Opdracht A

Beveiligingsmaatregelen

1. ISO 27002:2022 / IEC 62443 – Voorbeeldmaatregelen en implementatie

ISO 27002:2022 bevat vier hoofdcategorieën:

- **Organisatorisch**
- **Personeel**
- **Fysiek**
- **Technologisch**

Hieronder per categorie één maatregel met implementatievoorstel:

1.1 Organisatorisch – Informatiebeveiligingsbeleid

Maatregel (ISO 27002): Informatiebeveiligingsbeleid vaststellen en onderhouden.

Implementatie:

- Directie stelt formeel een informatiebeveiligingsbeleid vast.
- Rollen en verantwoordelijkheden (CISO, IT-beheer, proceseigenaren) worden benoemd.
- Beleid bevat: classificatie van informatie, wachtwoordbeleid, incidentmelding, back-upbeleid.
- Jaarlijkse review + update.
- Communicatie via intranet en onboarding-training.

Doel: Richting geven aan alle securityactiviteiten en compliance aantoonbaar maken.

1.2 Personeel – Security Awareness & Training

Maatregel: Security awareness programma.

Implementatie:

- Verplichte jaarlijkse e-learning over phishing, wachtwoorden, datalekken.
- Periodieke phishing-simulaties.
- KPI: klikratio < 5%.
- Awareness posters + korte kwartaalupdates.

Doel: Menselijke factor als zwakste schakel versterken.

1.3 Fysiek – Toegangsbeveiliging kantoor/ruimtes

Maatregel: Fysieke toegangscontrole tot kritieke ruimtes.

Implementatie:

- Toegang tot serverruimte via badge + logging.
- Cameratoezicht in IT-ruimtes.
- Bezoekersregistratie.
- Clean desk policy.

Doel: Voorkomen van diefstal, sabotage of ongeautoriseerde toegang.

1.4 Technologisch – Multi-Factor Authenticatie (MFA)

Maatregel: Sterke authenticatie.

Implementatie:

- MFA verplicht op alle cloudaccounts (M365, GitHub, VPN).
- Gebruik van authenticator-app of hardware token.
- Conditional Access (bijv. blokkeren vanaf onbekende landen).
- Logging en monitoring van loginpogingen.

Doel: Kans op accountovername drastisch verlagen.

2. NIST Cybersecurity Framework (CSF) – Reflectie

NIST CSF 2.0 bestaat uit zes functies:

Identify

- Assetinventarisatie
- Risicobeoordeling
- Data-classificatie

→ Zorgt voor overzicht en prioritering.

Protect

- Toegangscontrole (MFA)
- Encryptie
- Awareness
- Back-ups

→ Verlaagt kans op incident.

Detect

- Logging
- SIEM
- Monitoring login-anomalieën

→ Snelle detectie beperkt impact.

Respond

- Incident response plan
- Communicatieplan
- Rollen & escalatie

→ Beperkt schade en herstelt vertrouwen.

Recover

- Restore procedures
- DR-plan
- Evaluatie & verbeteracties

→ Continuïteit waarborgen.

Govern

- beleid, rollen, risicosturing
  → borgt verantwoordelijkheid en compliance.

Reflectie:
Het NIST CSF helpt organisaties gestructureerd werken. Het combineert preventie, detectie en herstel. Het sluit goed aan op ISO 27001/27002 en ondersteunt maturity-groei.

3. Hardening van Windows 11 – Onderzoek en evaluatie eigen laptop

Mijn laptop is ingericht voor school, werk en development met een set tools die passen bij mijn werkzaamheden (o.a. Visual Studio Community, VS Code, .NET SDK's, Git, Docker Desktop, SQL Server/SSMS, TablePlus, MySQL, Python, StarUML en Acrobat/Notepad++). Qua browsersetup werk ik bewust met meerdere browsers voor verschillende doelen: Opera is mijn standaardbrowser, Chrome gebruik ik vooral voor school en als back-up mocht Opera ooit niet werken voor mij en Firefox gebruik ik voor entertainment (films/series/YouTube). Edge heb ik verwijderd omdat ik die nooit gebruik.

Aan de beveiligingskant staan de basismaatregelen goed. Windows Security geeft aan dat virus- en bedreigingsbeveiliging, accountbeveiliging en app-/browserbeheer geen actie vereisen. Daarnaast staat de Windows Defender Firewall ingeschakeld met onderscheid tussen particuliere en openbare netwerken. Dit laat zien dat de standaard beveiligingslaag van Windows actief is en dat er geen directe waarschuwingen of urgente acties openstaan.

Tegelijk zie ik ook aandachtspunten voor hardening. Ik heb TeamViewer geïnstalleerd; dat is handig, maar remote access is een extra aanvalsvector als accounts of instellingen niet sterk genoeg zijn. Daarom is het belangrijk om dit type software zo beperkt mogelijk te gebruiken (alleen wanneer nodig), niet automatisch mee te laten opstarten en het account extra te beveiligen (bijvoorbeeld met sterke wachtwoorden en waar mogelijk MFA).

