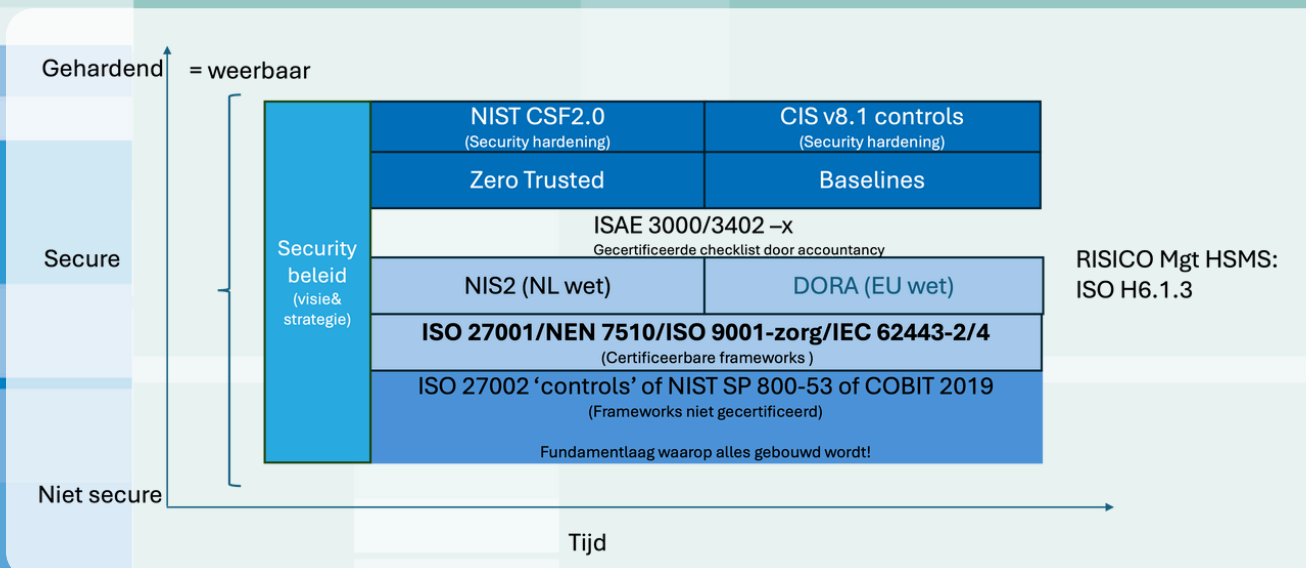
BEST PRACTICE

POSITION PAPER CYBERWEERBAARHEID

Harry van der Plas



knvi Open Standards

Colofon

Titel:	Position paper Cyberweerbaarheid
Auteur:	Harry van der Plas
Reviewers:	- dr. Barry Derksen (Director of Cyber Security/ Board member ISACA Nederland/Professor Antwerpen Management School) - Natascha van Duuren (Advocaat IT, Privacy & Cybersecurity) - Wouter Bronsgeest (duovoorzitter KNVI) - Anderen vanuit het KNVI
Redactie:	Van Haren Publishing
Publicatiedatum:	Oktober 2024

