Su vadovybe? Su žiniasklaida?

INCIDENTAS – TIKRAS TESTAS

2024.07.19

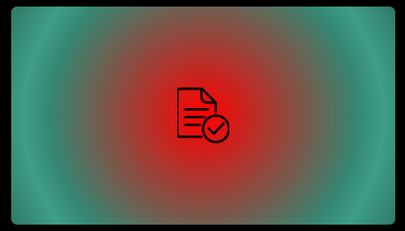
Crowdstrike Falcon – 1 klaida:

- 8,5 milijono įrenginių visame pasaulyje
- kiekvienas paveiktas įrenginys turėjo būti paleistas į atkūrimo režimą rankiniu būdu
- daugiau nei 10 milijardų USD nuostolių klientams
- CrowdStrike rinkos vertė nukrito daugiau nei 20 milijardų USD

Ar jūsų organizacija pasiruošusi tokiam scenarijui – kai tiekėjas tampa grėsme?

TESTAS PLANUI

Arba kaip atpažinti, kad planas veikia



„Nepopierinis”

Planą būtina išbandyti, įvertinti realiomis sąlygomis ir pritaikyti verslui.

Darbuotojai žino savo rolę

Darbuotojai žino ne tik ką daryti, bet ir ko nedaryti įvykus incidentui

Verslas įtrauktas

Kibernetinio saugumo rizikos valdymas yra organizacijos kultūros dalis

Geras planas gyvena organizacijoje. Jis nuolat atnaujinamas, peržiūrimas, pritaikomas – kai keičiasi produktas, paslauga, projektas ar partnerystė.

„Cybersecurity is not a problem to be solved. It's a risk to be reduced by working together." – Jen Easterly, CISA

Bendradarbiavimas

Komandų sinergija ir bendros pastangos

Informacijos dalinimasis

Grėsmių ir pažeidžiamumų apsikeitimas

Nuolatinis rizikos vertinimas

Reguliarus ir dinamiškas rizikos valdymas

Prevencinės priemonės

Tinklo ir sistemos saugumo užtikrinimas

Mokymai ir sąmoningumas

Darbuotojų elgesio ir žinių gerinimas

Vidinis bendradarbiavimas

Skatinkite komandų bendradarbiavimą ir atsparumo treniruotes.

Komunikacijos procesai

Tobulinkite komunikacijos procesus organizacijoje, ypač krizės metu.

Saugumo sąmoningumas

Nuolat didinkite darbuotojų kibernetinio saugumo sąmoningumą per mokymus ir kampanijas.

Reguliacija gali tapti pokyčio katalizatoriumi!

„NEXT SECURITY IS NOW"

It is not next, it is NOW.

Įvardinkite 3 svarbiausius procesus ir peržiūrėkite – ar jie testuoti?

Suorganizuokite l simuliaciją per artimiausias 30 dienų

Patikrinkite, ar dokumentuose nurodyti žmonės – **žino, ką daryti**

Ačiū!

vCard

Linkedin

Kibernetinis saugumas –
tai ne tik technologijos, bet ir kasdienės praktikos

Renata Karpavičė