# Cybersecurity Event

In samenwerking met

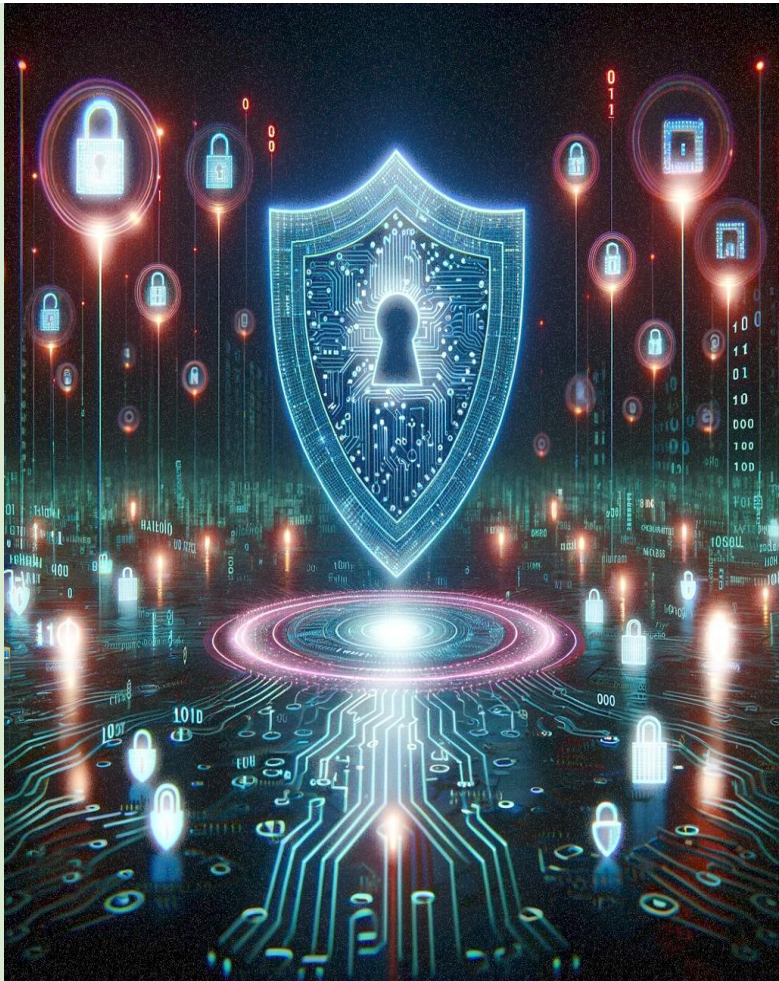
- Sectricity
- Cheops

Van Dessel
Insurance Brokers

SECTRICITY

# Outsmart the Hacker: Stay Ahead, Stay Secure

CYBERSECURITY

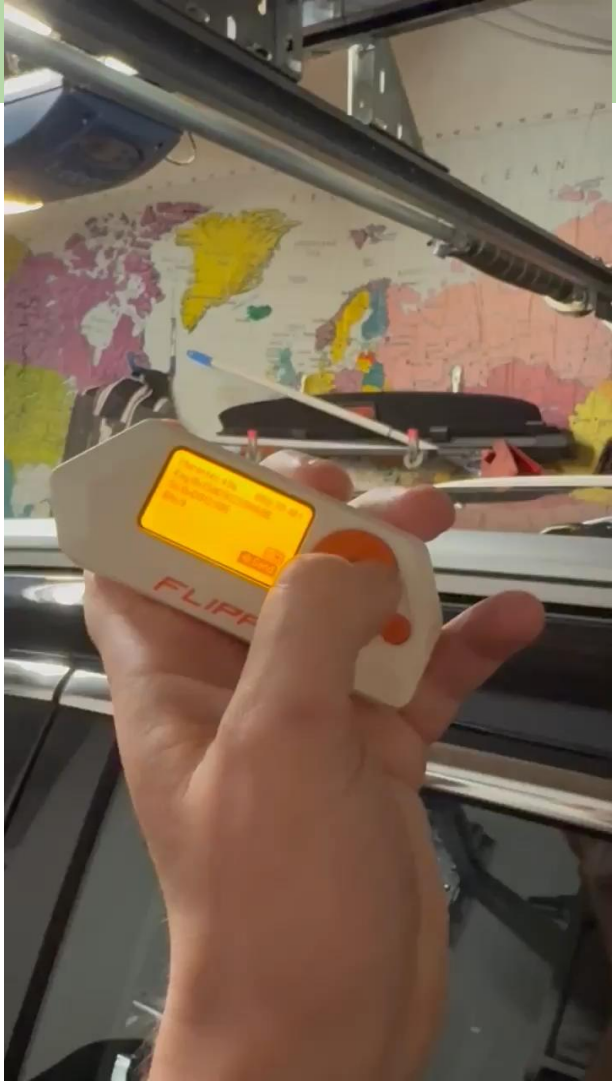


# Who am I?

- Preben Ver Eecke
- Ethical hacker @ Sectricity
- Bug bounty hunter
- Hacked FB, Snap, Tesla, ...

# New tactics - Flipper Zero

# New tactics - Flipper Zero



# New tactics - Flipper Zero

# Quishing

Scams

# Quishing attacks are targeting electric car owners: Here's how to slam on the brakes

Ever alert to fresh money-making opportunities, fraudsters are blending physical and digital threats to steal drivers' payment details

**Phil Muncaster**

15 Oct 2024 • 5 min. read

# Preventing Quishing

- Don’t scan QR codes in messages/emails
- Regularly update your smartphone's software
- Unknown QR code in private email? Forward to suspicious@safeonweb.be
- Treat QR codes with the same caution as you would an unknown link in an email or text message.

# Wi-Fi

# Wifi

- Wigle

# Password hacking

# Passwords

- 13AqJ3p!
- ikbenprebenenikwooningent

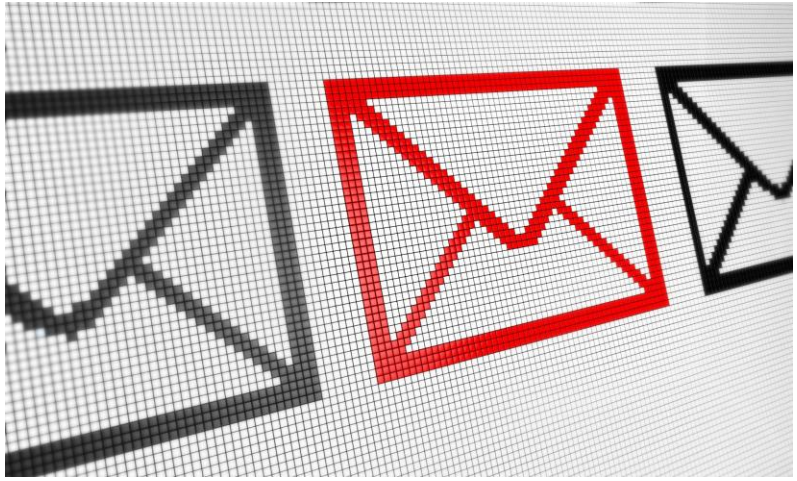
# Passwords

- hashing
- Passwords are saved in “encrypted” form
- Hashing ways / algorithms
- MD5, Sha1, ...

# Business email compromise

# Business Email Compromise (BEC)

- BEC is a form of cyber fraud where attackers **pretend to be a company executive or other trusted party** via email.
- The goal is to trick employees, customers, or partners into **transferring money** or sensitive information.
- BEC often involves social engineering and research, making it difficult to detect.



