
FOX IT
part of ncc group

FOX IT
part of ncc group

Hoe de energiesector wordt aangevallen

Een technische benadering

Presentatie voor Dutch Power
10 maart 2026

Together we're creating a more secure digital future

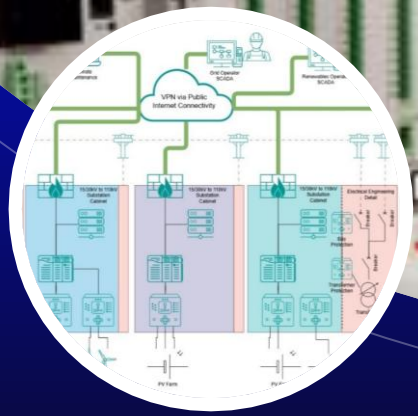
Commercial.restricted

Agenda

Aanvallen
Chris van den Hooven

Demo
Hendrik Schimmelpenninck van der Oye

Wat te doen
Chris van den Hooven



Aanval eind 2025 in Polen

Energie infrastructuur als doelwit

Op 29 december 2025 vonden er in de ochtend- en middaguren gecoördineerde aanvallen plaats in de Poolse cyberspace.

Ze waren gericht op meer dan **30 wind- en zonneparken**, een particulier bedrijf uit de productiesector, en een grote **gecombineerde warmte- en elektriciteitscentrale** die warmte leverde aan bijna een half miljoen klanten in Polen.

