Kamer van Koophandel Antwerpen-Waasland Alfaport

Inspiratiesessie: Cyber Resilience Awareness

7 oktober 2024

"Onze technologische vermogens nemen toe, maar daarmee ook de bijwerkingen en potentiële gevaren."

Alvin Toffler, Future shock

Situatieschets:

In 2023 kreeg 46% van de Belgische bedrijven te maken met minstens één cyberaanval.

39% van de bedrijven verwacht in 2024 slachtoffer te worden van een cyberaanval.

En toch is slechts 27% van deze bedrijven goed voorbereid op cyberincidenten.

Wat met havensector?

Programma

Aanpak cyberaanval stad Antwerpen, Youri Segers

Van Moer Logistics werkt aan cyberweerbaarheid, Joris Emanuel

Koffiepauze

Verborgen gevaren: wat het darknet onthult over Antwerpse havenbedrijven, Geert Baudewijns

Voorstelling van de rol en werking van de Belgian-Port ISAC op gebied van cyberveiligheid binnen de havencommunity, Nick Van Den Bergh

Van cyberaanval naar cyberfort

Alfaport Voka| Cybersecurity

7 oktober 2024

Youri Segers

CDO Stad Antwerpen
CEO Digipolis Antwerpen

- Groep stad Antwerpen
  - ca. 10.000 medewerkers
  - stadsdiensten, autonome gemeentebedrijven en vzw’s (VB PZA, BZA, AGSO, ZBA)

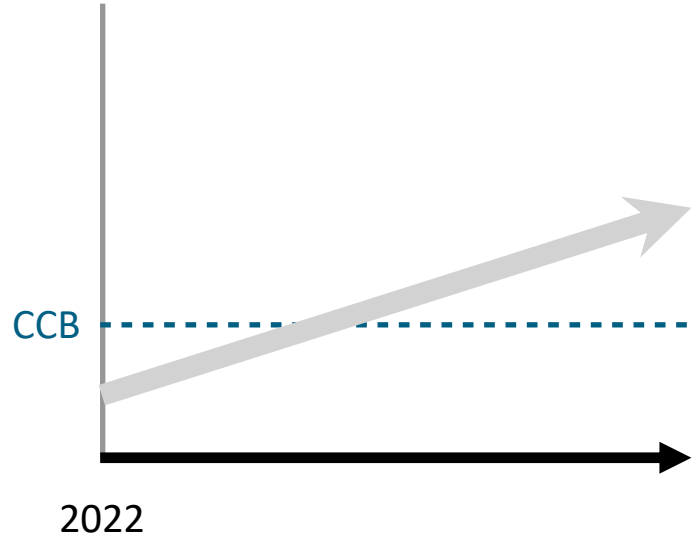
- AG Digipolis Antwerpen
  - IT voor het stedelijke netwerk (100% stedelijke diensten + delen van AG’s)
  - ca. 300 interne medewerkers en 150-tal consultants

Ons verhaal

Van cyberaanval naar cyberfort

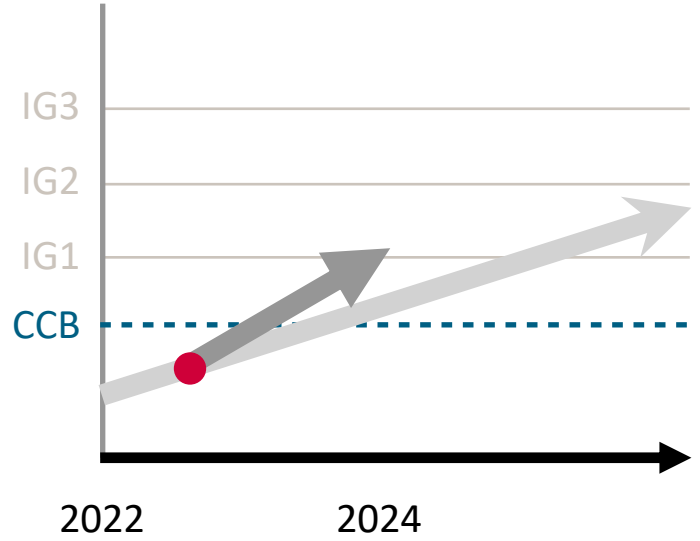
Cyberveiligheidsprogramma 1.0

- 10 noodzakelijke veiligheidsacties van Centrum voor Cybersecurity België
- 2024: niveau ‘minimale veiligheid en weerbaarheid’
- Een race tegen de tijd…



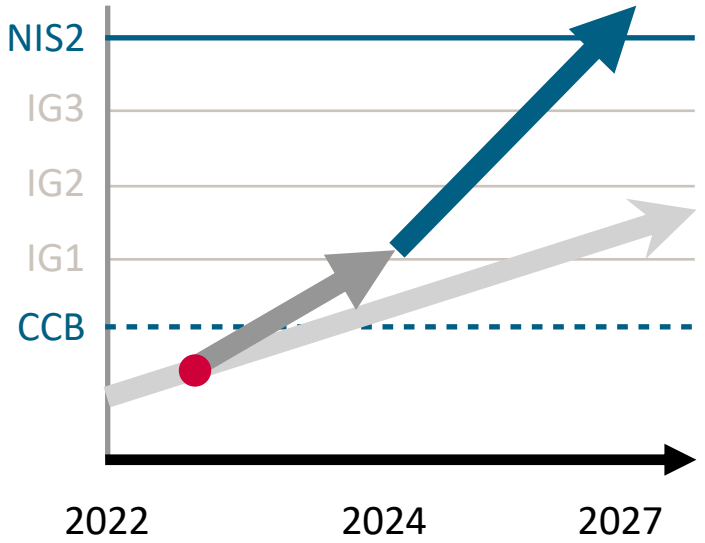
Cyberveiligheidsprogramma 3.0

- 6 december 2022: cyberaanval
  - Volgens gekende technieken
  - Enorme impact op dienstverlening stad Antwerpen
  - Grote awareness ‘opportuniteit’
- Quantumsprong in cyberveiligheid
  - CIS framework
  - Werken op technologie, processen en mensen



Cyberveiligheidsprogramma 4.0

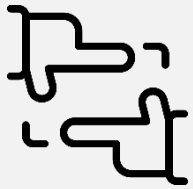
- Europese NIS2 regelgeving
  - Strengere cybersecurityvereisten voor essentiële bedrijven
  - Deadline = 18 april 2027



