Introduction

HUNT & HACKETT

OUTSMART YOUR DIGITAL ADVERSARIES

SOPHIE VAN DER WERF & MARCEL VAN OIRSCHOT

Tomorrow will be too late

DIGITALE AFHANKELIJKHEID

BEHEER

SECURITY

Hackaanval op Italiaans energiebedrijf Eni

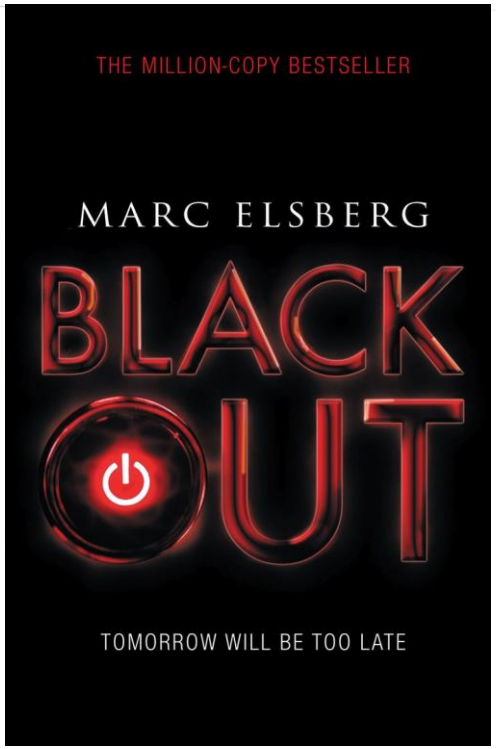
Ongeautoriseerde toegang tot bedrijfssystemen gedetecteerd.

© Eni

1 SEPTEMBER 2022

De computernetwerken van de Italiaanse oliemaatschappij Eni zijn de afgelopen dagen gehackt. De gevolgen lijken tot nu toe echter mee te vallen, zei het bedrijf woensdag.

Volgens een woordvoerder detecteerden de interne beschermingssystemen van het bedrijf de afgelopen dagen "ongeoorloofde toegang" tot het bedrijfsnetwerk. Het door de staat gecontroleerde bedrijf werkt samen met de autoriteiten om de gevolgen van de aanval te beoordelen.



bert hubert Retweeted

Bart Groothuis @bgroothuis · 6h

Gisteren liet de AIVD weten dat Russische hackers recent Nederlandse energie infrastructuur op zee als doelwit hadden, met het oog op sabotage. Vandaag laat de BBC weten dat een Russisch sabotageschip Nederlandse windparken heeft bezocht tussen 17-19 november. Alle hens aan dek!

> **Bart Groothuis** @bgroothuis · 6h
> This Russian 'commercial' ship preparing to sabotage offshore wind and internetcables in the North Sea is a huge deal. So: follow, hinder, inspect, move close, annoy, collect data, refuse access to our ports, refuse visa: we cannot allow this!
> bbc.com/news/world-eur...

4 38 61 10K

---- GEOPOLITIEK

Motivatie?

Politieke destabilisatie/informatie:

- Onderzoekschip Admiral Vladmirsky
- Afhankelijkheid groene energie
- Nordstream?

Financiele gewinning:

- Ransomware

Kennis:

- Diefstal van intellectueel eigendom
- Universiteiten

Attacks/Breaches | 9 MIN READ | NEWS

Lights Out: Cyberattacks Shut Down Building Automation Systems

Security experts in Germany discover similar attacks that lock building engineering management firms out of the BASes they built and manage — by turning a security feature against them.

Kelly Jackson Higgins
Editor-in-Chief, Dark Reading

December 20, 2021

Wat is er aan de hand?

Meer en meer omvormers zijn uitgerust met wifi. Om ze in te stellen, hebben ze een wifi access point. Dat betekent dat wanneer u in de buurt bent en op uw smartphone, tablet of PC zoekt naar beschikbare wifi netwerken, het wifi netwerk van de omvormer ook in beeld komt.

Als u erin slaagt om bijvoorbeeld uw PC met het wifi netwerk van de omvormer te verbinden, dan zou u in de omvormer in kunnen loggen. Als u in de omvormer kunt inloggen, zou u eventueel het wifi wachtwoord en de netwerknaam van het thuisnetwerk kunnen achterhalen. Dan zou u daarin in kunnen loggen en allerlei nare malware in het thuisnetwerk kunnen

NOS Nieuws • Maandag 12 juli 2021, 07:46

'Hackers kunnen stroomnet saboteren via zonnepaneel en laadpaal'

De overgang naar een duurzame energievoorziening maakt het Nederlandse stroomnetwerk kwetsbaarder voor hackers. Zij kunnen bijvoorbeeld zonnepanelen en laadpalen hacken, waardoor het hele netwerk uit balans kan raken en kan uitvallen. Daarvoor waarschuwt het Agentschap Telecom (AT) in het FD.

