HANZESTROHM

Van Hack naar herstel

Reis door een Ransomware aanval

10 juni 2025

Jaap van Veen

Eén op de vijf Nederlandse bedrijven werd in 2024 getroffen door een cyberaanval. Bij grote ondernemingen lag dat aantal zelfs op bijna drie op de tien. Financiële schade kwam het vaakst voor, gevolgd door verlies van data en verstoring van bedrijfsprocessen. 21 mei 2025

governance-web.nl
https://governance-web.nl › nieuws › cyberweerbaarhei...

Cyberweerbaarheid van Nederlandse bedrijven blijft achter bij ...

Over samenvattingen • Feedback

Dutch IT Channel
https://www.dutchitchannel.nl › news › bijna-negen-op-...

Bijna negen op de tien bedrijven kreeg in 2024 te maken ...

17 jan 2025 — Bijna negen op de tien **bedrijven** kreeg in **2024** te maken met aanvallen op hun netwerk.

agconnect.nl
https://www.agconnect.nl › partner › check-point › recor...

Recordpiek cyberaanvallen in Nederland - AG Connect

30 okt 2024 — **Nederlandse organisaties incasseren in Q3 2024 gemiddeld 865 cyberaanvallen per week**, een stijging van 69%; Zorgsector de meest getroffen ...

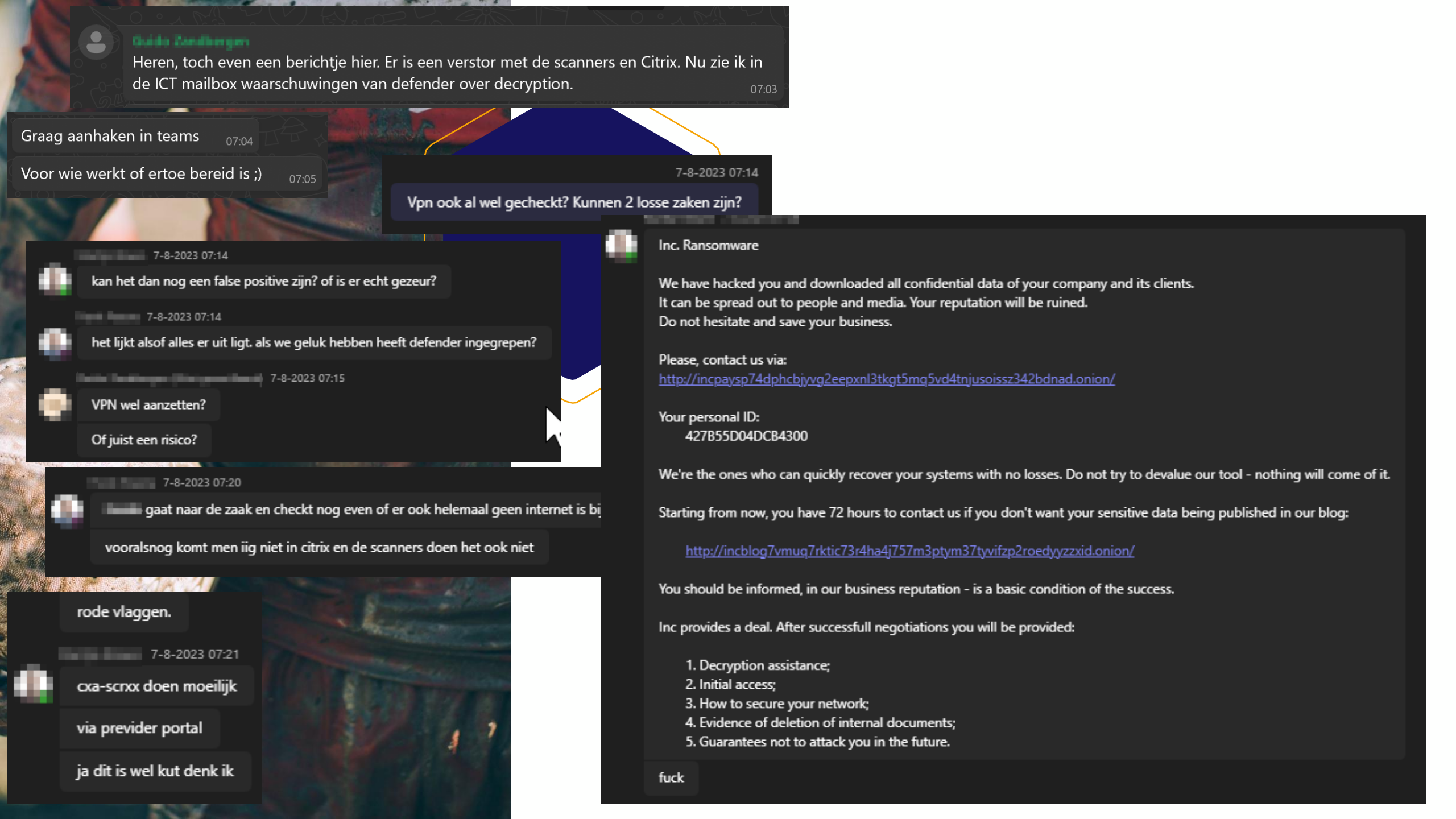
SecurityHive
https://www.securityhive.io › blog › een-op-de-vijf-ned...

