
eo
npo
hoppenbrouwers

Hack Hoppenbrouwers

Marcel de Boer

hoppenbrouwers

Totaalinstallateur met ambitie

VESTIGINGEN **20**

MEDEWERKERS **>1700**

OMZET IN € MLN **320**

Ambitie

Beste en duurzaamste installateur

met landelijke dekking

hoppenbrouwers

top EMPLOYER NEDERLAND THE NETHERLANDS 2023

CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Disciplines


Elektrotechniek


Werktuigbouwkunde


Industriële Automatisering


Beveiliging


Energietransitie


Smart building


Smart Industry


Technisch beheer


Sprinkler

hoppenbrouwers

De aanloop

Mandemakers Groep zwoegt door na hack: 'Er is een back-up van het systeem'

1 juli om 09:30 • Aangepast 8 juli om 13:51

Hoofdkantoor van De Mandemakers Groep (foto: ANP).

Twee dagen na de grote hack bij Mandemakers
altijd onveranderd. Het bedrijf heeft een back-
optie om daarop terug te vallen, maar die knoo
bedrijf verwacht zaterdag (uiterlijk maandag) d
starten.

‘Tientallen Nederlandse bedrijven getroffen door ransomware’

RECENT IN SECUR

Atlassian Confluence suite getroffen door ernstige kwetsbaarhei
6 september 2 min SEI

‘Bluetooth BrakTooth-bugs treffen mogelijk miljarden apparaten’
3 september 2 min SEI

‘Persoonlijke informat buitgemaakt na hackaanval op HAN Hogeschool’
3 september 1 min SEI