# How Phishers and Scammers Exploit Domains

# DNS – domain name system

- Quiz

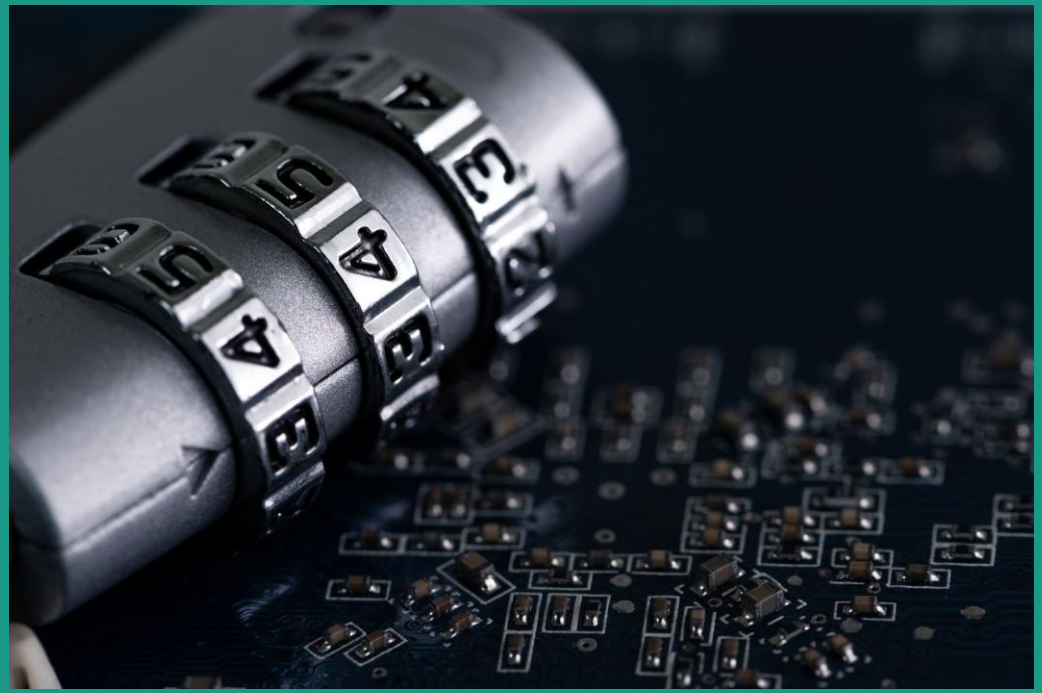
# Lookalike domains (=domain squatting)