Gigantische uitdaging

Toekomstgerichte en fundamenteel betere IT-omgeving

Veilig



Standaard

Privacy

Hybride

Uitdagingen en opportuniteiten

1

Gefaseerde heropbouw

2

NIS2 security programma

3

Cyberveiligheid toepassingen

4

Business continuity plan

5

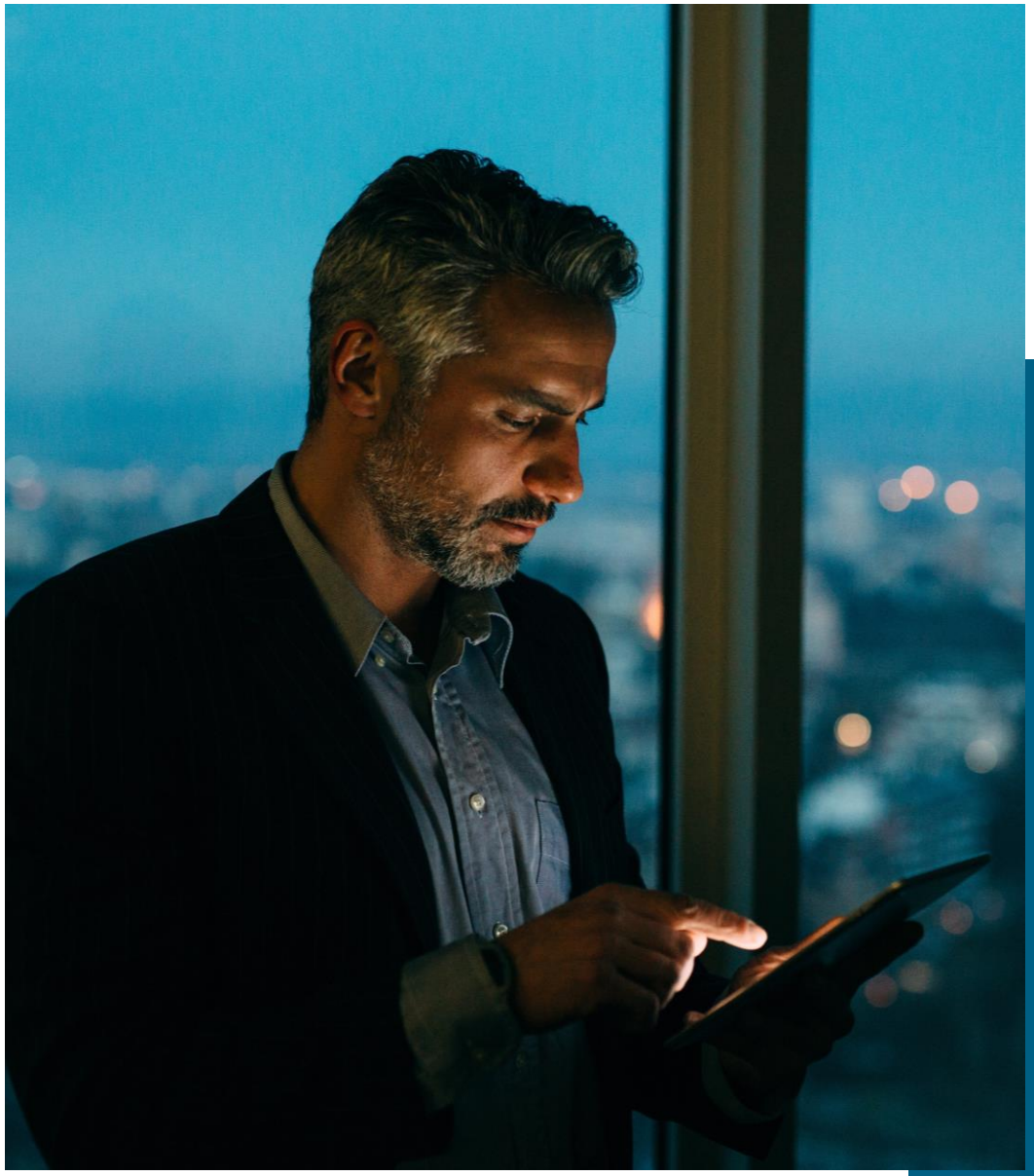
Privacy by design (GDPR)

Lessons learned

Kies voor een proactieve aanpak

Naar cyberveiligheid

- Start nu met basisbeveiligingen
  - Multifactor authenticatie en wachtwoordbeleid tegen phishing
  - Corporate managed omgeving tegen malware installatie
  - Security application + security operations center (SOC)
  - Back-ups beveiligen
  - Compartimentering
- Richt een cyberrisico stuurgroep op
  - om spanning tussen gebruikers (beleving & change) en specialisten (maximale voorwaarden) aan te pakken



Naar business continuïteit

Business is een belangrijke speler

- Zorg voor een crisismanager en neem cybersecurity op binnen crisismanagement
- Bepaal de ‘kroonjuwelen’
- Maak een offline scenario en back-up voor de kroonjuwelen

Naar eindgebruikers

- Bewustmaking
  - Gebruik Antwerpen als voorbeeld om het belang van cyberveiligheid aan te kaarten
- Versterk eindgebruikers
  - Geef trainingen (o.a. phishing) en voorkom kwetsbaarheid (o.a. black list websites)
- Gebruikersbeleving
  - Verwacht je aan discussies over de verminderde gebruikersbeleving

In de evolutie naar NIS2

- Cybersecurity is een continu proces – grote kost zit in clean-up
- Laat je inschalen en laat jouw situatie auditen
- Verwacht je aan strategische discussies in een groep met verschillende entiteiten
- Bereid de change goed voor, bij business en IT

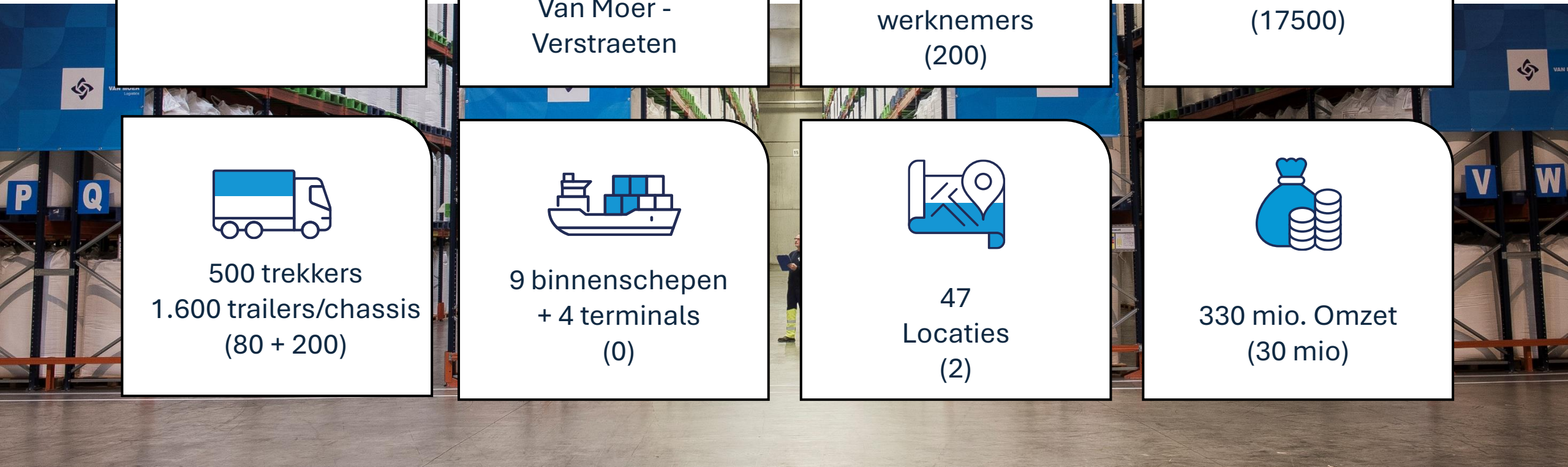
Bedankt

info@digipolis.be

VAN MOER
Logistics

Werkt aan cyberweerbaarheid

Van Moer Logistics vandaag (en in 2014)



Opgericht in 1990

Eigendom familie Van Moer - Verstraeten

2.200 werknemers (200)

800.000m^2 magazijn (17500)

500 trekkers
1.600 trailers/chassis
(80 + 200)

9 binnenschepen
+ 4 terminals
(0)

47
Locaties
(2)

330 mio. Omzet
(30 mio)

2014… Ieder afscheid, een nieuw begin.