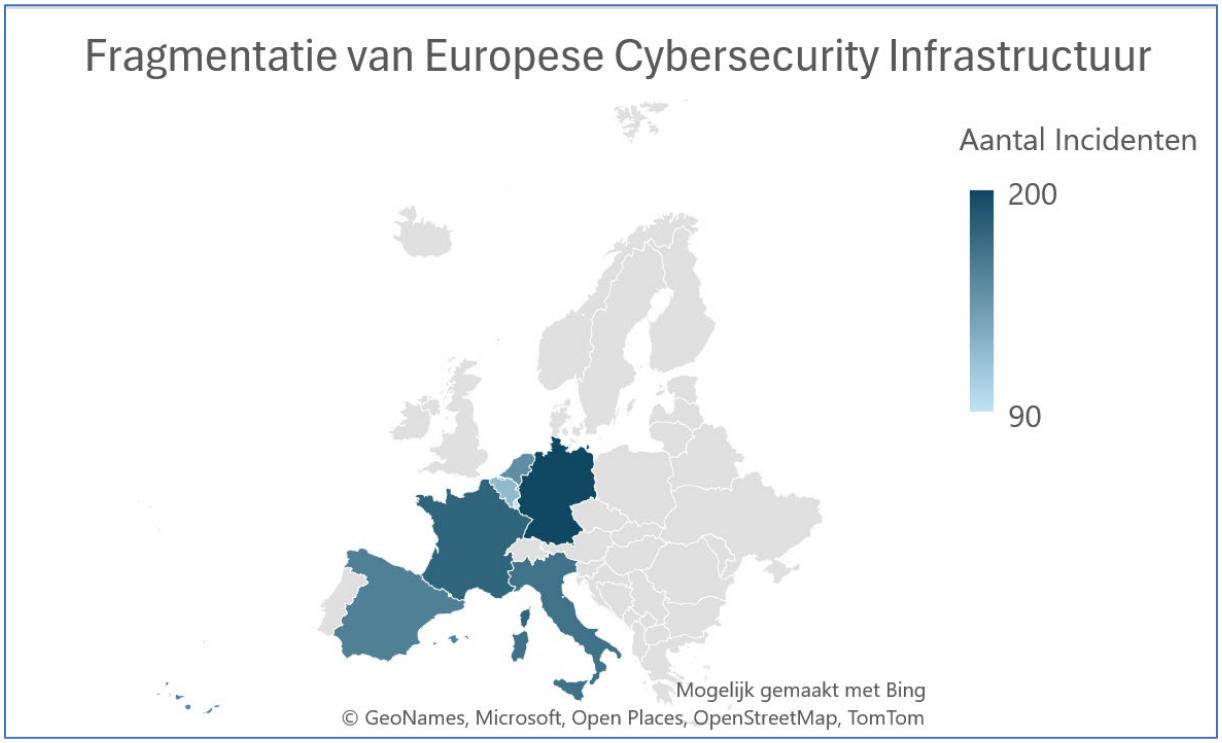
Woord vooraf

Dit paper biedt een uitgebreide momentopname van de huidige staat van cybersecurity in Europa, waarbij de belangrijkste bedreigingen en uitdagingen zijn onderzocht. De nadruk ligt op versterkte digitale weerbaarheid en samenwerking tussen lidstaten.

Versterking van cyberweerbaarheid in Europa

In de huidige digitale wereld, waarin cyberdreigingen voortdurend evolueren en toenemen, is het waarborgen van de cyberweerbaarheid van cruciaal belang voor de veiligheid en stabiliteit van onze samenleving, waarbij tevens de samenwerking tussen publieke en private sectoren essentieel is. Dit paper biedt een gedetailleerde analyse van de huidige staat van cybersecurity in Europa en identificeert de belangrijkste uitdagingen en risico's. Daarnaast presenteren we concrete aanbevelingen om de weerbaarheid tegen cyberaanvallen te versterken.

De fragmentatie van de Europese cybersecurity-infrastructuur en het tekort aan gekwalificeerde professionals zijn twee van de grootste uitdagingen die we vandaag de dag ondervinden. Tegelijkertijd worden cyberdreigingen steeds geavanceerder, wat een dringende noodzaak creëert voor een gecoördineerde en effectieve aanpak.



In dit document wordt het belang van sterk leiderschap en de betrokkenheid van het topmanagement benadrukt, evenals de noodzaak voor voldoende middelen en training om een cultuur van veiligheid binnen organisaties te bevorderen. We bespreken de implementatie van controlemaatregelen en incidentmanagement volgens internationale normen zoals ISO 27001:2022 en de wettelijke BIO2/NEN7510:2024-richtlijnen (gebaseerd op ISO27001:2022), en leggen uit hoe technologieën zoals SOC, SIEM en SOAR kunnen bijdragen aan proactieve cyberbeveiliging.