Eén op de vijf Nederlandse bedrijven leed schade door ...

In 2024 kreeg 20% van de Nederlandse bedrijven te maken met schade door cybercriminaliteit.
Ontdek hoe u uw organisatie effectief beschermt tegen deze ...

BeveiligingNieuws
https://beveiligingnieuws.nl › een-op-de-vijf-nederlandse...

Eén op de vijf Nederlandse bedrijven getroffen door


Heren, toch even een berichtje hier. Er is een verstor met de scanners en Citrix. Nu zie ik in de ICT mailbox waarschuwingen van defender over decryption.
07:03
Graag aanhaken in teams
07:04
Voor wie werkt of ertoe bereid is ;)
07:05
7-8-2023 07:14
Vpn ook al wel gecheckt? Kunnen 2 losse zaken zijn?
7-8-2023 07:14
kan het dan nog een false positive zijn? of is er echt gezeur?
7-8-2023 07:14
het lijkt alsof alles er uit ligt. als we geluk hebben heeft defender ingegrepen?
7-8-2023 07:15
VPN wel aanzetten?
Of juist een risico?
7-8-2023 07:20
gaat naar de zaak en checkt nog even of er ook helemaal geen internet is bi
vooralsnog komt men iig niet in citrix en de scanners doen het ook niet
rode vlaggen.
7-8-2023 07:21
cxa-scrxx doen moeilijk
via previder portal
ja dit is wel kut denk ik
Inc. Ransomware
We have hacked you and downloaded all confidential data of your company and its clients.
It can be spread out to people and media. Your reputation will be ruined.
Do not hesitate and save your business.
Please, contact us via:
http://incpaysp74dphcbjyvg2eepxnl3tkgt5mq5vd4tnjusoissz342bdnad.onion/
Your personal ID:
427B55D04DCB4300
We're the ones who can quickly recover your systems with no losses. Do not try to devalue our tool - nothing will come of it.
Starting from now, you have 72 hours to contact us if you don't want your sensitive data being published in our blog:
http://incblog7vmuq7rktic73r4ha4j757m3ptym37tyvifzp2roedyyzzxid.onion/
You should be informed, in our business reputation - is a basic condition of the success.
Inc provides a deal. After successfull negotiations you will be provided:
1. Decryption assistance;
2. Initial access;
3. How to secure your network;
4. Evidence of deletion of internal documents;
5. Guarantees not to attack you in the future.
fuck

Dag 1: Adrenaline en actie!

“Iedereen weet wat ‘ie moet doen — of denkt dat te weten.”

Alle IT medewerkers naar kantoor.

Wachtwoord resetten

Lijstjes maken

Afstemmen Directie

Partners bellen

Servers uit.

Taken verdelen

Wat kan wel?

Wat kun je niet?

Back-ups terughalen

Medewerkers opvangen

Hulp zoeken

Pizza’s bestellen

Firewall dichtzetten

Wat is er gebeurt?

Citrix platform heeft een lek gehad. Na 3 weken gepatcht.

Ondertussen backdoor toegang geplaatst.

User account van onze IT partner is gehackt. Had géén MFA.

Lessen van dag 1.

Teamtraining nu al geslaagd.

Team is top!

