Cyberweerbaar(der)

Open Dag Van der Hoff ICT, 3 oktober 2025

PVO / Limburg

Even voorstellen

Peter Cox

Adviseur en projectleider

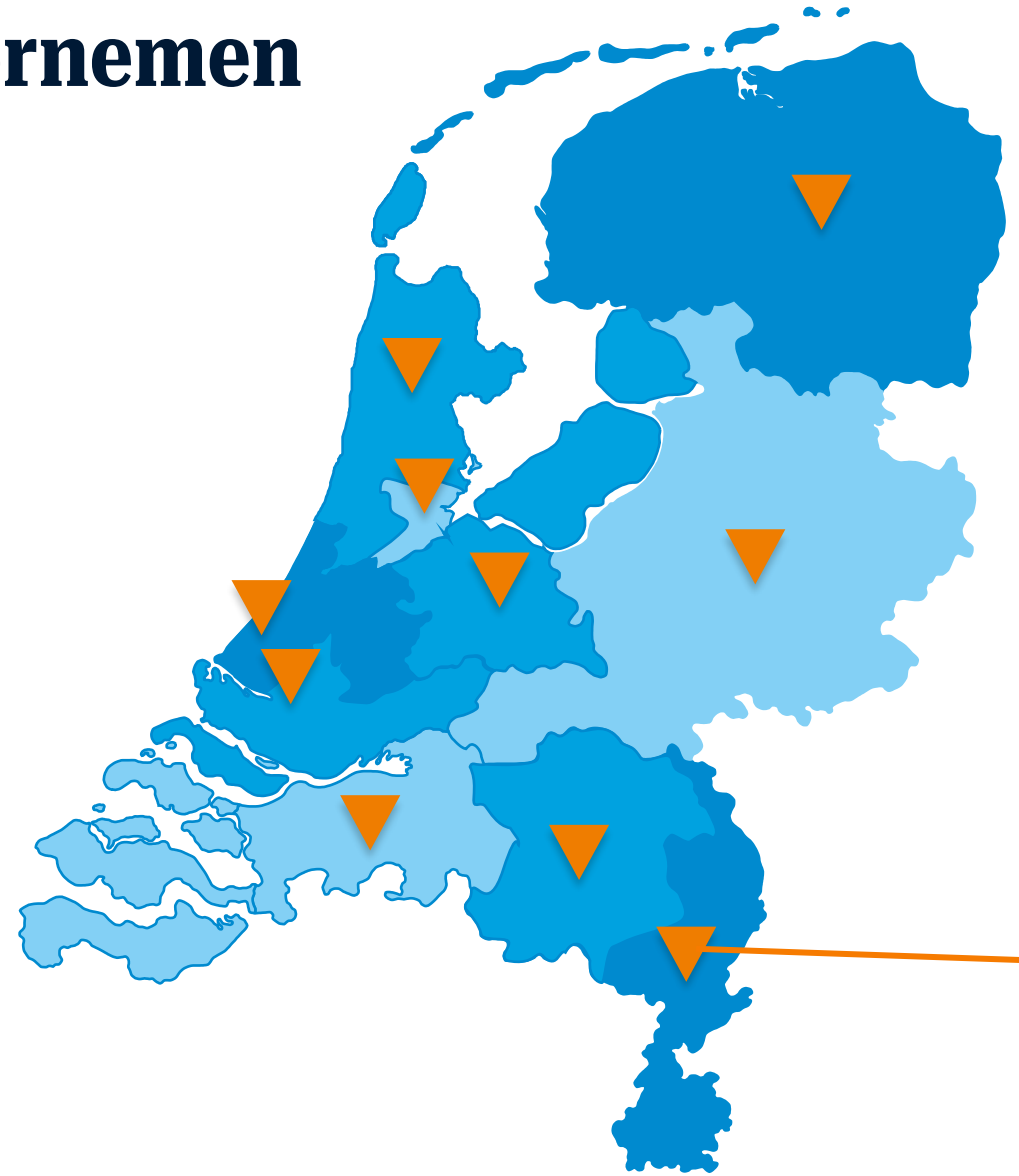
peter.cox@pvo-limburg.nl

06 12 06 51 11

- Adviseur bij projecten als Veilig Buitengebied, Keurmerk Veilig Ondernemen Winkelgebied/ Bedrijventerrein etc.
- Geven van presentaties en workshops over Cyberweerbaarheid.
- Projectleider diverse pilots.