hoppenbrouwers

Vrijdag 2 juli

18.30 uur

Eerste vermoedens

ICT trok snel de conclusie dat het een ernstige situatie was

Systemen en verbindingen uitgeschakeld

Crisisdienst Chubb Crawford ingeschakeld

In het nieuws: Kaseya, wereldwijde besmetting

22.30 uur

Crisisteam aanwezig op kantoor Udenhout

Team opgestart en beveiligingsbedrijf en collega's geïnformeerd en geactiveerd

23.12 uur

Eerste communicatie naar alle collega's

Splitsing gemaakt tussen ICT-activiteiten en organisatorische zaken

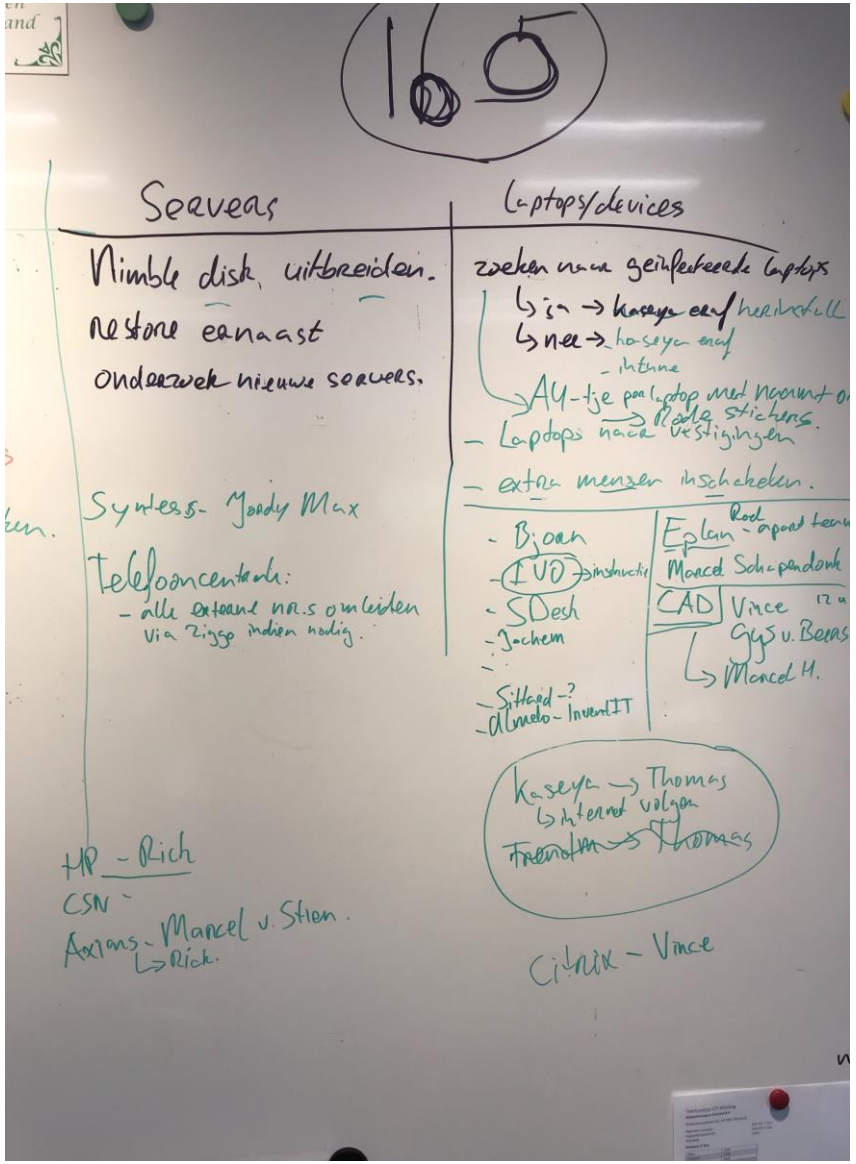
03.00 uur

Plan de campagne

Supply Chain Hacking

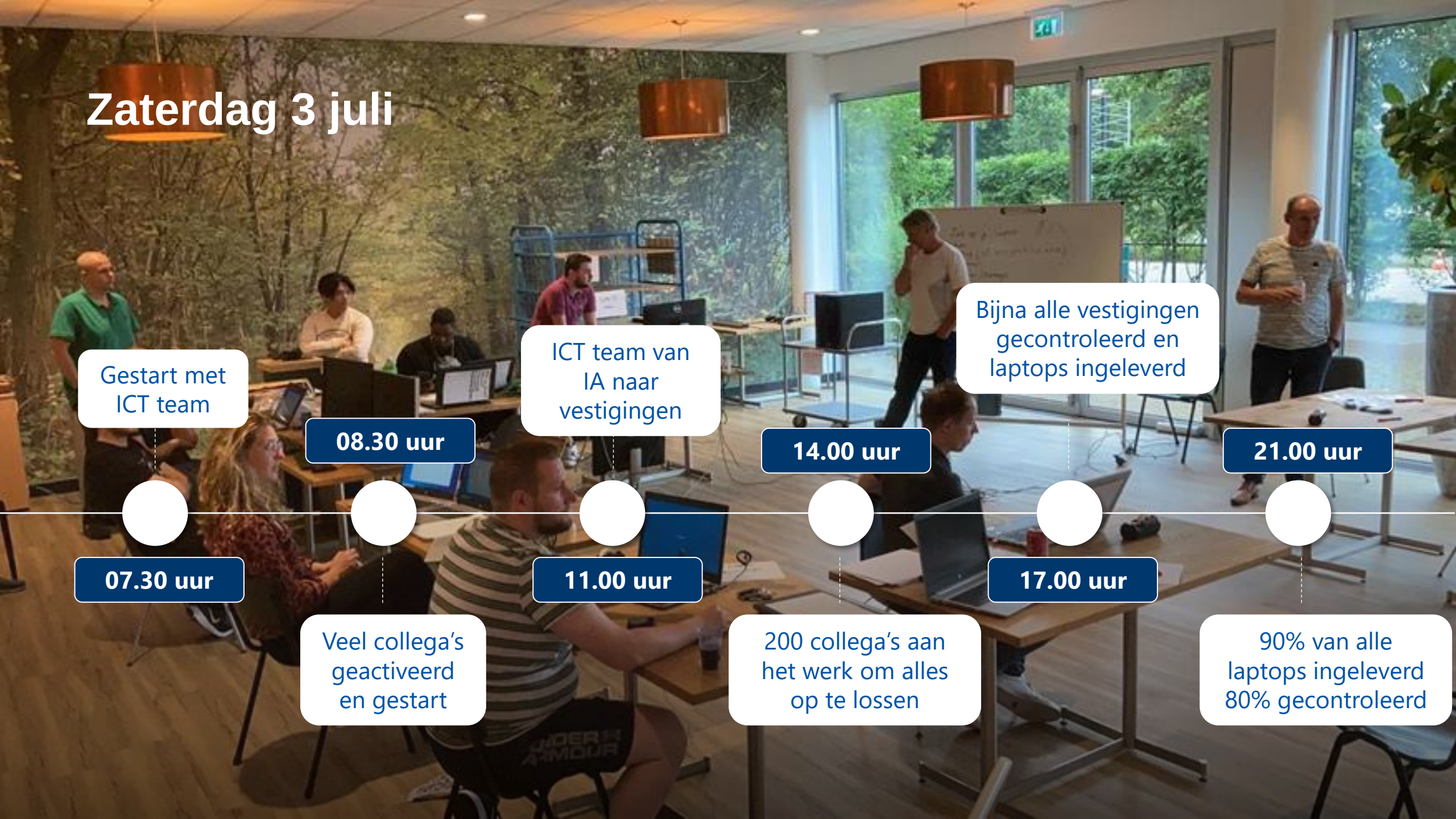
Datumtijd	Bron	Host	Gebeurtenis
2021-07-02 14:55	Firewall Logs	KS01	Aanvaller verbindt met Kaseya management server vanuit IP-adres 18.223.199.234
