Verstandig omgaan met IT-risico's

Ben Lankhaar

Stelling

‘We hebben allemaal last van risicoblindheid’

‘Je gaat het pas zien,
als je het doorhebt’

Als risico’s realiteit worden

30-07-2024

Microsoft 365 en Azure getroffen door een wereldwijde storing.

Als risico’s realiteit worden

22-08-2024

Gegevens van 3,2 miljoen Belgische WhatsApp-gebruikers zijn te koop op darkweb.

Als risico’s realiteit worden

28-08-2024

IT-incident op het defensienetwerk. Eindhoven airport, verschillende ministeries, gemeenten en andere overheidsdiensten getroffen.

- Mogelijkheden en kansen (FOMO)
- Schaalvergroting
- Decentralisatie

- Complexiteit
- Afhankelijkheid
- Risico’s
- Cybercriminaliteit


Accept
RISK
Management
Control
Mitigate
Transfer
trategy
Avoid
Reduce

Risicomanagement volwassenheid

- Reactief
- Risicobeleid en -strategie ontbreekt
- Kosten/opbrengsten vaak leidend

1. Ad Hoc

Risicomanagement volwassenheid

- Inconsistent
- Extern gemotiveerd
- Compliance-gericht

2. Initial

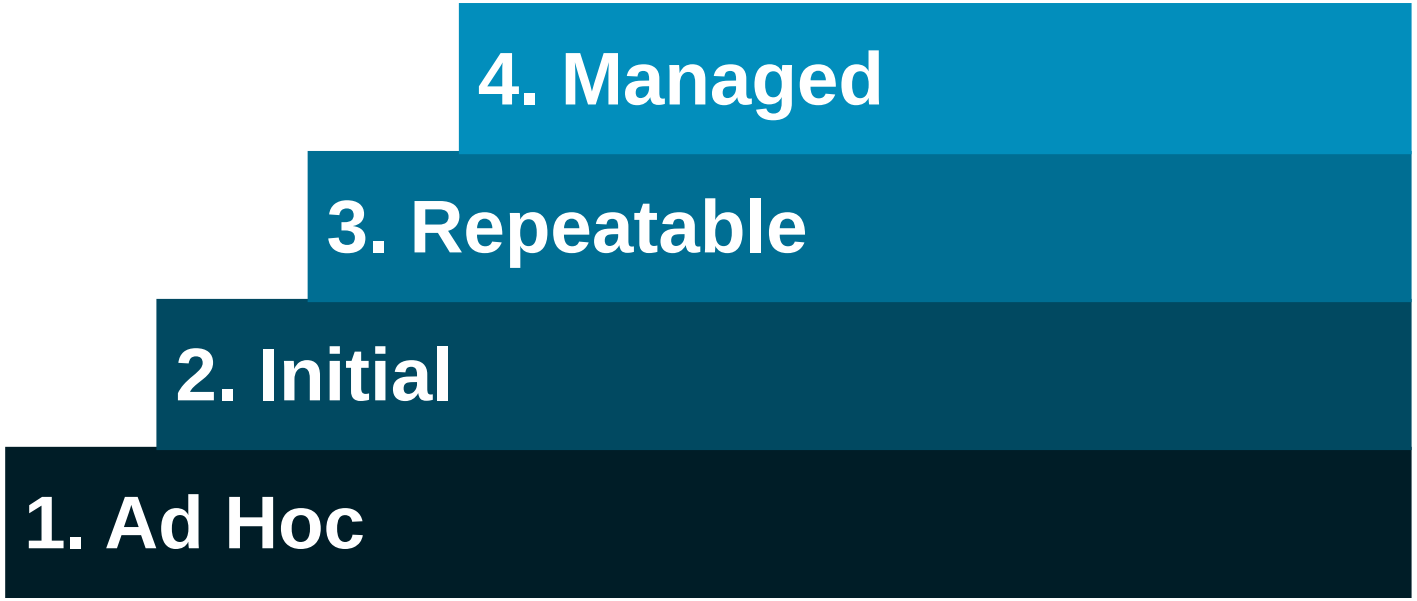
1. Ad Hoc

Risicomanagement volwassenheid

- Processen geïmplementeerd
- Nog niet volledig geïntegreerd

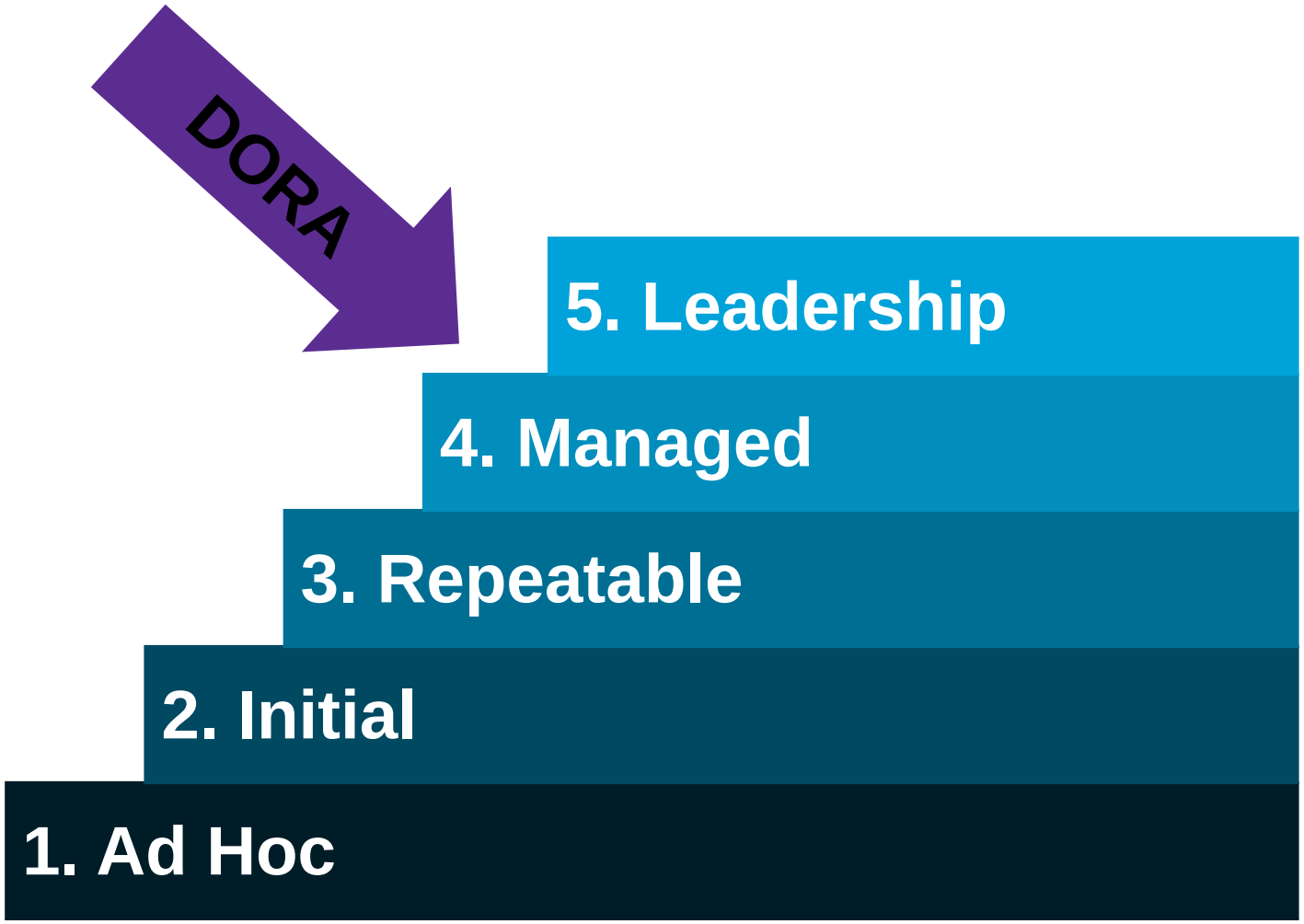
Risicomanagement volwassenheid

- Processen volledig geïntegreerd
- GRC-Tooling



Risicomanagement volwassenheid

- Pro-actief
- Strategisch op alle niveau's
- Risicogestuurde besluitvorming

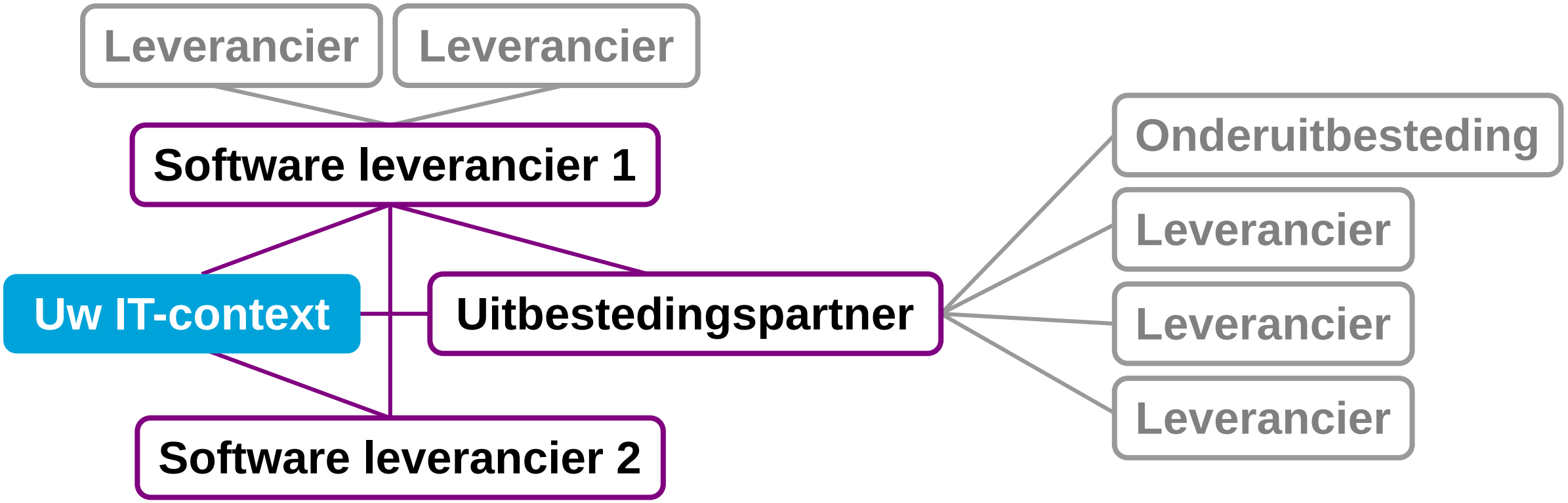


DORA 17-01-2025

- Volwassenheidsniveau 4/5 nodig
- Eigen governance en controlframework (ISO 27001)
  - Vanuit eigen context uitbestedingsrisico's beheersen

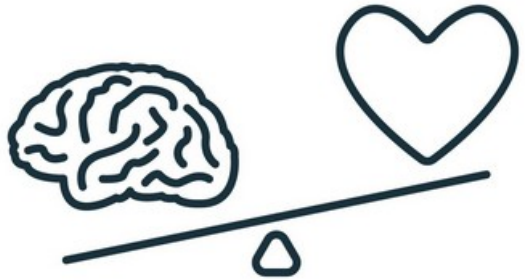
ICT risk management	Cyber incident reporting and respons	Operational resillience testing	Third-party risk management	Information sharing

Complex landschap



Let op!

- Verantwoordelijkheden
- Afhankelijkheden
- Ketenrisico’s
- Procesrisico’s
- Risicogestuurde besluitvorming



Missie

Top 5 Bruto risico’s

- Onbevoegde toegang tot (virtuele) server (**99**)
- Onbevoegde toegang tot netwerkverkeer (**99**)
- Onbevoegde toegang VPO Portal (**88**)
- Onbevoegde toegang tot softwaretoepassingen van klant (**81**)
- Software niet tijdig en volledig up-to-date (**81**)

Risicio-matrix

				Consequences		
		Verwaarloosbaar	Marginaal	Serieus	Kritiek	Catastrofaal
Probability		3	5	7	9	11
Zeer waarschijnlijk	9	27	45	63	81	99
Waarschijnlijk	8	24	40	56	72	88
Mogelijk	7	21	35	49	63	77
Onwaarschijnlijk	6	18	30	42	54	66
Zeer onwaarschijnlijk	5	15	25	35	45	55

ISMS

- Eisen, maatregelen, risico's, incidenten, audits,…
- 56 overkoepelende risico's
  - Meerdere gevolgen/oorzaken gekoppeld
  - Gebeurtenissen op assetniveau
- 185 maatregelen

