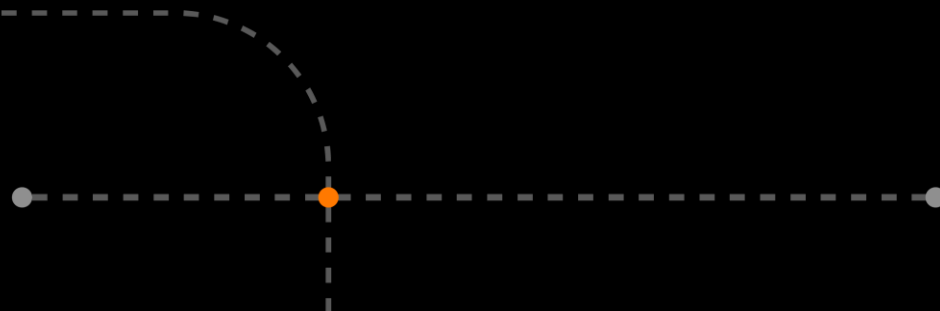




# Cyber-attack: the day after (en veel langer...)

**Ivo Jacobs**

Managing Director, H.H. Hospital of Mol





H. HARTZIEKENHUIS  
MOL

# It en onze organisatie



IT zou ons moeten ondersteunen, daar merk ik niet veel van.

Ik wil snelle en onbeperkte toegang tot de systemen.

Veel wisselen van wachtwoorden is ongemakkelijk.

Ik weiger '2 factor authenticatie' – het is pesterij.

Waarom maken ze (IT) het mij zo moeilijk?

Die 'black screens' binnen de 5' moeten afgeschaft worden.

.....

# Once Upon a Time



H. HARTZIEKENHUIS  
MOL

**Start IT mdwk – IT Performance issues**

+

7:15



H. HARTZIEKENHUIS  
MOL



# Start IT mdwk & performance issues

## Performance issues

- Zabbix – management console – IT departement  
Performance indicator → vertraging van de systemen
- Ongewone activiteit van de DC (domain controller)  
(scripts → account uitgeschakeld)



# Dinsdag, 2 februari 2021

Start IT mdwk & performance issues

7:15

8:00

Performance issues  
bevestigd  
Ransomware  
gevonden



# Dinsdag, 2 februari 2021

Start IT mdwk & performance issues

7:15



8:00

Performance issues  
bevestigd  
Ransomware  
gevonden





8:00



## Ransomware gevonden

Oops! Some files in your computer are encrypted!

You can try to contact data recovery companies, They will tell you that they cannot decrypt.

If you want to decrypt all files, you need to pay some fees. You can send me two small encrypted files and encrypted uuid to make sure I can decrypt them.

You can buy BTC through localbitcoins.com, I will send you the decryption tool when the payment is confirmed.

File Extension:  
.strike

Contact Emails:  
SheilaBeasley@tutanota.com  
CarolynDixon@tutanota.com

Attention! Please send the mail to all mailboxes at the same time!

Encrypted UUID:  
0f5cbf7b-741d-4576-9a8d-b71628a7acef2f



8:00



## Ransomware gevonden

- EPD niet aangetast
- Stop internet, intranet, programma's, intern/extern email verkeer...
- Isolatie backup files

Oops! Some files in your computer are encrypted!

You can try to contact data recovery companies, They will tell you that they cannot decrypt.

If you want to decrypt all files, you need to pay some fees. You can send me two small encrypted files and encrypted uuid to make sure I can decrypt them.

You can buy BTC through localbitcoins.com, I will send you the decryption tool when the payment is confirmed.

File Extension:  
.strike

Contact Emails:  
SheilaBeasley@tutanota.com  
CarolynDixon@tutanota.com

Attention! Please send the mail to all mailboxes at the same time!

Encrypted UUID:  
0f5cbf7b-741d-4576-9a8d-b71628a7acef2f





# Dinsdag 2 februari 2021

Start IT mdwk & performance issues

7:15

Performance issues  
bevestigd  
Ransomware  
gevonden

8:00

Crisis cell (management, vpken,  
artsen...): impact?

9:00



9:00



## Crisis cell (management, verpleging, artsen, ...): impact?

- Activatie intern rampenplan (noodplannen – business continuity)
- Contact met verzekering (cyber insurance)
- Contact CERT – politie, overheid
- Intake & study environment → Installeren recovery plan → Contact externe IT experts (verzekering).
  - Isolatie alle (mogelijk) geïnfecteerde systemen.
  - Complete IT shutdown



9:00



## Crisis cel impact

### Communicatie

- Intern: WhatsApp pyramide  
→ noodmaatregelen voor aanwezige patiënten  
Cave: conflict IT veiligheid vs patient veiligheid  
Wie beslist?
- Extern → partners, overheid, ZNI (koepel).  
Via beveiligde internet connectie

### Conflict

- IT afdeling: alles onmiddellijk stop zetten
  - Artsen/verpleging: data over aanwezige patiënten toegankelijk houden (EPD)
- Wie is 'in the lead'?





# Dinsdag 2 februari 2021

Start IT mdwk & performance issues

7:15

8:00

Crisis cell (management, vpken,  
artsen, ...): impact?