Daarnaast gebruik ik PC HelpSoft Driver Updater als praktische troubleshooting-tool wanneer drivers issues geven, zoals een instabiele Bluetooth/audio-verbinding met mijn JBL-speakers. Na zo'n update werkt het vaak weer normaal. Ik ben me er wel van bewust dat driver-updaters van een derde partij extra aanvalsoppervlak en mogelijk supply-chain risico kunnen introduceren. Daarom gebruik ik deze tool alleen bij concrete problemen (niet automatisch), controleer ik welke driver wordt aangepast en probeer ik eerst Windows Update of de fabrikant. Revo Uninstaller gebruik ik juist positief voor systeemhygiëne, zodat restanten van ongewenste software goed verwijderd worden.

Overall is mijn laptop functioneel én redelijk goed beveiligd voor een student/developer. De belangrijkste verbeterpunten zitten in het strikt beperken en afschermen van remote access en het bewust en minimaal houden van driver-updates via tools van derde partijen.

4. Pakket van maatregelen tegen “insider threat” (kwaadwillende of omgekochte interne medewerker)

- **Toegang & autorisatie (least privilege)**
    - Geef medewerkers alleen toegang tot wat ze écht nodig hebben (least privilege) en werk met rolgebaseerde toegang (RBAC).
    - Gebruik **Just-In-Time (JIT)** elevated access: adminrechten alleen tijdelijk en na goedkeuring.
    - Voer periodieke access reviews uit (bijv. maandelijks per team) en trek oude rechten direct in bij functiewijzigingen.

- **Identiteit & authenticatie**
    - Verplicht MFA voor alle accounts, vooral voor admins en toegang op afstand.
    - Gebruik Conditional Access (bijv. blokkeren vanaf onbekende landen, vereisen van compliant device).
    - Gebruik sterk wachtwoordbeleid + account lockout en voorkom gedeelde accounts.

- **Scheiding van taken (SoD) & 4-ogen principe**
    - Kritische acties (bijv. uitbetalingen, export van klantdata, wijzigen van logging, verwijderen van backups) altijd via 4-ogen controle.
    - Splits rollen: degene die ontwikkelt is niet dezelfde die deployt naar productie zonder review/goedkeuring.

- **Monitoring, logging & detectie (vroeg signaleren)**

  Centraliseer logs in een SIEM (of minimaal centrale logging) en bewaak op:

  - grote/ongebruikelijke downloads of exports,
  - toegang buiten werktijden,
  - inlogpogingen vanaf nieuwe locaties/devices,
  - massaal openen/kopiëren van bestanden.

  - Zet alerts op “high risk” events (data-export, privilege escalation, aanpassing van permissies, verwijderen van audit logs).

- **Data Loss Prevention (DLP) & datacontrole**

  Classificeer data (bijv. publiek/intern/vertrouwelijk) en stel regels in:

  - blokkeren of waarschuwen bij mailen/zippen/uploaden van vertrouwelijke data,
  - beperk USB/opslagmedia (alleen toegestaan indien nodig en gemonitord),
  - beperk cloud shares: geen “anyone with link”, gebruik expiratie en waar mogelijk watermerken.

  - Gebruik encryptie (BitLocker op endpoints, encryptie in transit/at rest) om datadiefstal minder bruikbaar te maken.

- **Endpoint hardening**

  - Zorg voor up-to-date devices (patching), EDR/Defender en beperk lokale adminrechten.
  - Whitelisting/controlled applications voor kritieke systemen (alleen goedgekeurde tools).
  - Zet “tamper protection” aan zodat beveiliging niet makkelijk uit kan.

- **Processen rondom HR & organisatie (voorkomen en beperken)**
    - Screening bij indiensttreding voor gevoelige functies + duidelijke gedragscode.
    - Awareness & training: herken omkoping/social engineering, meldplicht en omgang met data.
    - Offboarding strikt: op de laatste werkdag direct accounts blokkeren, tokens intrekken, devices innemen, toegang verwijderen.
    - Introduceer een vertrouwelijk meldpunt voor signalen (druk, conflicten, ronseling).

- **Incident response & herstel (als het tóch gebeurt)**
    - Maak een insider-threat playbook: wie beslist, welke logs nodig zijn, juridische stappen en communicatie.
    - Gebruik immutabele backups en test herstelprocedures, zodat sabotage (verwijderen/versleutelen) beperkt blijft.
    - Documenteer bewijs (forensisch) en hanteer minimaal “need-to-know” tijdens onderzoek.

- **Specifiek tegen sabotage in IT/DevOps**
    - Verplicht code reviews en branch protection (geen directe pushes naar main).
    - Gebruik signed commits (optioneel) en houd audittrail op changes in CI/CD.
    - Productie-deploy alleen via pipeline met approvals en logging.

Referentielijst

- Cybersecurity and Infrastructure Security Agency. (z.d.). *Insider threat*. https://www.cisa.gov/topics/physical-security/insider-threat
- National Institute of Standards and Technology. (2024, 26 februari). *The NIST Cybersecurity Framework (CSF) 2.0*. https://www.nist.gov/cyberframework
- National Institute of Standards and Technology. (2020). *Zero Trust Architecture (SP 800-207)*. https://csrc.nist.gov/publications/detail/sp/800-207/final
- Software Engineering Institute, Carnegie Mellon University. (2022). *Common Sense Guide to Mitigating Insider Threats (7th Edition)*. https://www.sei.cmu.edu/documents/619/2022_019_001_886876.pdf
- Verizon. (2025). *Data Breach Investigations Report 2025: Healthcare snapshot*. https://www.verizon.com/business/resources/infographics/2025-dbir-healthcare-snapshot.pdf