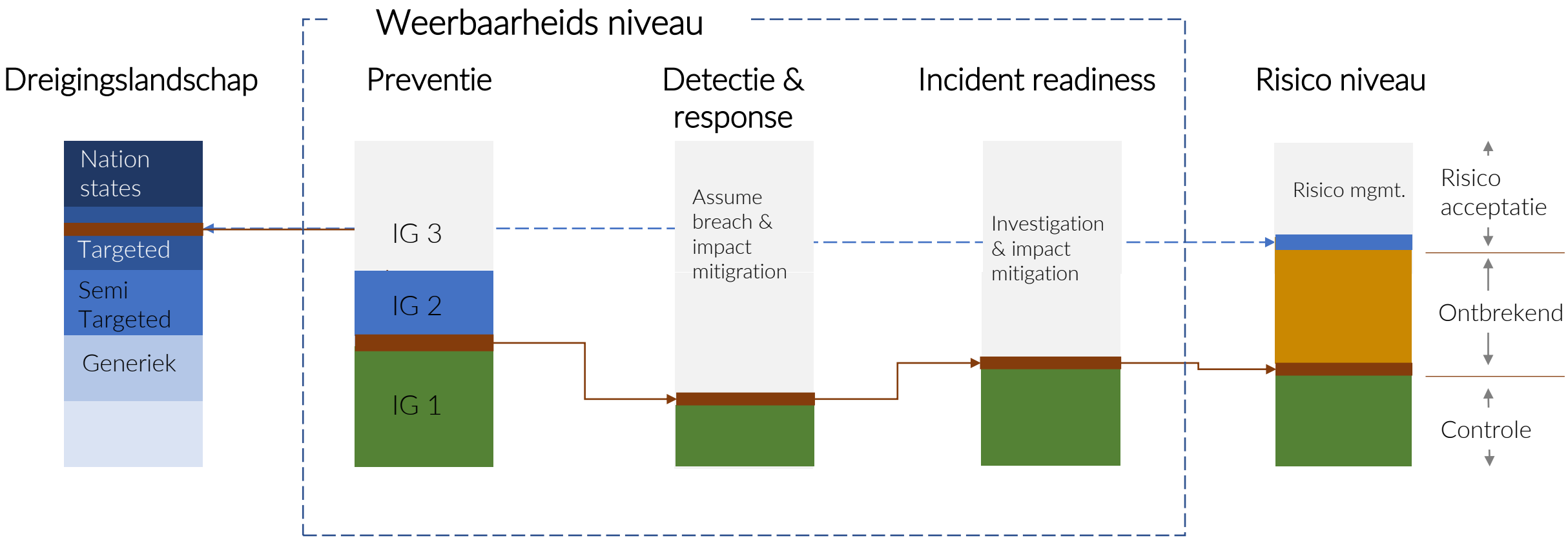
Volgens Angeline van Dijk, directeur van het AT, zijn producenten, gebruikers en leveranciers van nieuwe diensten en zogenoemde slimme apparatuur als laadpalen zich onvoldoende bewust van dat risico. "De manier waarop we de

Hackers treffen het ene Europese energiebedrijf na het andere

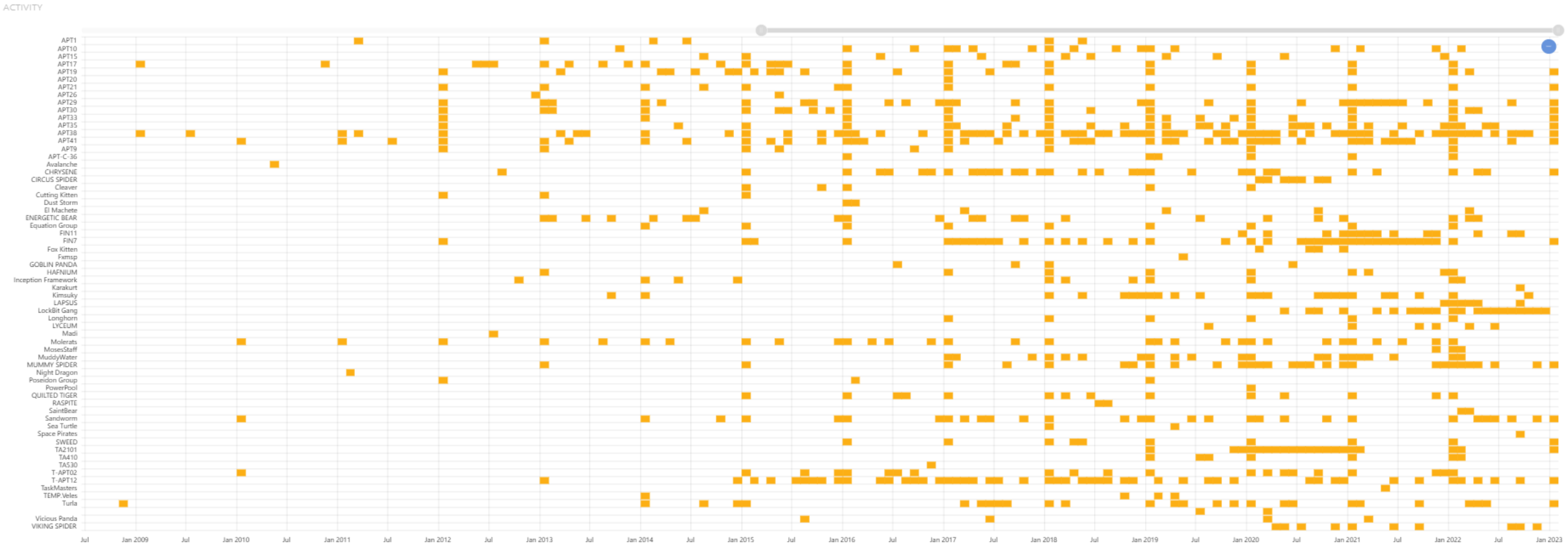
Verscheidene Europese gas- en elektriciteitsbedrijven kregen onlangs een aanval met gijzelsoftware te verwerken. Meer dan eens zaten daar Russische criminelen achter, en die lijken uit op meer dan geld.

Nikolas Vanhecke
Donderdag 15 september 2022 om 3.25 uur

Cybersecurity risicoacceptatie



Toename aantal actoren



HUNT & HACKETT

OUTSMART
YOUR DIGITAL
ADVERSARIES