In de rol van (v)CISO is het cruciaal om gebruik te maken van geavanceerde tools en technologieën zoals Security Information and Event Management (SIEM), Security Operations Center (SOC), en Security Orchestration, Automation and Response (SOAR). Deze tools helpen bij het real-time monitoren, analyseren en reageren op beveiligingsincidenten. Daarnaast zijn frameworks zoals ISO 27001, NIST 800-53 of Cyber Security Framework 2.0 of CIS v8.1 Controls onmisbaar voor het opzetten van een robuust Information Security Management System (ISMS).

Dit paper biedt praktische richtlijnen en strategieën voor organisaties om hun cyberweerbaarheid te verbeteren, met speciale aandacht voor de implementatie van de NIS2-richtlijn. We hopen dat deze inzichten en aanbevelingen bijdragen aan een veiliger en veerkrachtiger digitaal Europa.

Wij danken alle betrokken partijen en reviewers voor hun waardevolle bijdragen aan dit paper en kijken uit naar een toekomst waarin we gezamenlijk de uitdagingen van cybersecurity kunnen aangaan.

Doelgroepen en toepassing van het paper

In dit paper zijn de aanbevelingen en analyses afgestemd op verschillende doelgroepen. Hieronder volgt een overzicht van hoe de inhoud specifiek relevant is voor de hierna benoemde doelgroepen:

Beleidsmakers en regulerende instanties:

- **Focus:** Harmonisatie van regelgeving.
- **Doel:** Verbetering van richtlijnen en wetgeving, zoals de implementatie van de NIS2-richtlijn en de ontwikkeling van regelgeving voor niet-vitale bedrijven.

Bedrijven en instellingen (publiek en privaat):

- **Focus:** Versterking van interne cyberbeveiligingspraktijken.
- **Doel:** Inclusief risicobeheer, incidentbeheer, en leveranciersbeoordeling om de algehele cyberweerbaarheid te verbeteren.

Cybersecurityprofessionals en IT-afdelingen:

- **Focus:** Technische en operationele richtlijnen.
- **Doel:** Aanbieden van concrete stappen en best practices voor het versterken van de cyberweerbaarheid binnen hun organisaties.

De inhoud van het paper is met name van toepassing om de volgende doelen te realiseren:

1. **Verbeterde interoperabiliteit:** Door te kiezen voor open standaarden, kunnen professionals zorgen voor betere samenwerking tussen verschillende systemen en organisaties, wat essentieel is in een gedigitaliseerde en verbonden wereld.
2. **Verhoogde transparantie en toegankelijkheid:** Open standaarden maken specificaties en richtlijnen breed beschikbaar, wat niet alleen de naleving van wetgeving vergemakkelijkt, maar ook bijdraagt aan een transparanter en toegankelijker cybersecuritybeleid.
3. **Voorkoming van vendor lock-in:** Door te werken met open standaarden kunnen organisaties onafhankelijk blijven van specifieke leveranciers en hun flexibiliteit vergroten. Binnen de KNVI is er een ‘interessegroep Open Standaarden’ bezig om deze in kaart te brengen en te rubriceren op basis van een 9-vlaksmodel.
4. **Strategische integratie met wetgeving:** professionals moeten ervoor zorgen dat de implementatie van open standaarden in lijn is met de Europese en nationale regelgeving, zoals de NIS2-richtlijn en de nieuwe

AI-wetgeving. Dit helpt om niet alleen compliant te zijn, maar ook om proactief risico's te beheren en de organisatie te beschermen tegen toekomstige dreigingen.

Conclusie: Door de filosofie van open standaarden te omarmen, kunnen (IT-) professionals dus bijdragen aan de ontwikkeling van een robuuste en flexibele cyberweerbaarheid die bestand is tegen de uitdagingen van vandaag en de toekomst. Het strategisch inzetten van open standaarden zal niet alleen de operationele efficiëntie verbeteren, maar ook de naleving van wetgeving vergemakkelijken en de weg vrijmaken voor innovatieve en duurzame digitale ecosystemen.

