
https://youtu.be/6KvFO-Cbh3c

Hoppenbrouwers

TECHNIEK

Juli 2021

Hack Hoppenbrouwers

VNO-NCW Februari 2022

ONDERWERPEN

1. Hoppenbrouwers
2. Tijdspad Hack
3. Preventieve maatregelen
4. Maatschappelijke context

Totaalinstallateur met ambitie

VESTIGINGEN **17**

MEDEWERKERS **>1500**

OMZET IN € MLN **260**

top EMPLOYER NEDERLAND THE NETHERLANDS 2022
CERTIFIED EXCELLENCE IN EMPLOYEE CONDITIONS

Ambitie

Beste en duurzaamste installateur

met landelijke dekking

Disciplines


Elektrotechniek


Werktuigbouwkunde


Industriële Automatisering


Beveiliging


Duurzame energie


Inspecties


Panelenbouw


Beheer
Onderhoud
Service


Sprinkler


TIJDSPAD
HACK

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

VRIJDAG 2 JULI 2021

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

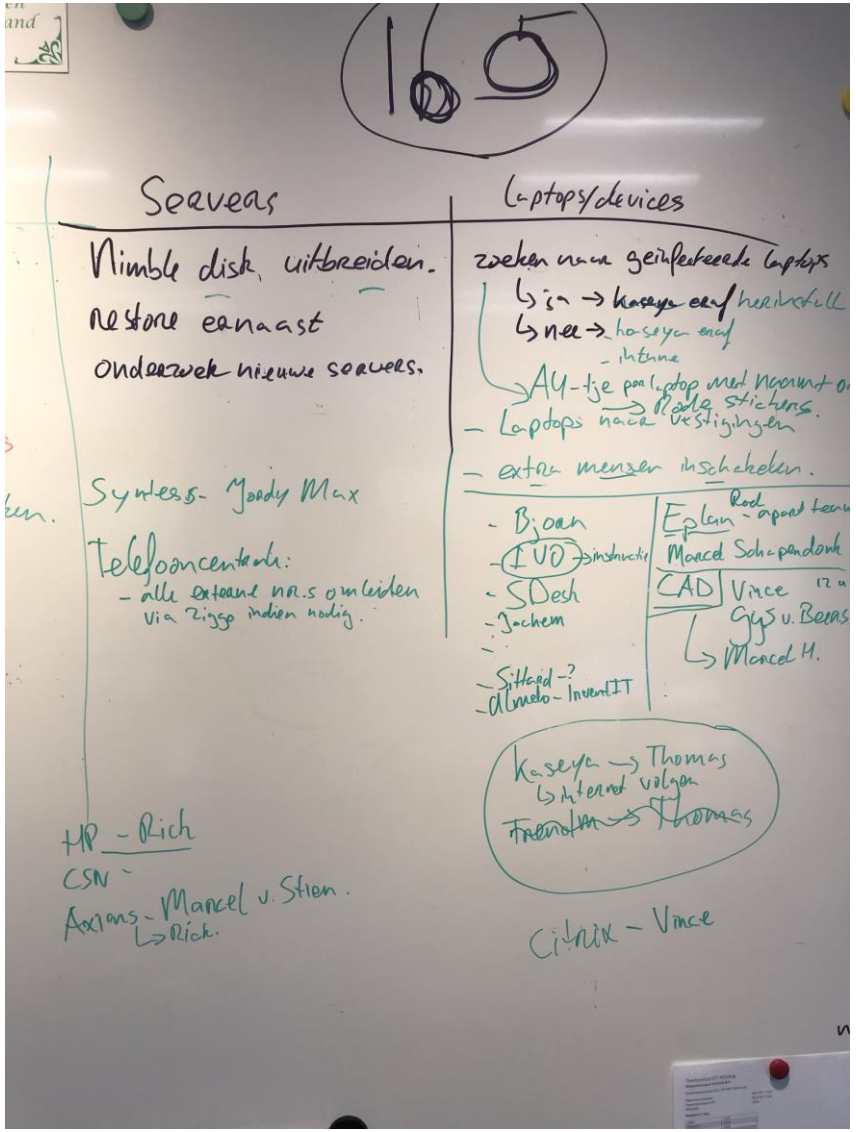
Eerste communicatie naar alle collega's

Splitsing gemaakt tussen ICT-activiteiten en organisatorische zaken

03.00 uur

Plan de campagne

Zaterdagochtend 03:00 uur



Endpoints Servers

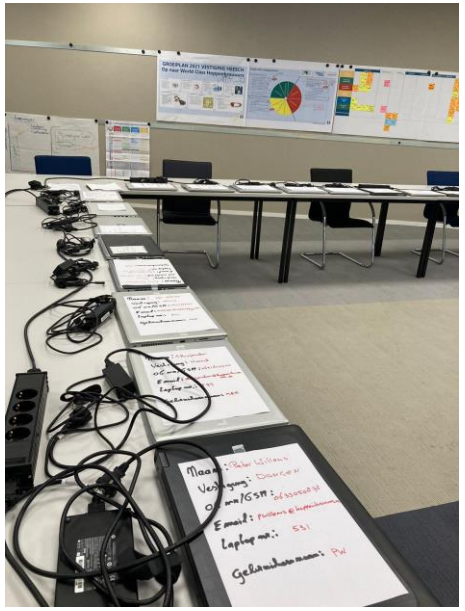
(laptops en PC's)

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


ZATERDAG 3 JULI 2021
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



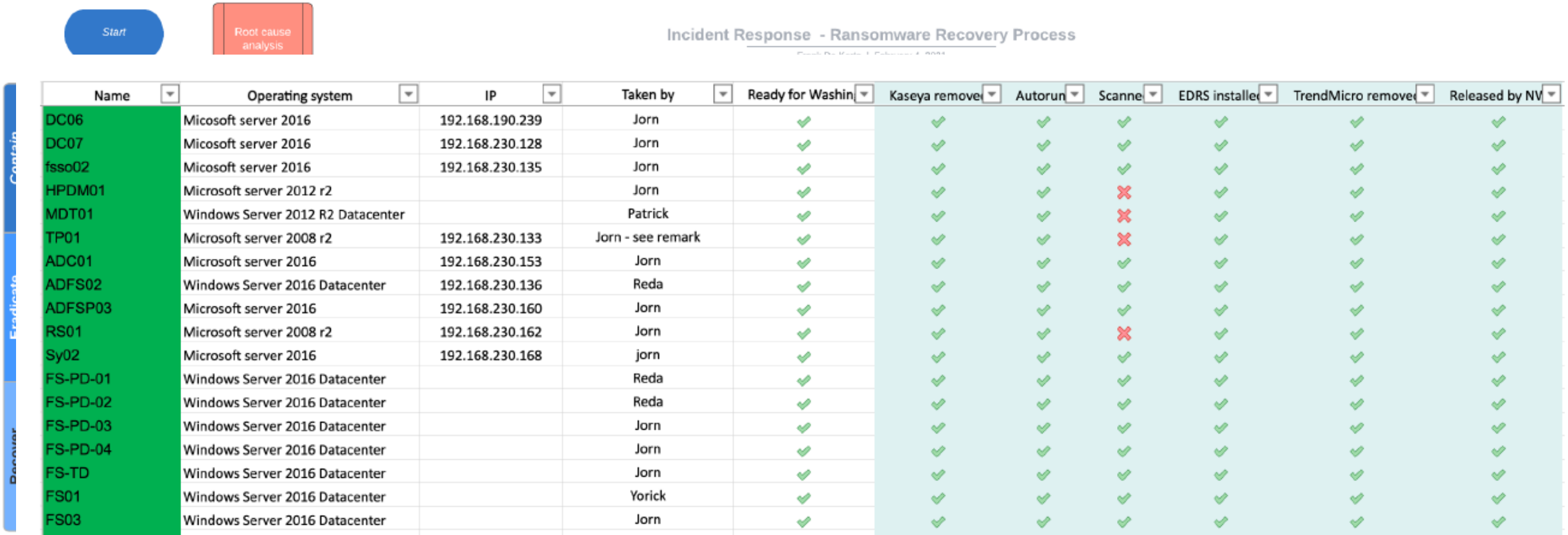
Onze beste vrienden

Don’t worry mate,
we’ll fix this!

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!