Mijn verhaal

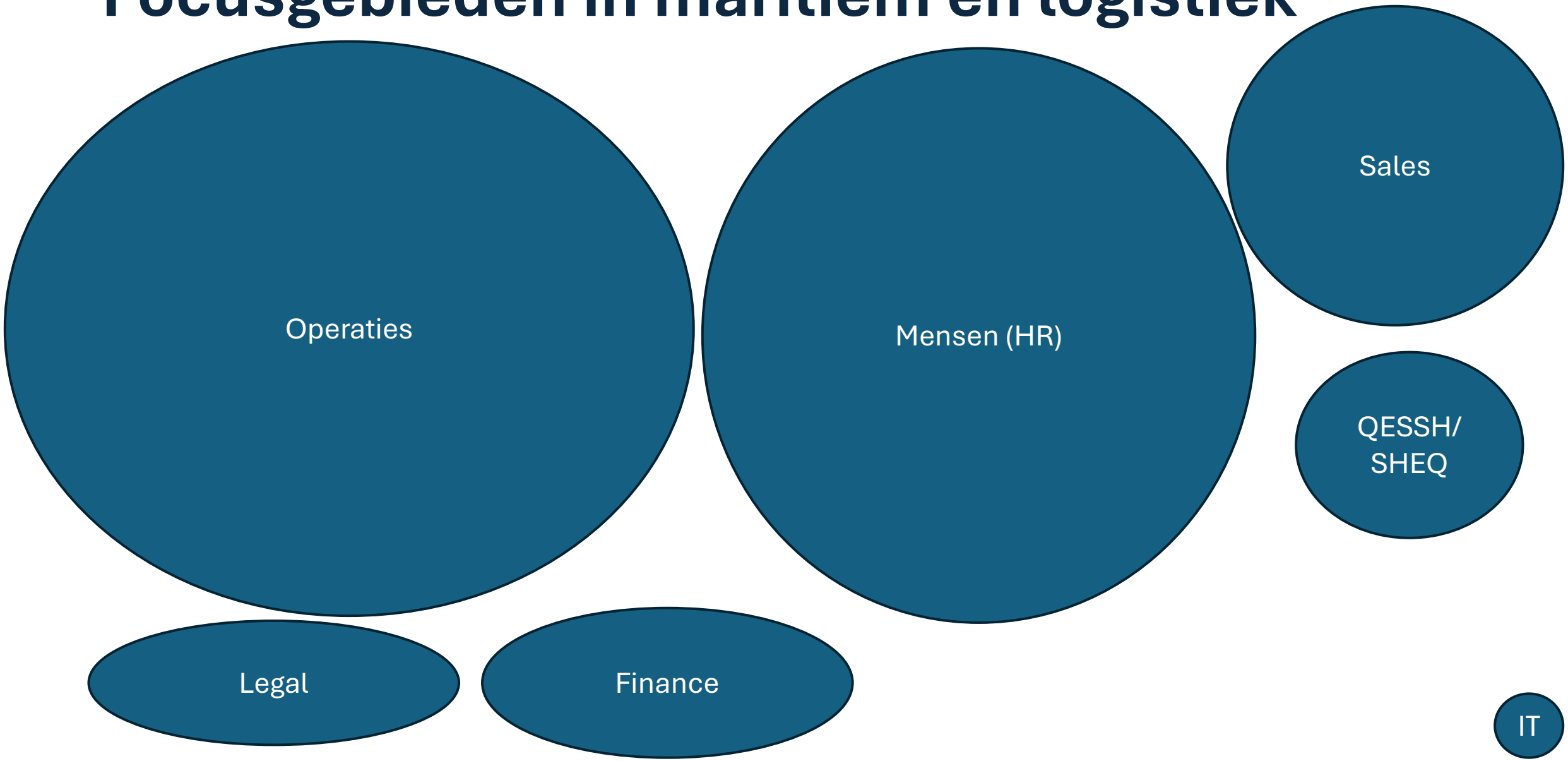
- Handelsingenieur (= geen IT-er)
- Wilde nautische wetenschappen studeren, maar mocht niet
- 20+ jaar in maritieme / logistieke omgeving (P&O / DP World)
- Gestart in operationele rollen (ladinginspectie, planning, automatisatie,…)
- Special thanks to Eric Noterman en Roger Roels…

Opdracht 1,…,n

- Vorm een team (1 externe consultant naast “god”)
- Beheer assets (= alle IT-ers/shops in groot Beveren zijn leverancier, kennis, vriend,…)
- Zorg voor applicatieportfolio (met Navision 2009 native database)
- Antwoord snel, oplossingsgericht en in verstaanbare taal op ALLE vragen
- Zorg dat het niet te veel geld kost (wat is “niet te veel”)
- “En voor de rest wil ik geen klachten horen”

(hebt U ergens security gehoord of gelezen ?)

Focusgebieden in maritiem en logistiek



Plan van aanpak ?

1. Begin vanuit de achterhoede (2014 – 2017)

- Local admin / domein accounts op individuele assets => weg
- Named accounts (aanloggen met loket / garage / magazijn / import => niet opnieuw)
- Breng in kaart wat er lokaal in de serverroom staat (in een daartoe ingerichte kamer, niet bij het archief of de schoonmaakproducten/-kar)
- Begin te sturen op data van shared file servers en waar die zich bevinden
- Breng toegangen tot je netwerk en key applicaties in kaart en vereenvoudig naar single sign on
- Implementeer Office365 (in 2015 = intern gek verklaard)

Plan van aanpak ?

2. Kom (voorzichtig) naar de oppervlakte (2018 – 2021)

- Move naar Public Cloud (eerste stappen op Azure) + exclusief privaat datacenter
- Implementatie MFA op individuele Windows accounts
- Controle proces op implementatie 3rd party software (niet basisveilig, niet starten), gekoppeld aan SaaS indien mogelijk
- Uitrol van antivirus detectie, de naam waardig
- Netwerksegmentatie (alles dicht standaard ipv open) + stricte topologie (VLAN)
- “Goedkope” cybersecurity verzekering (basisdekking) (1,5K / maand – 2019)

- Covid19
- Hacks op aantal haven/logistieke concullega’s

- Wijzigingen C-level
- Back Office > India
- Klanten die je netwerk ‘gratis’ gebruiken

Reactie binnen de organisatie

Never waste a good crisis…

Operator van de grootste tankcontainer terminal binnen Hamburg – Le Havre range

6000
tankcontainers
depot capacity

Waarvan
1500 gevuld met
ADR goederen

Plan van aanpak ?

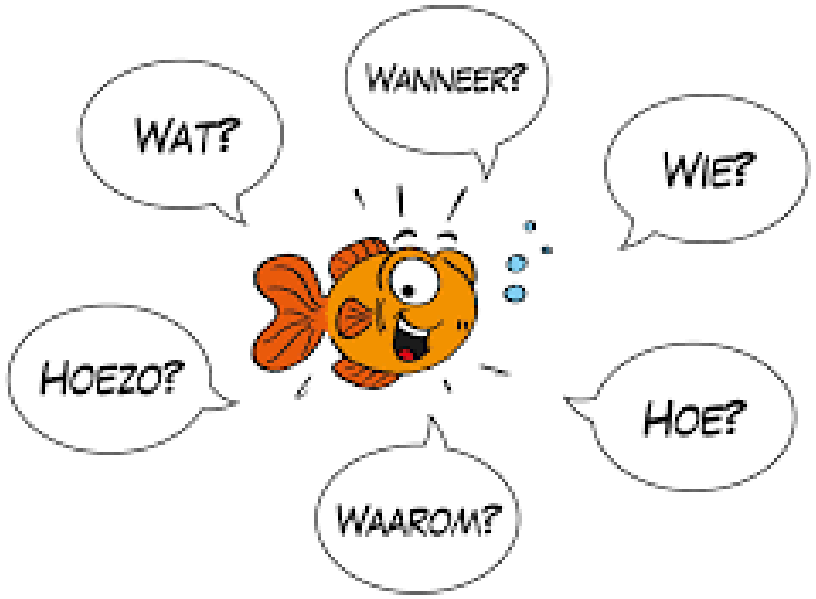
3. Duw door ! (2023 - …)

- ISO 27001 certifiëring
- Procedures, policies en penalties voor eindgebruikers / leveranciers (SLA met apart security luik)
- Afspraken met klanten voor het contract start – nee durven zeggen als het niet veilig is
- Bewustzijn bij medewerkers, actieve medewerking en alarmering
- Raad van Bestuur die cyberbeleid bekrachtigd (en financieel steunt)

Finish in zicht ?