Platform Veilig Ondernemen

- PVO Noord-Nederland
- PVO Oost-Nederland
- PVO Midden-Nederland
- PVO Noord-Holland
- PVO Amsterdam-Amstelland
- PVO Regio Den Haag
- PVO Regio Rotterdam
- PVO Zeeland West-Brabant
- PVO Oost-Brabant
- PVO Limburg



Stg PVO Limburg
Secretariaat:
Steegstraat 5
6041 EA Roermond

PVO / Limburg

provincie limburg

POLITIE

OPENBAAR MINISTERIE

RIEC Limburg

Gemeenten

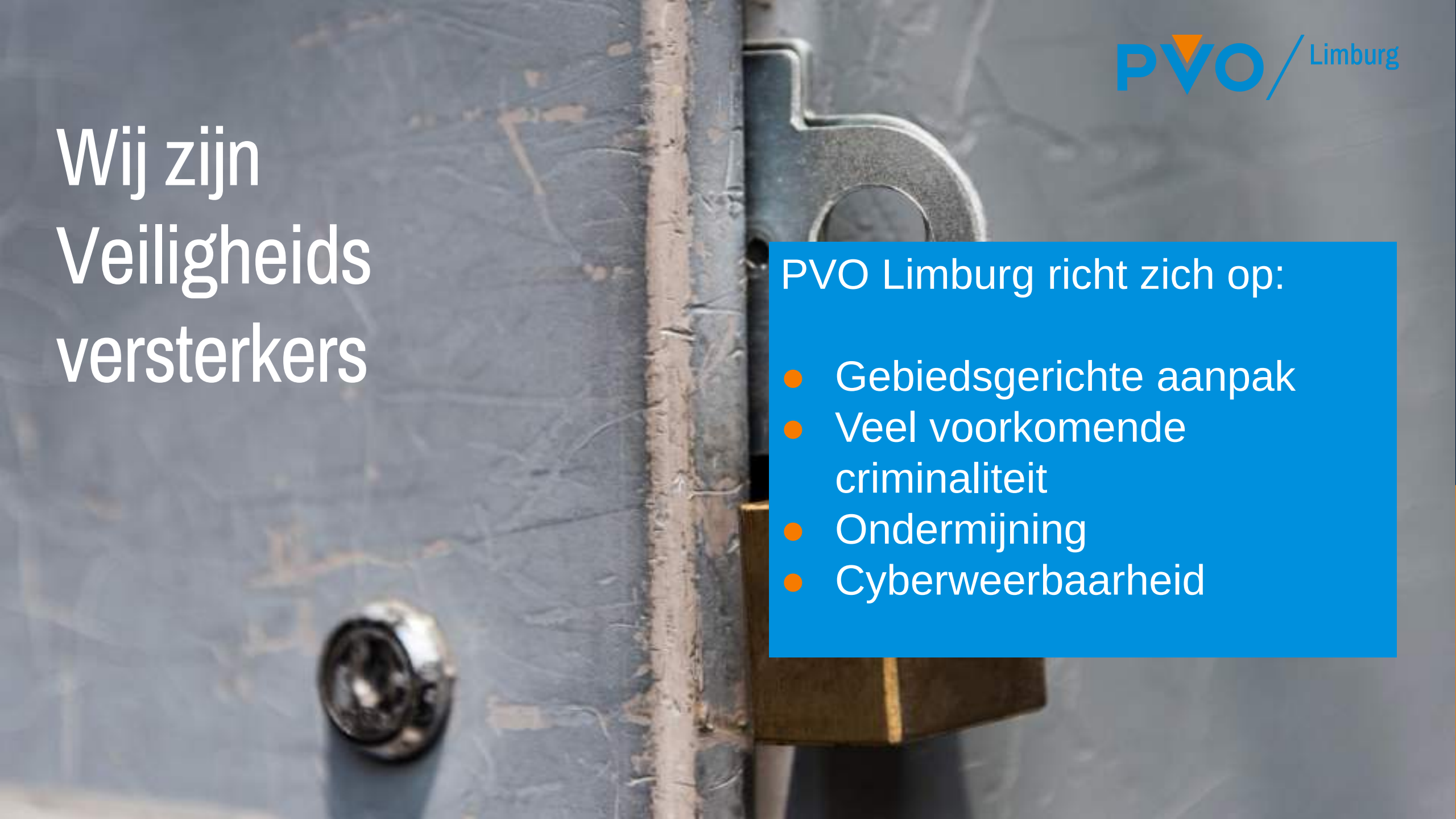
lwv

MKB LIMBURG

lltb Anders Durven Doen

Veilig ondernemen.
Daar maken we ons sterk voor.