2021-07-02 14:55	Filesystem, Kaseya Kupload log	KS01	Bestand agent.crt wordt geplaatst op systeem
2021-07-02 15:02	Kaseya AgentMon log	KS01	Commando reeks wordt uitgevoerd met een delay van ongeveer anderhalf uur
2021-07-02 16:31	Filesystem, Registry	KS01	REvil Ransomware wordt gedecodeerd uit agent.crt en uitgevoerd op het systeem

Zaterdagochtend 03:00 uur

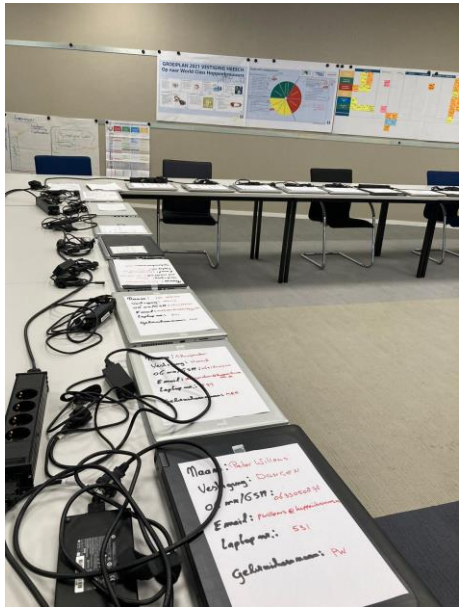


Endpoints Servers

(laptops en PC's)


Zaterdag 3 juli
Gestart met ICT team
07.30 uur
08.30 uur
Veel collega's geactiveerd en gestart
ICT team van IA naar vestigingen
11.00 uur
14.00 uur
200 collega's aan het werk om alles op te lossen
Bijna alle vestigingen gecontroleerd en laptops ingeleverd
17.00 uur
21.00 uur
90% van alle laptops ingeleverd 80% gecontroleerd

