

Valstybės rizika - įmonės rizika? Įmonės rizika - valstybės rizika?

Edvinas KERZA | VERSLO ATSPARUMO TARNYBOS VADOVAS



Turinys

01

Užsitvėriau tvorą, įjungiau signalizaciją. Ar aš jau saugus?

Gyvenimas yra dinamiškas, mane įtakoja išoriniai veiksniai

02

Praktiniai atvejai

Viena ataka gali „nušluoti“ įmonę?

03

Jei jau išlindau iš savo kiemo, ką daryti?

Informacijos daug, mūsų įmonę įtakoja daug veiksnių

04

Tai kaip gi suvaldyti rizikas?

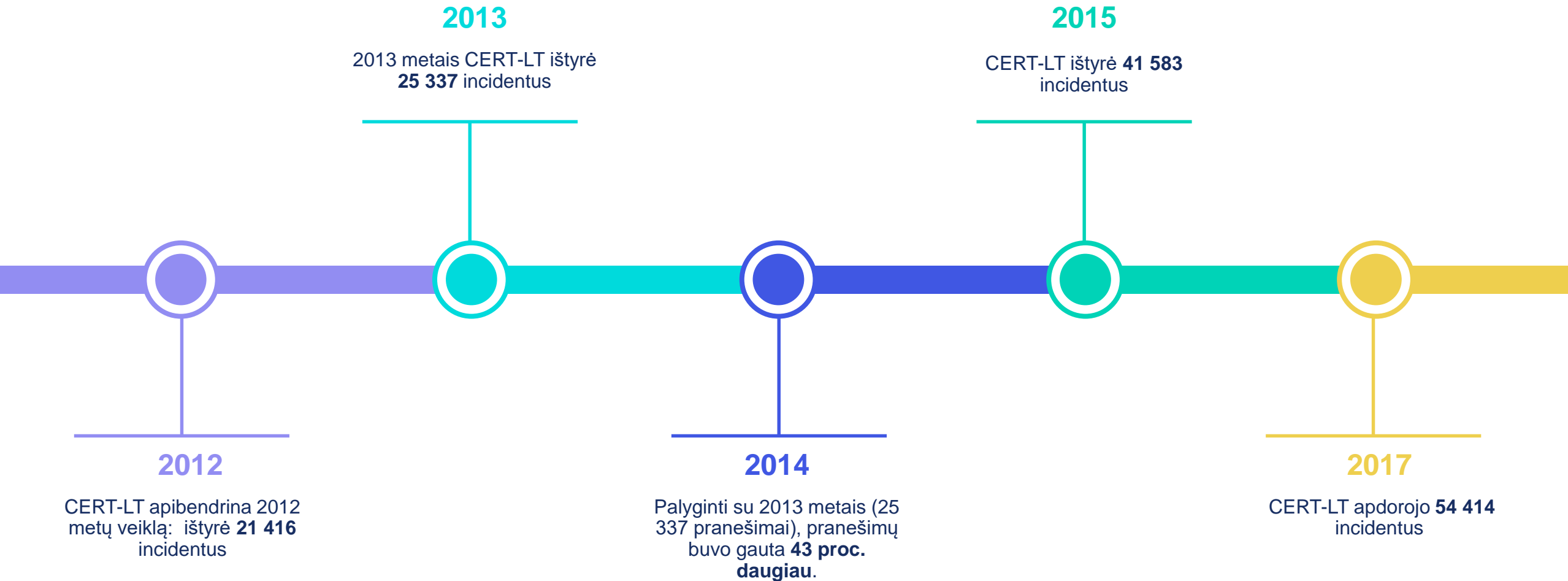
Gerosios praktikos, bendradarbiavimas, unikalūs sprendimai

05

Atsakymas

Kova su vėjo malūnais, ar vis dėlto prasmę turintis darbas?

Dinamiška aplinka



Gyvenimas iki COVID-19



Nuotolinis darbas – NEBE papildoma nauda, o standartas.



Atsižvelgiant į situaciją dėl koronaviruso plitimo, Vyriausybė šių metų kovo 15 d. neeiliniame posėdyje nutarė paskelbti karantiną visoje Lietuvos Respublikos teritorijoje.



Rizika – įmonę nušluos nuo žemės paviršiaus

... vienas valdybos narių, kuris papasakojo apie **2017** metais įvykusią kibernetinę ataką prieš bene didžiausią pasaulyje laivais krovinius gabenančią kompaniją. Nuo 10 iki 20 tūkstančių jūrinių konteinerių gabenančių laivų kas 50 minučių prisišvartuoja kažkuriame pasaulio uoste, tad akivaizdu, be informacinių technologijų logistika ir kita veikla čia neįsivaizduojama. Visi laivai taip pat aprūpinti technologinėmis priemonėmis.