- Taakverdeling gaat (bijna) vanzelf
- Veel kennis aanwezig
- Lek is boven
- Back-up strategie is goed > Z.s.m. recovery starten!
- Herstelstrategie is duidelijk

Zoek hulp

- Forensisch onderzoek
- Communiceren met hackers

Wij zijn verantwoordelijk!

- Controleer je uitbestede IT
- Houdt je omgeving up-to-date!

Dag 2: Wachten en onzekerheid.

Anderen laten werken is nog veel moeilijker

- Logging aanleveren
- Forensisch onderzoek vergt tijd
- Back-ups checken
- Communiceren, intern & extern
- Melding bij de Autoriteit Persoonsgegevens starten
- Besluiten wanneer je weer wilt gaan werken

Lessen van dag 2.

Blijf zelf in control.

Parate kennis

- Binnen 72 uur Melding AP doen
- Waar is je logging?

Behoud de leiding

- Intuïtief weet je team wat te doen
- Externen gaan geen beslissingen voor je maken

Blijf communiceren

- Medewerkers weten niet waar ze aan toe zijn

Dag 3: Stap voor stap weer aan het werk.

Wat is je herstelplan?

Wie heeft er recent een back-up plan getest?

Dag 3: Stap voor stap weer aan het werk.

Wat is je herstelplan?

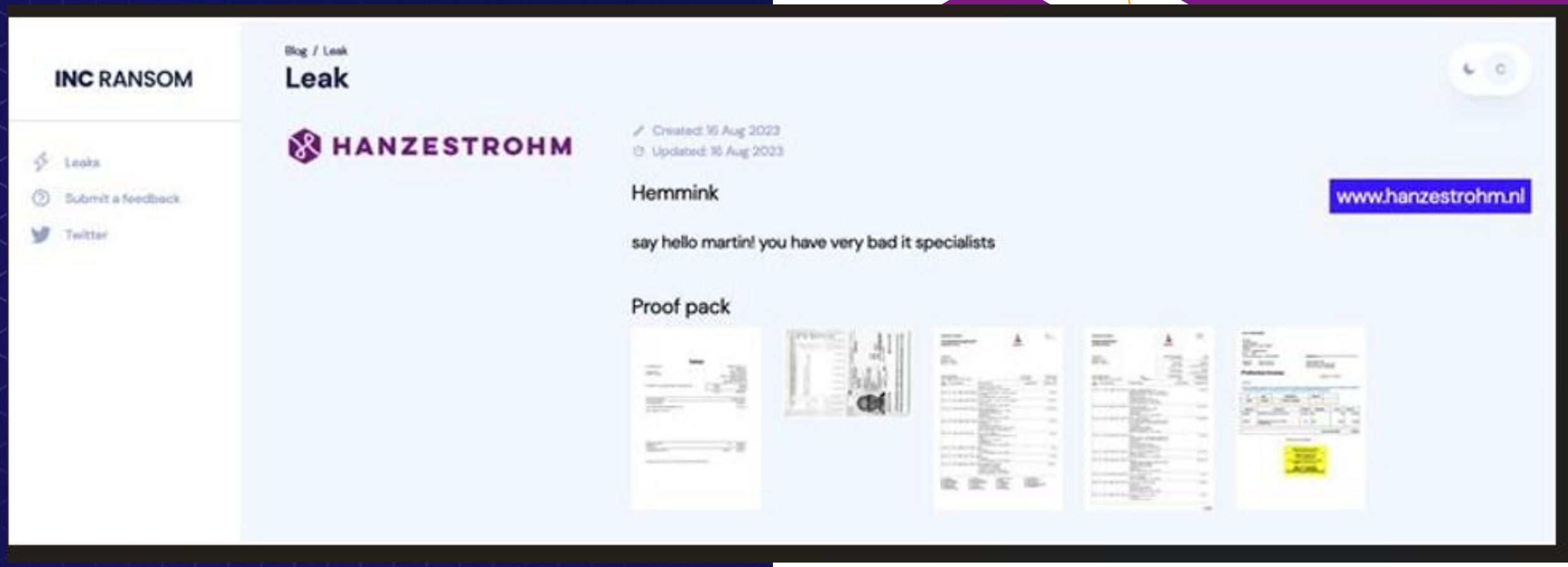
Wat je ook gaat doen die dag:

- Printers her-installeren die niet vanuit de back-up meer werken.
- Applicaties bigfixen omdat je niet weet waar het wachtwoord zit wat je hebt gereset.
- Iedereen opvangen die nog geen nieuw wachtwoord heeft ontvangen.
- **Heel veel begeleiden, communiceren, geruststellen en bevestigen dat men mag werken.**

De 2e klap

Impact en ontdekking van data diefstal

- Communiceren naar direct betrokkenen.