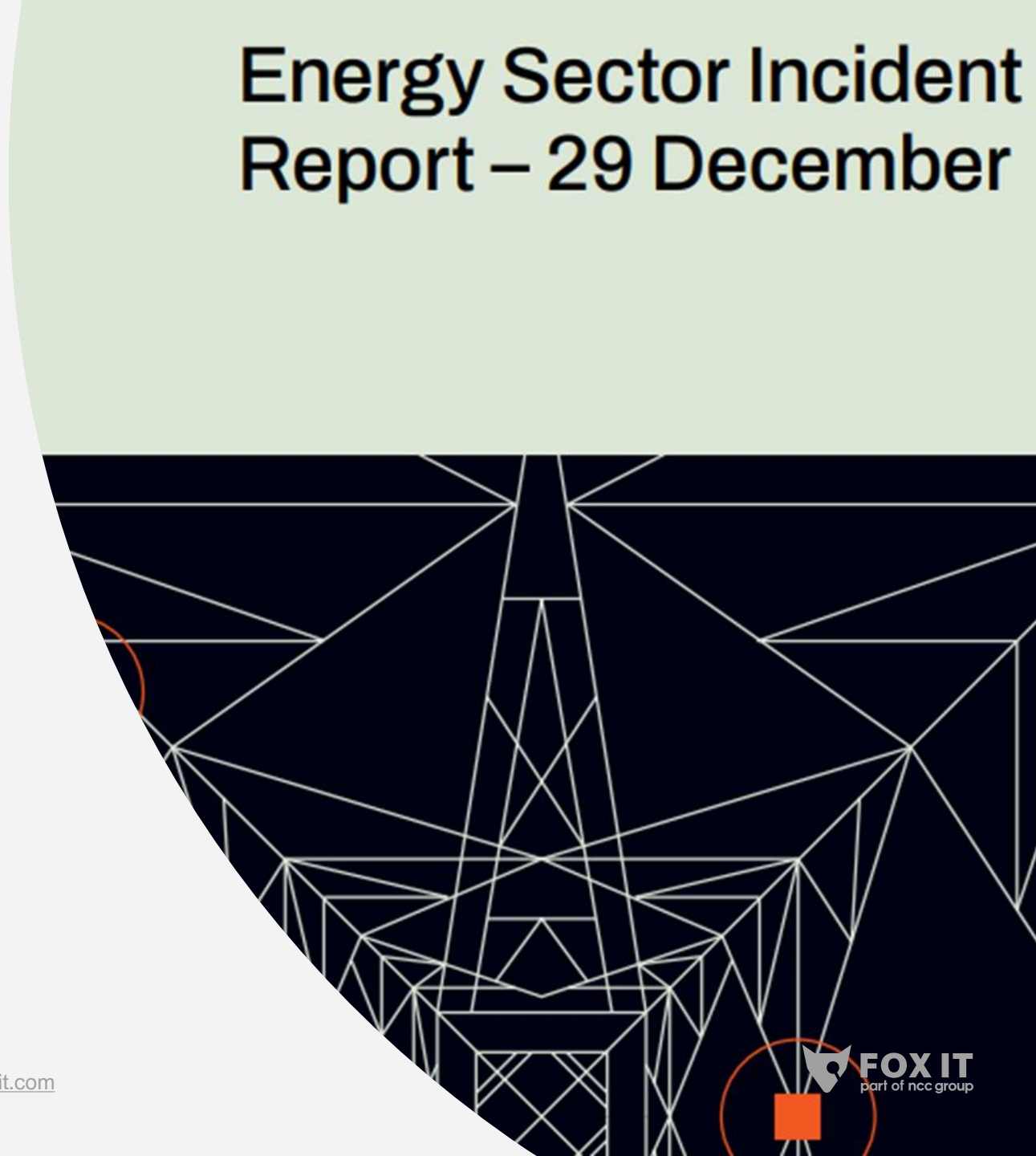
Picture: Hitachi Relion RTU560

Rapport CERT.PL

Energie infrastructuur als doelwit

CERT Polska

(CERT.PL) – a team operating within the structures of NASK – National Research Institute, carrying out the tasks of CSIRT NASK, one of the three national-level CSIRT teams operating within Poland’s national cybersecurity system



Picture: Report CERT.PL

Aanval op GCP (Grid Connection Point)

Zonneparken/windparken

01

FortiGate

- Gebruik gemaakt van een (remote code execution?) vulnerability voor het omzeilen van MFA
- Hergebruik van username/password
- Leidde tot VPN-toegang naar alle subnets

02

Hitachi RTU

- Default credentials actief
- Aanvaller uploaded corrupte firmware die resulteerde in een reboot-loop

03

Mikronika RTU

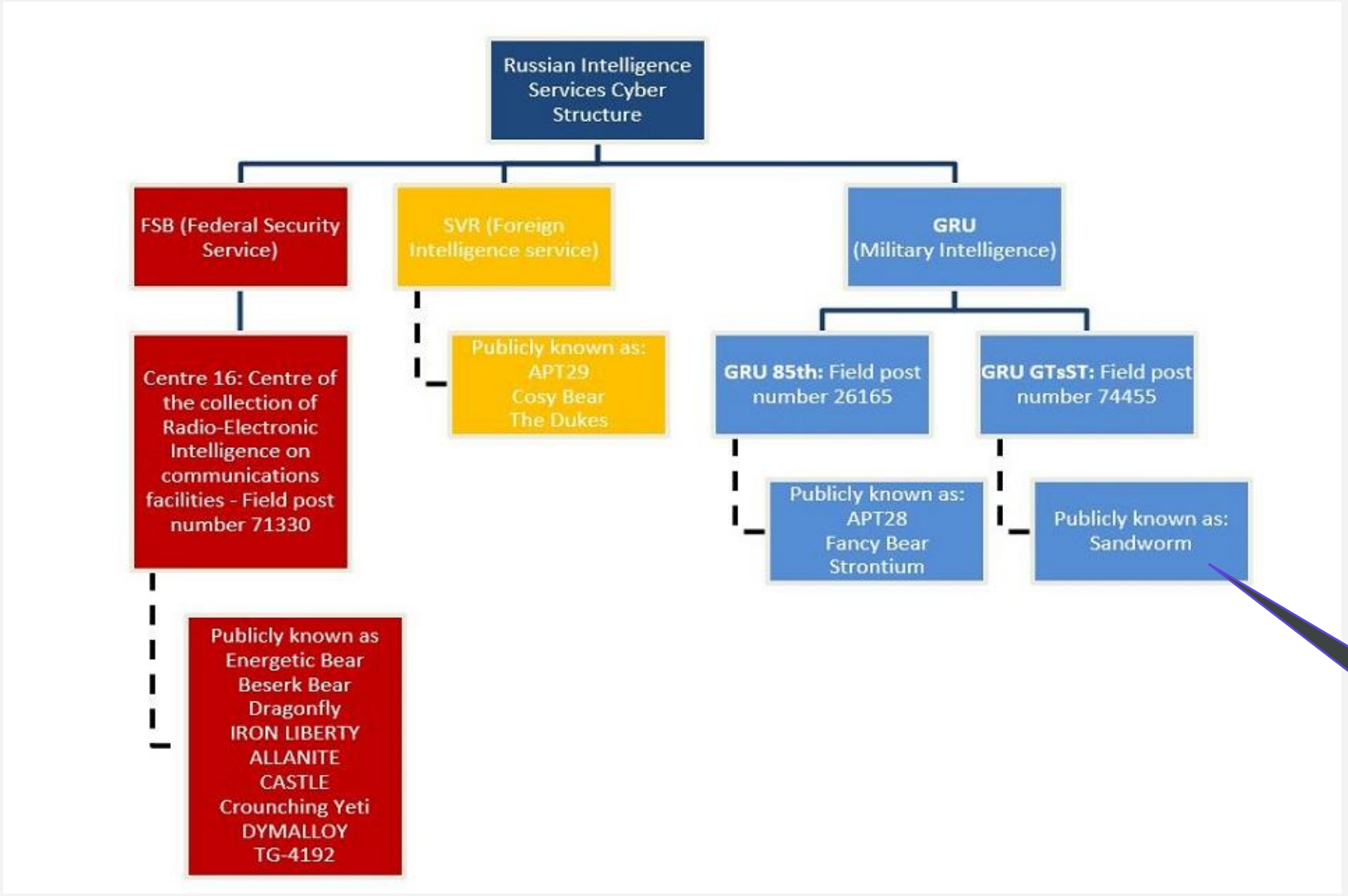
- Deze RTU is gebaseerd op Linux
- SSH met default credentials was actief
- Aanvaller heeft files gewist