9:00

16:00

Performance issues  
bevestigd  
Ransomware  
gevonden

Externe IT experts

Start recovery



16:00

## Externe IT experts

### Externe IT experts

- Objectieven
    - Definiëren 'gecorrumpeerde systemen' (50 van > 800)
    - Definiëren ransomware type
    - Definiëren backup and herstel opties
    - Definiëren en prioritiseren te herstellen systemen
- IT crisis team: analyse van de technische problemen/oplossingen



16:00

## Externe IT experts

- Operationele crisis cel → business continuity plan
  - Artsen, verpleging, administratie, receptie...
  - Planning, data verzameling, receptie, contacten, ...





### Start recovery plan (externe IT experts)

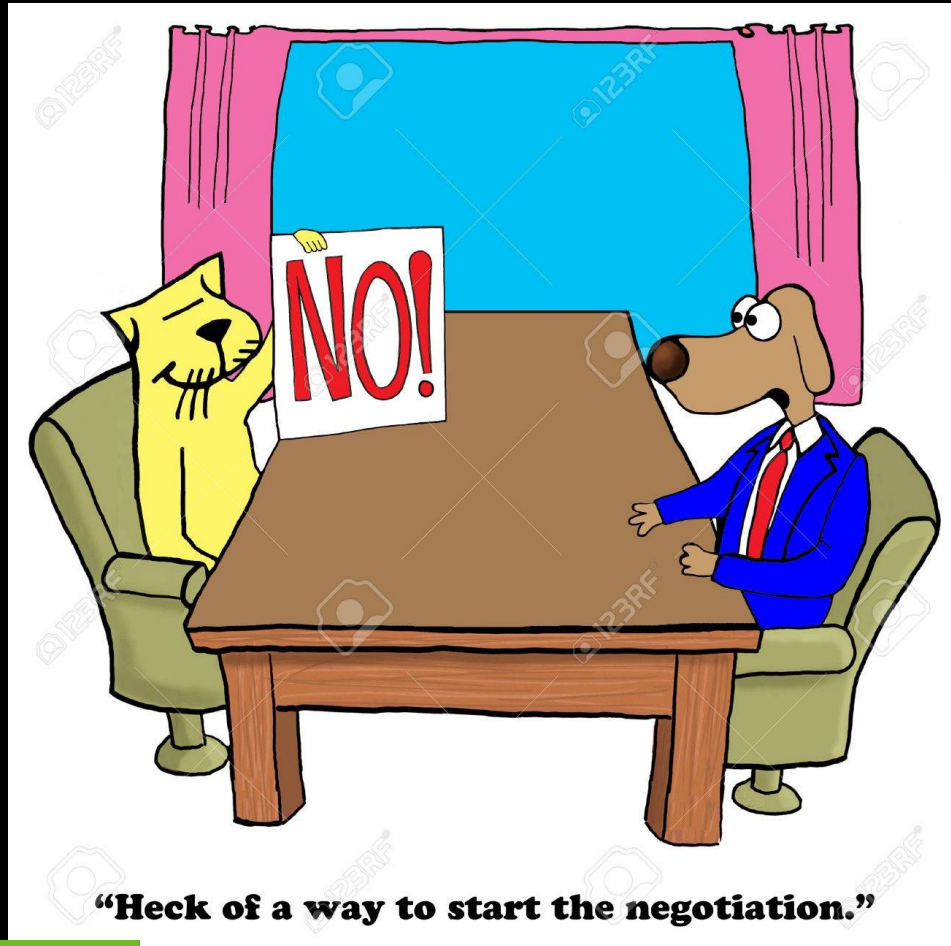
- Opdeling geïnfecteerde – niet geïnfecteerde systemen / Isolatie
- Re-installatie & cleaning: ‘Was straat’.
- Installeren complete antivirus software  
De-installeren antivirus ziekenhuis – nieuwe software
- Start installatie backup data



Contact met de aanvallers



# De volgende dagen



Onderhandelen met de 'aanvallers': IT experts + verzekering

- Ethische aspecten
- Schadekosten - recovery □ Wie beslist?
- Patiënt veiligheid in gevaar?

'Business model' cybercriminelen:

- Beloften?
- Veiligheidsissues?
- Data lekken?
- Geloofwaardigheid?  
→ Eerlijke bedriegers





Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?


Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f



Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f


Hello, if you want to decrypt all files, you need to pay  BTC.



Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay  BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.






Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay  BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.


If you don't want to pay, please don't bother me.



Hi,

It looks like you have encrypted our systems. We are a Belgium Hospital. Our patients are in serious danger. Can you provide us the decryption key please, so we can start recovering our environment?

Our UUID is: 0f5cbf7b-741d-4576-9a8d-b71628a7acef2f

Hello, if you want to decrypt all files, you need to pay  BTC.

Do you understand that you encrypted the network of a hospital? Lives of people could be at stake. I urge you to provide the decryptor for free and as soon as possible, so the impact is minimum.

If you don't want to pay, please don't bother me.

Ok, let me discuss this with the board of the Hospital.





# Conclusie



- Het zijn beleefde jongens, die criminelen....
- Maar je kan er niet mee onderhandelen....



# Conclusie



- Het zijn beleefde jongens, die criminelen....
  - Maar je kan er niet mee onderhandelen....
- TENZIJ....



# Conclusie



- Het zijn beleefde jongens, die criminelen....
- Maar je kan er niet mee onderhandelen....

