Informatiebeveiliging van vitale diensten en processen

(Cyber)security als implementatie van de Europese richtlijnen NIS-2 en CER

dr. Clemens H.J. Willemsen

ISBN: 978-94-0374-258-8

Gedrukt en gepubliceerd door: Managementboek

Inhoudsopgave

1 INLEIDING 5
2 DIGITALE VEILIGHEID 6
2.1 Cyberstrategie en -beleid 7
2.2 Wet- en regelgeving 12
2.3 Organisatie van de digitale veiligheid 41
2.4 Baseline Informatiebeveiliging Overheid (BIO) 45
2.5 Voorbereiding van de implementatie 47
3 FYSIEKE VEILIGHEID 49
3.1 Wet- en regelgeving 49
3.2 Organisatie van de fysieke veiligheid 56
3.3 Achtergrond veerkracht of weerbaarheid 56
4 AFSLUITING EN SAMENHANG VAN DE RICHTLIJNEN 59
BIJLAGE 1. CONSULTATIE / TOTSTANDKOMING WETGEVING 64
BIJLAGE 2. LITERATUURLIJST 65

Lijst van figuren

Fig. 1. Wet- en regelgeving NIS 15
Fig. 2. Check op aanbieder NIS 23
Fig. 3. (internet) consultatie 37
Fig. 4. Relatie NIS, CDR en DSA 40
Fig. 5. Organisatie van autoriteiten NIS 41
Fig. 6. Organisatie van de cybersecurity NIS 43
Fig. 7. Wet- en regelgeving CER 50
Fig. 8. Organisatie van autoriteiten CER 56
Fig. 9. Risicoanalyse en weerbaarheid 58
Fig. 10. Tijdlijn van beide richtlijnen 60

Lijst van tabellen

Tab. 1. Wet- en regelgeving NIS 14
Tab. 2. Overzicht meldplicht NIS 19
Tab. 3. Regels voor online diensten 21
Tab. 4. Aanbieders van digitale diensten 28
Tab. 5. Autoriteiten en toezichthouders NIS 29
Tab. 6. Sectoren onder NIS en NIS-2 34
Tab. 7. Diensten CSIRT en SOC 44
Tab. 8. Verschillen NIS-2 en BIO 1.4 47
Tab. 9. Voorbereidende maatregelen 48
Tab. 10. Wet- en regelgeving CER 50
Tab. 11. Categorieën vitale infrastructuur 54
Tab. 12. Sectoren vitale infrastructuur 55
Tab. 13. Weerbaarheidsmatrix 58
Tab. 14. NIS-2 en CER naast elkaar 62

1 Inleiding

Dit boek beschrijft de achtergrond, totstandkoming en implementatie van richtlijnen, wetgeving, e.d. op het gebied van (cyber)security, in het bijzonder de in 2024 in werking tredende richtlijn Netwerk- en Informatiesystemen (NIS-2)[1] en blikt vooruit naar wat er nog meer verwacht kan worden. Ook is er oog voor de hiermee samenhangende fysieke beveiliging van essentiële, kritieke of vitale[2] diensten via de richtlijn Critical Entities Resilience (CER). De samenhang zie je b.v. bij een kerncentrale die beveiligd dient te worden tegen hackers doch ook tegen personen die zich onbevoegd op het terrein willen begeven of het met wapentuig willen aanvallen. Zo op het oog is er meer aandacht voor en meer beschreven over NIS-2 dan over CER. Ik probeer met name de samenhang tussen beide soorten van beveiliging te beschrijven door soortgelijke tabellen en figuren op te nemen. In het laatste hoofdstuk kijk ik naar de gezamenlijke tijdlijn en gemeenschappelijke aspecten. De titel van dit boek bevat de term informatiebeveiliging maar zoals ook in mijn eerdere boeken, gaat het ook deels in op de fysieke beveiliging. Ook wordt voor hen die werkzaam zijn bij de overheid de Baseline Informatievoorziening Overheid (BIO) benoemd waarin de NIS-2 zal worden verwerkt. De beschrijving van de BIO vind je ook op enkele plaatsen terug in mijn boek '*Organisatie van de informatiebeveiliging en vertrouwelijkheid van informatie'* maar daar is het voornamelijk beperkt tot bespreking van het onderwerp vertrouwelijkheid [Willemsen 2021, p. 23]. De NIS kan worden gerelateerd aan ISO 27001 en 27002 maar ik beperk mij tot relatering aan de BIO voor de overheid die op zijn beurt ook gerelateerd is aan de beide ISO standaarden [Willemsen 2021, p. 7]. Dit boek is in zo verre incompleet dat de beide richtlijnen in Nederland nog tot wetgeving na consultatie moeten worden geïmplementeerd nadat het boek verschenen is. Het is in het bijzonder zinvol en geschreven voor degenen die beide richtlijnen binnen hun organisatie willen verwezenlijken.

[1] In Nederland heet dit ook wel de Netwerk- en Informatiebeveiligingsrichtlijn (NIB) maar ik gebruik meestal de internationale afkorting NIS.

[2] De termen worden nog wel eens door elkaar gebruikt waarbij kritiek of vitaal vaak slaat op de infrastructuur en essentieel het belang daarvan aangeeft.