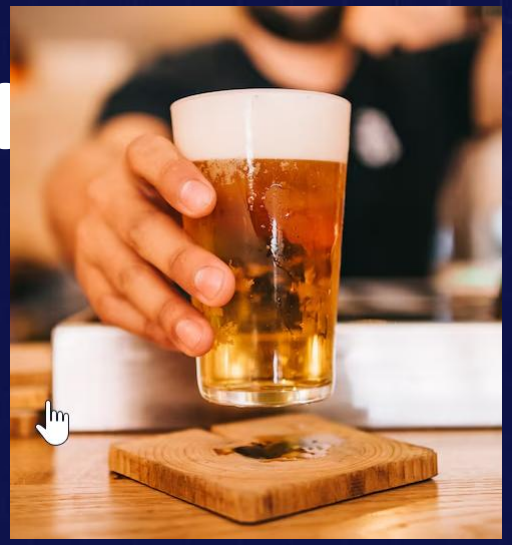


Lessen van dag 3.

Het lijkt erger dan het is

- Directie is ondersteunend
- Medewerkers zijn behulpzaam
- Klanten hebben begrip
- Hackers spelen blufpoker
- je data staat niet gelijk online
- Journalisten vinden dit interessant

Einde v/d weel



werk achterstand logistiek ingehaald.

Melding bij de

ifte bij de politie proberen te doen.

Korte termijn

En dan begint het werk pas…

Je team voelt zich slecht!

Stap 1. Doe alles wat je snel kunt fixen:

- Servers updaten
- Software weggooien
- Bestanden opschonen
- Account rechten limiteren
- MFA verplichten, ook waar het niet kan
- Protocollen blokkeren
- Password manager buiten netwerk
- Firewall opschonen