De uitdaging wordt enkel complexer

Hou de juiste snelheid aan en behoud het overzicht


WAT?
WANNEER?
WIE?
HOEZO?
HOE?
WAAROM?

Koffiepauze

PREVENT NOW ◆ SECURE TOMORROW

INTRO

About me

- **+ 25 years** of experience
- Started at **McAfee**
- Established Secutec in **2005**
- Experienced **negotiator**
- **Technology & Cybersecurity** addict

Secutec
Cyber security intelligence

About Secutec

25M

25 MIL. EUR

60

ACTIVE IN 60 COUNTRIES

800

CUSTOMERS

85

EMPLOYEES

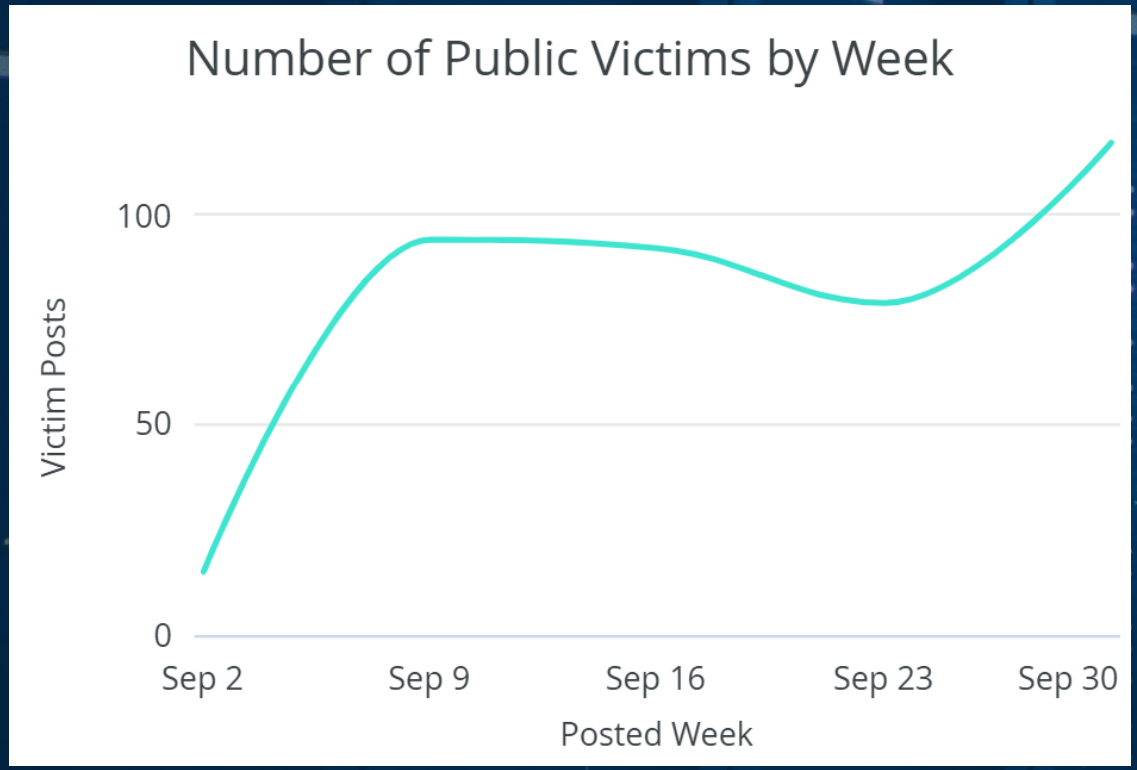
22Y

EXPERIENCE IN CYBERSECURITY

Secutec
Cyber security intelligence

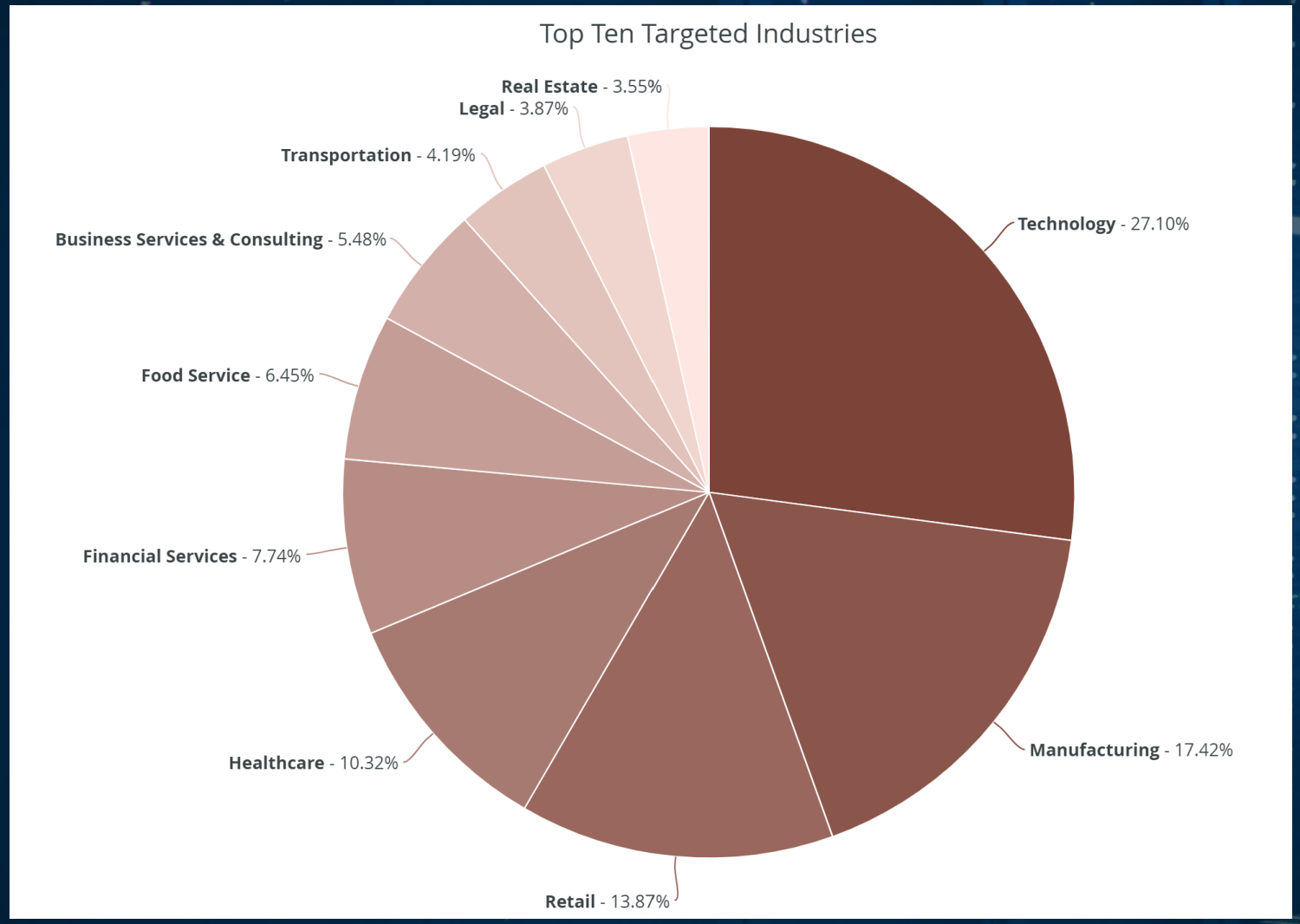
Aantal cyberincidenten wereldwijd september 24

