VERSLAG JUBILEUMCONGRES

04 Cybersecurity en digitale weerbaarheid

Petra Oldengarm, *Northwave Cyber Security*



AI heeft het digitale dreigingslandschap fundamenteel veranderd. Fysiek en digitaal lopen steeds meer in elkaar over en technologie is politiek geworden: besluiten van een handvol techbedrijven raken direct de nationale veiligheid. Klassiek risicomanagement schiet tekort; wie wil blijven leveren, moet in scenario's denken en vertraging inbouwen.

> ***"Ieder voor zich is geen houdbare strategie meer."***
> Petra Oldengarm, *Northwave Cyber Security*

VIER TRENDS

TREND 1

De patchcyclus is ingestort

Kwetsbaarheden worden vaak al misbruikt voordat er een update is.

TREND 2

Identiteitsfraude met AI

Stem, gezicht en schriftstijl zijn overtuigend na te maken.

TREND 3

Europese OT onder vuur

Operationele technologie in fabrieken en netten is doelwit.

TREND 4

Eerste volledig AI-gestuurde aanval

In april in het eigen CERT waargenomen.

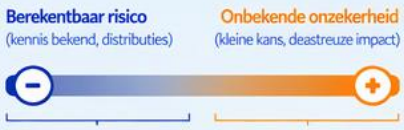
TIJD TUSSEN BEKENDMAKING KWETSBAARHEID EN MISBRUIK



misbruik gemiddeld een week vóór de patch

Spreker refereerde aan informatie van Google/Mandiant.

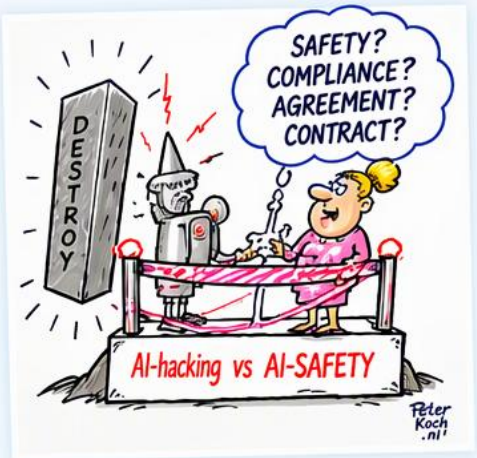
RISICO VERSUS ONZEKERHEID



Naar de risico-onzekerheidsschaal van prof. Dr. Bibi van den Berg (Universiteit Leiden).

WAT ER GEBEURDE IN HET CERT (APRIL)

1. Aanvallers lieten een AI-model (Claude) geloven dat het een geautoriseerde pentest uitvoerde, met een nagemaakt toestemmingsformulier.
2. De AI volgde meerdere aanvalspaden tegelijk, veel sneller dan een menselijke aanvaller.
3. De detectie gaf alleen lage en middelhoge alarmen: makkelijk te missen.



WAT ORGANISATIES KUNNEN DOEN

- **Barrières:** uitzetten wat niet online hoeft, vertraging inbouwen met segmentatie en sandboxing.
- **Glokaal:** globaal waar het moet, lokaal waar het kan, met "eilandjes" en meerdere leveranciers.
- **Scenario's:** wat als Microsoft 365 wegvalt, of AI tien tot honderd keer duurder wordt?
- **Bestuur:** blijf kritische vragen stellen, maak iemand eigenaar en denk in ketens.

AI is wapen én schild.

Verdedigers zetten AI in met de mens in de lus; aanvallers hebben voorlopig een voorsprong in tempo en vrijheid.

Samenwerking in het ecosysteem en Europese soevereiniteit in cloud en AI worden daarmee strategische vraagstukken, ook voor bestuurders buiten de IT.