2 Digitale veiligheid

Cyber security

Er wordt veel gesproken over cyber security of cyber beveiliging zonder dat er een definitie van gegeven wordt. Er is een [Woordenboek] cybersecurity dat dit krachtig beschrijft. De verordening 2019-881 waar ik verderop meer in ga, stelt in artikel 2 lid 1: *"cyberbeveiliging: de activiteiten die nodig zijn om netwerk- en informatiesystemen[3], de gebruikers van dergelijke systemen, en andere personen die getroffen worden door cyber-dreigingen[4], te beschermen"* en "*cyberdreiging: elke potentiële omstandigheid, gebeurtenis of actie die netwerk- en informatiesystemen, de gebruikers van dergelijke systemen en andere personen kan schaden, verstoren of op andere wijze negatief kan beïnvloeden".* Zouden we met cyber niet meer of minder bedoelen dan digitaal is de vraag als we analoge systemen zoals papieren administraties achterwege laten? Een goed naslagwerk voor terminologie vind ik altijd de [NIST glossary] die cyber definieert als: "*refers to both information and communications networks*". Op zich zegt dat weinig maar [NISTIR 8074, p. 1] refereert wel naar cyberspace. Wikipedia definieert dat laatste als een digitaal verbonden of virtuele wereld. Deze term is opgekomen vanuit de science fiction en door de komst van het internet populair geworden[5].

[Azmi & Kautsarina 2019] schrijven hierover als volgt. Het Cooperative Cyber Defence Center of Excellence verzamelt meerdere definities die laten zien dat cyber kan slaan op fysieke infrastructuur, communicatie, systemen, apparaten en virtuele omgeving. De 'beste' definitie vind ik als volgt [Azmi & Kautsarina 2019, p. 15]: '*Cyber verwijst naar een samenhangend netwerk van informatie technologie en infrastructuur met inbegrip van technologische hulpmiddelen zoals het internet, telecommunicatie netwerken, computer systemen alsmede andere processoren en controllers'*. Deze definitie is op zijn beurt afkomstig van het [World Economic Forum 2012]. Cyberspace staat voor de globale (elektronische) omgeving die bestaat door samenhangende combinatie van informatiesystemen. Cyber security is het beveiligen van de cyberspace. Voor het doel van dit boek spreek ik over cyber beveiliging of digitale beveiliging.

---

[3] Ik spreek in dit boek over netwerken en informatiesystemen anders zijn de termen informatiebeveiliging en informatiesysteem wat 'overdone'.

[4] Zie meer over dreigingen in [Willemsen 2021, p. 59 e.v.].

[5] https://en.wikipedia.org/wiki/Cyberspaceyberspace

2.1 Cyberstrategie en -beleid

Cyberstrategie Europese Unie (EU)

De EU-strategie inzake cyberbeveiliging voor het digitale tijdperk is een gezamenlijke mededeling 2020-18 [Cyber strategie 2020] aan het Europees parlement en de raad. Cyberdreigingen doen zich meer en meer voor naarmate meer en meer apparaten met elkaar verbonden zijn. Daarbij is het internet gedecentraliseerd opgezet, heeft geen centrale structuur en kent een besturing door meerdere stakeholders wat het lastiger maakt om het geheel te beveiligen. Veel soorten criminaliteit hebben een digitale component in zich en de EU beschikt niet over voldoende collectieve situationele kennis over cyberdreigingen. De strategie geeft aan hoe de EU (zich) zal gaan beschermen tegen cyberdreigingen waarbij drie gebieden worden aangepakt: veerkracht[6], operationele capaciteit en het bevorderen van een mondiale open cyberspace. Dat laatste wordt ook wel gelijk gesteld met het internet. De hervormde NIS-richtlijn zal de basis vormen voor het vergroten van die veerkracht van de kritieke infrastructuur. De Commissie stelt voor om een netwerk van Security Operations Centers op te bouwen in de EU. Dit netwerk zal via een duurzame samenwerking tijdig waarschuwingen over cyberbeveiligingsincidenten uitsturen naar autoriteiten en naar alle betrokken belanghebbenden, waaronder de gezamenlijke cybereenheid. Het zal fungeren als een cyberbeveiligings-schild voor de EU. Er komt een nieuwe zorgvuldigheidsplicht voor de fabrikanten van verbonden apparaten om zwakke plekken in software aan te pakken, onder meer door software- en beveiligingsupdates te blijven aanbieden en ervoor te zorgen dat persoonsgegevens en andere gevoelige gegevens aan het einde van de levensduur van deze apparaten worden verwijderd. De Commissie zal samen met de lidstaten en de sector de toepassing versnellen van essentiële internet-standaarden en standaarden voor internetbeveiliging, en goede praktijken voor Domain name servers, routering en e-mailbeveiliging.

[6] De Engelstalige term in EU-verband is 'resilience' wat soms als 'veerkracht' en soms m.n. bij cyber als 'weerbaarheid' wordt vertaald, dus ook in dit boekwerk afhankelijk van de gebruikte bron. Zie meer in het hoofdstuk fysieke veiligheid.