TENZIJ....

- De gevraagde 'ransom' daalt snel.
- Desinteresse



# De volgende dagen

## Root cause analysis.

- Hacking website (Sharepoint) → toegang via een oud DC account (op systeem niveau)

## Probleem: service account suppliers & remote support

## Externe communicatie

- Wat is er gebeurd?
- Impact intern
- Impact op patiënten?
- Wat hebben we gedaan om snel herop te starten?
- Timing van recovery?

## Uitvoeren recovery plan (vervolg)

- Reinstalleren van alle connecties
- Nieuwe username and password 'big bang' (papier!)
- 2 Factor Authentication



# Lessons learned





# Lessons learned

## Organisatie

- Information Security Management System (PDCA cyclus) □ ISO27001 of NEN7510
- Investeer in IT-team (training in cybersecurity en recovery)
- Fysieke veiligheid (access control)
- Business Continuity Plan
- Procedure Cyber Verzekering – wees klaar voor het ‘CERT’ (network description)

## Policy

- Policy (clean-desk, accurate password policy, incident readiness, ...)

## Gedrag

- Awareness!

## Technisch



# Lessons learned

## Technisch

- Nieuwe website
- Investeer in security monitoring, detectie and antwoord
- Office 365 migratie
- MFA (multi factor authentication)
- Uitzuiveren Active directory & remote support & service (SilverFort)
- Vulnerabilities en patches
- Netwerk segmentatie
- Netwerk toegangscontrole (802.1x)
- Backup & recovery (belang van off-line backup)
- Uitzuiveren IAM (bvb. Na ontslag!)
- Verbeter werkstation security (Anti virus next level - EDR solution)
- Forensic readiness (controle logs)
- Backup internet en telefoon lijnen
- (RDP – Citrix – Office macro's - ....)



# Financiële schade...

## Directe kosten

- IT Experts – 450 €/u...  
5 dagen, 12 u/dag, 4 pers + remote... → Totale kost van 180K
- Eigen (human) resources (MDs, secretariaten, receptie...)
- Aanschaf nieuwe software/hardware



## Indirecte kosten

- Onmiddellijke schade: stop medische activiteiten (bvb alle onderzoeken, operaties,... )
  - Toekomstige schade: gemiste (nieuwe) afspraken
  - Verlies van informatie (rekeningen, ...?)
  - Herstellen van gemiste informatie
  - Reputatie schade
  - Medische schade?
  - Wat als vragen (data lekken, ...)
- Totale kost: 700 – 1.000 K.



# We hebben nu geen verzekering meer ...

- Onmiddellijke stopzetting huidige polis
- Eerst de exacte schade (claim) bepalen, vooraleer nieuwe 'offerte'
- Geen andere maatschappijen meer bereid gevonden
- Strenge voorwaarden (offers you can't refuse)...
- Externe supervisie – controle?

Outsource IT?