04

Hitachi IED

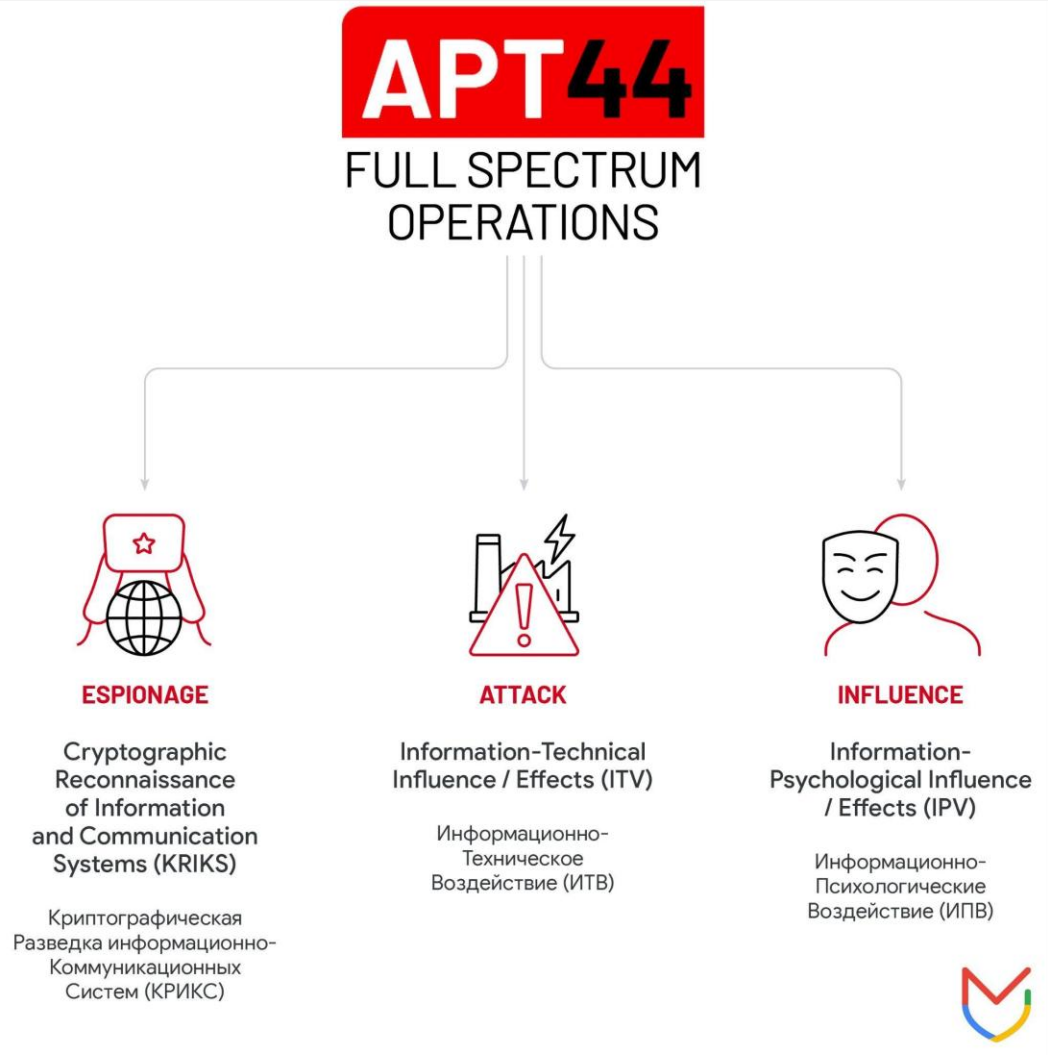
- FTP met default credentials was actief
- Aanvaller heeft files gewist

