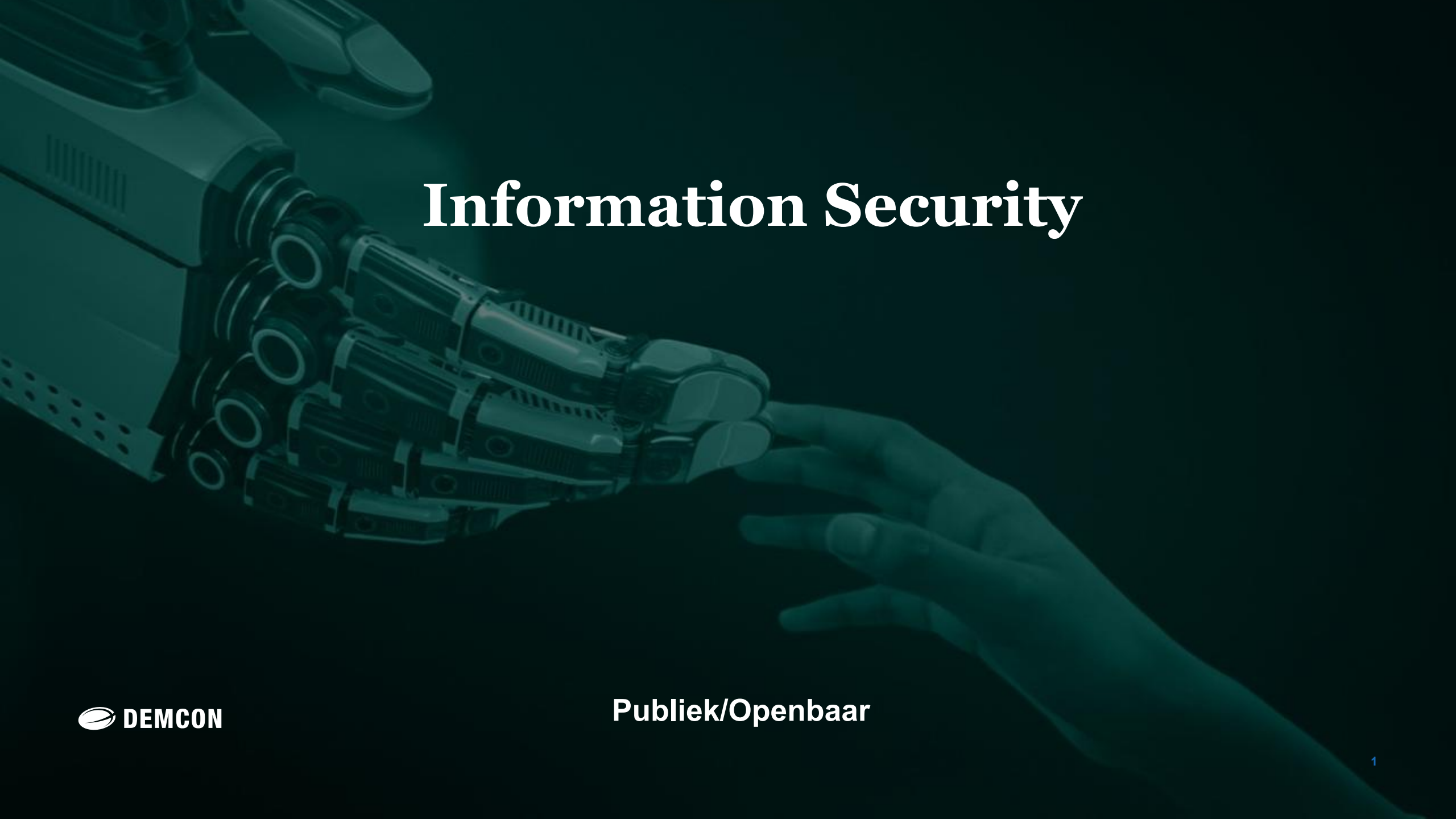


Information Security

DEMCON

Publiek/Openbaar

Datalek ODIDO

- Social Engineering op basis van AI.
- IT Helpdesk en klantenservice.
- Toegang tot CRM.
- Bewaartermijnen.
- Wat kunnen wij hier van leren? Herkennen wij de juiste signalen?

Wat is informatiebeveiliging?

- Informatiebeveiling beschermt wat het meest waardevol is: onze informatie.
- Combinatie van mens, proces en techniek.
- Confidentiality, Integrity en Availability (CIA).
- Organisatiebrede verantwoordelijkheid.

Dreigingsbeeld, wat komt er op ons allen af?

- Wat kunnen we leveren van beschikbare informatie en rapporten?

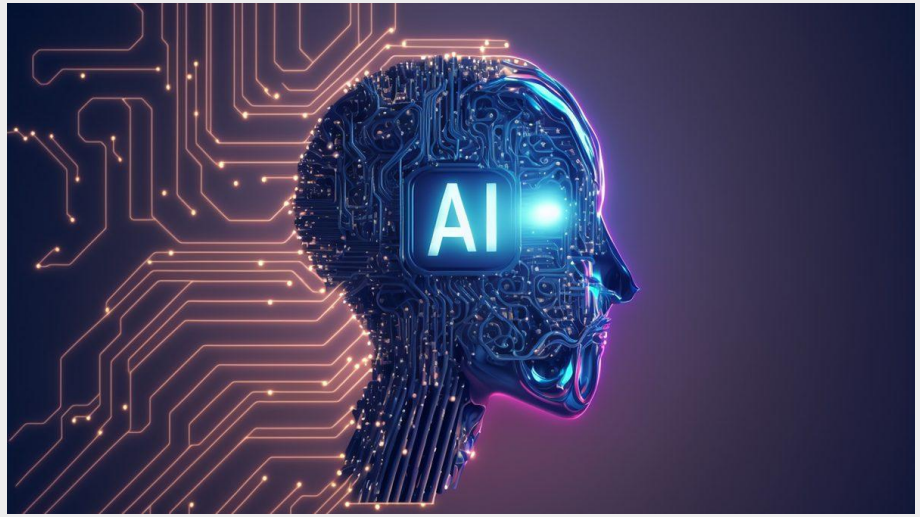
- Generative AI ingezet voor offensieve en defensieve acties.
  - Informatie verzamelen en acties voorbereiden (social engineering).