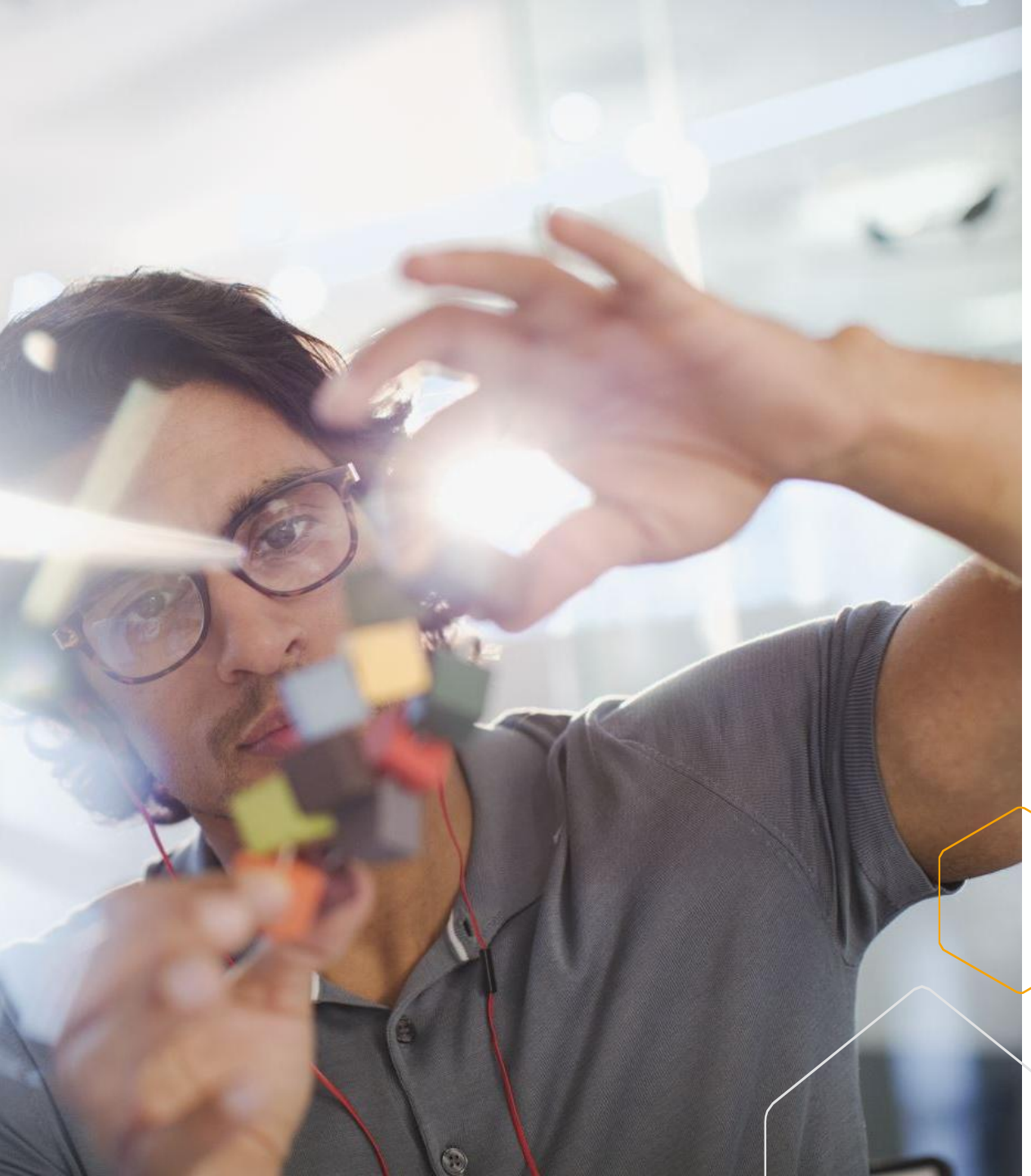
Midellange termijn

En dan begint het werk pas…

Hoe doen we dit beter?

Stap 2. Werk aan een toekomstbestendige structuur

- Security verantwoordelijke aanstellen
  - Pentesten organiseren
  - Security Awareness training
  - Baselines opzetten naar best practices
- Teamafspraken maken
  - Iedere dag lezen we security.nl
  - Hoe gaan we om met security dreigingen?
- Systemen verminderen, up-to-date brengen/houden
  - Citrix Uitfaseren, Servers updaten
- Informatiebeveiligingsbeleid schrijven



Lange termijn

En dan begint het werk pas…

Hoe borgen we dit?

Stap 3. Wees altijd in control

- Houdt je personeel up-to-date en scherp
  - Blijf communiceren & trainen
- Laat je auditen, om te leren en verbeteren
  - Blijf pentesten, iedere keer een stapje verder
- NIS2 & ISO27001 Certificeringen
  - Richt je procedures in, en toon aan dat je ze doet.
    - Screen nieuwe applicaties
    - Check en test je back-ups
    - Review je rechten & rollen
    - Check onveilige software & protocollen

Wat doen we (nog) niet?

En dan begint het werk pas…

Cyber risico verzekering.

Managed Detection & Respons.

De nieuwe realiteit

Hoe heeft dit nu impact op de gehele organisatie?

- Patchen gaat vóór werken
- MFA, SSO, IAW
- Verplichte Training
- Minder ICT tijd naar Business
- Wachtwoord Managers
- Applicatie screening
- Phishing Tests
- Business Continuity Plan

Zijn we dan klaar?