Organisatie van de aanvaller



Electrum wordt geassocieerd met Sandworm (APT44)

Organisatie van de aanvaller



- Mandiant heeft vastgesteld dat APT44 spionageoperaties uitvoerde in Noord-Amerika, Europa, het Midden-Oosten, Centraal-Azië en Latijns-Amerika.
- APT44 richt zich voornamelijk op defensie-, transport-, energie-, media- en maatschappelijke organisaties in de buurt van Rusland. APT44 richt zich ook vaak op overheidsorganisaties en andere kritieke infrastructuuroperators in Polen en Kazachstan, evenals binnen Rusland.
- APT44 heeft "herhaaldelijk westerse kiessystemen en -instellingen aangepakt, waaronder die in huidige en toekomstige lidstaten van de NAVO."

Bron: Unearthing APT44: Russia's Notorious Cyber Sabotage Unit Sandworm | Google Cloud Blog

Organisatie van de aanvaller

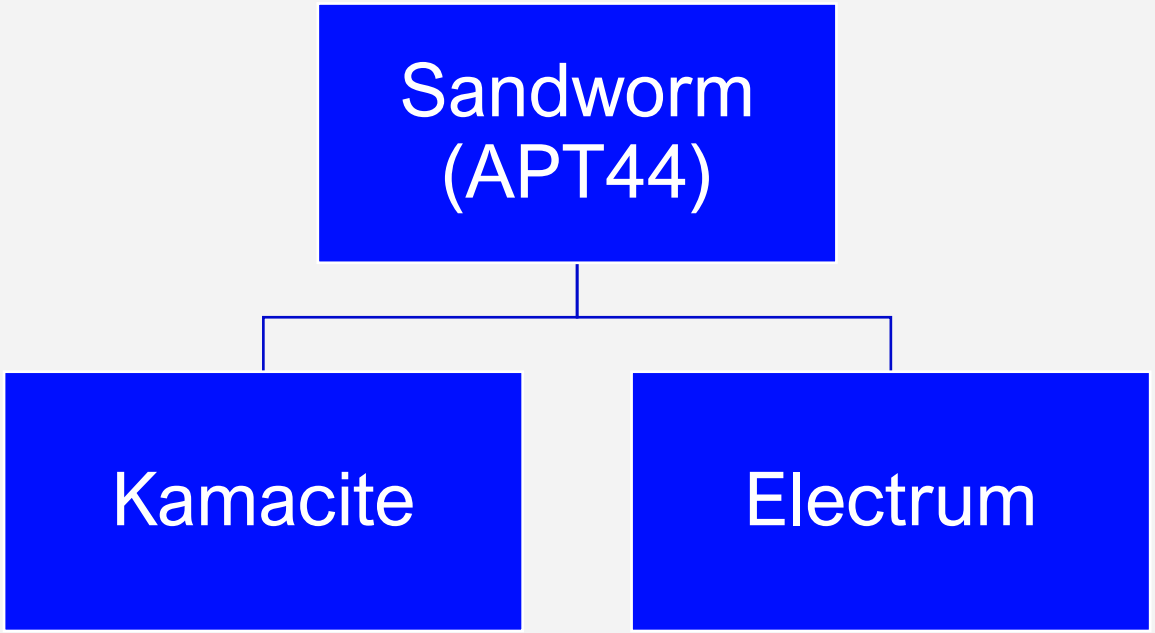
Sandworm (APT44)

Als onderdeel van de Russische militaire inlichtingendienst (GRU) is APT44 een dynamische en operationeel volwassen dreigingsactor, actief betrokken bij het volledige spectrum van spionage-, aanval- en beïnvloedingsoperaties.