De “wasstraat”



Name	Operating system	IP	Taken by	Ready for Washin	Kaseya remove	Autorun	Scanne	EDRS installe	TrendMmicro remove	Released by NV
DC06	Micosoft server 2016	192.168.190.239	Jorn	✓	✓	✓	✓	✓	✓	✓
DC07	Micosoft server 2016	192.168.230.128	Jorn	✓	✓	✓	✓	✓	✓	✓
fsso02	Micosoft server 2016	192.168.230.135	Jorn	✓	✓	✓	✓	✓	✓	✓
HPDM01	Microsoft server 2012 r2		Jorn	✓	✓	✓	✗	✓	✓	✓
MDT01	Windows Server 2012 R2 Datacenter		Patrick	✓	✓	✓	✗	✓	✓	✓
TP01	Microsoft server 2008 r2	192.168.230.133	Jorn - see remark	✓	✓	✓	✗	✓	✓	✓
ADC01	Microsoft server 2016	192.168.230.153	Jorn	✓	✓	✓	✓	✓	✓	✓
ADFS02	Windows Server 2016 Datacenter	192.168.230.136	Reda	✓	✓	✓	✓	✓	✓	✓
ADFSP03	Microsoft server 2016	192.168.230.160	Jorn	✓	✓	✓	✓	✓	✓	✓
RS01	Microsoft server 2008 r2	192.168.230.162	Jorn	✓	✓	✓	✗	✓	✓	✓
Sy02	Microsoft server 2016	192.168.230.168	jorn	✓	✓	✓	✓	✓	✓	✓
FS-PD-01	Windows Server 2016 Datacenter		Reda	✓	✓	✓	✓	✓	✓	✓
FS-PD-02	Windows Server 2016 Datacenter		Reda	✓	✓	✓	✓	✓	✓	✓
FS-PD-03	Windows Server 2016 Datacenter		Jorn	✓	✓	✓	✓	✓	✓	✓
FS-PD-04	Windows Server 2016 Datacenter		Jorn	✓	✓	✓	✓	✓	✓	✓
FS-TD	Windows Server 2016 Datacenter		Jorn	✓	✓	✓	✓	✓	✓	✓
FS01	Windows Server 2016 Datacenter		Yorick	✓	✓	✓	✓	✓	✓	✓
FS03	Windows Server 2016 Datacenter		Jorn	✓	✓	✓	✓	✓	✓	✓
FS04			Jorn	✓	✓	✓	✓	✓	✓	✓
FS06			Jorn	✓	✓	✓	✓	✓	✓	✓
FS07			Jorn	✓	✓	✓	✓	✓	✓	✓
FS10			Jorn	✓	✓	✓	✓	✓	✓	✓
FS11			Jorn	✓	✓	✓	✓	✓	✓	✓
FS12			Jorn	✓	✓	✓	✓	✓	✓	✓