- Quiz

# URL shorteners

- Quiz

# Ransomware

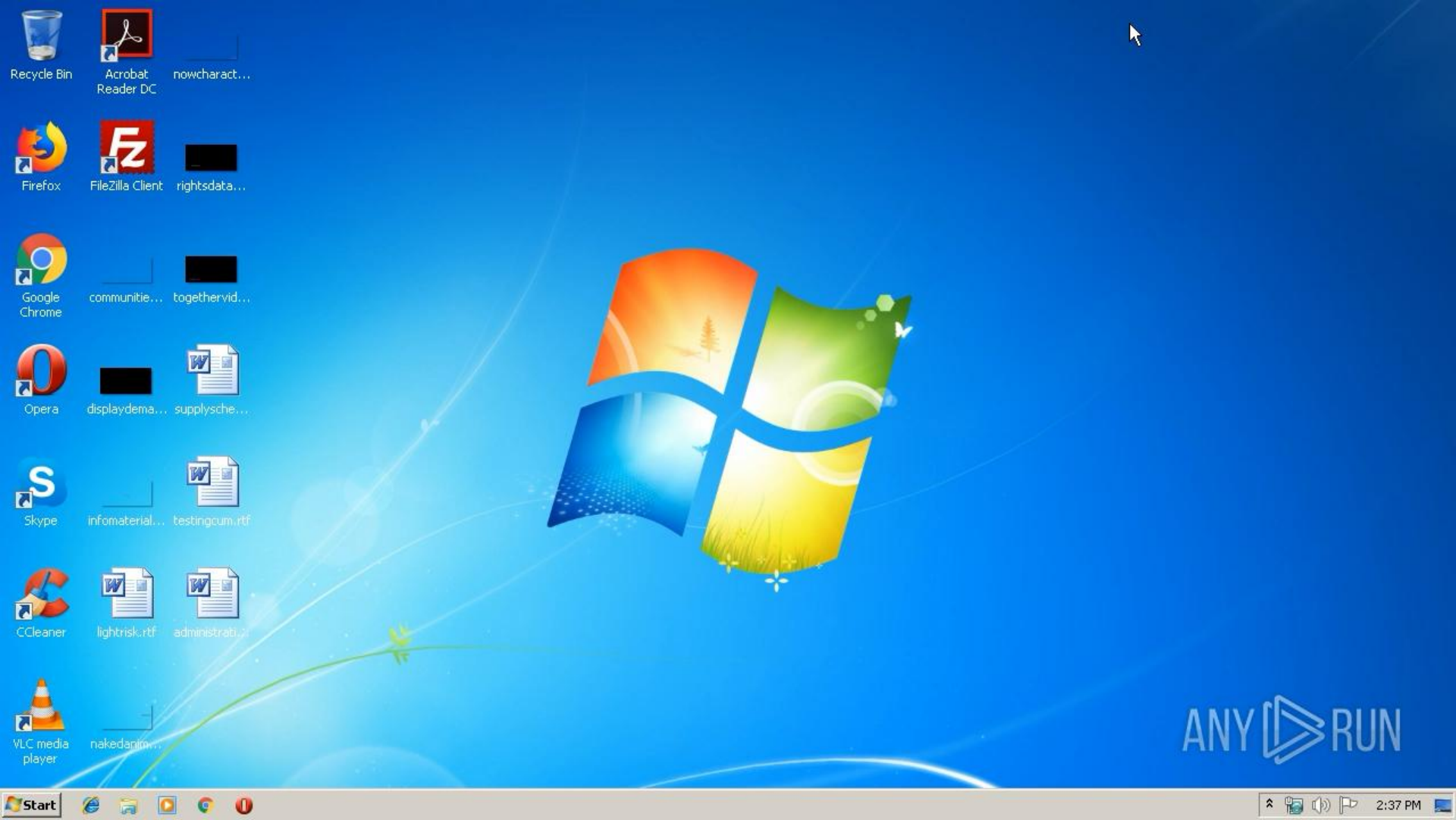


# What is Ransomware?

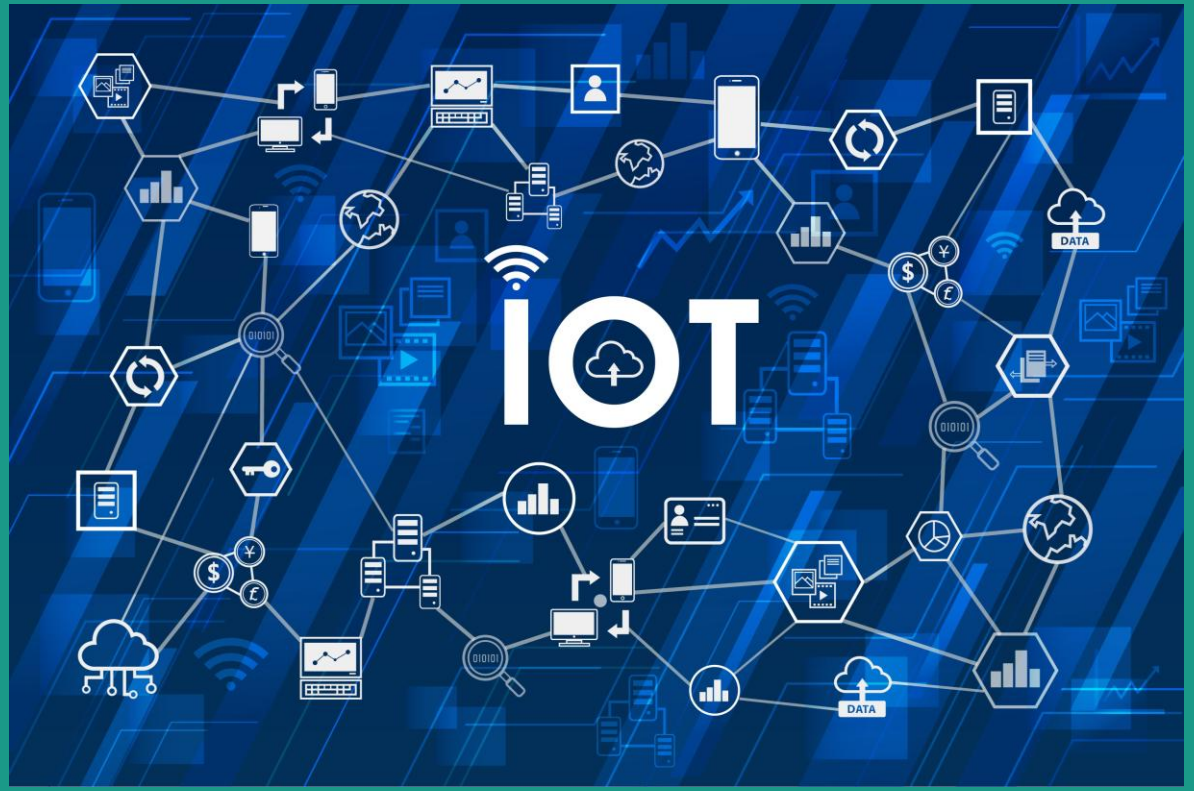
- Ransomware is a type of **malware** that **encrypts a user's files and demands payment to restore access.**
- Ransomware can be delivered via malicious (email) attachments, infected websites, usb or software vulnerabilities.
- Paying the ransom is no guarantee that files will be restored

# What is Ransomware?

- WannaCry Demo
- 2017
- 200 000 PC’s infected


Recycle Bin
Acrobat Reader DC
nowcharact...
Firefox
FileZilla Client
rightsdata...
Google Chrome
communitie...
togethervid...
Opera
displaydema...
supplysche...
Skype
infomaterial...
testingcum.rtf
CCleaner
lightrisk.rtf
administrati...
VLC media player
nakedanim...
ANY RUN
Start
2:37 PM

# Internet of Things



# Internet of Things

- IoT at home?
- “Smart” Dishwasher, lights, vacuum, doorbell, cameras, lawn mower, ...
- Smart = connected to Wi-Fi
    - (not your smartphone / computers / tablet)

# Shodan

- Demo

# Q&A

# Cheops – managed service & IT partner

Enkele cruciale beveiligingsmaatregelen

Van Dessel
Insurance Brokers

# Van Incident tot Actie: Cybersecurity & NIS2

Donderdag 23.10.2025


cheops

# Pleased to meet you

## Eric Primus

Director Managed Services

26 jaar ervaring
Bij Cheops sinds 2020

Wie zijn we?

01

Verloop van een Incident

02

NIS2

03

# Wie zijn we?

01


Leading **Managed Service Provider** in IT & Business Technology Services.

Big enough **to deliver**, small enough **to care**.

**Let’s talk ambition.**

# Cheops is een duurzame, steeds groeiende Managed Service Provider

**Actief sinds 1989**

**35+ jaren**

**Gecertificeerd als**

**Great Place To Work**

**Genomineerd tot**

**Trends Gazelle voor 13 jaar**

**450+**

**medewerkers**

**400+**

**Klanten**

in diverse marktsegmenten

cheops

**5**

**Locaties**

Kontich - Antwerpen – Gent – Brussel - Herentals

**80M**

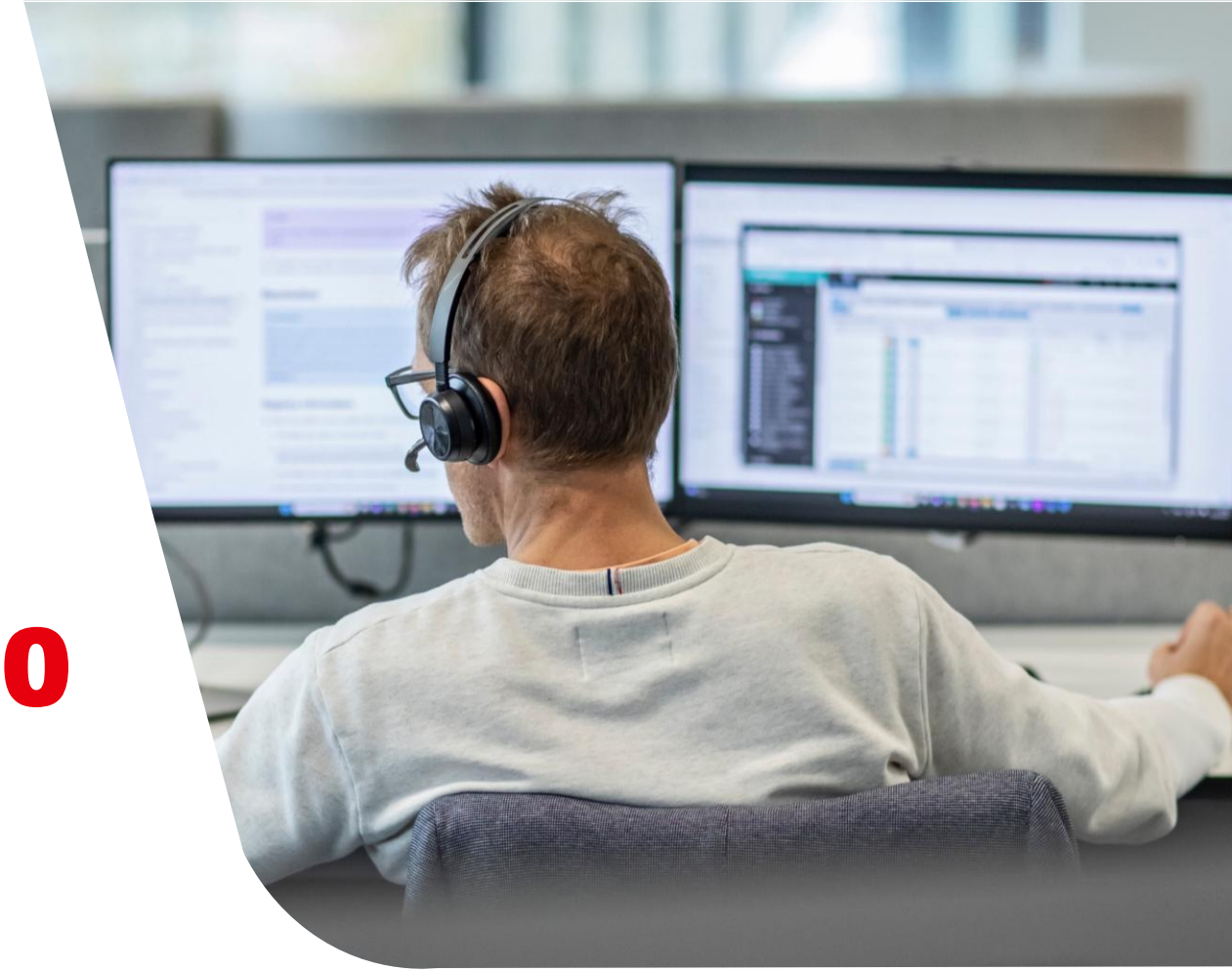
**Omzet**

**64**

**NPS**

**9,4/10**

**Eindgebruikerstevredenheid**



cheops

# Cheops heeft een uniek, hybride portfolio van oplossingen

## Managed Services

### Project Services

Migraties, systeem integraties & onboarding

### Shared Services

Managed IT as-a-Service oplossingen gebouwd op standaarden

### Dedicated Services

Managed IT as-a-Service oplossingen gebouwd op maat

## Professional Services

### Infrastructure

IT-omgeving Experts & Managed Teams

### Applications

IT Applications Experts & Managed Teams

# Een divers klantenportfolio doet beroep op onze expertises

# Het verloop van een incident

02

**Donderdag 12/10**
**7:00 AM**

**Donderdag 12/10**
**7:30 AM (+30 min)**

cheops

# Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

**To decrypt your files** you need to buy our special software - **General-Decryptor**

**Follow the instructions below.** But remember that you do not have much time

## General-Decryptor price

the price is for all PCs of your infected network

You have 8 days, 20:59:12

* If you do not pay on time, the price will be doubled
* Time ends on Okt 20, 16:30:12