Cybercrime is een groeiende business

NCSC

2019: 13% Nederlander slachtoffer

2023: 16% Nederlander Slachtoffer

Kaspersky

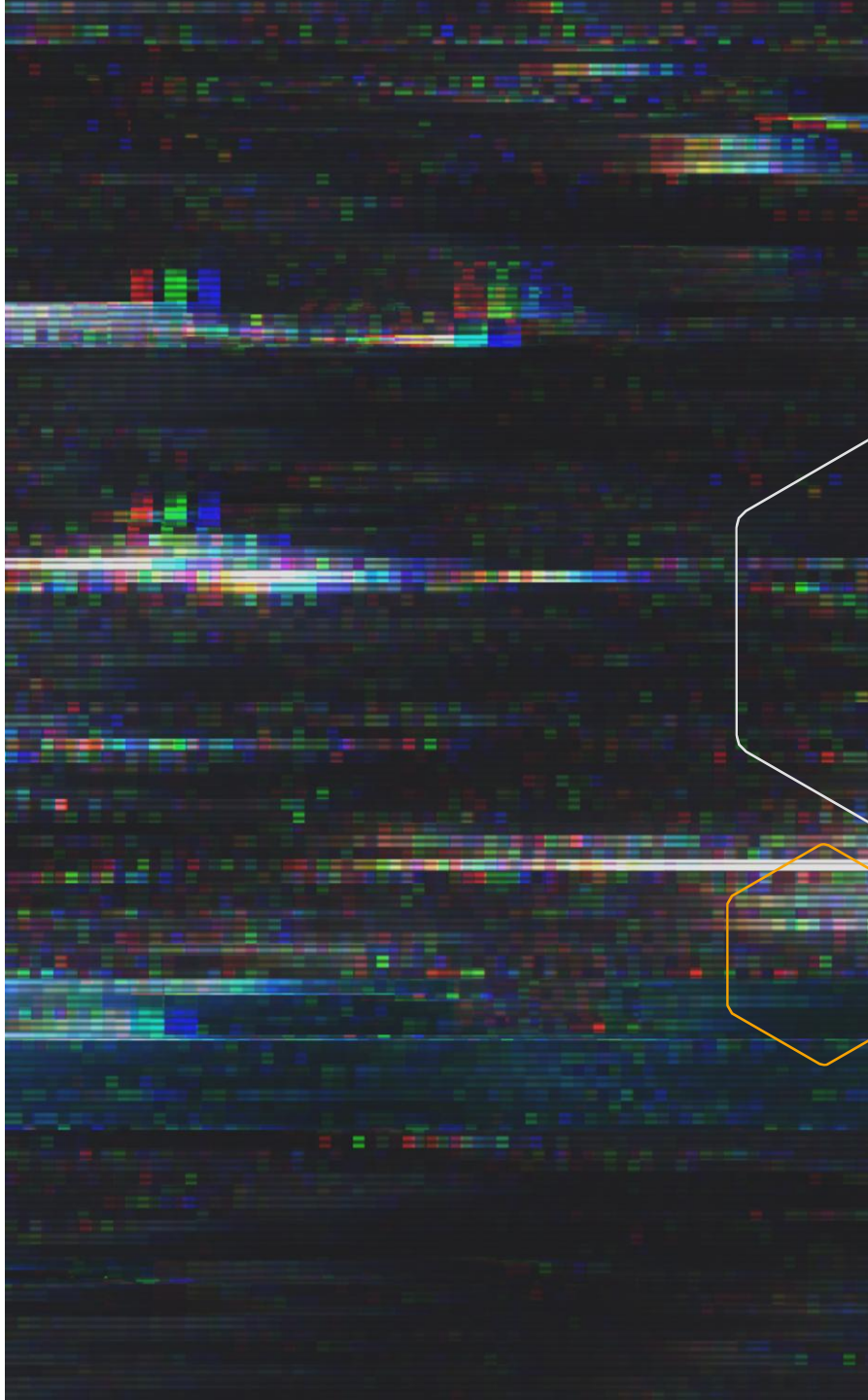
2023-2024 77% MKB Cybercrime

€ 270.000,- Schade per incident

1 op de 6 bedrijven doet een melding

1 op de 4 MKB bedrijven: groot risico

28% MKB bedrijven is voorbereid



Uitdagingen in de toekomst

Hackers verplaatsen zich naar Cloud Applicaties

Hoe bereid je je voor op de toekomst?

Quantum Computing gaat wachtwoorden kraken makkelijker maken

Artificial Intelligence gaat Phishing verbeteren en intensiveren

Multi Factor Authenticatie kan ook gehackt worden

Als je business digitaliseert, ben je hier ook verantwoordelijk voor

Interactie & Reflectie

Is jouw onderneming:

Bewust van risico op een cyber aanval?

Klaar voor een ransomware aanval?

In control op cyber security?

Vanuit de directie betrokken by cyber security?

Klaar voor de cyber beveiliging wet (NIS2)?

Verzekerd tegen cyber risico’s?

Kom in contact

Jaap van Veen

ICT Manager

j.van.veen@hanzestrohm.nl 06-10313416 Popovstraat 1, 8013 RK, Zwolle

HANZESTROHM