400 slachtoffers (gerapporteerd)



Secutec
Cyber security intelligence

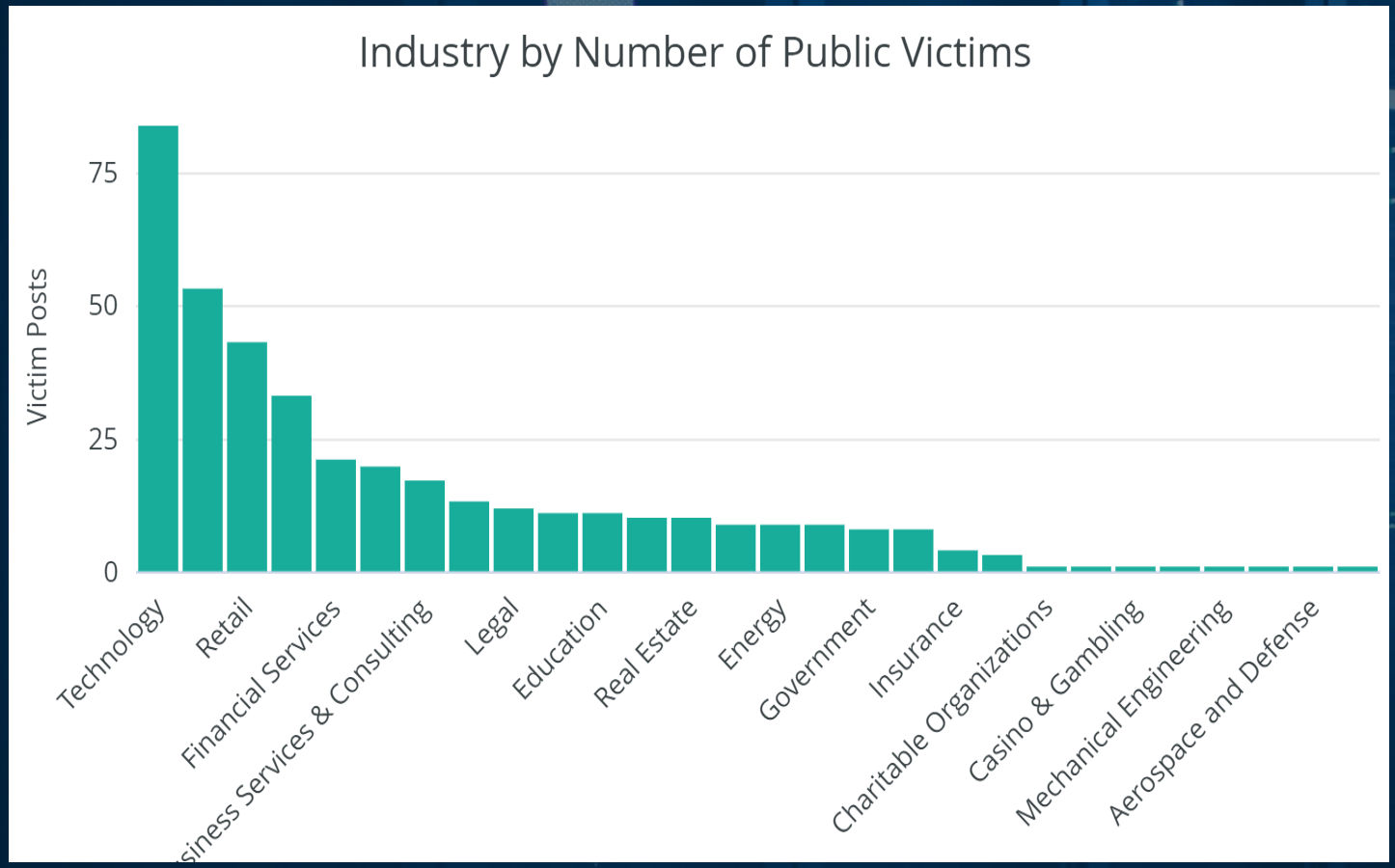
September 24



Secutec
Cyber security intelligence

Aantal cyberincidenten wereldwijd september 24

400 slachtoffers (gerapporteerd)