Current price: 214151 XMR ≈ 5,000,000 USD

After time ends: 428302 XMR ≈ 10,000,000 USD

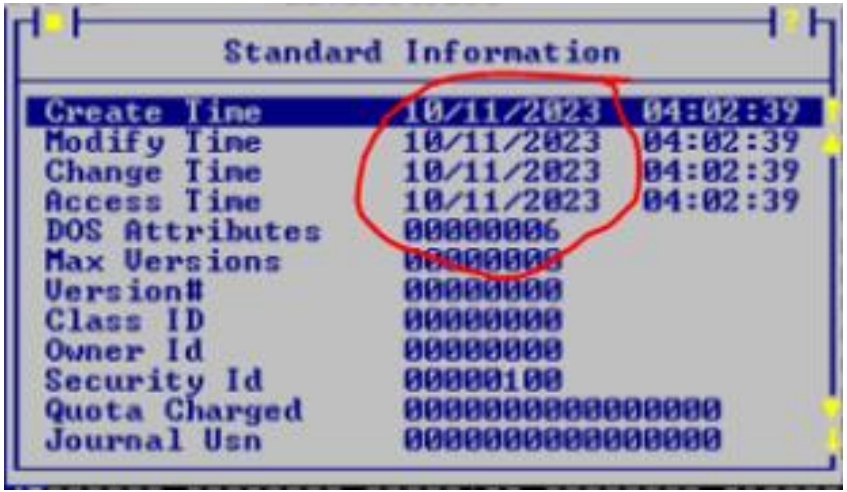
**Donderdag 12/10**
**9:00 AM (+2u)**

## Crisis Meeting

1. Bepalen van de omvang van de aanval
2. Isoleren van de geïnfecteerde apparaten
3. Opzetten van gescheiden communicatie
4. Opzetten van een crisisteam
5. Informeren van het CCB
6. Communiceren
7. Wettelijke verplichtingen

cheops

**Donderdag 12/10**
**12:00 PM (+5u)**




## Omvang van de aanval:

- Alle servers en opslag zijn vergrendeld.
  - Geen offertes, orders, bestellingen, facturen, …
- Alle kassasystemen en PC's zijn vergrendeld.
  - Geen transacties
- Vaste telefoonnummers onbereikbaar.
- Mail werkt nog.
- Personeel wordt naar huis gestuurd.
- **Er is data is gestolen.**
- **De Back-up is gewist.**
- **De hackers luisteren mee…**

cheops

**Donderdag 12/10**
**14:00 PM (+7u)**

Gegevensbeschermingsautoriteit

cheops

**Donderdag 12/10**
**16:00 PM (+9u)**

## Plan van aanpak:

- Mail wordt “gereset”.
- Een nieuwe omgeving wordt opgezet in de Cloud.
- Alle Pc's en kassasystemen worden gewist en geherinstalleerd.
- Oude telefooncentrale wordt door Teams vervangen.
- Inschakelen van een forensisch labo om te controleren of de back-up hersteld kan worden.

cheops

**Donderdag 12/10**
**18:00 PM (+11u)**

## Plan A:

Backup vertrekt op transport naar een gespecialiseerd labo in Duitsland.

Versleutelde bestanden worden verstuurd om te onderzoeken of er een “ontsleuteling” mogelijk is.

Vrijdag 13:00 PM wordt een eerste analyse verwacht.


Forensische resultaten…

## Vrijdag 13/10
## 9:00 AM (+26u)

**Status:**

- Winkels gaan terug open met een skeleton crew.
- Van digitaal naar papier.
- 220 medewerkers blijven technisch werkeloos.
- Prioriteit aan het nieuwe systeem en aan telefonie.

**Zonder backup, geen data.**

cheops

**Vrijdag 13/10**
**10:00 AM (+27u)**

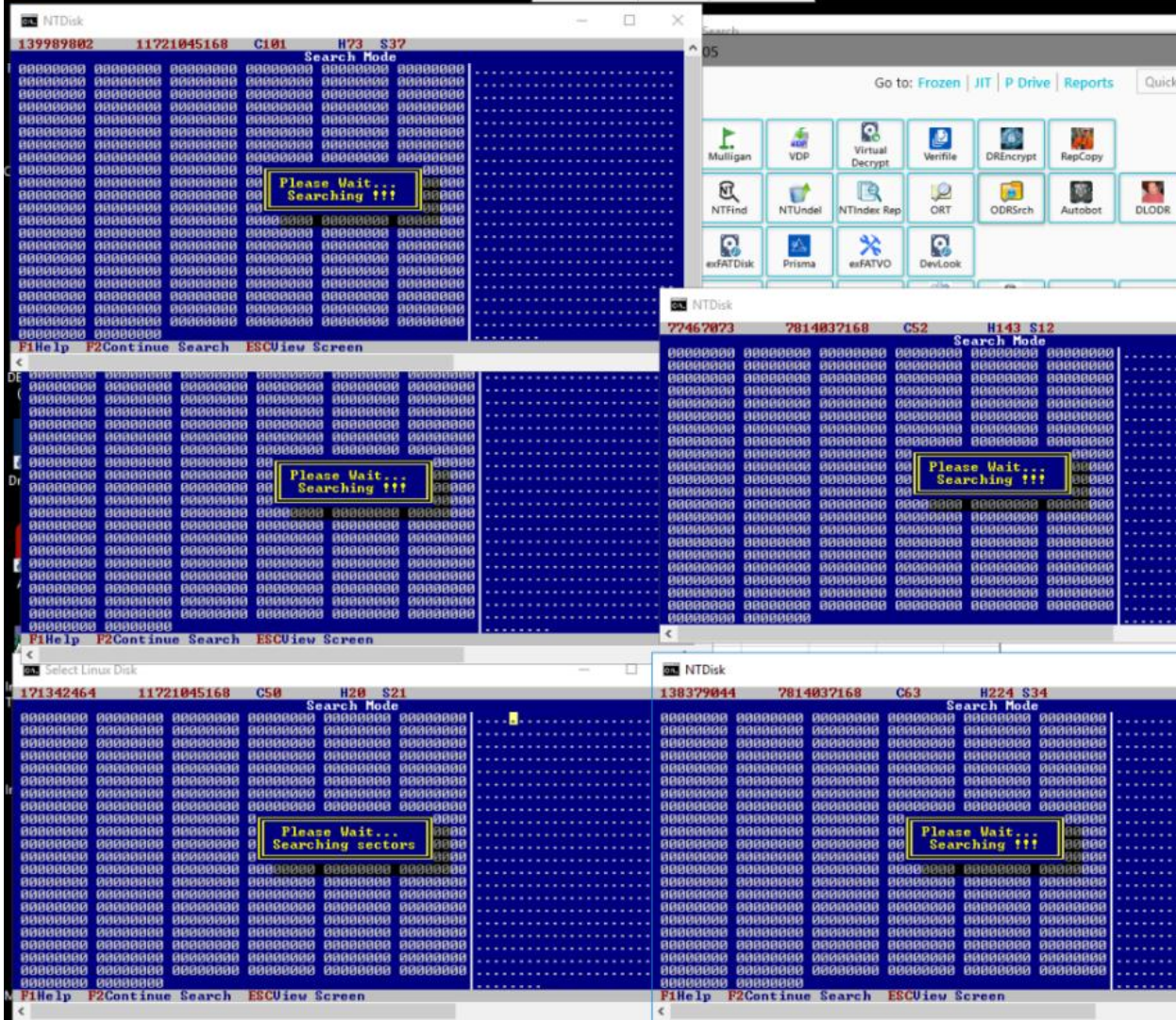
**Alle hoop op plan A, maar …**
**PLAN B:**
Aanstellen van onderhandelaars