# Actie plan



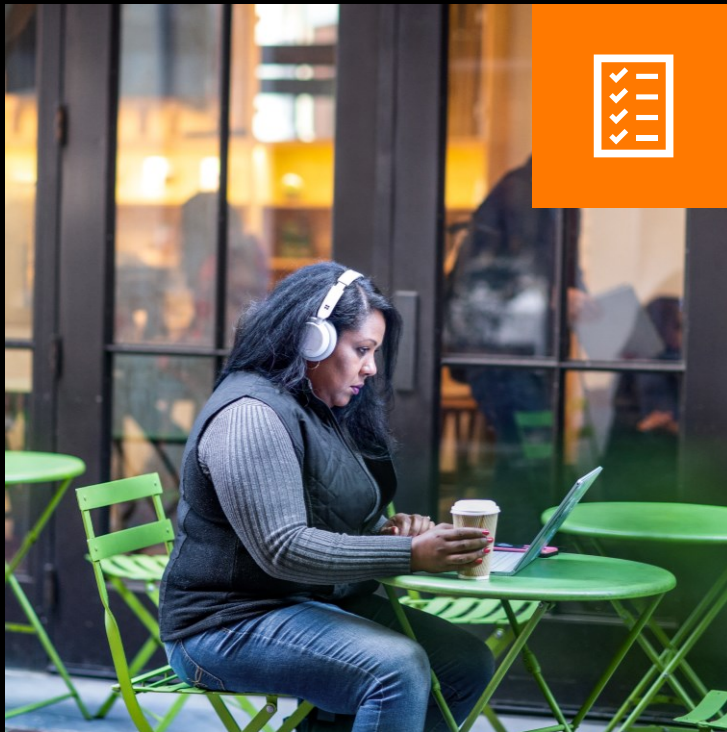
H. HARTZIEKENHUIS  
MOL



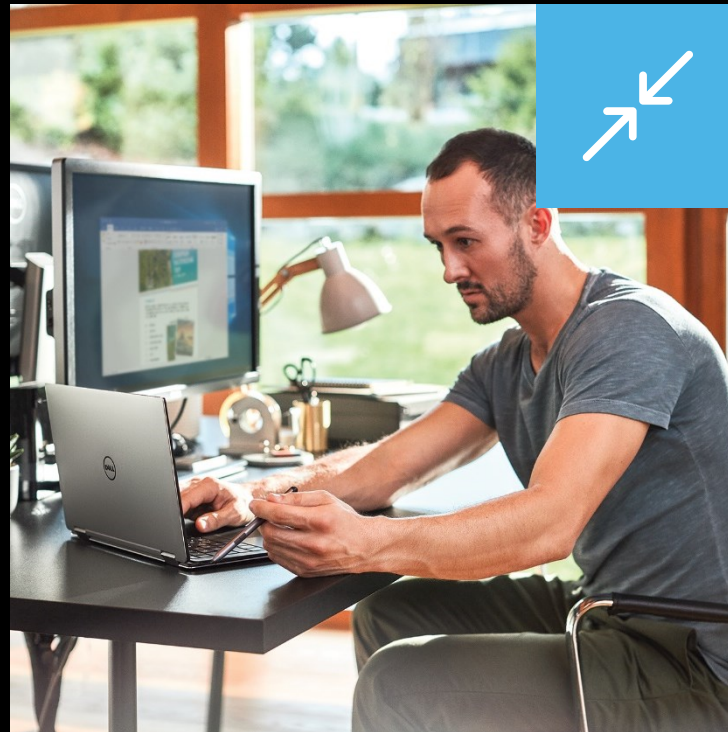
# Tijd voor een 'Zero Trust' benadering....



# Zero Trust: een nieuwe realiteit noopt tot nieuwe principes...



Verify explicitly



Use least privileged access



Assume breach







# Zero Trust set-up H.H. Mol

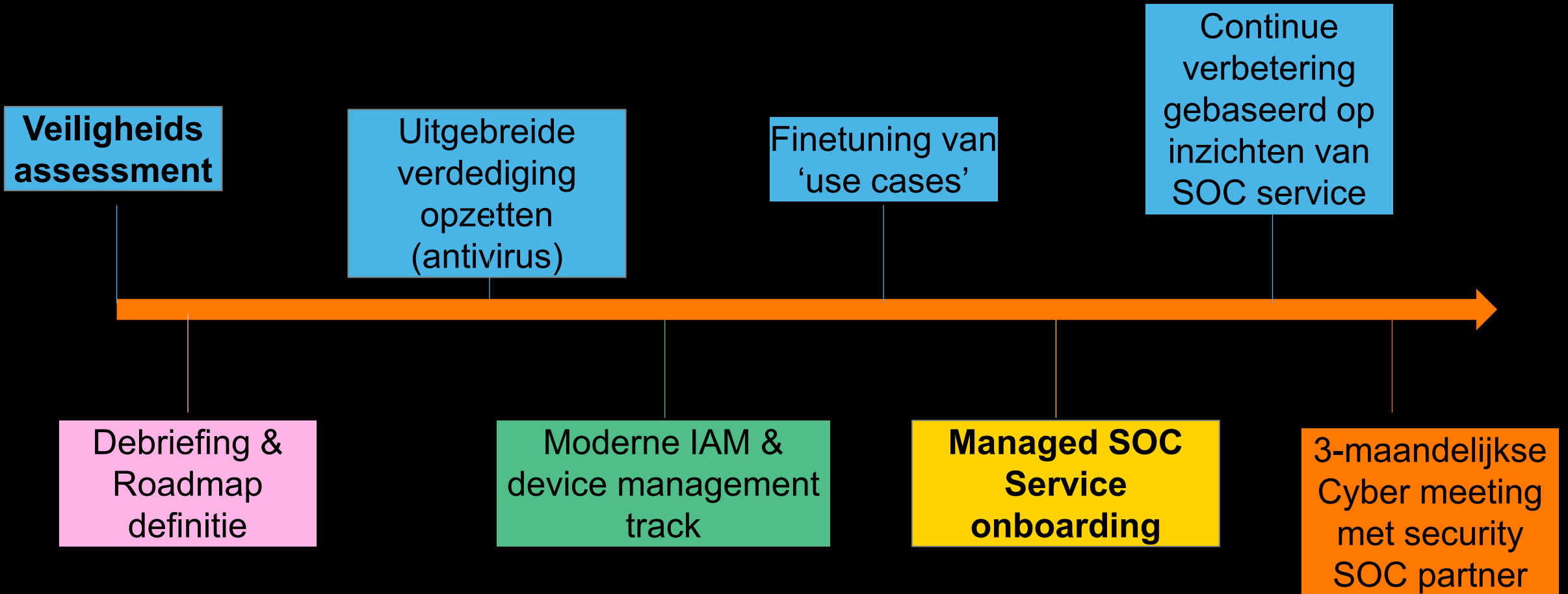


H. HARTZIEKENHUIS  
MOL



H. HARTZIEKENHUIS  
MOL

# Tijdslijn H.H. Mol



# Waarom SOC as-a-service?

- **Ontlasten eigen diensten: cybersecurity follow-up is complex: gespecialiseerde kennis en & 'resources' zijn vereist**
- **Follow-up is nodig**

## Proactief

- Inzichten van SOC zijn de basis voor steeds evoluerende verbeteracties, door zowel technologische evolutie als door (toenemende kennis van) 'secops' (security operationals).
- Maandelijks SOC rapport + 3-maandelijkse meeting waarbij open kwetsbaarheden en aanbevelingen opgelijst en bediscussieerd worden.

## Reactief

Incidenten worden niet altijd 'automatisch' opgelost door de technologie – manuele opvolging en interventie zijn (soms) nodig.