Secutec
Cyber security intelligence

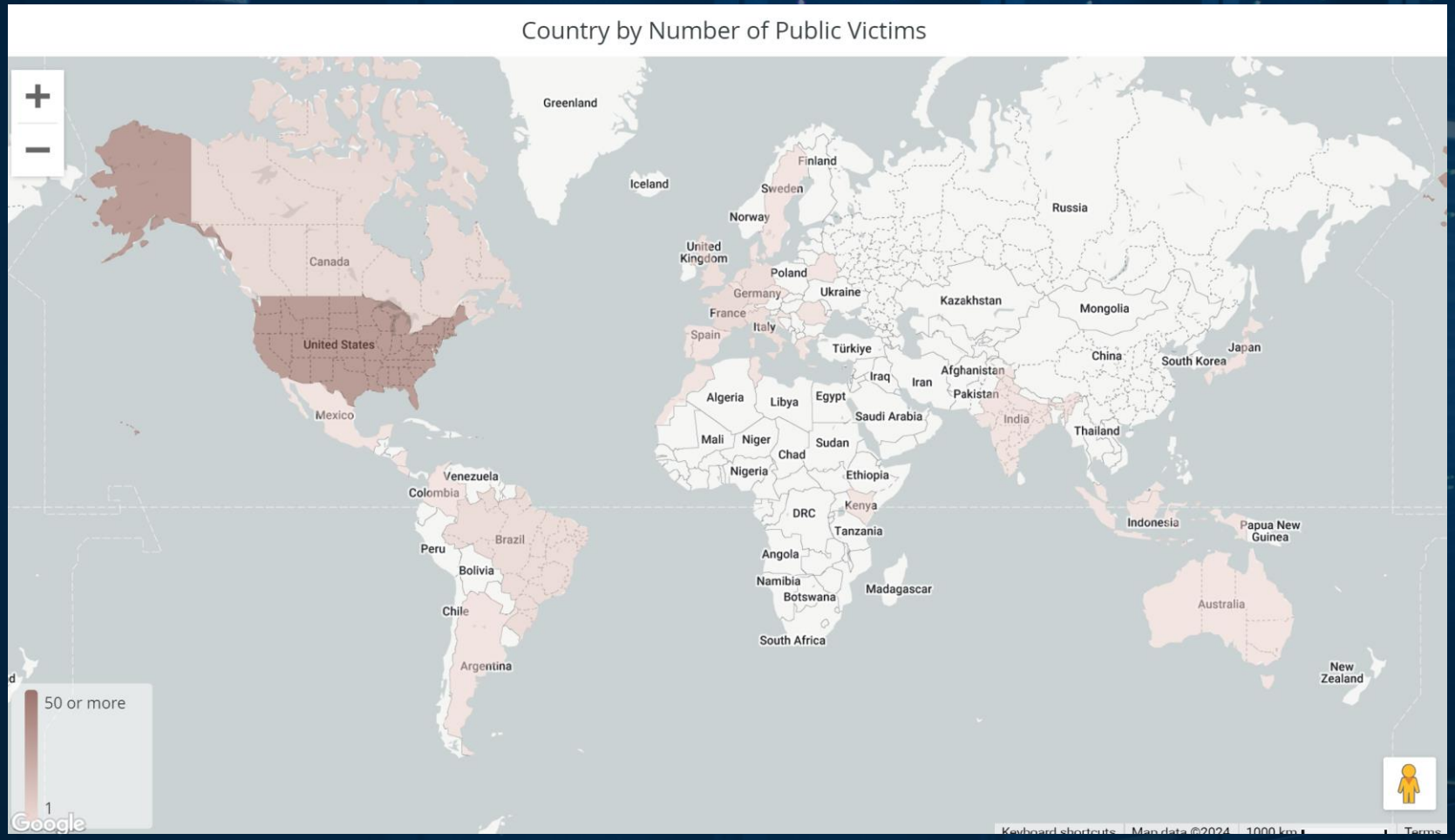
Cyberaanvallen wereldwijd,

transportsector,

laatste 12 maanden

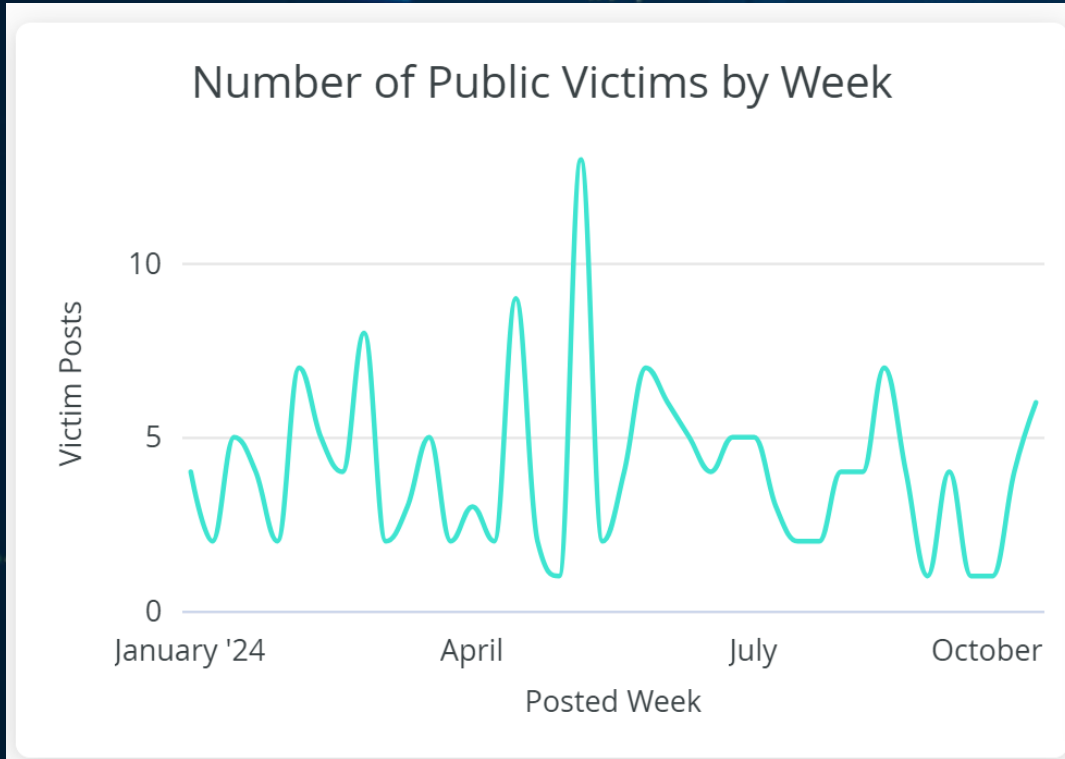
Secutec
Cyber security intelligence

Cyberaanvallen wereldwijd:
165 in transportsector, laatste 12 maanden



Secutec
Cyber security intelligence

Cyberaanvallen wereldwijd: 165 in transportsector, laatste 12 maanden



Groups by Victim Count

Ransomer Name	Victim Posts
LockBit	28
Akira	12
BianLian	9
Play	8
Cactus	8
RansomHub	7
8Base	7
Hunters International	7
Kill Security	6
Medusa	6
Black Basta	6

Secutec
Cyber security intelligence

Cyberaanvallen wereldwijd: 165 in transportsector, laatste 12 maanden

List of Public Victims

Victim Name	Victim Domain	Ransomer Name	Victim Industry	Victim Country	Posted Date	First Observed	Detailed Victim View
Nexus-Shinozaki...	nexus-shinozaki.c...	Sarcoma	Transportation	Japan	2024-10-04	2024-10-04	View
Transtec SAS	transtec.com.co	ORCA Ransomwar...	Transportation	Colombia	2024-10-04	2024-10-04	View
Nora-Lindefrakt...	noralindefrakt.com	Sarcoma	Transportation	Sweden	2024-10-04	2024-10-04	View
Rio Marine	riomarine.com	Sarcoma	Transportation	United States	2024-10-04	2024-10-04	View
Road Distributio...	roaddistributions...	Sarcoma	Transportation	Australia	2024-10-04	2024-10-04	View
GenPro Inc.	genproinc.com	BlackSuit	Transportation	United States	2024-10-04	2024-10-04	View
Divine Interprise...	divineinterprises....	INC	Transportation	United States	2024-09-29	2024-09-29	View
porter.in	porter.in	Kill Security	Transportation	India	2024-09-29	2024-09-29	View
www.vbrlogistica...	vbrlogistica.com.br	RansomHub	Transportation	Brazil	2024-09-26	2024-09-27	View
Eurobulk	www.eurobulk.gr	Play	Transportation	Greece	2024-09-23	2024-09-23	View
Cruz Marine (cru...	cruz.local	Lynx	Transportation	null	2024-09-16	2024-09-16	View
Evans Distributio...	www.evansdist.c...	Play	Transportation	United States	2024-09-10	2024-09-10	View
Partnership	partnership.com	Everest	Transportation	United States	2024-09-07	2024-09-07	View
riomarineinc.co...	www.riomarinein...	Cactus	Transportation	United States	2024-09-06	2024-09-06	View
www.parknfly.ca...	parknfly.ca	RansomHub	Transportation	Canada	2024-09-05	2024-09-05	View
YCH	ych.com	Mad Liberator Ra...	Transportation	Singapore	2024-09-04	2024-09-04	View
South American T...	southamericanto...	Meow Leaks V2	Transportation	South America	2024-08-26	2024-08-26	View
prasarana.com.m...	prasarana.com.my	RansomHub	Transportation	Malaysia	2024-08-25	2024-08-25	View
HL Lawson & Son...	hl-lawsonandsons...	INC	Transportation	United States	2024-08-22	2024-08-24	View
instadriver.co	instadriver.co	Kill Security	Transportation	Kenya	2024-08-22	2024-08-22	View
The Transit Auth...	https://www.tank...	Akira	Transportation	United States	2024-08-19	2024-08-19	View
OSG.COM	osg.com	RansomHub	Transportation	United States	2024-08-15	2024-08-19	View
megatravel.com....	megatravel.com....	DarkVault	Transportation	Mexico	2024-08-15	2024-08-15	View
Valley Bulk	www.valleybulkin...	Cicada3301	Transportation	United States	2024-08-14	2024-08-02	View
M&M Transport S...	mmtransport.com	dAn0n	Transportation	United States	2024-08-14	2024-08-14	View
startaxi.com	startaxi.com	Kill Security	Transportation	Romania	2024-08-14	2024-08-14	View