**Positionering t.o.v. cybercriminelen**
Is er nog data ter beschikking?
Is er data gestolen?
Ethisch vs. Realistisch

# Vrijdag 13/10
# 13:00 PM (+30u)

## Slecht nieuws…

cheops



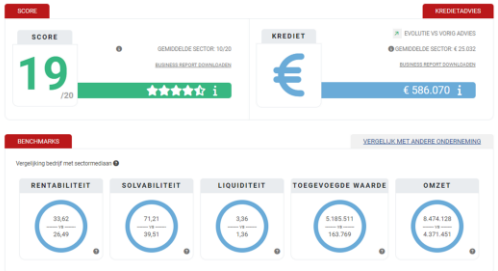

**Vrijdag 13/10**
**15:00 PM (+32u)**

En daar stopt het niet…

# Terug naar af …

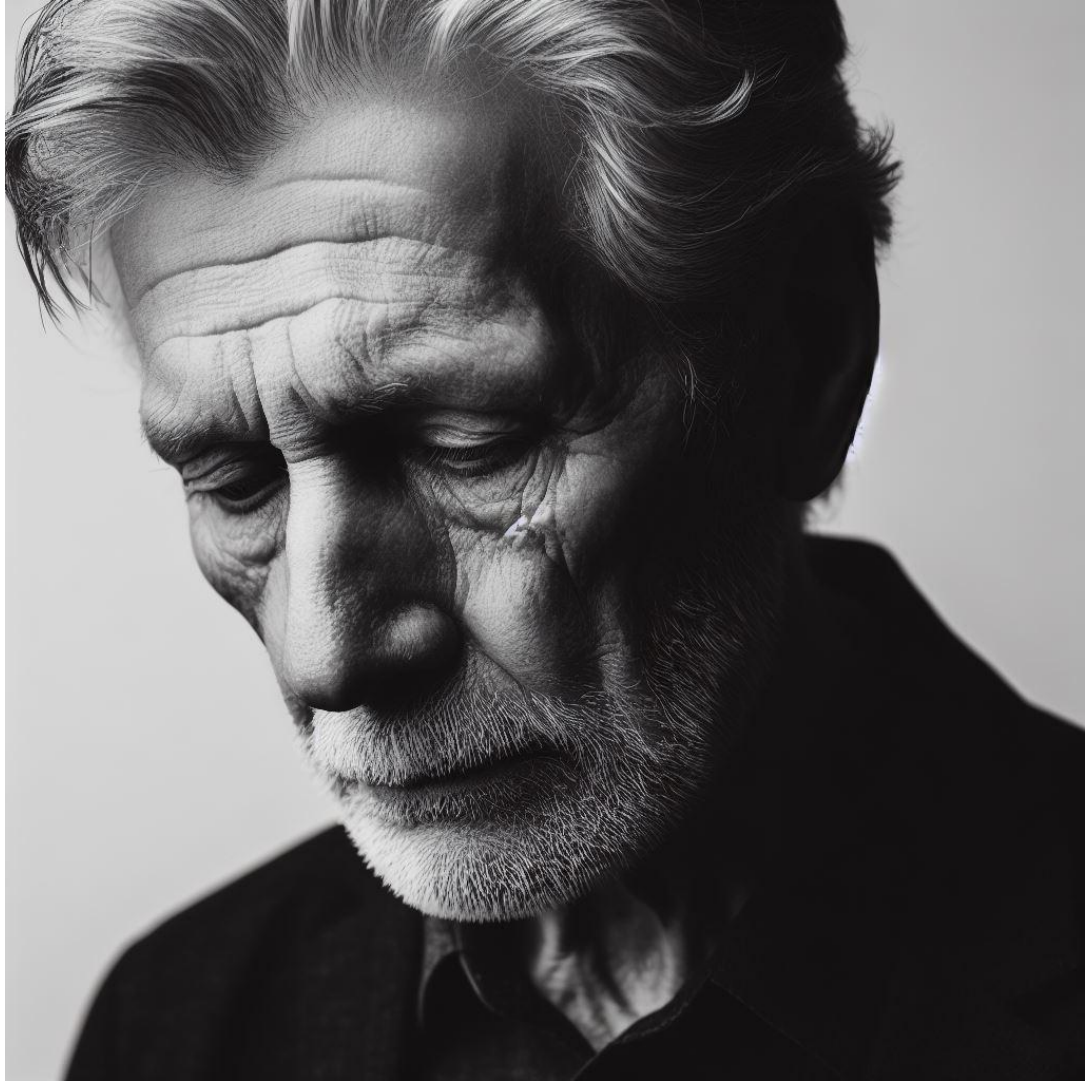
## Hoe wordt de prijs bepaald?

- Wat hebben ze in handen?
  (en vraag een voorbeeld)
  - Kan de data misbruikt worden?
    (bankgegevens, persoonsgegevens,
    concurrentieel nadeel, …)
- Wat heb jij in handen?
  (back-up)
- Hoe ziet je balans er uit?




**Zondag 15/10**
**13:30 PM ( +78,5u)**

cheops



## Maandag 16/10
## 12:00 PM (+4 dagen)

### Nieuwe tegenslag…

- De vraagprijs is te hoog.
- Feedback CCB
  “Hackersgroepering is erop uit om schade toe te brengen.”
- State-sponsored?

# Dinsdag 17/10
# 9:00 AM (+5 dagen)

## Een geluk bij een ongeluk…

**Back-up gevonden van 3m oud.**

- Gat van 3 maanden in je boekhouding.
  - Offertes, orders, doorbestellingen, facturen, …

## Woensdag 18/10
## 9:00 AM (+6 dagen)

### Basisfunctionaliteit hersteld:

- Medewerkers kunnen terug mailen en gebruik maken van Office.
- Teams Telefonie is geactiveerd.
- Bancontactterminals in de shops werken terug.

cheops

# Nasleep (+ 14 maanden)

## Het stopt hier niet…

- Data verloren en gelekt op het darkweb.
- Continue pogingen tot digitale inbraak.
- Phishingaanvallen.
- Phone Spoofing.
- Teams Spoofing.

# NIS2

03

# Network and Information Security Directive

# NIS2

## Uw verantwoordelijkheid, onze zorg

cheops

# Overzicht NIS2


- NIS2 is de nieuwe Europese richtlijn voor cyberbeveiliging die vanaf **oktober 2024** de bestaande NIS-richtlijn zal vervangen.

**18**
**sectoren**

- Het is de **meest uitgebreide EU-wetgeving op het gebied van cyberbeveiliging** tot nu toe, die 18 sectoren beslaat.