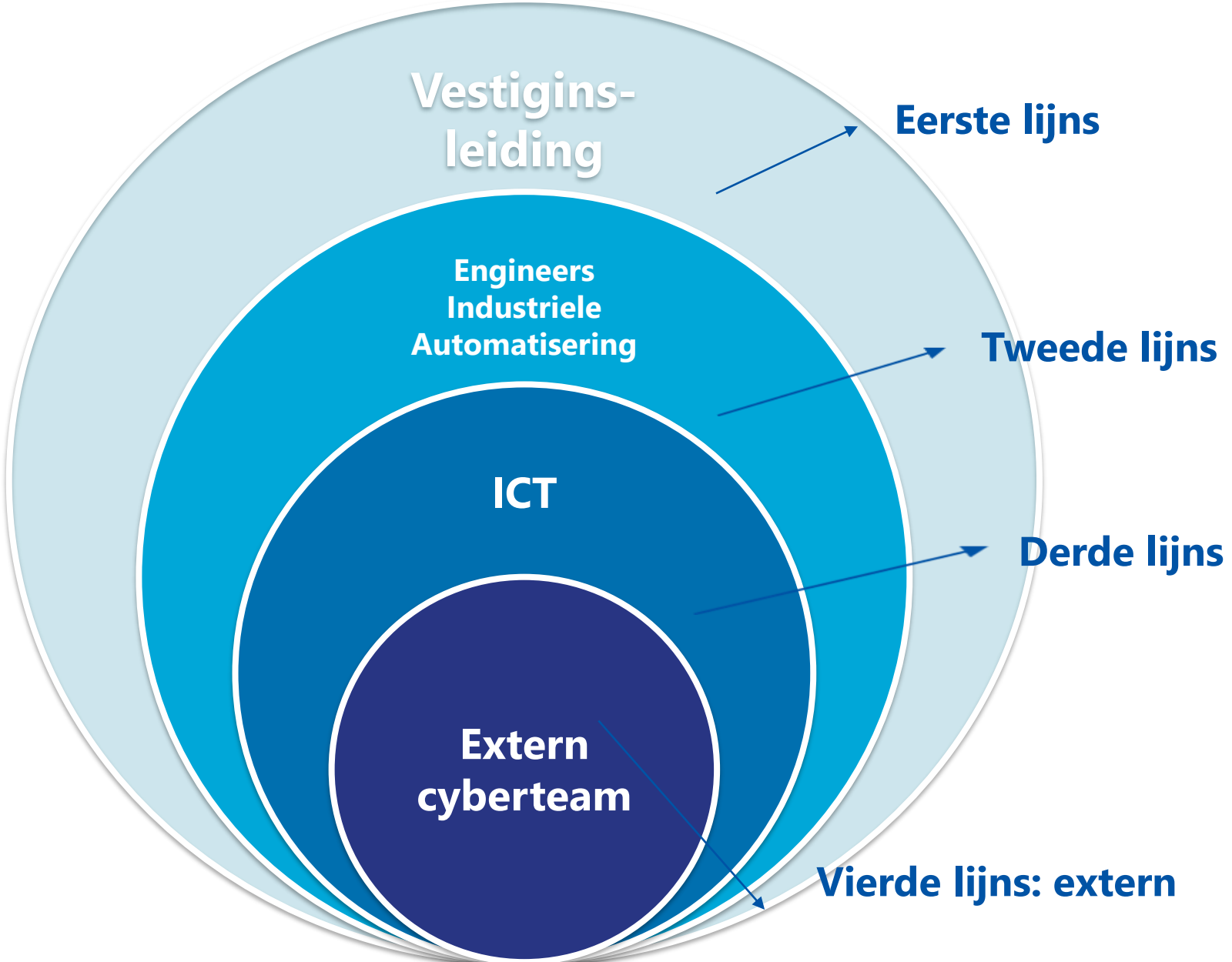
Figuur 4: Asset & status lijst


ZONDAG 4 JULI 2021
Gestart met ICT team
08.00 uur
Eerste servers weer actief
Laptops worden ingeleverd en opgeschoond. Moeilijkere gevallen verder onderzocht
Opgeschoonde laptops worden opgehaald
Alle vestigingen beoordeeld en stap voor stap schoon verklaard
Veel in- en externe communicatie
Veel rest werkzaamheden
Vooruitgekeken naar maandag. Duidelijke protocollen gemaakt en FAQ
Webinar medewerkers
20.00 uur

OPNIEUW 200 MENSEN AAN HET WERK

Zondag- en maandagavond webinars voor medewerkers

ICT lijnen: Eerste lijns tot vierde lijns



ELK PROJECTTEAM EEN CRISISTEAM

Nadenken over vragen van klanten en neem eventuele zorgen weg

Op geen enkele projectlocaties 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






Status per vestiging - maandagavond

Vestiging	Update
Amelo/Oldenzaal	90%
Arnhem	95%
Barendrecht	95%
Breda	98%
Best	90%
Deurne	75%
Dongen	85%
Heesch	95%
Kaatsheuvel	85%
Rosmalen	90%
Roosendaal	99%
Sittard	65%
Utrecht	90%
203	98%
Technisch beheer	95%
Beveiliging	90%
Industrie/Water	85%
U&W	90%
Ziekenhuizen	85%