PVO / Limburg



Wij zijn Veiligheids versterkers

PVO Limburg richt zich op:

- Gebiedsgerichte aanpak
- Veel voorkomende criminaliteit
- Ondermijning
- Cyberweerbaarheid

Achtergrond Cybercrime


Wie heeft het
standaard wachtwoord
op zijn “digitale apparaten”
veranderd?

Cybersecurity strategy NL

1. Digitale weerbaarheid van overheden, ondernemingen en sociale instellingen vergroten

2. Veilige digitale producten en diensten aanbieden in Nederland

3. Digitale dreiging van criminelen en statelijke actoren bestrijden

4. Digitale weerbaarheid van de bevolking vergroten

Wel een risico, maar geen bedreiging?

Ook jij bent interessant, want:

*"Jij bent **wel** groot genoeg"*

*"Jouw data zijn **wel** interessant"*

*"Jij hebt **wel** iets te verbergen"*

NIEUWS | *30 september 2024*

Mkb heeft te weinig oog voor eigen cyberveiligheid

Leestijd van ongeveer 2 minuten

Een derde van de kleine bedrijven onderneemt geen enkele actie om veilig online te zijn. **Een nieuwe richtlijn voor de versterking van de digitale en economische weerbaarheid, is nog onbekend bij het merendeel van de medewerkers. Phishing is nog steeds de meest voorkomende vorm van cybercriminaliteit op het werk.**

Dat zijn enkele uitkomsten van het Alert Online-trendonderzoek naar kennis en beleving van de digitale veiligheid, uitgevoerd in opdracht van het ministerie van Economische Zaken. De resultaten van het onderzoek zijn gepresenteerd in deelrapporten, zoals het deelrapport Bedrijfsleven.

Ruim een kwart (27 procent) van de medewerkers schat de eigen kennis over online veiligheid in als (zeer) goed. In 2023 was dat nog 21 procent. Het aandeel ICT-verantwoordelijken dat zijn of haar kennis als (zeer) goed beoordeelt, is 53 procent. tegelijk maken vier op de tien ICT-verantwoordelijken zich zorgen over de eigen online veiligheid op het werk. Voor andere medewerkers is dit percentage veel lager (23 procent).

Bron: https://www.accountant.nl/nieuws/2024/9/mkb-heeft-te-weinig-oog-voor-eigen-cyberveiligheid/

De alarmerende stijging van ransomware-aanvallen:
een toename

Gepubliceerd op 27 september 202

Nieuws • 28 april 2025 - 09:00

Sterke stijging cyberaanvallen in eerste kwartaal, Nederland boven wereldgemiddelde

In het eerste kwartaal van 2025 is het aantal cyberaanvallen wereldwijd met 47 procent gestegen tot gemiddeld 1.925 aanvallen per organisatie per week. Nederland zit daar zelfs boven, met een toename van 53 procent, blijkt uit het nieuwste rapport van Check Point Software Technologies. De aanvallen worden niet alleen frequenter, maar ook geavanceerder. Nederlandse bedrijven worden vooral getroffen via gecompromitteerde infrastructuur in de Verenigde Staten, Nederland zelf en Duitsland.

De meeste aanvallen op Nederlandse organisaties lijken afkomstig uit de VS (44%), gevolgd door Nederland (13%) en Duitsland (8%). Dit zijn echter de landen van waaruit de aanval technisch gezien wordt verzonden — het daadwerkelijke land van herkomst ligt vaak elders. Cybercriminelen maken gebruik van botnets en gecompromitteerde systemen om geografische blokkades te omzeilen en hun ware locatie te maskeren.

1. Elke 14 seconden vindt er een ransomware aanval plaats

Bij een ransomware aanval worden bestanden en data van de gehackte organisatie vergrendeld. Om weer toegang te krijgen tot deze bestanden moet het bedrijf dan losgeld betalen, vaak in de vorm van cryptocurrency (uiterst dom, maar dat is een verhaal voor een andere keer).

Ransomware is slechts één van de vele vormen van cyberaanvallen, maar er is gemiddeld elke 14 seconden een incident, wat neer komt op 257 aanvallen per uur. Dit zijn er maar liefst 6.171 per dag en op jaarbasis komt dit neer op 2.252.571 ransomware aanvallen.