Teamwork



hoppenbrouwers

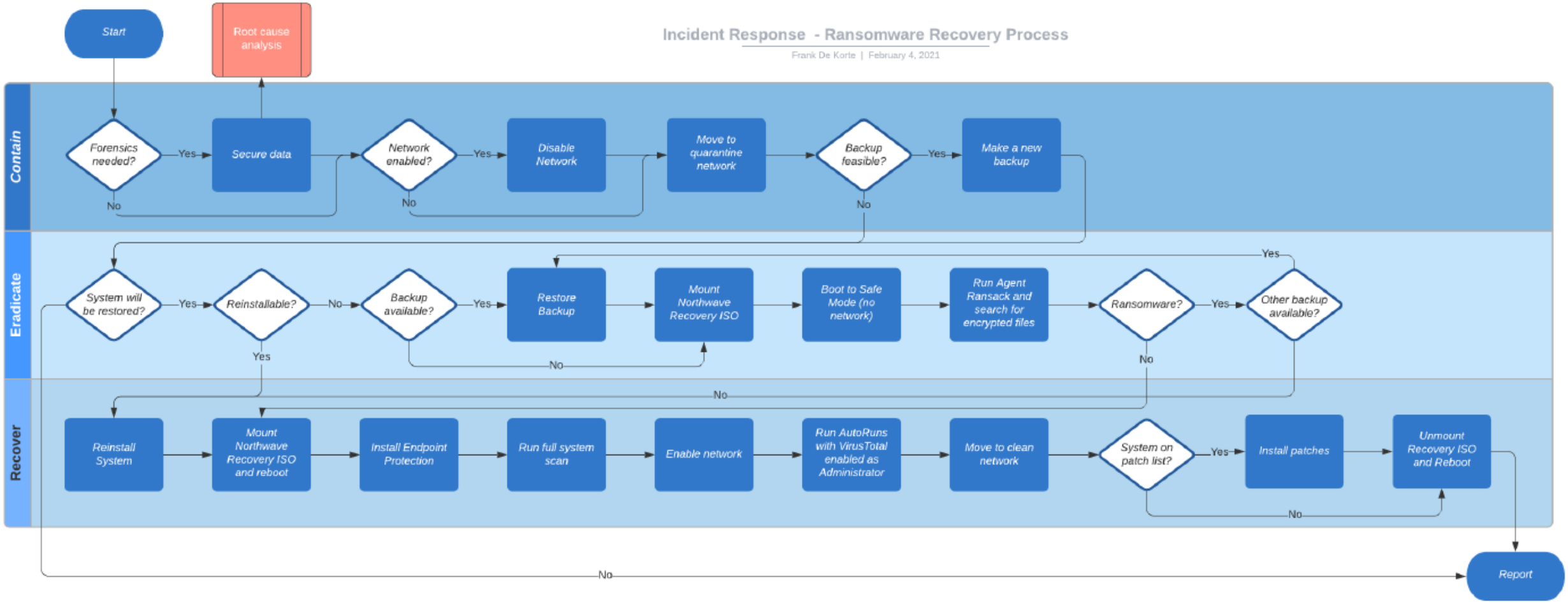
Onze beste vrienden

Verschillen Backups en Snapshots

	Backups	Storage Level Snapshots
	Meestal eens per dag	Foto op verschillende momenten per dag
	Wordt gemaakt op server niveau	Wordt gemaakt op storage block niveau
	Kopie van alle of gewijzigde data	Legt metadata vast (geen kopie)
	Kost tijd om te maken	Kost nauwelijks tijd om te maken
	Tijdrovend in geval van disaster recovery	Kost nauwelijks tijd om te restoren -> 150 servers, 75Tb in 3 minuten!

hoppenbrouwers

De “wasstraat”