COMMUNICATIE KLANTEN

Mailing gestuurd naar alle klanten

Eerste statement van Northwave voor belanghebbenden

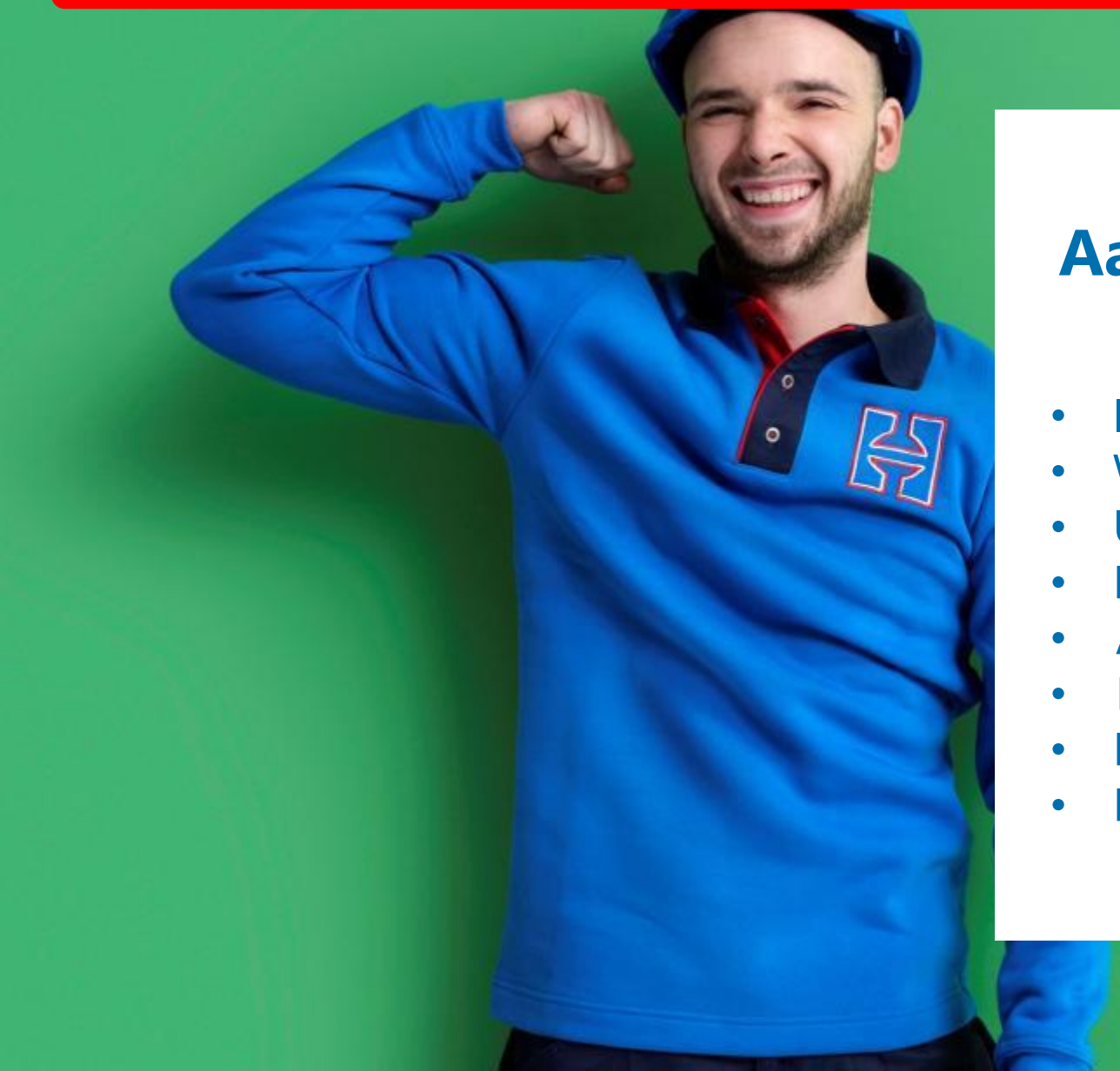
Veel positieve reacties op aanpak

Weigeren laptops en afsluiten van systemen

IT afdelingen kunnen contact opnemen met Marcel de Boer

PREVENTIEVE MAATREGELEN

PREVENTIEVE MAATREGELEN ZIJN KEY!



Aanwezig, maar te verbeteren

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

PREVENTIEVE MAATREGELEN ZIJN KEY!

Niet aanwezig, dus in te richten:

- Security monitoring & response
- Uitwerken crisesplan
- Beleid accounts met hoge rechten
- Conditional Access

SUCCESSEN

Samen maken we Hoppenbrouwers

Mens

Zeer veel betrokkenheid medewerkers

Veel ICT kennis in huis

Organisatie

Binnen 2 dagen weer aan de slag

Geen vertragende protocollen

Communicatie snel op gang

Landelijk in het nieuws

Goed verzekerd

Techniek

Techniek in de basis goed op orde

MAATSCHAPPELIJKE CONTEXT

14 januari, 2022 17:41 2min Geert van der Klugt SECURITY

Hackgroep REvil opgepakt door Russische inlichtingendienst

FEATURED

Bescherm gegevens, want je zult aangevallen worden

9 februari 5 min SECURITY

RECENT IN SECURITY

Oekraïense banken en overheid getroffen door cyberaanval

16 februari 1 min SECURITY

Europese Unie start onderzoek naar privacy-inbreuk door overheden

Hoppenbrouwers

TECHNIEK

Bedankt voor uw aandacht