Definities van belangrijke begrippen

Begrip	***Definitie***	***Bron/Framework***
Cyberweerbaarheid	Het vermogen van een organisatie om zich voor te bereiden op, te reageren op en zich te herstellen van cyberaanvallen en andere digitale bedreigingen.	ISO 27001, NIST 800-53
Interoperabiliteit	Het vermogen van verschillende systemen en organisaties om effectief samen te werken door middel van gedeelde standaarden en protocollen.	ISO 27001, NIST 800-53
Open standaarden	Publiek toegankelijke en vrij te gebruiken standaarden die interoperabiliteit, transparantie en toegankelijkheid bevorderen.	ISO 27001, NIST 800-53
NIS2-richtlijn	Europese wetgeving gericht op het verbeteren van de beveiliging van netwerk- en informatiesystemen binnen de lidstaten.	NIS2, Wetsvoorstel Cyberbeveiligingswet
Security Operations Center (SOC)	Een centrale eenheid binnen een organisatie die verantwoordelijk is voor continu toezicht, monitoring en verbetering van de cyberveiligheid.	ISO 27001, NIST 800-53
Security Information and Event Management (SIEM)	Technologie die beveiligingsgegevens verzamelt, correleert en analyseert in real-time om cyberdreigingen te detecteren en hierop te reageren.	ISO 27001, SOC frameworks
Security Orchestration, Automation and Response (SOAR)	Technologie die beveiligingsprocessen automatiseert en incidentrespons coördineert om de efficiëntie van beveiligingsteams te verhogen.	ISO 27001, NIST 800-53
Quantum computing	Een technologie die kwantummechanica gebruikt om berekeningen uit te voeren die sneller kunnen zijn dan traditionele computers.	Wetenschappelijke literatuur, emerging tech frameworks
Artificial Intelligence (AI)	Technologie die machines in staat stelt om taken uit te voeren die normaal menselijke intelligentie vereisen, zoals leren, redeneren en probleemoplossing.	ISO 27001, AI security guidelines