Birželio 27 įmonė užfiksavo nejprastą veiklą, kuri per kelias valandas visiškai paralyžiavo kompaniją. Kiek vėliau nustatyta, kad tai Ukrainos programinę įrangą paveikusių viruso atvejis. Laivybos įmonės viduje buvo įdiegta ši PĮ - kaip ir kitose įmonėse dirbančiose su Ukraina. Duomenų vagystės hipotezė nepasiteisino, tikrasis **tikslas buvo jų užšifravimas ir sunaikinimas!** Rezervinės kopijos - jų turėjo, bet toli gražu ne viską ir ne pilna apimtimi. Atstatymas esamoje infrastruktūroje atrodė netikslingas, tad įmonė nusprendė viską įsigyti naujai ir pilnai įdiegti nuo nulio (panaudojant ką įmanoma iš rezervinių kopijų). Skaičiai įspūdingi - įsigijo 4000 serverių, 15000 kompiuterių, įdiegė 2500 pagrindinių aplikacijų. Visa tai kainavo tik apie **250-300 mln. dolerių.**

O juk jie net nebuvo pagrindinis taikiny, tai šalutinis poveikis!



You became victim of the PETYA RANSOMWARE!

The harddisks of your computer have been encrypted with an military grade encryption algorithm. There is no way to restore your data without a special key. You can purchase this key on the darknet page shown in step 2.

To purchase your key and restore your data, please follow these three easy steps:

1. Download the Tor Browser at "<https://www.torproject.org/>". If you need help, please google for "access onion page".
2. Visit one of the following pages with the Tor Browser:

```
http://petya[REDACTED].onion/g
http://petya[REDACTED].onion/g
```

3. Enter your personal decryption code there:

```
a6[REDACTED]
nF[REDACTED]y1
```

If you already purchased your key, please enter it below.

Key: _

e.sveikata dar neveikia

"Vis dėlto tai yra technologiniai dalykai, kurie, deja, bet ne visuomet priklauso nuo žmogiškųjų pastangų. Darome viską, kad sistema kuo greičiau pradėtų funkcionuoti"



Jei jau išlindau iš kiemo, ką daryti?



Bendradarbiavimas

Ar yra panašių į mane?
Valstybė yra partneris



Stebėsena

KRI
Viešų šaltinių analizė
Partnerių patirtys



Nauji atradimai, naujos galimybės

Ar tikrai turiu daryti kaip visi?
Gal geriau išlaukti?

Lietuva – drąsių žmonių šalis!



Cyber security index

Pasaulyje Lietuva iš 57 vietos pakilo į 4!



CRRT

Six European countries – Lithuania, Estonia, Croatia, Poland, the Netherlands and Romania – have united counter-cyber threat efforts in developing joint international rapid response capabilities.



AKVS diegimas

Standartų diegimas yra ne tik SIPA rodiklių gerinimas, tačiau ir rizikų valdymo instrumentas.



Verslo atsparumo tarnyba

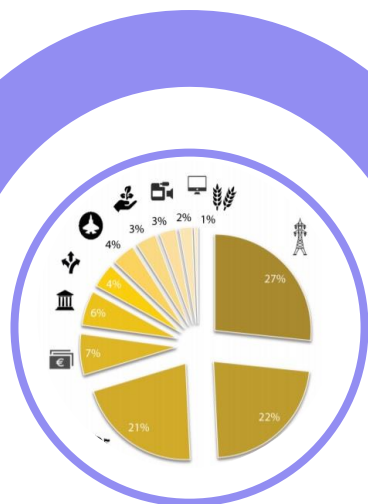
Prevencija, fizinė sauga, rizikos, atitiktis, ADA, veiklos tęstinumas, darbų sauga, aplinkosauga, kibernetinis saugumas, lyčių lygybė, etika

Rizikas valdyti ĮMANOMA

ENERGETIKA- TAIKINYS NR. 1

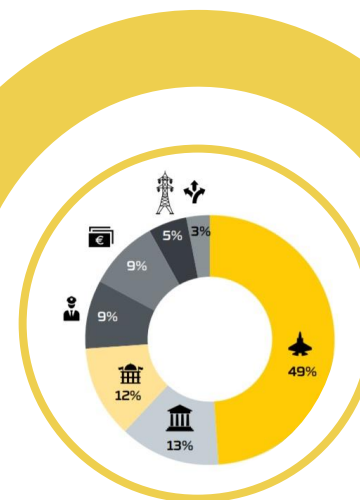
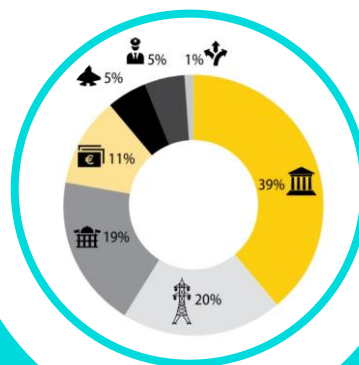
Daugiausia žalingos programinės įrangos veikimo atvejų užfiksavo energetikos sektoriuje – 27 %

Užfiksuotų atvejų sumažėjo iki 5 %



2017

2018



2019

Per metus nuo 27 % iki 20 %

Rizikas valdyti įmanoma!