Lidstaten hebben **tot 17 oktober 2024** de tijd om de richtlijn om te zetten in nationale wetgeving. Dit betekent dat elke organisatie die onder de richtlijn valt, **wettelijk verplicht is om voor het vierde kwartaal van 2024 aan de eisen van de richtlijn te voldoen.**

Voor **18 maart 2025** moeten bedrijven in kritieke sectoren zich registreren bij het **Centre for Cybersecurity Belgium.**

# Het doel van NIS2

1. één **basisniveau van beveiligingsmaatregelen** vast te stellen voor leveranciers van digitale diensten en exploitanten van essentiële diensten
2. het **risico van cyberaanvallen** te **beperken**
3. het **algemene niveau van cyberbeveiliging** in de EU te **verbeteren**

# Valt uw organisatie onder de NIS2-richtlijn?

## Zeer kritieke sectoren en subsectoren

**Energie**

Elektriciteit, verwarming & koeling, gas, waterstof, olie

**Transport**

Via lucht, spoor, water, weg

**Bank**

Kredietinstellingen

**Financiële markt en infrastructuur**

Handelsplatformen, centrale partijen

**Gezondheid**

Zorgverleners, onderzoekslaboratoria, R&D, productie van farmaceutica

**Drinkwater**

Drinkwaterleveranciers

**Afvalwater**

Alleen als het een essentieel onderdeel is van de activiteit

**Digitale infrastructuur**

Vertrouwensdiensten, DNS service providers, naamregisters, digitale communicatiediensten, cloud service providers, datacenter service providers, content delivery netwerkleveranciers

**ICT-service management (B2B)**

Managed Service Providers, Managed Security Service Providers

**Overheid**

Centrale en regionale diensten, optioneel ook lokaal

**Ruimtevaart**

Operatoren van infrastructuur op de grond

# Valt uw organisatie onder de NIS2-richtlijn?

## Kritieke sectoren

**Post- en koerierdiensten**

Aanbieders van post- en koerierdiensten

**Voeding**

Productie, bewerking en verdeling

**Digitale diensten**

Online marktplaatsen, zoekmachines, sociale netwerken

**Afvalbeheer**

Indien het de hoofdactiviteit is

**Chemische producten**

Productie en verdeling

**Productie**

Medische apparaten, computers, elektronica, optica, elektrische toestellen, machines, motorvoertuigen, aanhangwagens, opleggers, andere transportmiddelen

**Research**

Onderzoeksorganisaties

# Valt uw organisatie onder de NIS2-richtlijn?

## Altijd essentieel

- aanbieders van **openbare elektronische communicatienetwerken of -diensten;**
- entiteiten die op **nationaal niveau** als kritiek zijn aangemerkt, zoals de sectoren energie, vervoer, elektronische communicatie en de financiële sector;
- **overheidsdiensten** (centraal niveau);
- **gekwalificeerde aanbieders** van vertrouwensdiensten en topniveau-domeinnaamregisters en DNS-dienstverleners.

## Essentiële entiteit

Actief in een **zeer kritieke sector** en een **groot bedrijf.**

## Belangrijke entiteit

Actief in een **zeer kritieke sector** en een **middelgroot bedrijf,** of actief in een **andere kritieke sector** en een **middelgroot of groot bedrijf.**

---

Een bedrijf wordt als groot beschouwd als het minstens **250 werknemers** heeft, of een jaaromzet van minstens 50 miljoen euro, of een balanstotaal van minstens **43 miljoen euro.**

Een bedrijf is middelgroot als het **50 tot 250 werknemers** heeft, of een jaaromzet of balanstotaal van meer dan **10 tot 50 miljoen euro.**

**NIS2 legt deze verhoogde beveiligingseisen ook op aan toeleveranciers en dienstverleners.**

# Het management kan verantwoordelijk worden gehouden

## Verantwoordelijkheden & sancties

### Verantwoordelijkheden

- Actief toezien op cybersecuritymaatregelen
- Cyberrisico's integreren in het bedrijfsrisicomanagement
- Budgetten en middelen vrijmaken.
- Regelmatige audits en controles
- Bewijsvoering bij controles
- Cybersecuritytraining voor bestuurders

### Sancties

- Bestuurlijke sancties, boetes voor de organisatie én het management
- Verbod om leidinggevende functies te bekleden
- Persoonlijke aansprakelijkheid bij grove nalatigheid

Niet-naleving kan resulteren in:

Boete van **>10 miljoen euro of 2% van de wereldwijde jaarlijkse omzet** voor essentiële entiteiten **en >1,7 miljoen euro of 1,4% van de wereldwijde jaaromzet** voor belangrijke entiteiten.

# Belangrijkste verplichting

**Zorgplicht**

Als een ‘goede huisvader’.

**Meldplicht**

- Binnen 24u – Escalatie
- Binnen 72u – Incidentmelding
- Binnen 1 maand – Eindrapport

NIS2
Directive

# Wanneer ben je “een goede huisvader”?

1

**Risico-analyse**

Breng en hou de netwerkomgeving in kaart en identificeer potentiële risico’s en kwetsbaarheden.

2

**Basisbeveiliging & procedures**

Stel beveiligings-protocollen en -procedures in en beperk je niet tot het IT-matige.

3

**Monitoring & auditing**

Voer een continue monitoring van de omgeving uit, met een proactieve aanpak, waarbij incidenten en acties bewaard worden in logboeken.

4

**Incident Response Plan**

Stel een incident response plan op (en test het).

5

**Training & Bewustwording**

Train medewerkers in cybersecurity op volcontinue basis om de kans op menselijke fouten te minimaliseren.

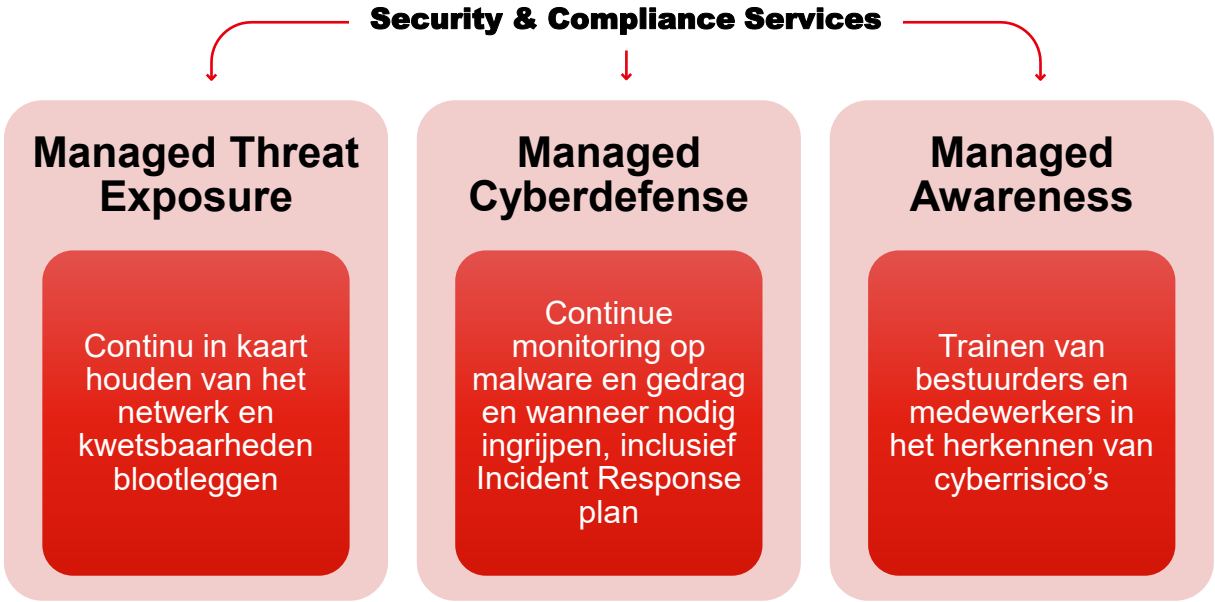
6

**Periodieke reviews & verbeteringen**

Volg op, rapporteer en verbeter waar mogelijk.

cheops

# Hoe Cheops u helpt de NIS2-principes af te dekken



# Key take aways

1. NIS2 is niet alleen een verantwoordelijkheid van IT. Het is een bedrijfsverantwoordelijkheid

2. NIS2 = Proactiviteit.

3. NIS2 = Een commerciële opportuniteit.

cheops

# Uw verantwoordelijkheid, onze zorg

- **Wat houdt NIS2 precies in?**
- **Hoe implementeert u de nieuwe Europese richtlijn stap voor stap?**
- **Hoe kan Cheops u hierbij ondersteunen?**

In deze whitepaper geven we u antwoord op de bovenstaande vragen.