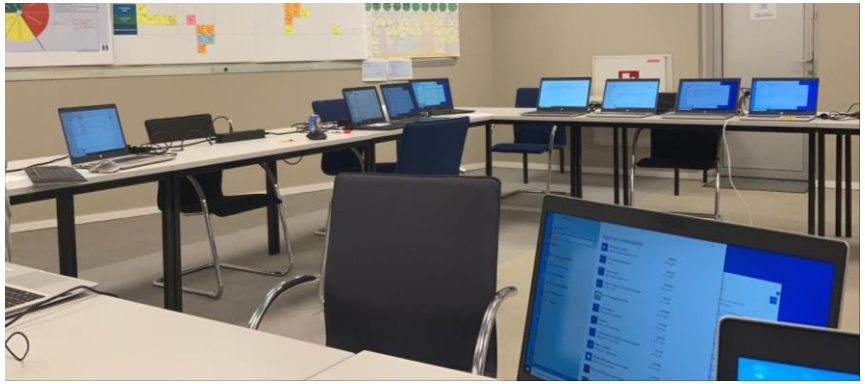


Figuur 5: Ransomware recovery workflow

hoppenbrouwers

Zondag 4 juli 2021

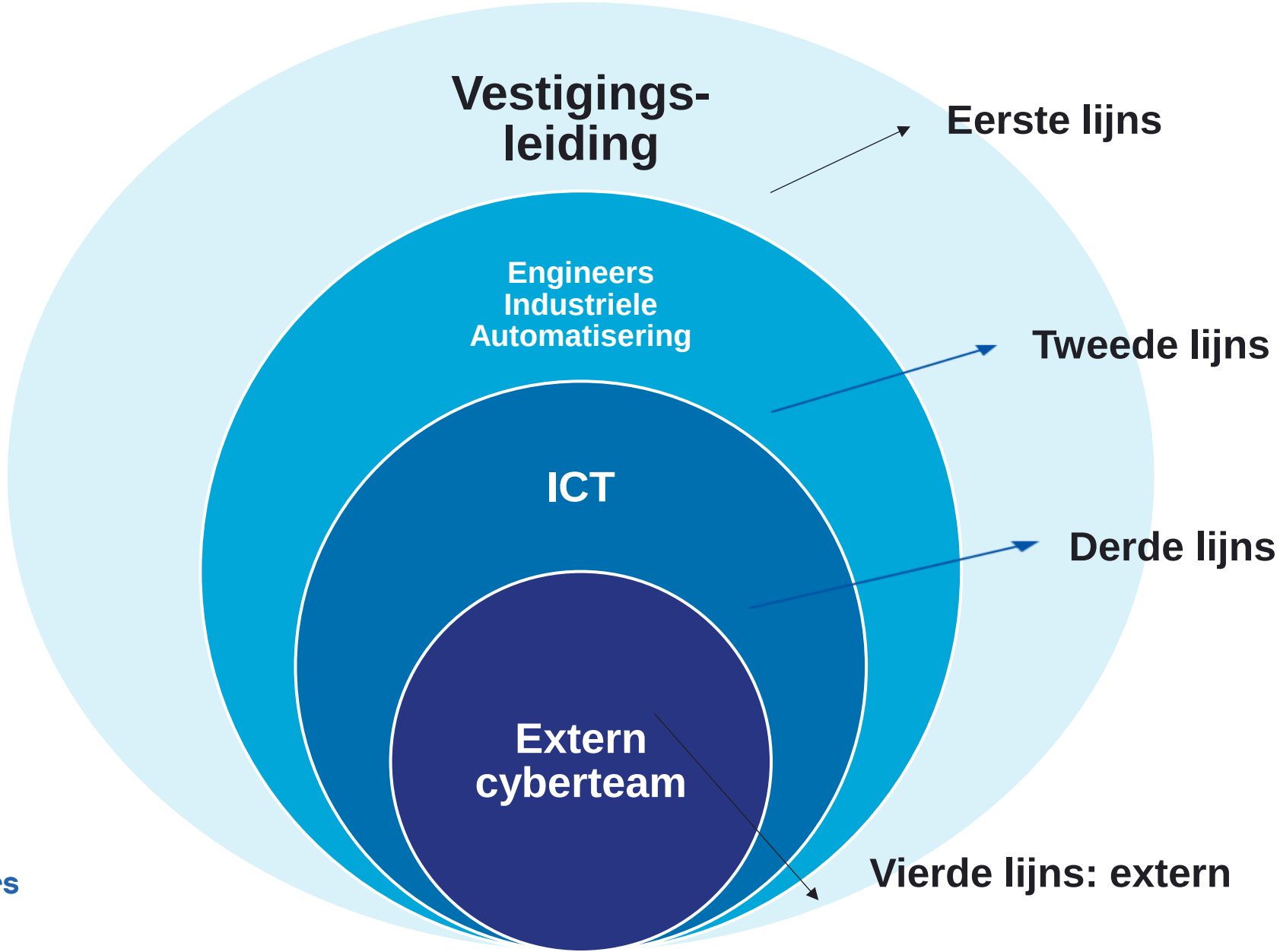
Opnieuw 200 mensen aan het werk



Zondag- en maandagavond webinars voor medewerkers

hoppenbrouwers

ICT lijnen: Eerste lijns tot vierde lijns



hoppenbrouwers

ELK PROJECTTEAM EEN CRISISTEAM

Nadenken over vragen van klanten en neem eventuele zorgen weg

Op geen enkele projectlocatie kun je spullen gebruiken die er nog staan

Help mee met vestigingen en andere teams

Denk na wat hebben wij na vrijdag 12.00 uur nog gedaan

Kunnen mijn monteurs morgen meteen aan het werk of eerst naar de zaak?

Kunnen mensen niet aan de slag, denk aan alternatief werk

Verzamel alle vragen bij 1 persoon

Maandag 5 juli 2021

Om 13:00 uur waren alle vestigingen weer online.

Contactpersonen zijn IA engineer en Vestigingsleider

Wachtwoorden nog niet allemaal gewijzigd

Protocol 99 naar 100% wordt uitgerold

Meeste monteurs konden gewoon doorwerken

Tekenstations nog niet werkend en laptops zijn nog niet allemaal terug

Maandag: dagstart op elke vestiging






hoppenbrouwers

Financiële impact

	€uro
Eigen uren	150.000
Northwave	100.000
Overige externe ondersteuning	35.000
Bedrijfsschade	90.000
Overige	35.000
Totaal	400.000

hoppenbrouwers

Potentiële bedrijfsschade

Bruto winst per jaar: € 125 miljoen

Schade per werkdag: circa € 500 duizend

Schade in 3 weken:

circa 7,5 miljoen

hoppenbrouwers

Communicatie klanten

Mailing gestuurd naar alle klanten

Eerste statement van Northwave voor belanghebbenden

Veel positieve reacties op aanpak

Weigeren laptops en afsluiten van systemen

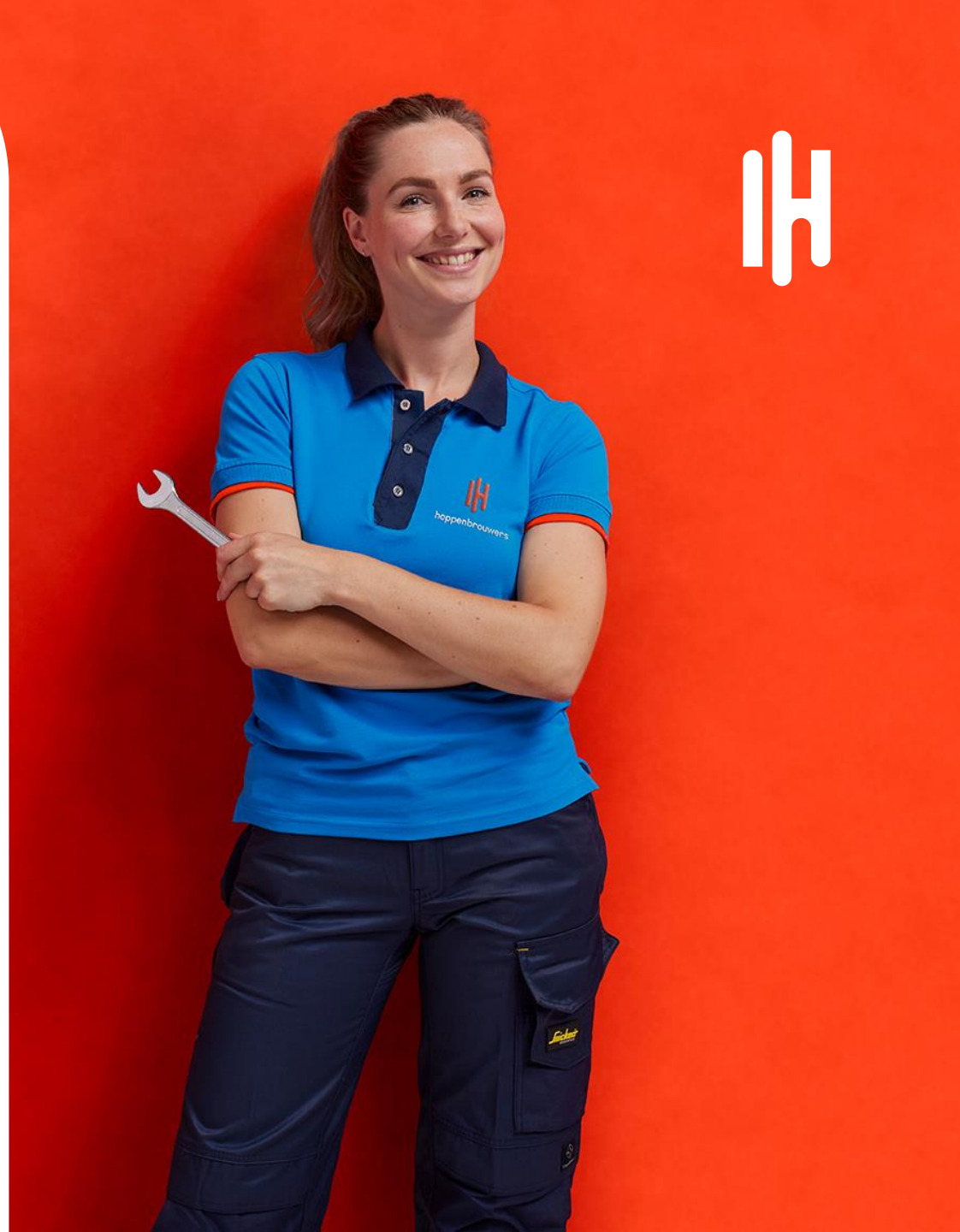
IT afdelingen kunnen contact opnemen met Marcel de Boer

Preventieve Maatregelen

hoppenbrouwers

Voor de Hack waren deze maatregelen al geïmplementeerd

- Inrichten informatiebeveiligingsbeheer, bv ISO27001
- Wachtwoordbeleid
- Update / patch management
- Bewustzijn medewerkers verhogen
- Advanced Treat Protection
- Multifactor authenticatie
- Netwerksegmentatie
- Backup strategie (3-2-1)