Secutec
Cyber security intelligence

Overzicht Cyberaanvallen België,

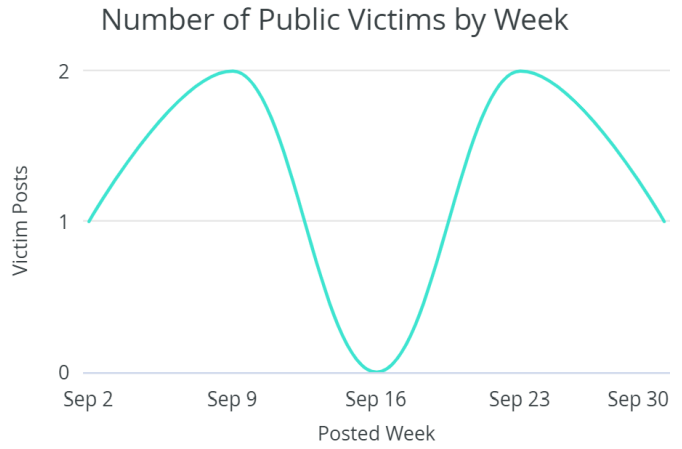
Secutec
Cyber security intelligence

Aantal cyberincidenten in België september 24

6 slachtoffers (gerapporteerd)

6

Victim Count



Groups by Victim Count

Ransomer Name	Victim Posts
Kill Security	3
Hunters International	1
Medusa	1
BlackSuit	1

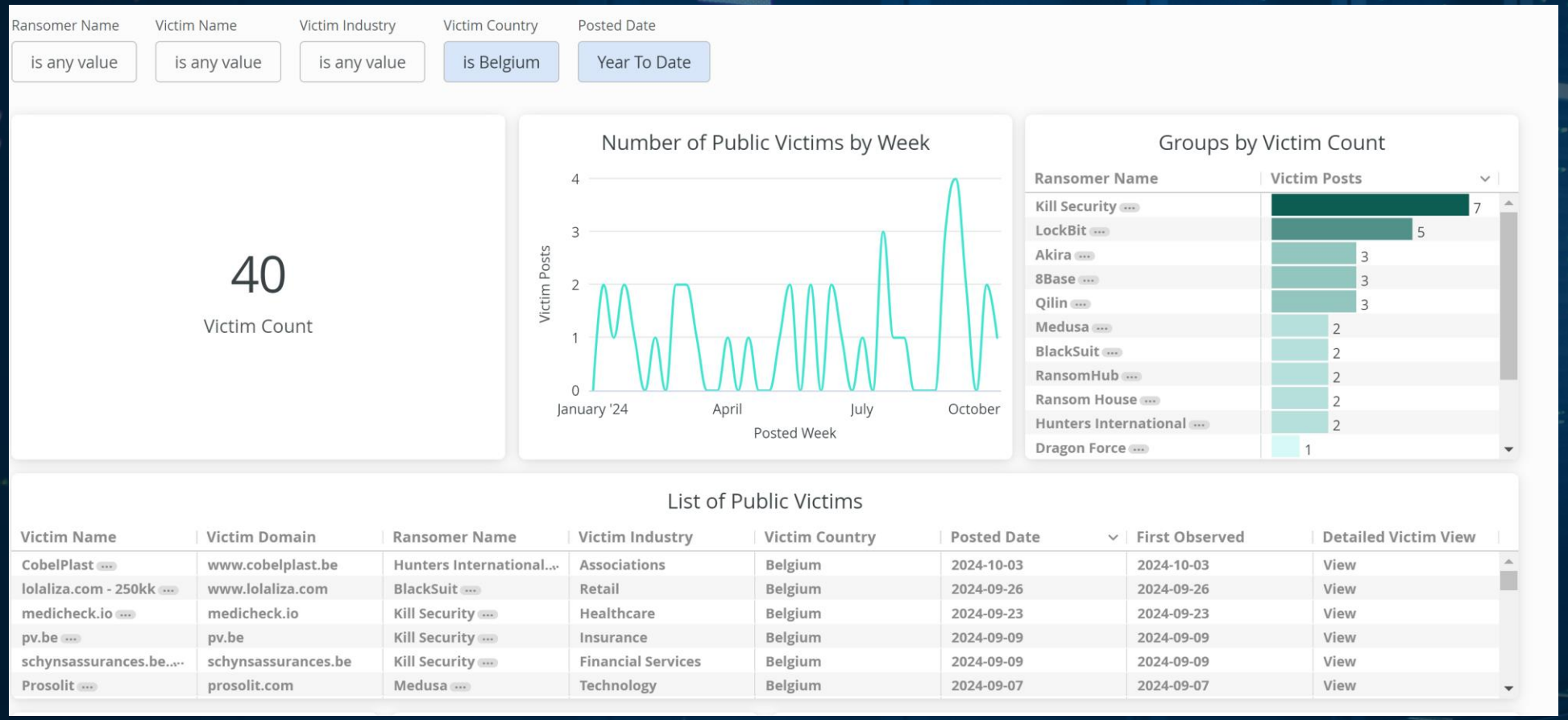
List of Public Victims

Victim Name	Victim Domain	Ransomer Name	Victim Industry	Victim Country	Posted Date	First Observed	Detailed Victim View
CobelPlast	www.cobelplast.be	Hunters International...	Associations	Belgium	2024-10-03	2024-10-03	View
lolaliza.com - 250kk	www.lolaliza.com	BlackSuit	Retail	Belgium	2024-09-26	2024-09-26	View
medicheck.io	medicheck.io	Kill Security	Healthcare	Belgium	2024-09-23	2024-09-23	View
pv.be	pv.be	Kill Security	Insurance	Belgium	2024-09-09	2024-09-09	View
schynsassurances.be...	schynsassurances.be	Kill Security	Financial Services	Belgium	2024-09-09	2024-09-09	View
Prosolit	prosolit.com	Medusa	Technology	Belgium	2024-09-07	2024-09-07	View

Secutec
Cyber security intelligence

Aantal cyberincidenten in België laatste 12 maanden

40 slachtoffers (gerapporteerd)



Secutec
Cyber security intelligence

Cyberaanvallen op Antwerpse havenindustrie 2019 - 2023

Jaar	Aantal cyberaanvallen	Soort aanvallen	Gerapporteerde schade	Ingevoerde veiligheidsmaatregelen	Regelgeving en initiatieven
2019	12	Phishing, Malware	Financiële verliezen, verstoring van logistiek	Implementatie van basis cyberbeveiligingssystemen	Start van de Europese richtlijn NIS (Network and Information Security) in havens
2020	18	Ransomware, DDoS	Verstoring van scheepvaart- en havenactiviteiten, gegevensdiefstal	Grootschalige investeringen in firewalls en endpoint-beveiliging	Uitbreiding van internationale samenwerking en monitoring
2021	25	Supply chain attacks, DDoS, insider threats	Groeiende kosten door datalekken, downtime in havenactiviteiten	Implementatie van geavanceerde monitoring en incident response-teams	Oprichting van de IMO (International Maritime Organization) cybersecurity richtlijnen
2022	30	Ransomware, Zero-day attacks	Verspreiding van malware, bedreigingen voor maritieme infrastructuur	Meerderheid van havens adopteert Security Operations Centers (SOC)	NIS 2-richtlijn van kracht in de EU voor havenbeveiliging
2023	35	Ransomware, Phishing, Malware-as-a-Service	Gegevensverlies, aanzienlijke verstoring van wereldwijde logistieke ketens	Uitrol van AI-gestuurde detectiesystemen en incident response	Toename van samenwerkingen tussen private en publieke sectoren op cybersecurity gebied

Secutec
Cyber security intelligence

In België is het aantal cyberaanvallen de laatste 5 jaar enorm gestegen

Toename van incidenten: In 2020 registreerde het Centrum voor Cybersecurity België (CCB) al 5.387 meldingen van cyberaanvallen en incidenten, een stijging ten opzichte van 2019 toen er 4.484 meldingen waren. Het aantal meldingen steeg daarna verder in de jaren daarna.