Kamacite
Toegang tot stand brengen en behouden

Electrum

Voer acties uit op het doel



Aanval op CHP (Combined Heat and Power)

01

FortiGate and Jumphost

- Gebruik gemaakt van username/password (accounts zonder MFA)
- Toegang tot jumphost via RDP. Credentials daarvan waren opgeslagen in de FortiGate.

02

Aanval Domain controller

- Reverse SOCKS proxy tunnel opgezet
- Edge gebruikt om software te downloaden
- Impacket gebruikt
- Lsass of memory dump
- Rubeus tool gebruikt
- Diamond Kerberos ticket gemaakt

03

Zoeken SCADA hosts

- Windows gebaseerd
- Met in de naam “SCADA”
- Screenshots gemaakt
- Tasklist, netstat, etc.

04

Vernietigen Windows

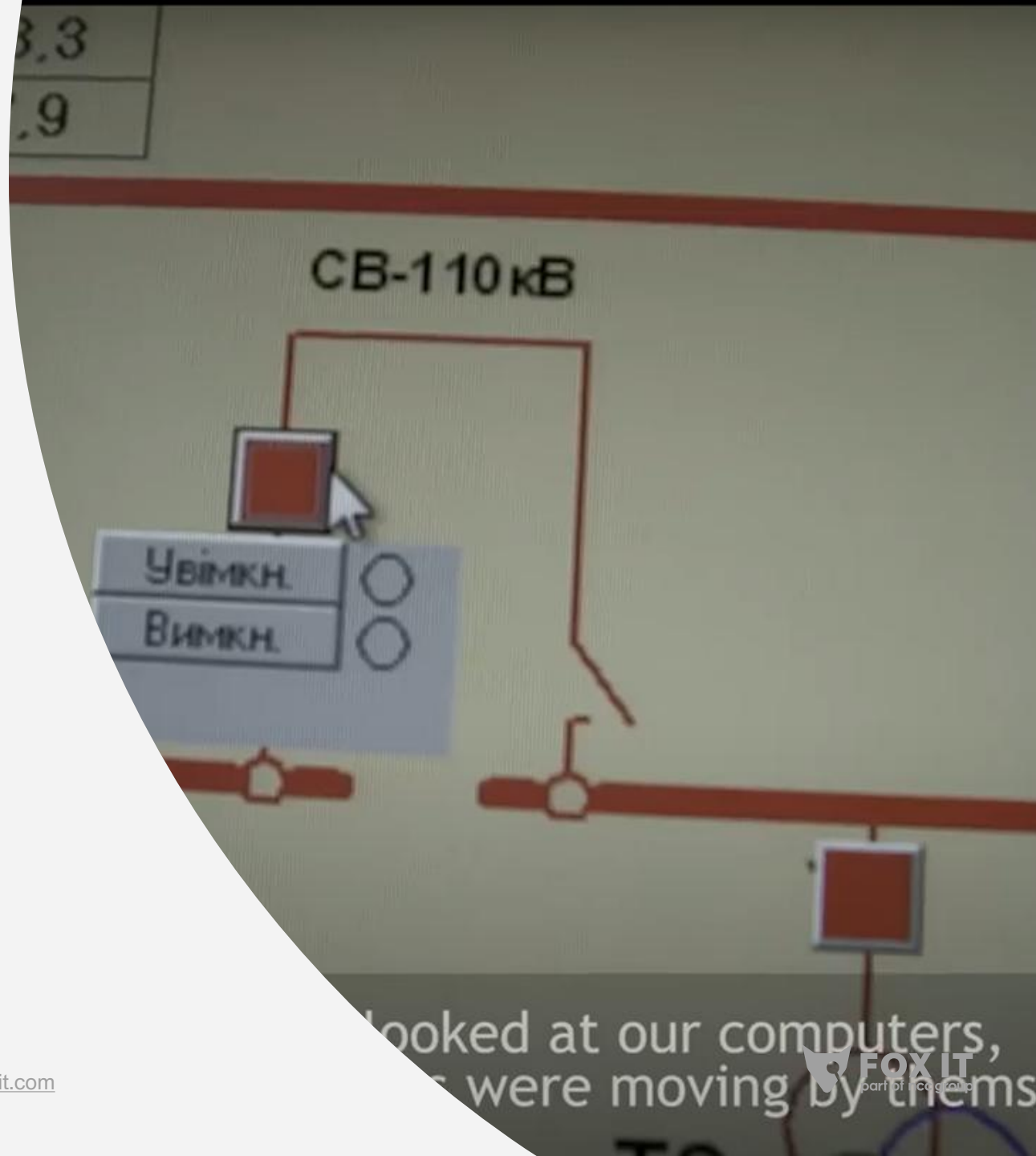
- DynoWiper
- EDR heeft het overschrijven van files op meer dan 100 machines geblokkeerd.