hoppenbrouwers

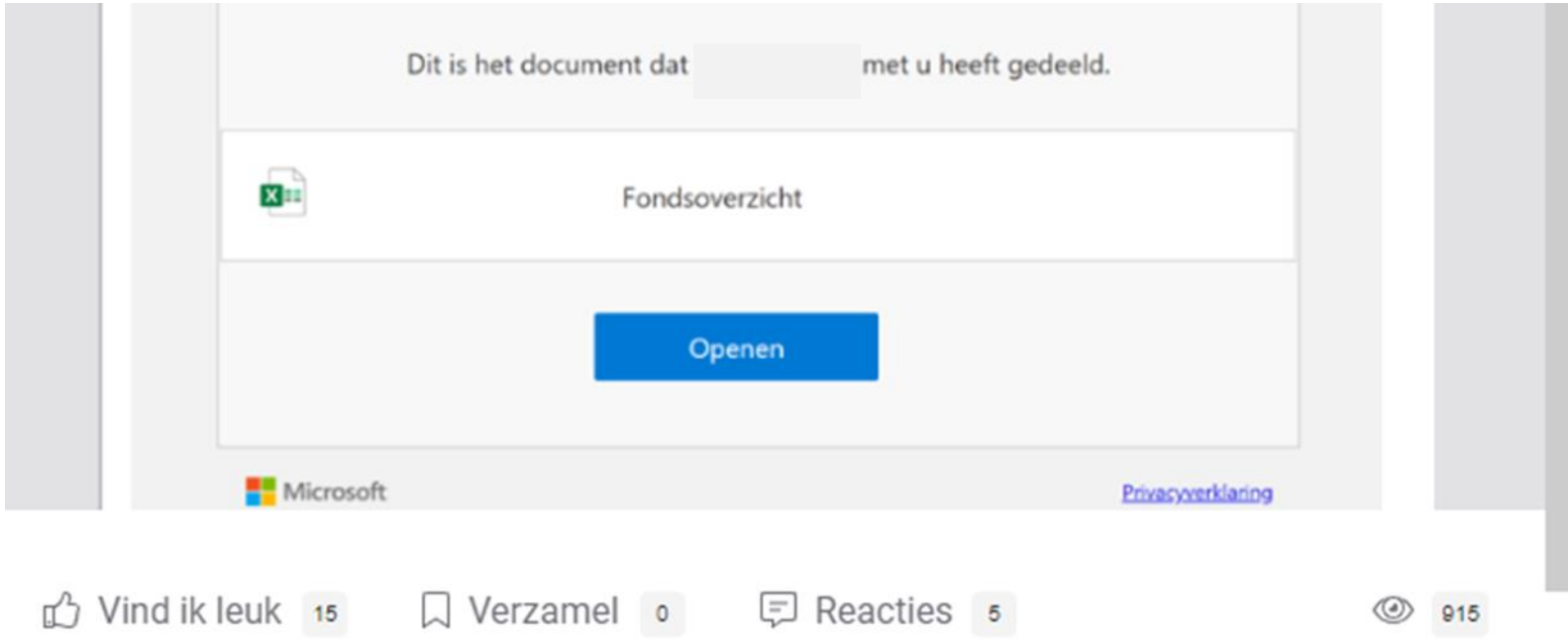
Nadat alle stof was neergedaald…
…scherpere focus op security

- Uitgebreid monitoring & response ingericht
- Endpoint security geïmplementeerd
- Rechten van systeembeheerders zijn beperkt
- Patch management strakker ingeregeld
- Documentatie van IT middelen verbeterd
- Crisisplan is verder uitgewerkt
- Security officer aangesteld
- Leveranciers worden beter gecontroleerd
- Regelmatige bewustwoordingscampagnes voor medewerker
- We communiceren regelmatig over dreigingen

hoppenbrouwers

Open cultuur

- Mensen voelen zich vrij om fouten toe te geven
- Het maakt de organisatie weerbaarder



Vind ik leuk 15 Verzamel 0 Reacties 5 915

hoppenbrouwers

Scan QR voor
het E-Book

Scan QR voor
de Podcast- HACK

hoppenbrouwers

hoppenbrouwers

Bedankt voor uw aandacht

Zijn er nog vragen?