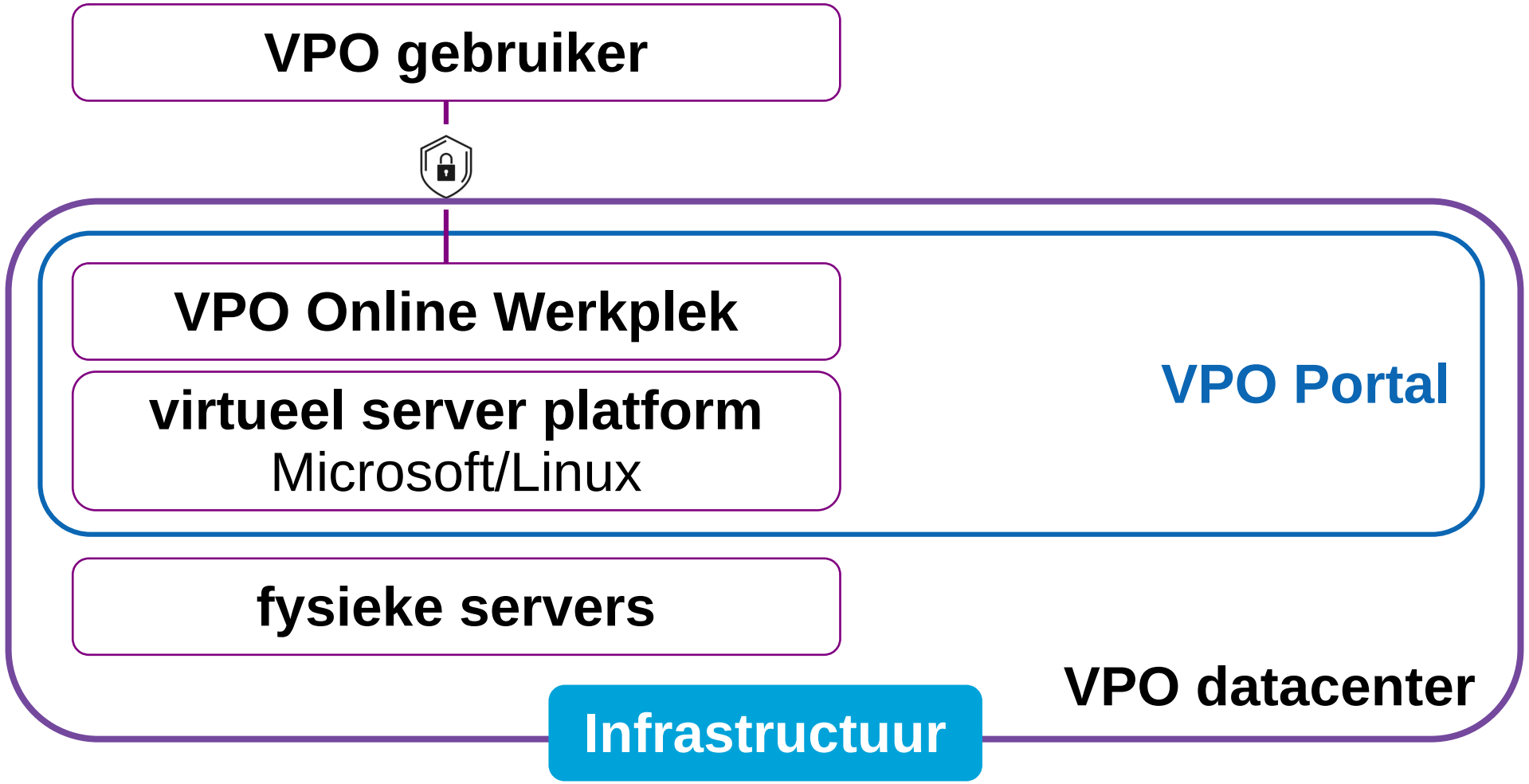
Top 5 Netto risico's

- Onbevoegde toegang tot VPO Portal (**55**)
- Zware beschadiging datacenter (**55**) met VPO+ (**35**)
- Onbevoegde toegang tot (virtuele) server (**54**)
- (On)opzettelijk verkeerd handelen door medewerker (**54**)
- Beschadiging serverruimte (**54**)

Uitgangspunten VPO (Risk-based)