- Geopolitieke ontwikkelingen leggen afhankelijkheden bloot.
  - Afhankelijkheden van bijvoorbeeld de VS, mogelijk invloed op beschikbaarheid en veiligheid (vendor lock-in).

- Toenemende cybercapaciteiten waardoor dreigingen steeds complexer worden.
  - Landen met een offensief cyberprogramma tegen Nederlandse belangen.

Trends, welke ontwikkelingen zien we?

- Generative Artifical Intelligence (GenAI)
  - ChatGPT, CoPilot, Gemini, Claude, Perplexity en ….
- Snelle digitalisering van organisaties.
  - Informatie gedreven bedrijfsvoering.
- Quantum Computing.
  - Oplossen van complexe problemen.



Waarom informatiebeveiliging?

- (Vertrouwelijke) informatie is voor organisaties tegenwoordig één van de belangrijkste bedrijfsmiddelen. Binnen organisaties is veel informatie aanwezig die door klanten en medewerkers aan de organisatie wordt toevertrouwd.

- De wereld verandert razendsnel. Cyberdreigingen evolueren dagelijks.

- Als organisatie moet je je weerbaar maken tegen deze dreigingen, en voorbereid te zijn om te acteren wanneer er iets mis gaat.

- Toenemende wet- en regelgeving, dit jaar komt hier de Cyberbeveiligingswet/NIS2 bij.

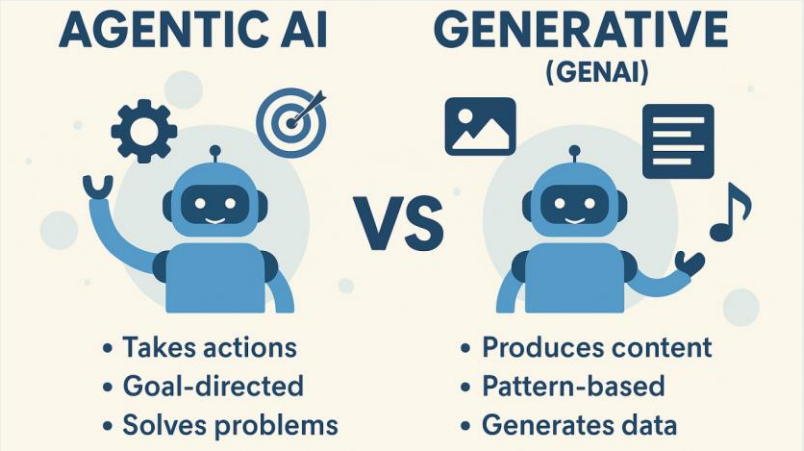
Cyberbeveiligingswet – NIS2

- Veel meer organisaties vallen onder de wet.
  - *Essentiële* en *belangrijke* entiteiten.
- Zorgplicht: verplicht risicomanagement en passende beveiligingsmaatregelen.
  - Op basis van risicobeoordelingen en het Cyberbeveiligingsbesluit.
- Registratieplicht en ketentransparantie.
  - Organisaties moeten zich registeren in het entiteitenregister via het NCSC.
- Strikte meldplicht voor incidenten.
  - ‘Bij significante incidenten’ binnen 24 uur eerste waarschuwing, binnen 72 uur volledige melding.
- Bestuurlijke verantwoordelijkheid & stevige sancties.
  - Aantoonbare kennis bij bestuurder, met hoofdelijke aansprakelijkheid bij nalatigheid.

Basis maatregelen NIS2

- Beleid op risicomanagement en informatiebeveiliging.
- Incidentmanagement.
- Business Continuity Management.
- Supply chain beveiliging.
- Beveiliging bij het aankopen, ontwikkelen en onderhouden van systemen.
- Awareness en bewustzijn.
- Beleid voor het gebruik van cryptografie.
- Beleid voor logische en fysieke toegang.

Gen AI vs. Agentic AI



- Generative AI = de briljante tekst- en beeldmaker.
- Agentic AI = een slimme collega met jouw sleutels, pincode en agenda.
- Aandacht voor controle op output.
- Toename van aanvalsoppervlak door het kunnen uitvoeren van acties, waar toe heeft een agent toegang?
- Ontwikkelingen binnen bekende platformen gaan in een snel tempo, hoe houd ik hier zicht op?

Hoe vind ik balans tussen dreigingen en trends?

- Uitvoeren van risicoanalyses en het managen van risico's.
  - Welke risico's zijn voor onze organisatie acceptabel?

- Veiligheid vs. innovatie.

- Het implementeren van een managementsysteem biedt hierin handvaten.
  - ISO 27001 als paraplu.

- Het certificeren van een organisatie, helpt bij het aantonen van compliance.
  - Waaronder de NIS2 en aan bijvoorbeeld klanten en partners.

Vragen?