2. De geschatte schade door cybercriminaliteit is 6 biljoen in 2022

Om u even een beeld te geven: dit is ongeveer gelijk aan de totale marktwaarde van Tesla, Alphabet (moederbedrijf van o.a. Google), Amazon en Microsoft samen!

Wanneer een bedrijf getroffen wordt door een cyberaanval heeft dit vaak catastrofale gevolgen, omdat veel bedrijven hier niet op voorbereid zijn. Het gaat hier niet alleen om de kosten van het verdrijven van de hacker, de verloren data, de beveiliging- en herstelkosten, maar zeker ook de verloren productietijd.

Onderzoek van de Rabobank wijst uit dat 60% van MKB'ers die gehackt worden binnen 6 maanden failliet gaat. Dit voornamelijk door het verlies aan omzet als gevolg van de verloren productietijd.

3. Kleine bedrijven zijn in bijna de helft van alle cyberaanvallen het doelwit

bron: https://heliview.com/security-leadership/7-kritieke-cybersecurity-statistieken-voor-2023/


GREENLAND
CANADA
RUSSIA
UNITED STATES
CHINA
MEXICO
INDIA
BRAZIL
AUSTRALIA
ARGENTINA
1917466
1373898
1051721
622638
3813172
0
45077
OAS
ODS
MAV
WAV
IDS
VUL
KAS
BAD

De mogelijkheden zijn eindeloos

Malware

Phishing

Helpdeskfraude

Datadiefstal

Ransomware


ENCRYPTION WARNING!
YOU ARE HACKED
ALL YOUR FILES ARE ENCRYPTED
Your computer is LOCKED
and all files will be deleted in 48 hours.
Send $500 worth of bitcoin to specified address.
Authorities will not help you. You will lose your files if you contact them.
Check payment
Enter decrypt code
SYSTEM ENCRYPTED


Breng risico's in kaart

Bevorder veilig gedrag

Bescherm systemen, apparaten en applicaties


Beheer toegang

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2024

Hardware: 12 x RTX 4090 | Password hash: bcrypt

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	3 secs	6 secs	9 secs
5	Instantly	4 secs	2 mins	6 mins	10 mins
6	Instantly	2 mins	2 hours	6 hours	12 hours
7	4 secs	50 mins	4 days	2 weeks	1 month
8	37 secs	22 hours	8 months	3 years	7 years
9	6 mins	3 weeks	33 years	161 years	479 years
10	1 hour	2 years	1k years	9k years	33k years
11	10 hours	44 years	89k years	618k years	2m years
12	4 days	1k years	4m years	38m years	164m years
13	1 month	29k years	241m years	2bn years	11bn years
14	1 year	766k years	12bn years	147bn years	805bn years
15	12 years	19m years	652bn years	9tn years	56tn years
16	119 years	517m years	33tn years	566tn years	3qd years
17	1k years	13bn years	1qd years	35qd years	276qd years
18	11k years	350bn years	91qd years	2qn years	19qn years

HIVE SYSTEMS

> Learn more about this at hivesystems.com/password

Bereid voor op incidenten

Het ‘probleem’ zit tussen toetsenbord en stoel…?

De oplossing zit ook tussen toetsenbord en stoel!

Ons aanbod

Cyberweerbaar: Hoe kan PVO Limburg helpn?

Bewustwording

“Wat is het probleem en waarom gaat mij dat aan?”

In actie komen

“Welke maatregelen kan ik nemen om erger te voorkomen/ beperken?”

Monitoring

Collectieve inkoop voor permanente digitale bewaking.

Bewustwording

Interactieve Presentatie

PVO / Limburg

Bewustwording Cybercrisis Training

CIC RIC
Cyber Chain Resilience Consortium

PVO / Limburg

Bewustwording

Cyberscan / Cyberadvies-gesprek

PVO / Limburg

In actie komen

Met Rapport Cyberscan naar IT-partner

PVO / Limburg

In actie komen

Workshop Back on Track

PVO / Limburg

In actie komen

VR Experience

PVO / Limburg

Monitoring

- Collectieve Inkoop:
- Op Mens/ Proces/ Techniek
- Samen met lokale IT-partners
- Maandelijks dashboard
- “Digitale Ster”

PVO / Limburg

PVO Limburg

Interesse?

mail:

info@pvo-limburg.nl

Of geef je visitekaartje

PVO / Limburg

En wat als het toch fout gaat

politie.nl/checkjehack
hackhelpdesk.nl
fraudehelpdesk.nl
haveibeenpwned.nl
digitaalveiliglimburg.nl
nomoreransom.org


Cyber Attac