Wendbaarheid is belangrijk in cybersecurity.

- **SOC is (vaak) een voorwaarde voor (betaalbare) cybersecurity verzekering**





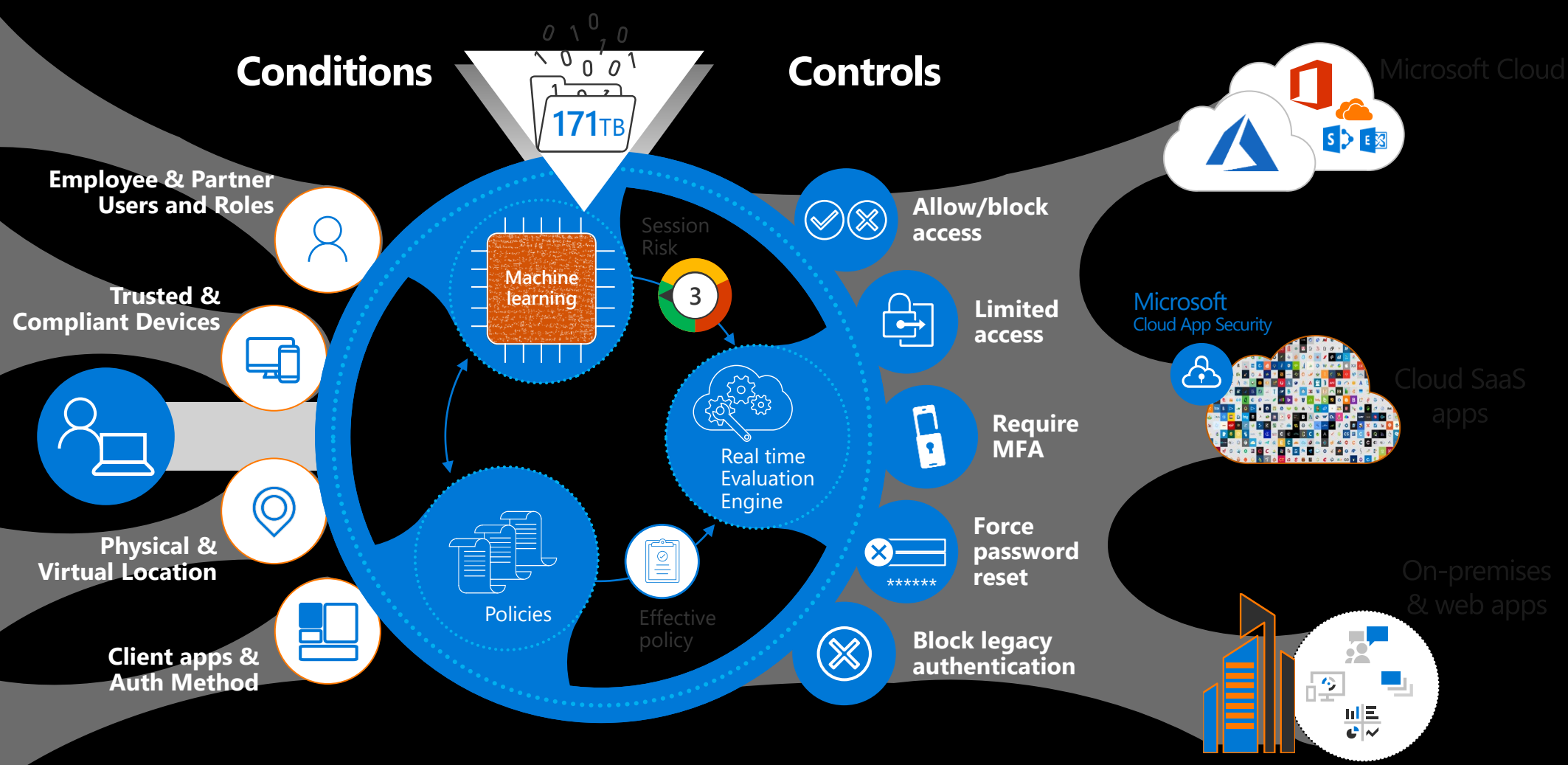
# Azure AD Conditional Access + Identity Protection

- Azure AD
- ADFS
- MSA
- Google ID

- Android
- iOS
- MacOS
- Windows
- Microsoft Defender for endpoints

- Geo-location
- Corporate Network

- Browser apps
- Apps



# Algemene conclusies



# Algemene conclusies



*Elk nadeel  
HEB ZIJN  
voordeel  
- Johan Cruijff*



# Algemene conclusies



*Elk nadeel  
HEB ZIJN  
voordeel  
- Johan Cruijff*

Als wij de bal hebben kunnen  
hun niet scoren.

- Johan Cruijff

Citaten.NET



H. HARTZIEKENHUIS  
MOL

# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES



H. HARTZIEKENHUIS  
MOL



# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES



H. HARTZIEKENHUIS  
MOL

# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin

AZ QUOTES

For every level  
there's another Devil.

Tyrese Gibson

RAISE  
AWARENESS !