Ransomware blijft een grote bedreiging. In 2023 steeg het aantal Ransomware-incidenten in België met 24%, hetgeen overeenkomt **met 120 gemelde incidenten** (Centre for Cyber security Belgium)

De gezondheidszorg en kritieke infrastructuur zijn daarbij vaak doelwitten.

Algemene stijging in België: Het aantal cyberaanvallen steeg in sommige jaren met wel 32%, waarbij het werkelijke aantal incidenten waarschijnlijk veel hoger ligt, omdat veel bedrijven en particulieren cyberincidenten niet rapporteren.

Secutec
Cyber security intelligence

Belangrijke resultaten voor deelnemers

Secutec
Cyber security intelligence

Darknetmonitoring: resultaten deelnemers event

87% van de bedrijven hebben gebruikers met wachtwoorden op het darknet door algemene datalekken obv gehackte website

Bij 53% van de bedrijven is er data van paswordstealers terug te vinden op het darknet door medewerkers, klanten of leverenaciers die inloggen op het corporate netwerk

Bij testing bleek dat we op 29% van de bedrijven konden inloggen op het netwerk obv deze bekomen wachtwoorden wat ERG ALARMEREND is!

Secutec
Cyber security intelligence

24 Oktober 2024

Secutec
Cyber security intelligence

Any questions?

CEO – FOUNDER

Official Cyber Crime Negotiator

geert.baudewijns@secutec.be

+32 477 69 05 05

CONTACT US

Secutec
Cyber security intelligence

BELGIAN PORT ISAC

VOKA Alfaport

07/10/2024

MISSION STATEMENT

Members of the Belgian Port ISAC aim to increase the collaboration between the members to be able to disclose and analyze information to increase the cyber resilience within the Belgian port ecosystem. Members agree to support each other and contribute in engagements that strengthen the sectoral maturity on cyber- and information security.

ISAC OBJECTIVES

- Build trusted environment for information scharing
- Vulnerability analysis and problem solving
- Enhancement of cyber resilience
- Strengthen public-private collaboration
- Executive cybersecurity awareness
- Increase intra-sectoral collaboration

CURRENT MEMBERS

AET

BASF
The Chemical Company

CEWEZ

cepa

CMA CGM

C. Steinweg

DP WORLD

ENGIE

EUROPORTS

ExxonMobil

FLUXYS

ilomar
holding nv

INFRABEL
Right On Track

KATOEN NATIE
OUR PEOPLE MAKE THE DIFFERENCE

LBC
TANK TERMINALS

MSC

NxtPort

Port of Antwerp Bruges

PORTMADE

PSA

VAN MOER
Logistics

Vopak

ZUIDNATIE

NIPPON SHOKUBAI

CENTRE FOR CYBERSECURITY BELGIUM

economie
FOD Economie, K.M.O., Middenstand en Energie

Federale Politie
Police Fédérale

FEDERALE OVERHEIDSDIENST
MOBILITEIT EN VERVOER

Vlaanderen
is mobiliteit & openbare werken

ADVANTAGES OF JOINING

BP ISAC members:

- Receive the opportunity **to share and receive relevant information** from other members
- Engage in strategic and tactival **analysis of threat reports** shared by members and security partners
- Receive **first-hand confidential information** during and after an incident of members within their ecosystem
- Enjoy from **positive publicity** and come across stronger for future businesses ready to dock in the geographic area
- **Collaborate with European ports** through the membership of the BP ISAC within the EU Maritime ISAC.

Members contribute through:

- Presence in **quarterly meet-ups**
- **Presence in workshops** and meetings on specific technical topics
- Help assist in the preparation and execution of the ISAC meetings and **influence legal frameworks**
- **Share information** with regard to incidents under clear sharing rules.

MEMBERSHIP APPLICATION PROCEDURE

1

Request membership

Submit your membership application via email to the president of the BP-ISAC. You can find the contact information of the president on the last slide of this deck.

2

Introductory call

The president will review the application, and will contact you to schedule an introductory call. The purpose of this call is to get acquainted and to answer any questions that you might have.

3

Sign the Terms of Reference (ToR)

The ToR describes how the BP-ISAC works, what we expect from our members and what they can expect from us in return, and how we share information between each other.

4

Review by current BP-ISAC members

Your application will be submitted to all current BP-ISAC members for review. If there are no objections, your application is approved.

5

Onboarding

You will be added to the mailing list and you will be invited to all future BP-ISAC meetings.

TARGET MEMBERS

- PORT AUTHORITY REPRESENTATIVES
- PUBLIC OR PRIVATE ENTITIES ON THE GROUNDS OF BELGIAN PORTS
- MAJOR SUPPLIERS TO THE ECOSYSTEM

REACH OUT TO US FOR MORE INFORMATION

Nick Van den Bergh

IT Security manager
President BP-ISAC

nick.vandenbergh@dpworld.be
+32 477 96 15 71

Yannick Herrebaut

Cyber Resilience Manager
Secretary BP-ISAC

Yannick.herrebaut@portofantwerpbruges.com

NIS2 wetgeving: 18/10/24

Deze richtlijn is vastgesteld door de Europese Unie (EU) en bedoeld om de cyberbeveiliging en weerbaarheid van essentiële diensten in EU-lidstaten te verbeteren waaronder ook maritiem vervoer. Wie van de havenspelers er binnen of volledig buiten het toepassingsgebied vallen is nog niet helemaal duidelijk.

Vragen: beroepsverenigingen en CCB

De NIS2-richtlijn : wat betekent dit voor mijn organisatie? | Centrum voor Cybersecurity België (belgium.be)

NIS2 snelstartgids | CCB Safeonweb

Centre for Cybersecurity Belgium
13,801 followers
2d • Edited •

+ Follow ···

📢 Webinar: NIS2 - All You Need to Know!

On October 18, the Belgian law on NIS2 and the Royal Decree will come into force. Many organisations have not waited for this day to prepare, others are still waiting to see what happens.

Do you have questions about this new legislation? Join us for our online webinar, where we will cover:
- The legal obligations of NIS2
- The CyberFundamentals framework

You will also have the opportunity to interact with experts from the Centre for Cybersecurity Belgium in dedicated discussion rooms! 🛡️

🗓️ When? October 9
⏰ Time? 9:30 AM
💻 Format? Online
👉 Register now and be ready to tackle this new regulation! https://lnkd.in/enkkRkFQ

#NIS2 #CyberSecurity #CCB #Webinar #Legislation #CyberFundamentals

Samen voor
een cyberveilige haven!

info@alfaportvoka.be