- Eerste acties in **maart** en mei 2025
- In **juli** is een dump van de Active Directory gemaakt
- Onvoldoende logging beschikbaar voor volledige reconstructie

Aanval 2015 in Oekraine

Energie infrastructuur als doelwit

Toegeschreven aan de Russische APT-groep Sandworm, moet de aanval worden gezien in de context van een tijdelijke pauze in de voortdurende Russisch-Oekraïense oorlog, die begon met de annexatie van de Krim en de oorlog in Donbas.



Afbeelding: What happens when a power plant comes under cyber attack?
from the NATO YouTube channel

Aanval op 30 elektriciteitscentrales

01

Spear Phishing

- Word-marcro's
- BlackEnergy3 geinstalleerd (RAT)
- Verspreiden Killdisk (niet op SCADA)
- VPN gegevens buitgemaakt

02

Inventarisatie

- Malware verspreid
- Verzamelen van login gegevens
- Keylogger
- VPN, Workstations, Domain Controller

03

Verplaats naar OT

- Gebruik gemaakt van malware in combinatie met buitgemaakte accounts
- Vernietig RTU, IED, serial2IP, etc

04

Ondersteunende systemen

- Telefonie
- Callcenter (TDoS)
- UPSsen

Demo

FOX IT
part of ncc group

Wat kun je doen?

Together we're creating
a more secure digital future

National Cyber Security Centre

10 Steps to Cyber Security

Defining and communicating your Board's Information Risk Regime is central to your organisation's overall cyber security strategy. The National Cyber Security Centre recommends you review this regime – together with the nine associated security areas described below, in order to protect your business against the majority of cyber attacks.

Network Security

Protect your networks from attack. Defend the network perimeter, filter out unauthorised access and malicious content. Monitor and test security controls.

User education and awareness

Produce user security policies covering acceptable and secure use of your systems. Include in staff training. Maintain awareness of cyber risks.

Malware prevention

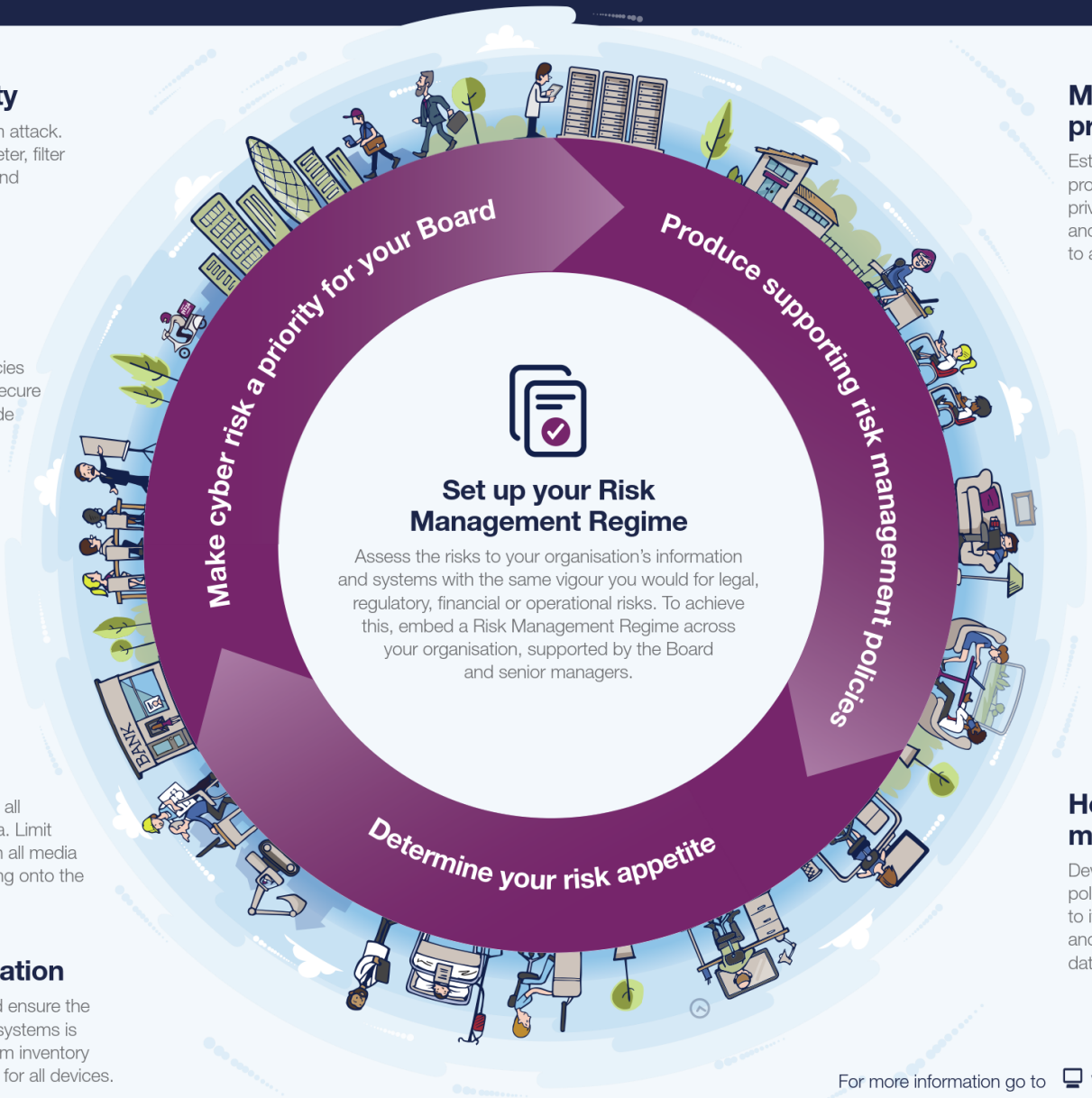
Produce relevant policies and establish anti-malware defences across your organisation.

