



Kibernetinis saugumas realybėje

dr. Donatas VITKUS
Ignitis grupės Skaitmeninės saugos vadovas

Veiklos segmentai

Kuriame energetiškai sumanų pasaulį



TINKLAI

Skirstymo valdymo sistemos
Išmanieji skaitikliai (~1,2 mln)
Duomenų mainų platforma

**Atsparus ir efektyvus
energijos skirstymas,
sudarantis prielaidas
energetikos pokyčiams**

~125.000 km elektros tinklų ilgis
~9.000 km dujotiekio tinklų ilgis



ŽALIOJI GAMYBA

Vėjo parkai
Saulės parkai
Hidro energija
Kogeneracinė energija

**Kryptinga, tvari ir pelninga
plėtra ne tik Lietuvoje, bet
ir užsienio rinkose**

1,6–1,8 GW instaliuota galia 2023 m.
4 GW instaliuota galia 2030 m.



LANKSČIOJI GAMYBA

Tretinis galios rezervas
Kitos sisteminės paslaugos
Komeracinė gamyba

**Patikima ir lanksti
energetikos sistema**

Elektrėnų kompleksas
455 MW kombinuotojo ciklo blokas



SPRENDIMAI KLIENTAMS

Nepriklausomas tiekimas
Elektromobilių įkrovimo
sprendimai
Nutolusių saulės ir vėjo parkų
platforma

**Sumanūs sprendimai
lengvesniam gyvenimui ir
energetikos vystymuisi**

Per 2,2 mln. privačių klientų Lietuvoje
>20 tūkst. verslo klientų Lietuvoje
Didžiausią rinkos dalį užimantis

Regioninė lyderystė



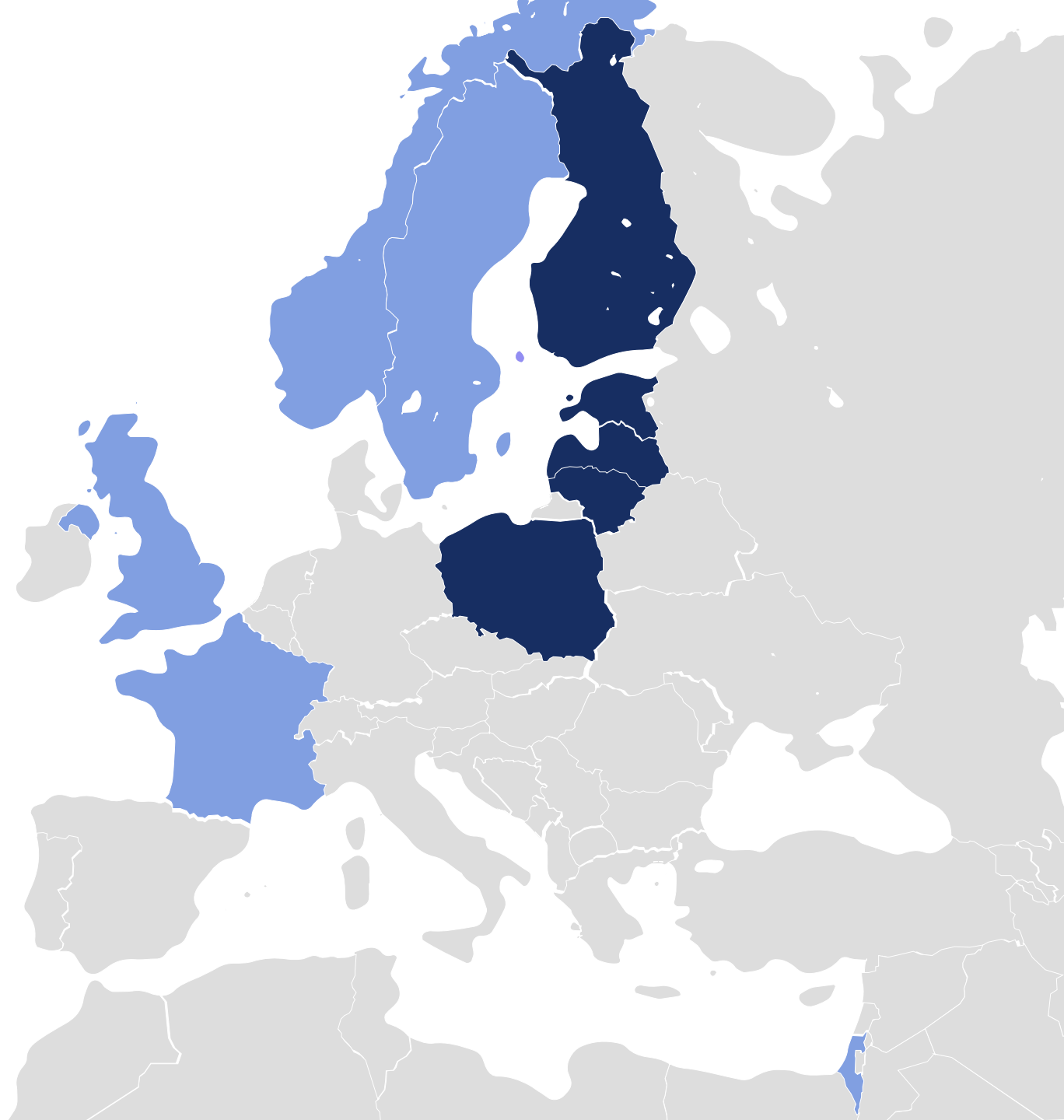
Veikla:

Lietuva, Latvija, Estija, Lenkija, Suomija



Investicijos į startuolius:

Norvegija, Švedija, Jungtinė Karalystė, Prancūzija, Izraelis



Kibernetinis saugumas energetikos sektoriuje

2022

The subdivision Sea-Tank in Belgium had to stop all operations for 2 days. Activities at ports were stopped.

2022

About 2,000 wind turbines in Germany were down for a day following the attack.

2023

22 energy companies breached in Denmark's critical infrastructure

90%

90% of the world's 48 largest energy companies experienced a third-party breach in the past 12 months *(according to SecurityScorecard)*

100%

All (100%) of the top 10 US energy companies experienced a third-party breach in the past year.



Danijos kritinės infrastruktūros atakos



2023-04-25

Zyxel announced that a critical vulnerability had been found in a number of their products (FW)

2023-05-01

Denmark's SektorCERT issued an additional warning to install the latest update

2023-05-11

First wave of attacks (11 attacks)

2023-05-22/25

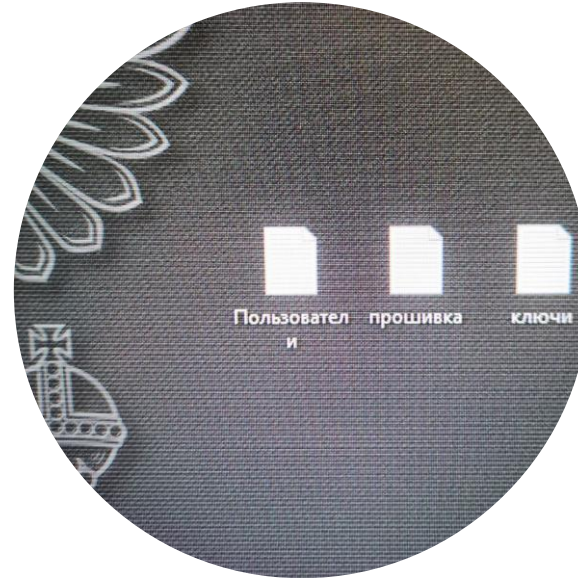
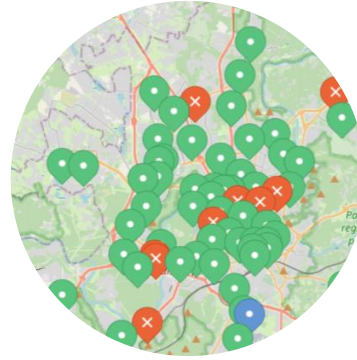
Second wave of attacks (+11 attacks)

