Opdracht workshop 2 Risicodenken en -management

CYBERBEVEILIGINGSWET (CBW) – NEDERLANDSE IMPLEMENTATIE VAN DE NIS2-RICHTLIJN

1. Onderzoek de wet- en regelgeving en normen die van kracht zijn rond cybersecurity, zowel op nationaal als internationaal niveau. Ieder groepslid kiest hierbij één norm of wet.

Ik heb als individuele keuze de **Cyberbeveiligingswet (Cbw)** gekozen. Dit is de Nederlandse wet die de Europese NIS2-richtlijn omzet naar nationale verplichtingen voor organisaties die onder de reikwijdte vallen.

Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

2. Focus op relevante wetten, regelgevingen en normen, zoals, maar niet uitsluitend: AVG (GDPR), ISO27001, NIST Cybersecurity Framework, NIS2 maar bijvoorbeeld ook de wet Computercriminaliteit III.

Mijn focus ligt op de Cyberbeveiligingswet (Cbw). Waar nodig verwijs ik naar de achterliggende Europese basis (NIS2), omdat de Cbw daarop gebaseerd is.

Bron (NIS2 EUR-Lex): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

3. Gebruik verschillende bronnen, waaronder overheidswebsites, officiële publicaties, en betrouwbare organisaties op het gebied van cybersecurity.

Gebruikte bronnen:

- Digitale Overheid – Cyberbeveiligingswet: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/
- Digitale Overheid – Verplichtingen Cyberbeveiligingswet: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/verplichtingen-cyberbeveiligingswet/
- EUR-Lex – NIS2 (Richtlijn 2022/2555): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng
- Rijksoverheid – Update/ontwikkeling implementatie NIS2/CER: https://www.rijksoverheid.nl/actueel/nieuws/2024/10/23/implementatie-nis2-en-cer-in-nederland-vertraagd-wat-betekent-dat-voor-u
- NIST – Cybersecurity Framework 2.0 (officiële publicatie): https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

4. Beantwoord de volgende vragen als leidraad voor jullie onderzoek:

1. Welke nationale en internationale wetten zijn van toepassing op cybersecurity?

- **Nationaal (NL): Cyberbeveiligingswet (Cbw)** – Nederlandse wetgeving voor cybersecurity (implementatie van NIS2).

Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

- **Internationaal/EU: NIS2-richtlijn (EU) 2022/2555** – Europese richtlijn waarop de Cbw gebaseerd is.

Bron: https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

2. Wat zijn de belangrijkste vereisten van deze wetten en regelgevingen met betrekking tot cybersecurity?

De Cyberbeveiligingswet (Cbw) (NIS2-implementatie) vereist in hoofdlijnen dat organisaties:

- **Passende maatregelen** nemen om risico's voor netwerk- en informatiesystemen te beheersen (zorgplicht/risicomanagement).
- **Cybersecurity bestuurlijk beleggen** (governance: verantwoordelijkheden, beleid en aansturing).
- **Incidenten afhandelen en melden** volgens de meldprocedures bij significante incidenten.
- **Keten- en leveranciersrisico's** meenemen (supply chain security).
- **Continuïteit en herstel** organiseren (bijv. back-ups, crisisprocessen, herstelprocedures).

Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/verplichtingen-cyberbeveiligingswet/
Achtergrond (NIS2): https://eur-lex.europa.eu/eli/dir/2022/2555/oj/eng

3. Welke normen worden vaak gebruikt als referentie voor best practices in cybersecurity? Op welke sectoren zijn ze van toepassing?

- **ISO/IEC 27001 + 27002** – veel gebruikt als best practice om informatiebeveiliging te organiseren (ISMS + controls); **breed toepasbaar in vrijwel alle sectoren**.
- **NIST Cybersecurity Framework (CSF 2.0)** – framework om cybersecurity te structureren (o.a. governance en risicosturing); **breed toepasbaar in vrijwel alle sectoren**.

  Bron: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

- **(Overheid) BIO** – normenkader voor informatiebeveiliging bij overheden; **toepassing binnen overheid en (semi-)publieke organisaties**.

4. Hoe worden deze normen toegepast in de praktijk binnen organisaties?

Organisaties gebruiken normen zoals ISO 27001/27002 of NIST CSF als **referentiekader** om hun beveiliging in te richten. Ze zetten dit om naar **beleid**, **processen** en **technische maatregelen** (bijv. toegangsbeheer/MFA, patchmanagement, logging/monitoring, back-ups en een incidentproces). Vervolgens wordt periodiek gecontroleerd of dit werkt (audits/controles) en wordt de beveiliging continu verbeterd op basis van nieuwe risico's en incidenten.

5. Wat zijn de voordelen voor organisaties om te voldoen aan deze wetten, regelgevingen en normen?

- **Minder kans en impact van cyberincidenten** en daardoor minder verstoring van dienstverlening.
- **Snellere en effectievere respons** door processen voor incidentafhandeling en meldingen.
- **Aantoonbare compliance** richting toezichthouder en ketenpartners.
- **Meer vertrouwen** bij klanten, partners en auditors.

Bron (Cbw-context): https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

6. Wat zijn de recente ontwikkelingen of updates in wet- en regelgeving die van invloed zijn op cybersecurity?

- De grote ontwikkeling in Nederland is de invoering van de **Cyberbeveiligingswet (Cbw)** als **implementatie van NIS2**, waarmee strengere en bredere cybersecurity-verplichtingen worden ingevoerd voor relevante organisaties.

Bron: https://www.digitaleoverheid.nl/overzicht-van-alle-onderwerpen/cyberbeveiligingswet/

- De Nederlandse implementatie van **NIS2/CER** is onderwerp van actualiteit (planning/vertraging), wat je kunt noemen als recente update.

Bron: https://www.rijksoverheid.nl/actueel/nieuws/2024/10/23/implementatie-nis2-en-cer-in-nederland-vertraagd-wat-betekent-dat-voor-u