Removable media controls

Produce a policy to control all access to removable media. Limit media types and use. Scan all media for malware before importing onto the corporate system.

Secure configuration

Apply security patches and ensure the secure configuration of all systems is maintained. Create a system inventory and define a baseline build for all devices.



Managing user privileges

Establish effective management processes and limit the number of privileged accounts. Limit user privileges and monitor user activity. Control access to activity and audit logs.

Incident management

Establish an incident response and disaster recovery capability. Test your incident management plans. Provide specialist training. Report criminal incidents to law enforcement.

Monitoring

Establish a monitoring strategy and produce supporting policies. Continuously monitor all systems and networks. Analyse logs for unusual activity that could indicate an attack.

Home and mobile working

Develop a mobile working policy and train staff to adhere to it. Apply the secure baseline and build to all devices. Protect data both in transit and at rest.

For more information go to www.ncsc.gov.uk @ncsc

FOX IT part of ncc group

OT detectie uitdagingen

5	**Enterprise Network** Not directly controlling industrial processes, but uses data from production	Corporate / data center network	Web server	DNS server	Mail server	User Endpoints	NDR	
4	**Site Business Planning & Logistics** Coordinates production schedules, material flows and business objectives							
3.5	**Industrial DMZ** The IDMZ is crucial to minimise attack surface and safely bridge IT-OT data flows	Patch server	Historian server	Jump server			NDR For OT	
3	**Operations/ Industrial Control Systems** Acts as the brain overseeing process control systems below	Workstation	Historian	I/O server				
2	**Control Systems** Automatic control of production equipment, process automation	SCADA	HMI	Remote Jump Server				OT Only Sensors
1	**Intelligent Devices** Converting physical processes into digital data and vice versa	PLCs	RTUs					
0	**Physical Processes** The physical world: sensors, actuators	Sensors	Actuators					

NDR **NDR for OT** **OT Only Sensors (with Partners)** = **Full coverage**

Hendrik Schimmelpenninck van der Oye
Executive Consultant | Fox-IT
e: schimmelpenninck@fox-it.com
p: +31 (0)85 799 0680
m: +31 (0)6 4190 1021
w: www.fox-it.com
LinkedIn

Chris van den Hooven
Executive Consultant | Fox-IT
e: chris.vandenhooven@fox-it.com
p: +31 (0)85 799 0680
m: +31 (0)6 41244346
w: www.fox-it.com
LinkedIn

Thank you.

Together we're creating a more secure digital future