Elke organisatie heeft de verantwoordelijkheid om zelf stappen te ondernemen rond de NIS2-regelgeving.

# Let's talk!


**Hoofdzetel**
Business Park Gate 7
Prins Boudewijnlaan 7 B – 2550 Kontich
T +32 3 880 23 00

**Brussel**
Corporate Village
Leonardo da Vincilaan 1 – 1935 Zaventem
T +32 2 486 13 00

**Gent**
Planet Group Arena
Ottergemsesteenweg-Zuid 808 B – 9000 Gent
T +32 9 274 15 00

**Kempen**
Dikberd 34 – 2200 Herentals
T +32 14 43 45 52

**Antwerpen**
Bredestraat 19 – 2000 Antwerp
T +32 3 500 00 25



cheops

# Van Dessel – Cyber Risk Solutions

De continuïteit en digitale veiligheid van uw onderneming op maat verzekerd

Van Dessel
Insurance Brokers


# Cyberverzekering

**Dekking van financiële kosten voor uw bedrijf tegen hackers en de impact van een ongeoorloofde toegang tot IT systemen of netwerk:**

- **Cyberaanval (hack, virus)**
- **Onderbreking van activiteiten**
- **Aansprakelijkheid (cyberincident, datalek, virusoverdracht)**

Van Dessel
Insurance Brokers

# Cyberrisico's voor uw bedrijf:

**Eigen personeel**
nog steeds
"zwakke schakel"

**+ 85%**
**ransomware**

**Kans op**
**cyberincident in**
België?

**Gemiddeld**
**€ 1.000.000**
**losgeldbedrag**

Van Dessel
Insurance Brokers

# Top 10 sectoren

- Industrie
- Technologie
- Gezondheidszorg
- Financiële diensten
- Consumentendiensten
- Zakelijke diensten
- Bouw
- Onderwijs
- Publieke sector

Van Dessel
Insurance Brokers

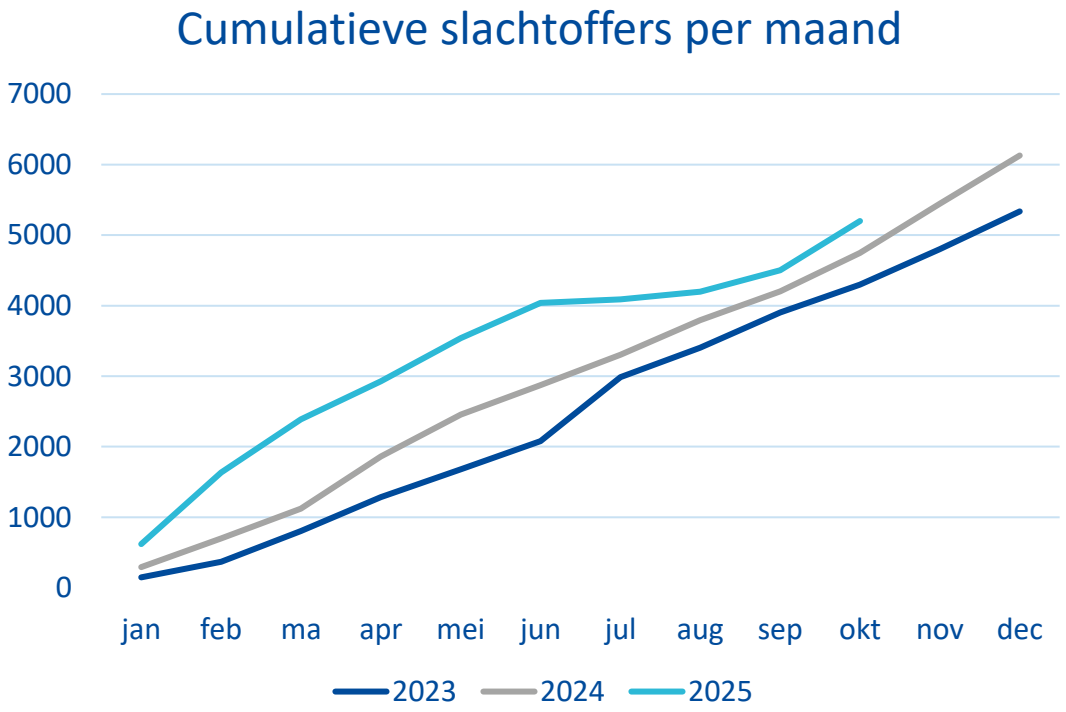
# Top Cyberaanvallen in 2024

1. **Social Engineering/Phishing**
   meest voorkomende aanval via e-mail en sms.
2. **Ransomware**
   data versleuteld, losgeld geëist
3. **DDoS**
   overbelasting van systemen

| | | |
|---|---|---|
| Zero-Day Exploits | Man-in-the-middle | Spoofing |

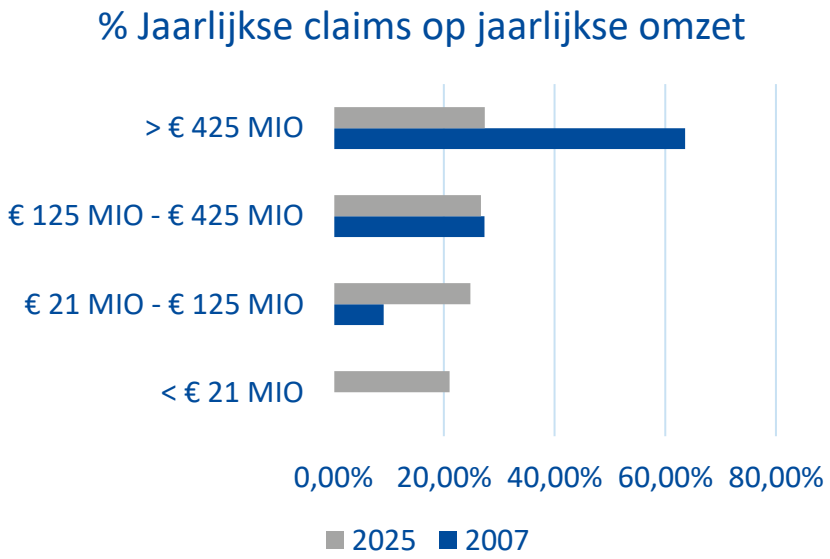
Van Dessel
Insurance Brokers

# Statistiek




Van Dessel
Insurance Brokers

# Risico verschuift



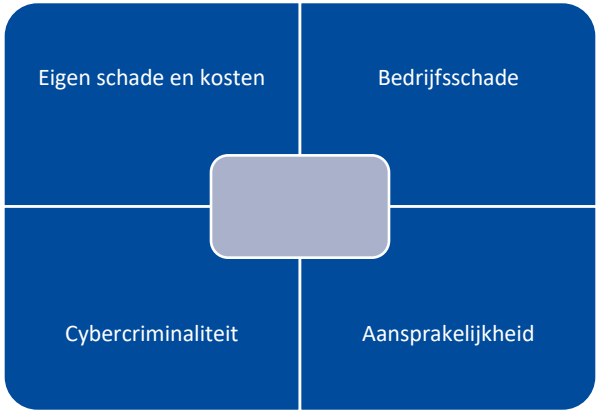

Van Dessel
Insurance Brokers

# Misvattingen over cyberveiligheid

| | |
|---|---|
| “Wij zijn te klein om interessant te zijn voor hackers.” | Ook kleine bedrijven zijn doelwit van phishing |
| “Een cyberincident heeft weinig impact, wij kunnen manueel werken..” | Incidenten leiden vaak tot grote operationele en financiële schade |
| “Onze beveiliging is goed en wij werken met een IT-partner.” | Vaak liggen menselijke fouten aan de basis, ook bij de IT-partner |
| “De cyberverzekering is te duur en zal niet tussenkomen bij schade.” | De hogere premie waarborgt bescherming en continuïteit bij de IT-incidenten |
| “Ons bedrijf gebruikt MFA en back-ups, dus wij zijn veilig.” | MFA kan omzeilt worden en back-ups zijn soms niet toegankelijk |