H. HARTZIEKENHUIS  
MOL

technisch werk - Google Zoeken x H. Hartziekenhuis Mol Phished A x +

https://azmol.phishedacademy.io/nl/auth


Favorieten importeren | HHMOL | Feedback betreffen... | Introductiepagina - ... | Geïntegreerde labo... | Algemene Ziekenh... | Web Access - Tresorit | Traffic



## Welkom bij H. Hartziekenhuis Mol Phished Academy!

E-mail

Meld je aan

 Dutch

14:55 3/10/2023



# Awareness: opleidingen.

Phished Academy

https://azmol.phishedacademy.io/nl/academy/modules/b95a9b49-48df-4436-98af-96f80dff1635/session/935495d4-f959-4d33-95ee-c59d57bfd03/content/quiz/7ac57dce-be0b-4573-aa27-147ce8...

Favorieten importeren HHMOL Feedback betreffen... Introductiepagina... Geïntegreerde labo... Algemene Ziekenh... Web Access - Tresorit Traffic

**H. HARTZIEKHUIS MOL**

- Dashboard
- Trainingen
- Jouw score
- Let's Secure This Now 17
- Threats 1

Dutch

Privacy

[> Meld je af

3 van 9

**Je krijgt een onverwacht berichtje van een pakjesdienst. Ze zouden een pakje voor je hebben dat ze niet kunnen bezorgen. Waarom is dit verdacht?**

Kies het juiste antwoord. Meerdere antwoorden mogelijk.

- Ik heb geen pakje besteld
- Het e-mailadres ziet er vreemd uit
- In de e-mail staat een volgnummer
- De e-mail is niet opgemaakt in de gebruikelijke huisstijl van het bedrijf
- Het tijdstip waarop de e-mail is verzonden
- De aanspreekvorm is onpersoonlijk

Terug

Verzend

FEDEX <hfdka45@live.com> 01/07/2022 05:36am

Stefan Vergucht

Dag,

Er werd een pakje naar jou gestuurd met trackingnummer 484938372625373901. Vandaag tussen 7.00u en 18.00u zal het jou worden bezorgd. Om je pakket te kunnen ontvangen, vul dan je gegevens aan via deze [link](#). Indien je dit niet doet, zal het pakket vertraging oplopen.

Groet,  
Het FedEx departement

**FedEx.**

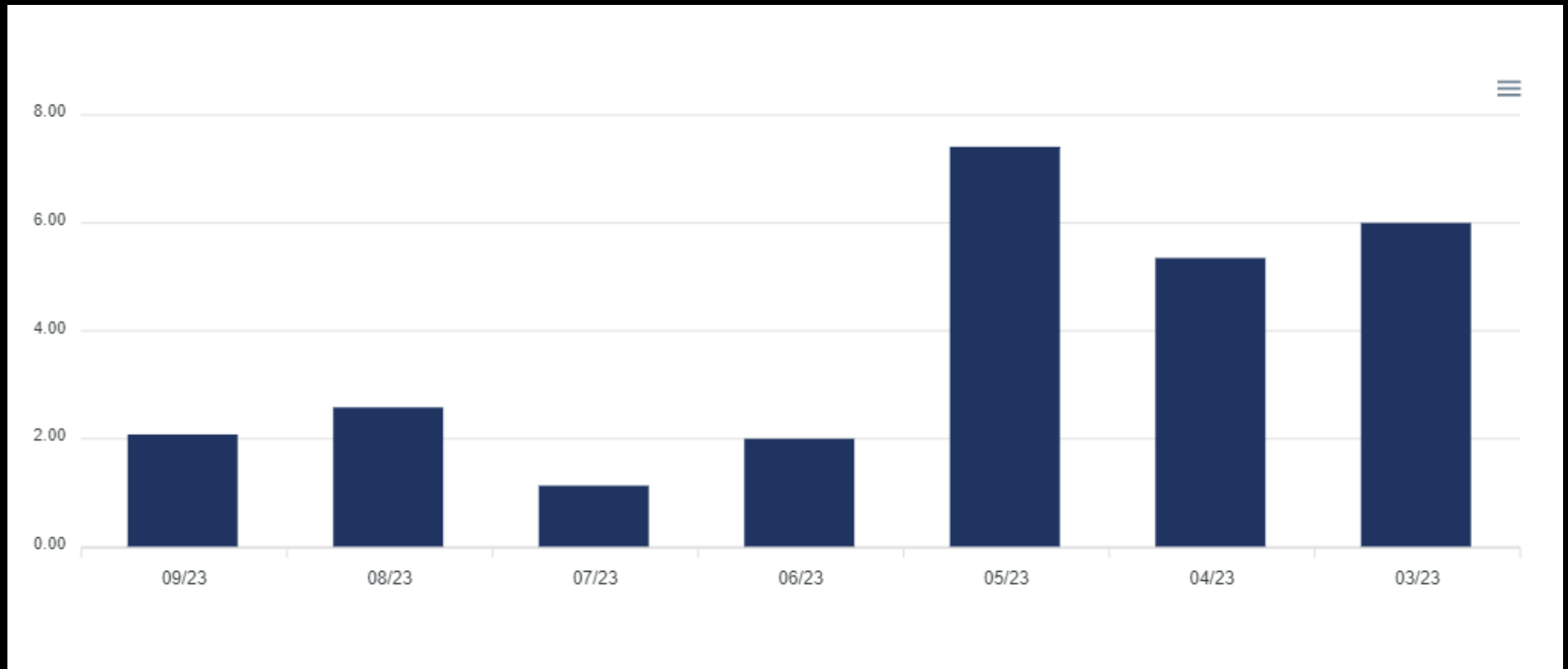
Feedback

15:41  
13/09/2023



‘phished’....