2023-05-25

Attack handled. Denmark's SektorCERT share information about attacks

EV įkrovimo atvejis

- ~20K el. pašto adresų, iš jų ~1,6K leidžia identifikuoti asmenį
- ~2 val. EV įkrovimo stotelių trikdymas
- ~20 klientų skambučiai dėl veiklos sutrikimų
- ~6,5k RFID žetonų, iš jų 1,3K buvo naudoti mėnesį prieš
- ~100 užklausų dėl asmens duomenų



JUST EVIL

⚠ IGNITIS GRUPE y Vas 2 часа!
Я отключил уже 1000 человек.
Каждые 10 минут, удаляю по 1000 человек!

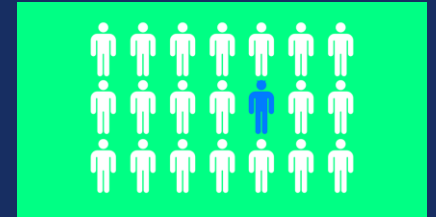
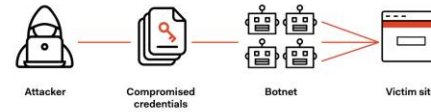
⚠ IGNITIS GRUPE You have 2 hours!
I have already disconnected 1000 people. Every 10 minutes, I delete 1000 people!



71 Million Leaked Credentials From Naz.API Stolen Account List Added to Have I Been Pwned

SCOTT IKEDA · JANUARY 22, 2024

Anatomy of a credential stuffing attack



NEWS

Password-stealing Chrome extension smuggled on to Web Store

Kaip tai galėjo pavykti?

Use passwords across your devices

You can sign in to apps and sites on different devices using passwords saved to your Google Account when you either:

Ne taikinyš, o priemonė – socialiniai tinklai

kad sukčiai intensyviai naudojosi „Ignitis“ prekės ženklu:

- 14 „Facebook“ paskyrų, kurios apsimeta „Ignitis“
- 22 „Facebook“ reklamos, kurias sukčiai leido iš netikrų „Ignitis“ paskyrų
- 122 Reklamos, kuriose minimas „Ignitis“, o vartotojas nukreipiamas į išgalvotą straipsnį. Jame siūloma investuoti į neegzistuojančią įmonę „Ignitis profit sense“
- 1,33 M Kartų šios reklamos parodytos „Facebook“ vartotojams



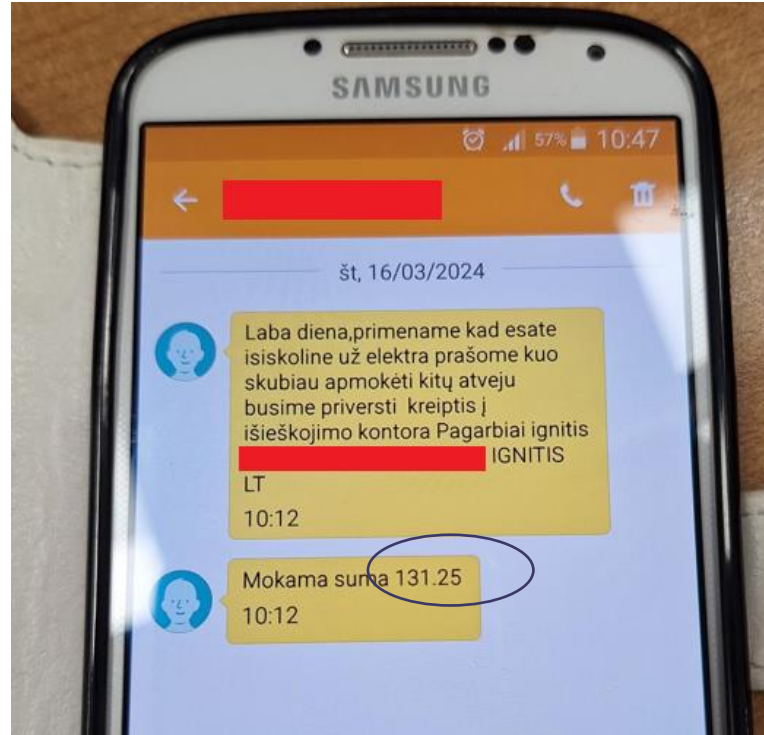
Kaip Jūs manote, ar tai buvo mūsų neapgalvota bendrovės strategija, kuri privedė prie kraupios nelaimės? Mes turime paaiškinimą