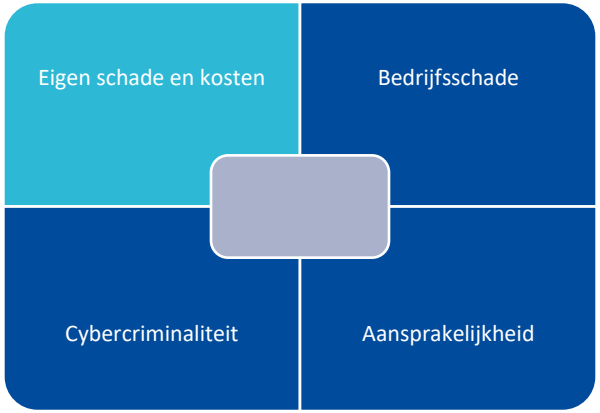
Van Dessel
Insurance Brokers

# Wat dekt de Cyberpolis?




Van Dessel
Insurance Brokers

# Wat dekt de Cyberpolis?

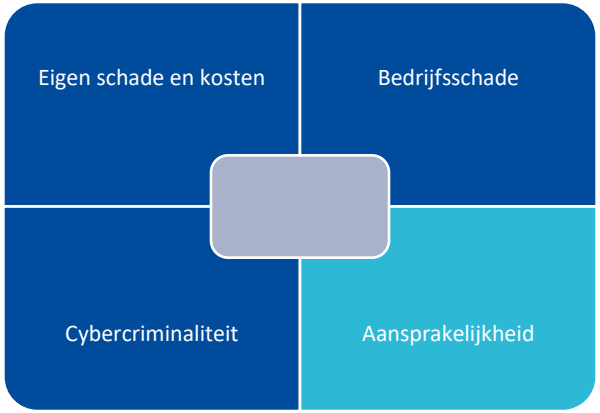



## Eigen schade en kosten

- **24/7 Bijstand**
- **Herstel data/systemen/software**
- **Kosten voor experten**
- **Administratieve onderzoeken & boetes**
- **Herstel reputatie & imago (beperkt!)**

Van Dessel
Insurance Brokers

# Wat dekt de Cyberpolis?

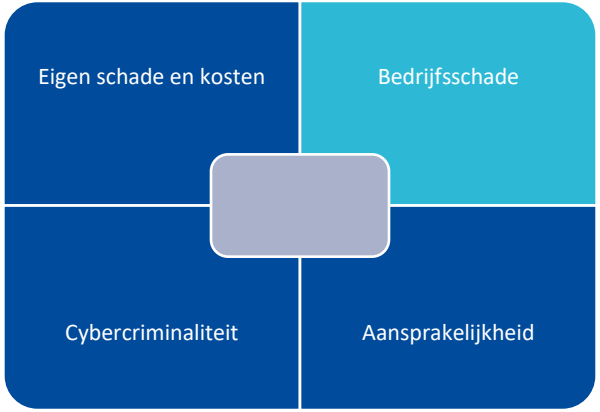



## Aansprakelijkheid

- **Multimedia aansprakelijkheid**
- **Privacy en netwerkaansprakelijkheid**
- **Verdedigingskosten en juridische bijstand**

Van Dessel
Insurance Brokers

# Wat dekt de Cyberpolis?

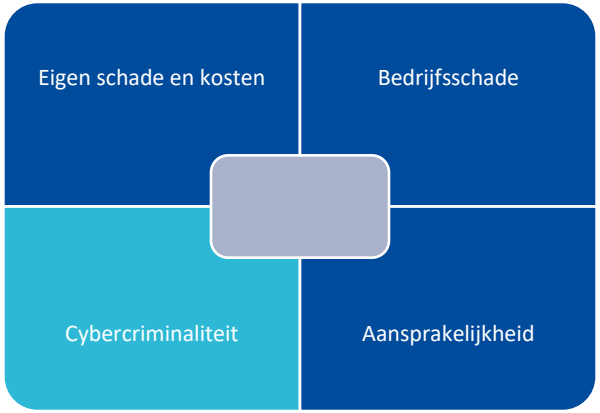



## Omzetverlies

- **Systeemfalen**
- **Cyberincident**
- **Uitbreiding IT-partners**
- **Uitbreiding non IT-partners (beperkt!)**

Van Dessel
Insurance Brokers

# Wat dekt de Cyberpolis?




## Cyber criminaliteit

- **Cyberafpersing & losgeld**
- **Cyberdiefstal (beperkt!)**
- **Hacking telefoonsysteem (beperkt!)**

Van Dessel
Insurance Brokers

# Van check-in tot grenscontrole: waarom hack bij één toeleverancier Brussels Airport zo zwaar treft

Jaguar Land Rover heeft nog steeds last van de gevolgen van een cyberaanval begin deze maand. De Britse automaker heeft de productiestop bij zijn drie Britse fabrieken verlengd tot 1 oktober.

De Waregemse onderdelenspecialist TVH heeft te lijden onder de gevolgen van een cyberaanval. De criminelen eisen losgeld van het bedrijf.


De Standaard

HACKING HACKING

Cyberaanval Antwerpen zal stad 'tot zeventig miljoen euro' kosten

05/01/2023 om 07:10

**Bedrijf verliest tienduizenden euro's na cyberaanval: "We raden hackingslachtoffers nochtans af te betalen"**

**$6 000 000 000 000**
Kost internetcriminaliteit wereldwijd in 2021

De Tijd

## Cyberaanval kost Antwerps bedrijf 300.000 dollar: 'Er was geen andere optie'

De zware ransomwareaanval die het Antwerpse ITxx en 65 bedrijven trof, is uitgelopen op de betaling van 300.000 dollar losgeld. 'Als de hackers wisten hoeveel klanten ITxx had, waren z

**Gemiddelde kost cyberaanval (BE):**
**€440.000** schade per incident

De brouwerijen van Duvel Moortgat zijn getroffen door een cyberaanval. Dat meldt Het Laatste Nieuws en het bedrijf bevestigt de info. De producties van alle Belgische brouwerijen liggen stil en ook de site van Kansas City in de Verenigde Staten.

**Kledingketen Lolaliza slachtoffer van cyberaanval, persoonlijke gegevens van klanten en personeel gehackt**

In 2022 kampte ons land met 37.982 cybercriminaliteitsincidenten.

Van Dessel
Insurance Brokers

# Uw eerste contact
# **bij Van Dessel**

**Robin Verlinden**
Business Developer Cyber

03 428 15 30
robin.verlinden@vandessel.be

Van Dessel
Insurance Brokers

# Bedankt voor uw aandacht!

Zijn er nog vragen?

Van Dessel
Insurance Brokers

# Wat wij doen, werkt voor u.

Vandaar, Van Dessel.

**Verzekeringskantoor Van Dessel NV/SA**
Misstraat 112, B-2590 Berlaar

+32 (0)3 482 15 30
info@vandessel.be

IBAN BE52 3200 7340 3509
BIC BBRUBEBB

www.vandessel.be