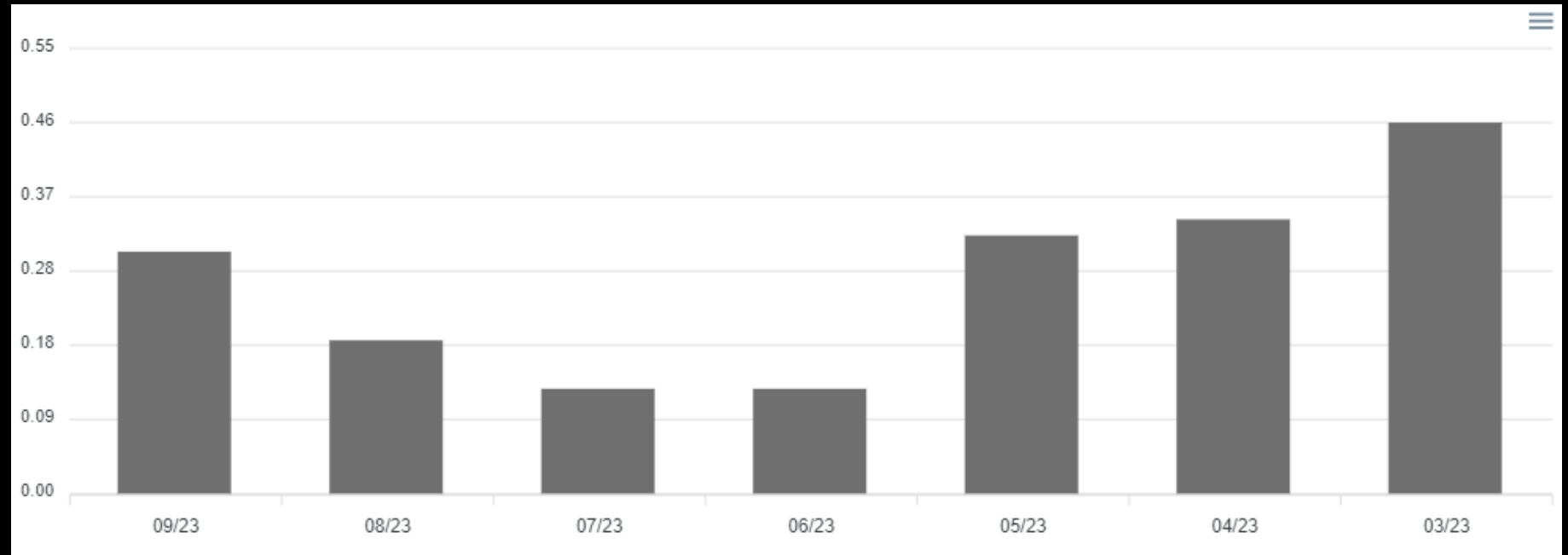
% personen die op link geklikt hebben.





'phished' ....

% personen die bijlage geopend hebben.