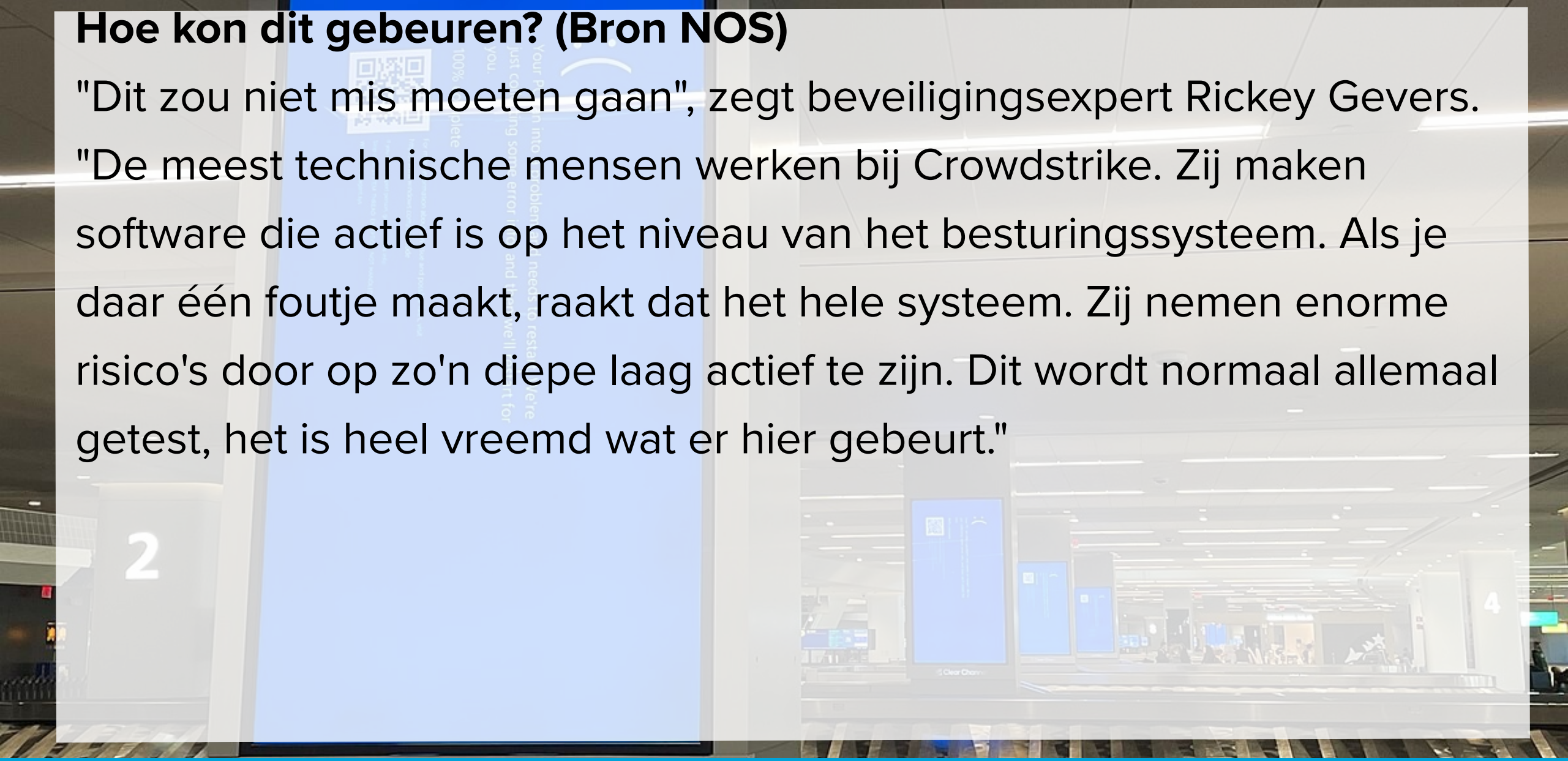
- Centraliseren
- Afhankelijkheid derden minimaliseren
- Complexiteit vermijden
- Uitzonderingen vermijden
- Omvang systemen afstemmen op beheers- en herstelbaarheid

Private cloud – eigen datacenter



Roadmap VPO

- Tweede eigen datacenter (VPO+)
- Focus op Open Source
- Mapping DORA met huidige eisensets
- ISO27001 continuering
- ISAE3000 Type II behalen
- Dialoog ketenrisico’s stimuleren



Hoe kon dit gebeuren? (Bron NOS)

"Dit zou niet mis moeten gaan", zegt beveiligingsexpert Rickey Gevers. "De meest technische mensen werken bij Crowdstrike. Zij maken software die actief is op het niveau van het besturingssysteem. Als je daar één foutje maakt, raakt dat het hele systeem. Zij nemen enorme risico's door op zo'n diepe laag actief te zijn. Dit wordt normaal allemaal getest, het is heel vreemd wat er hier gebeurt."

Bedankt!

e.lankhaar@vpo.nl