Opdracht A

Risicoanalyse en Risicobeoordeling

1. Echte voorbeelden van aanvallen door verschillende typen kwaadwillenden

Cybercriminelen – ransomware/afpersing

- **Colonial Pipeline (VS, 2021) – DarkSide ransomware**
  Colonial Pipeline werd getroffen door ransomware van de groep DarkSide. Hierdoor werd de bedrijfsvoering tijdelijk stilgelegd en ontstond verstoring van brandstofdistributie. Dit incident wordt in een officiële "joint advisory" van CISA/FBI beschreven, inclusief typische aanvalspaden en mitigaties (Cybersecurity and Infrastructure Security Agency [CISA] & Federal Bureau of Investigation [FBI], 2021).
- **Jaarbeeld Ransomware 2024 (NL) – Project Melissa / NCSC**
  In het Jaarbeeld Ransomware 2024 worden trends in ransomware-incidenten in Nederland samengevat op basis van incidentinformatie van o.a. NCSC/politie en aangesloten securitypartijen. Het rapport is bedoeld als input voor risicobeoordelingen en weerbaarheidsmaatregelen (Project Melissa, 2025).

Cybercriminelen – phishing / social engineering / account takeover

- **MGM Resorts (VS, 2023) – social engineering + verstoring bedrijfsprocessen**
  MGM Resorts rapporteerde een cybersecurity-incident met substantiële operationele impact (o.a. uitval van systemen). Het bedrijf lichtte dit publiek toe via een officiële melding richting investeerders (MGM Resorts International, 2023).

Statelijke actoren / APT – supply chain / spionage

- **SolarWinds Orion (2020) – supply-chain compromis**
  De SolarWinds Orion-compromittering is een klassiek voorbeeld van een geavanceerde (APT) supply-chain aanval, waarbij via vertrouwde software-updates toegang werd verkregen bij overheden en organisaties. CISA publiceerde hierover meerdere alerts/analyses en verwijst naar de bekende activity alert AA20-352A (CISA, 2021).

2. Risicomatrix

Voor punt 2 en 3 verwijs ik naar onze ingevulde Excel: Risk assessment table_filled.xlsx

(tabblad **Risk matrix** + het impact-overzicht met meerdere invalshoeken).
Daarin staat o.a.:

- **Kans (1–5)** met frequentie-ankerpunten (bijv. 1 = <1x per 5 jaar, 5 = wekelijks/maandelijks).
- **Impact (A–E)** met meerdere invalshoeken/dimensies (zoals financieel, health & safety, reputatie, environmental, compliance, neighborhood disturbance).
- De **kleurcodering** (groen/geel/oranje/rood) die de risicoprioriteit visualiseert.

3. Beoordelen van de kans van risico's

Werkwijze

1. **Bepaal scenario + scope** (asset, proces, periode, aannames).
2. **Kans-score kiezen (1–5)** op basis van:
    - blootstelling (hoe vaak komt dit voor?),
    - aanvalsmogelijkheid (hoe makkelijk is het?),
    - sterkte van huidige maatregelen (hoeveel "frictie" voor de aanvaller?),
    - historie/sectortrends (rapporten/incidenten).
3. **Impact-score kiezen (A–E)** met impactdefinities (meerdere invalshoeken).
4. **Risico = Kans × Impact** (Kleuren in de matrix).
5. **Maatregelen koppelen**:
    - Preventief → kans omlaag
    - Correctief → impact omlaag / herstel sneller
6. **Her-score** (residual risk) en kies **accept/mitigate/transfer/avoid**.

Bow-tie analyse

Ter verdieping van de risicoanalyse is een bow-tie analyse opgesteld voor het top event ongeautoriseerde toegang / verlies van integriteit. De bow-tie visualiseert de relatie tussen oorzaken (zoals phishing, zwakke wachtwoorden, malware en fysieke diefstal), het centrale risico en de mogelijke gevolgen (zoals datalekken, fraude en reputatieschade). Daarnaast maakt de bow-tie expliciet onderscheid tussen preventieve maatregelen die de kans verlagen en correctieve maatregelen die de impact beperken. Deze analyse vormt de onderbouwing voor het risicoregister en de gekozen beheersmaatregelen.

4. Kwetsbaarheden en bedreigingen

Op basis van literatuur en erkende cybersecurityrapporten zijn veelvoorkomende kwetsbaarheden en bedreigingen geïnventariseerd die relevant zijn voor dit project.

Veel voorkomende **kwetsbaarheden** zijn onder andere zwakke of hergebruikte wachtwoorden, het ontbreken van multi-factor authenticatie, onvoldoende patchmanagement, onjuiste configuratie van cloud-diensten (zoals publieke deel-links) en het ontbreken van adequate logging en monitoring. Deze kwetsbaarheden vergroten de kans dat een aanval succesvol is of pas laat wordt gedetecteerd.

Daarnaast zijn diverse **bedreigingen** structureel terug te zien in de praktijk. Rapporten van onder andere CISA, ENISA en Verizon tonen aan dat een groot deel van incidenten begint met phishing of misbruik van gelekte inloggegevens. Ook ransomware, malware-infecties, supply-chain aanvallen en insider threats komen frequent voor. Deze bedreigingen sluiten aan bij de in dit project geïdentificeerde risico's, zoals ongeautoriseerde toegang, datalekken en verstoring van beschikbaarheid.

De combinatie van deze kwetsbaarheden en bedreigingen vormt de basis voor het risicoregister en de verdere risicoanalyse. De gebruikte bronnen bevestigen dat de gekozen risico's realistisch zijn en representatief voor actuele cybersecuritydreigingen in de praktijk.

Referentielijst

- Cybersecurity and Infrastructure Security Agency, & Federal Bureau of Investigation. (2021, 11 mei). *Joint cybersecurity advisory: DarkSide ransomware: Best practices for preventing business disruption from ransomware attacks (AA21-131A).* National Security Archive. https://nsarchive.gwu.edu/document/21226-06-20210211-aa21-131adarksideransomware
- Cybersecurity and Infrastructure Security Agency. (2021, 15 april). *CISA and CNMF analysis of SolarWinds-related malware* (verwijst naar Alert AA20-352A). https://www.cisa.gov/news-events/alerts/2021/04/15/cisa-and-cnmf-analysis-solarwinds-related-malware
- Cybersecurity and Infrastructure Security Agency. (2021, 14 mei). *Remediating networks affected by the SolarWinds and Active Directory/M365 compromise* (o.a. context/doorverwijzing naar AA20-352A). https://www.cisa.gov/news-events/news/remediating-networks-affected-solarwinds-and-active-directorym365-compromise
- MGM Resorts International. (2023, 12 september). *Form 8-K (Current report) – Cybersecurity incident disclosure.* U.S. Securities and Exchange Commission. https://www.sec.gov/Archives/edgar/data/789570/000119312523251667/d461062d8k.htm
- Project Melissa. (2025). *Jaarbeeld ransomware 2024.* Nationaal Cyber Security Centrum (NCSC). https://cyberveilignederland.nl/project-melissa
- Associated Press. (2021, 7 mei). *U.S. pipeline hacked, forcing closure; gasoline shortages feared.* https://www.cisa.gov/news-events/news/attack-colonial-pipeline-what-weve-learned-what-weve-done-over-past-two-years

- Reuters. (2021, 8 mei). *U.S. gasoline pipeline Colonial shuts after cyberattack.* https://www.reuters.com/business/energy/view-cyberattack-pipeline-spotlights-holes-us-energy-security-2021-05-08/