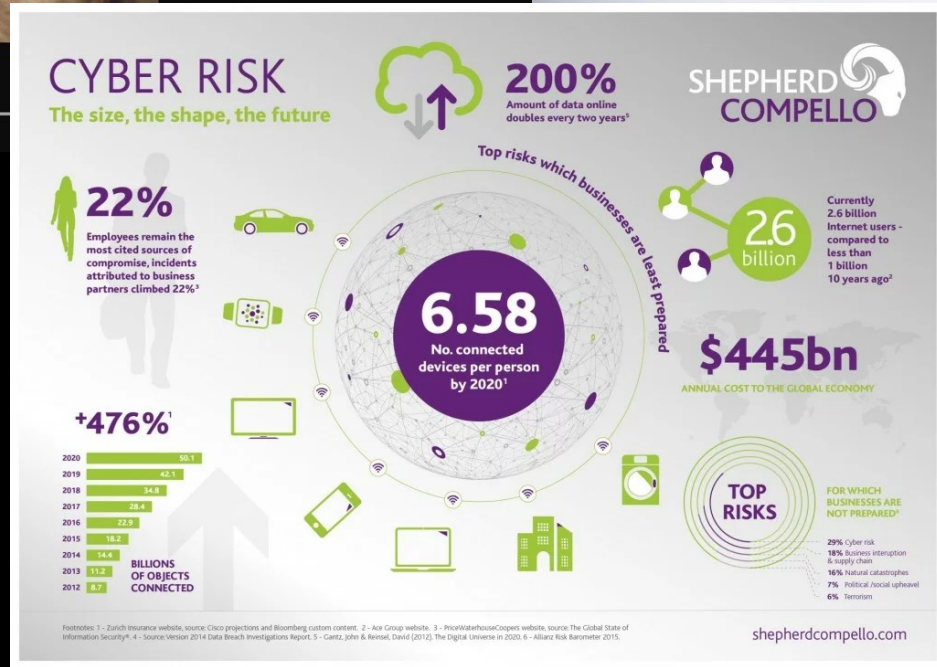


# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin



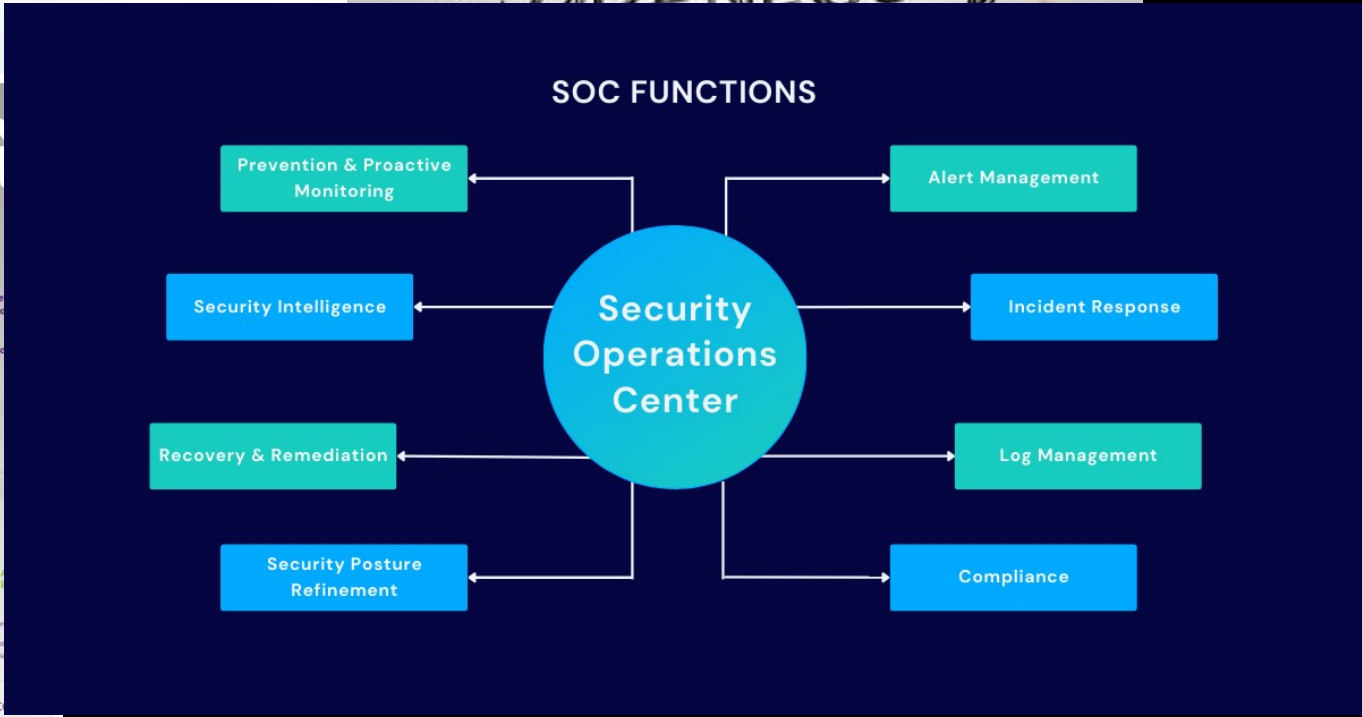
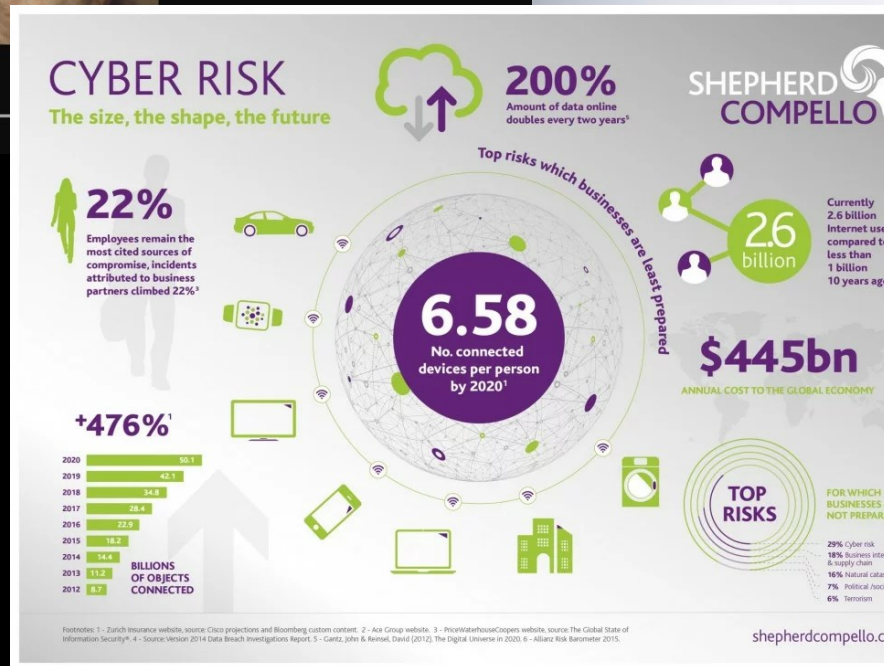
H. HARTZIEKENHUIS  
MOL

# Take home message



By failing to prepare, you are preparing to fail.

~ Benjamin Franklin



# Dank voor uw aandacht!

*The End*



H. HARTZIEKENHUIS  
MOL

# Q&A

