Digitaal Weerbare Waterbouw

Johannes Braams,
Leading professional Cybersecurity IA, Haskoning

Agenda

1. Definities
2. Risico’s
3. Wet-en regelgeving
4. Voorbeelden

Definities

Cybersecurity

is het geheel aan technische, organisatorische en fysieke maatregelen om schade door verstoring, uitval of misbruik van ICT systemen (en IA-systemen) te voorkomen.

Die schade kan bestaan uit de aantasting van

- de Veiligheid,
- de Beschikbaarheid,
- de Integriteit of
- de Vertrouwelijkheid

van systemen en de daarin opgeslagen informatie dan wel (IA) de door die systemen bestuurde processen

Definities

Cyberweerbaarheid

is het geheel aan technische, organisatorische en fysieke maatregelen die er op zijn gericht om, in geval van een verstoring van de ICT/IA-systemen (b.v. t.g.v. een aanval), de gevolgen van de verstoring tot een minimum te beperken.

Denk daarbij aan:

- Duur van de verstoring
- Impact van de verstoring
- Forensisch bewijs (!)

Definities

Risico acceptatie

is de bereidheid van een organisatie om een bepaald risiconiveau te accepteren.

Belangrijk:

- Risico's bewust beoordelen op de vraag of het risiconiveau acceptabel is
- Maatregelen treffen om risico's tot acceptabel niveau te beheersen
- Plan hebben (en oefenen) hoe te handelen als een risico optreedt

Risico’s

- Risico’s op het gebied van informatiebeveiliging
  - Als gevoelige informatie niet wordt beschermd (dreiging)
  - dan kan het in handen van onbevoegden vallen (ongewenst)
  - met als gevolg dat … (negatief gevolg)
- Risico’s op het gebied van installaties
  - Als onbevoegden toegang krijgen tot de besturing (dreiging)
  - dan kan de pomp worden uitgeschakeld (ongewenst)
  - met als gevolg dat er een overstroming ontstaat (negatief gevolg)

Risico inventarisatie

1. Bepaal wat een acceptabel risico is
2. Bepaal het systeem waarvoor je de risico’s wilt inventariseren
3. Voer een high level risico inventarisatie uit voor het systeem
4. Verdeel het systeem in zones en verbindingen
5. Voer een detail risicoanalyse uit per zone en verbinding
6. Bepaal welke risico’s niet acceptabel zijn
7. Bepaal beheersmaatregelen

Wet en regelgeving (Europees)

- Critical Entities Resilience Directive (CER) (2022/2557)
  - Door overheid aan te wijzen kritiek entiteiten
  - gaat vooral over fysieke weerbaarheid
- Network and Information Systems Directive (NIS2) (2022/2555)
  - Essentiële en belangrijke entiteiten
  - Plichten (Opleidingsplicht, Zorgplicht, Meldingsplecht)
  - Rechten (Vrijwillig melden, bijstand)
  - Toezicht
    - Essentiële entiteiten: vooraf
    - Belangrijke entiteiten: achteraf
  - Sancties
    - Essentiële entiteiten: maximum van 2% wereldwijde jaaromzet of 10M€, ontheffing bestuurder(s) uit hun functie
    - Belangrijke entiteiten: maximum van 1,4% wereldwijde jaaromzet of 7M€

Wet en regelgeving (Europees)

- Cybersecurity Resilience Act (2024/2847)
  - Producten en Product Ontwikkeling moeten “secure by default” zijn
  - Conformiteitseisen voor Belangrijke en kritieke producten
  - Eisen aan fabrikanten, minimum ondersteuningsperiode (5 jaar)
  - Eisen voor importeurs
  - Eisen voor distributeurs
  - Conformiteitseisen en documentatie eisen
  - Overgangsperiode tot december 2027
- Machinery Regulation (2023/1230)
  - Legt relatie tussen machine veiligheid en cybersecurity
- CE Markering
  - Voldoen aan CRA, Machine Regulation, RED 3.3

Wet en regelgeving (Nationaal)

- Wet weerbaarheid kritieke entiteiten (Wwke)
  - Nederlandse implementatie van de CER
  - Wetsvoorstel bij Tweede kamer voor behandeling
- Besluit weerbaarheid kritieke entiteiten (Bwke)
  - Aanvullende regels hoe te voldoen aan de Wwke
- Cyberbeveiligingswet (Cbw)
  - Nederlandse implementatie van de NIS2
  - Wetsvoorstel bij Tweede kamer voor behandeling
- Cyberbeveiligingsbesluit (Cbb)
  - Aanvullende regels hoe te voldoen aan de Cbw
- Algemene maatregelen van Bestuur

Casus Stuwdam

Casus Blankenburgverbinding

- Eise
- Daa
  - V
  - N
  - S
- Ma
- Opl
- Vas
- Bes
- Ext
- Gev

omgeving

g