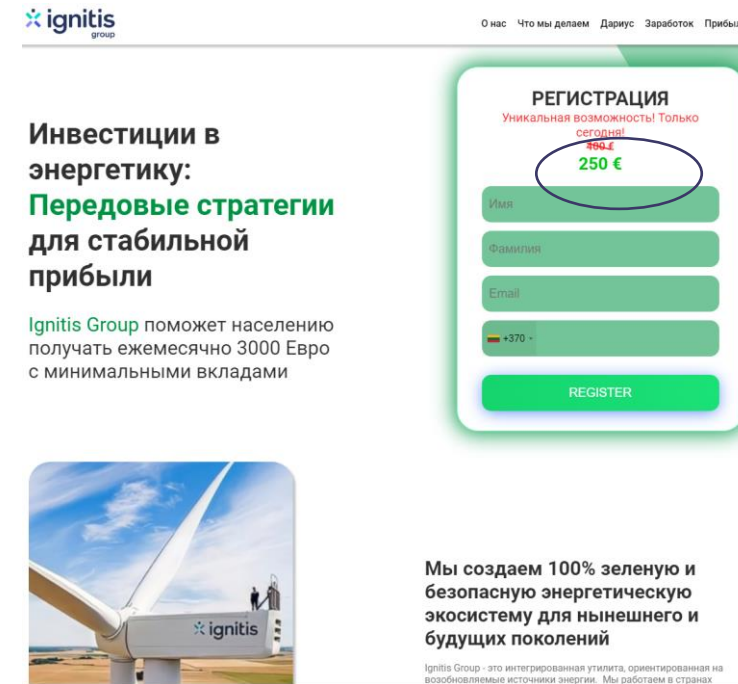
Kaip Jūs manote, ar tai buvo mūsų neapgalvota bendrovės strategija, kuri privedė prie kraupios nelaimės? Mes turime paaiškinimą



Ne taikiny, o priemonė – *sukčiavimas*



Sukčiau jama prisidengiant Ignitis vardu SMS žinutėmis



Netikri WEB puslapiai

Tendencijos

- Ransomware platinimas
- Slaptažodžių vagystės
- Dirbtinio intelekto panaudojimas
- Mažėja apetitas – dingsta *per daug gerai, kad būtų tiesa* efektas
- Deepfake panaudojimas

Patarimai

- Kibernetinių incidentų valdymo pratybos, pratybos, pratybos...
- Komunikacijos personalo įtraukimas vos tik įvykus reikšmingam incidentui
- Teisininko/DPO įtraukimas
- Darbuotojų švietimas, švietimas, švietimas...
- Trečiųjų šalių rizikos valdymas
- Kibernetinės saugos kultūros diegimas/higiena
 - Kelių faktorių autentifikacija visose sistemose
 - Reguliarus slaptažodžių keitimas
 - Patikimos slaptažodžių tvarkyklės
 - Reguliari paskyrų peržiūra



Dėkoju už dėmesį