Inleiding

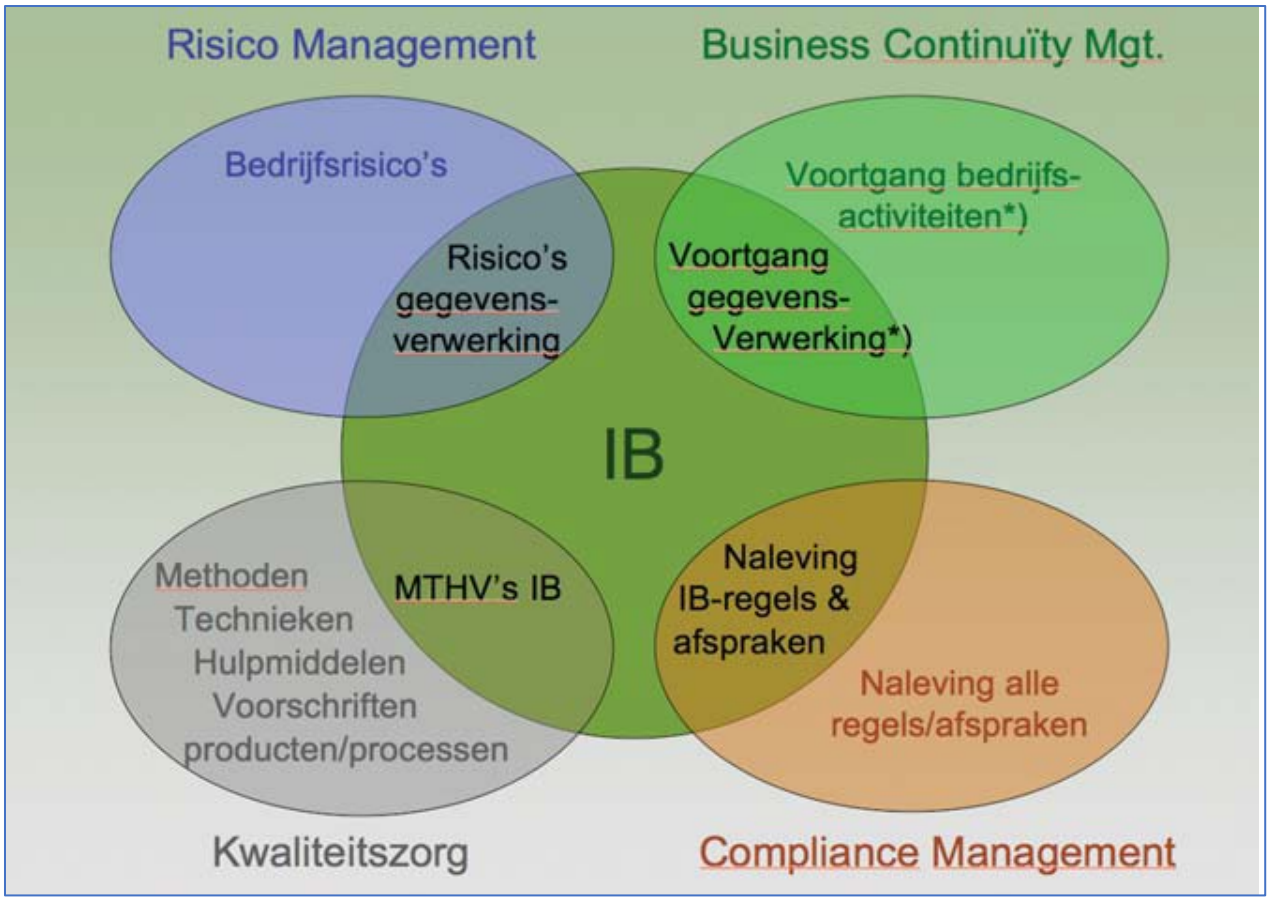
In de snel evoluerende digitale wereld van vandaag is cyberweerbaarheid een essentieel aspect van de veiligheid en stabiliteit van onze samenleving. Cyberaanvallen worden steeds geavanceerder en doen zich steeds frequenter voor, wat een serieuze bedreiging vormt voor zowel publieke als private sectoren. Dit paper is opgesteld om de huidige stand van cybersecurity in Europa te inventariseren en te analyseren, de belangrijkste uitdagingen te identificeren en concrete aanbevelingen te doen om de cyberweerbaarheid te verbeteren.

Er is getracht dit paper op te zetten volgens de Harmonized Structured Management System (HSMS)-structuur conform de ISO-richtlijn Annex SL uit 2022. Dit is de als opvolger van de high level structure, de manier langs welke opzet elke nieuwe ISO-norm wordt gestructureerd. De auteur past dit ook toe in Baselines die hij gemaakt heeft voor Life Cycle Management (LCM) en Role Based Access Controll (RBAC) als fundamenteel onderdeel van de ISO 27001 Annex A bewijslast documenten binnen de te nemen maatregelen.

De opzet conform de HSMS-opzet van dit paper is als volgt:

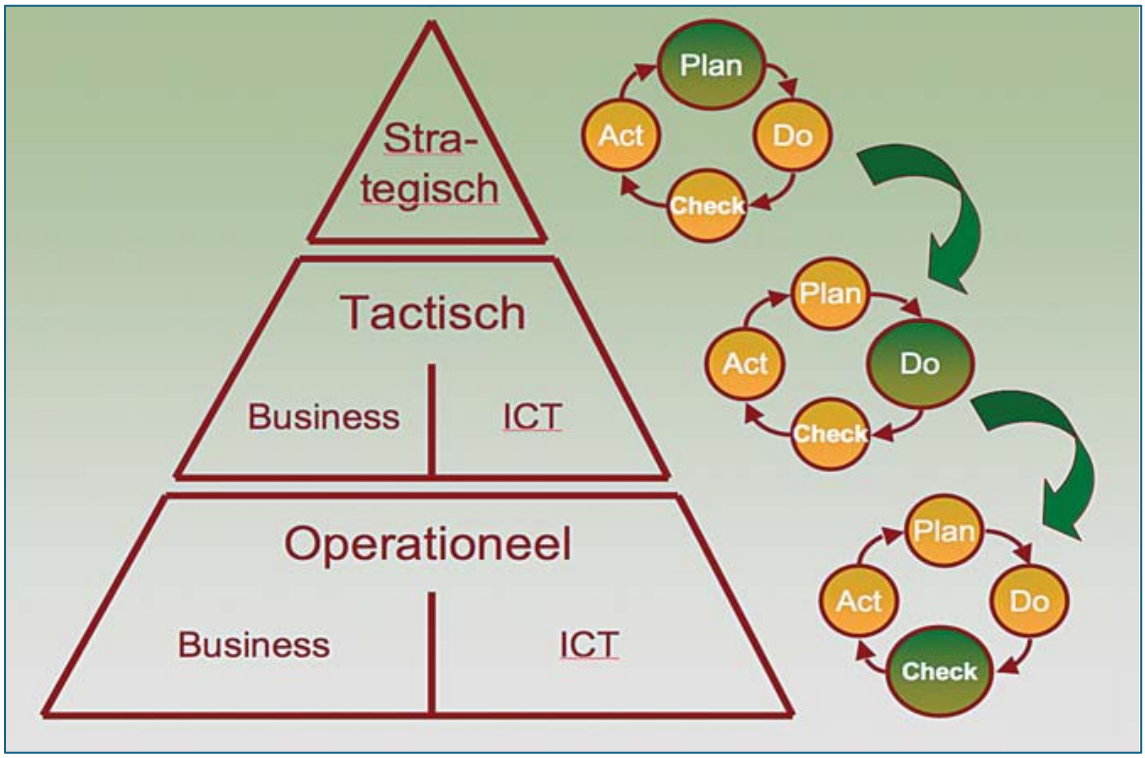
1. **Context van de organisatie**: Analyse van de huidige cybersecuritysituatie in Europa, inclusief uitdagingen zoals gefragmenteerde infrastructuur, complexiteit van dreigingen en tekort aan talent.
2. **Leiderschap**: Het belang van een sterke beleidsverklaring, duidelijke verantwoordelijkheden en betrokkenheid van het topmanagement.
3. **Planning**: Methodes voor risicobeoordeling en -beheer, inclusief het stellen van SMART-doelen voor IT en OT.
4. **Ondersteuning**: Beschikbare middelen, training en bewustwordingsprogramma’s, alsmede communicatieplannen op het gebied van cybersecurity
5. **Operationele planning en beheersing**: Implementatie van controlemaatregelen en incidentmanagement.
6. **Prestatie-evaluatie**: Monitoring, interne audits en managementbeoordelingen.
7. **Verbetering**: Corrigerende maatregelen en aanpak voor voortdurende verbetering van het managementsysteem.
8. **Kritieke infrastructuur en cyberweerbaarheid**: Specifieke uitdagingen en maatregelen voor kritieke sectoren zoals energie, telecommunicatie, datacenters en transport.
9. **Ketencyberweerbaarheid van leveranciers**: Evaluatie en beoordeling van de cyberveiligheidspraktijken van leveranciers.
10. **Conclusie**: Samenvatting van de bevindingen en toekomstvisie op de ontwikkeling van cyberweerbaarheid in Europa.

In deze paper is gebruikgemaakt van deze methodiek, een gesystematiseerde en gestandaardiseerde aanpak, om zo te komen tot een consistente en geïntegreerde wijze van risicobeheer en naleving van regelgeving en/of toepassing van maatregelen te bevorderen.



Bron: *Functies-in-de-informatiebeveiliging-nl* van 2017

1. Context van de organisatie

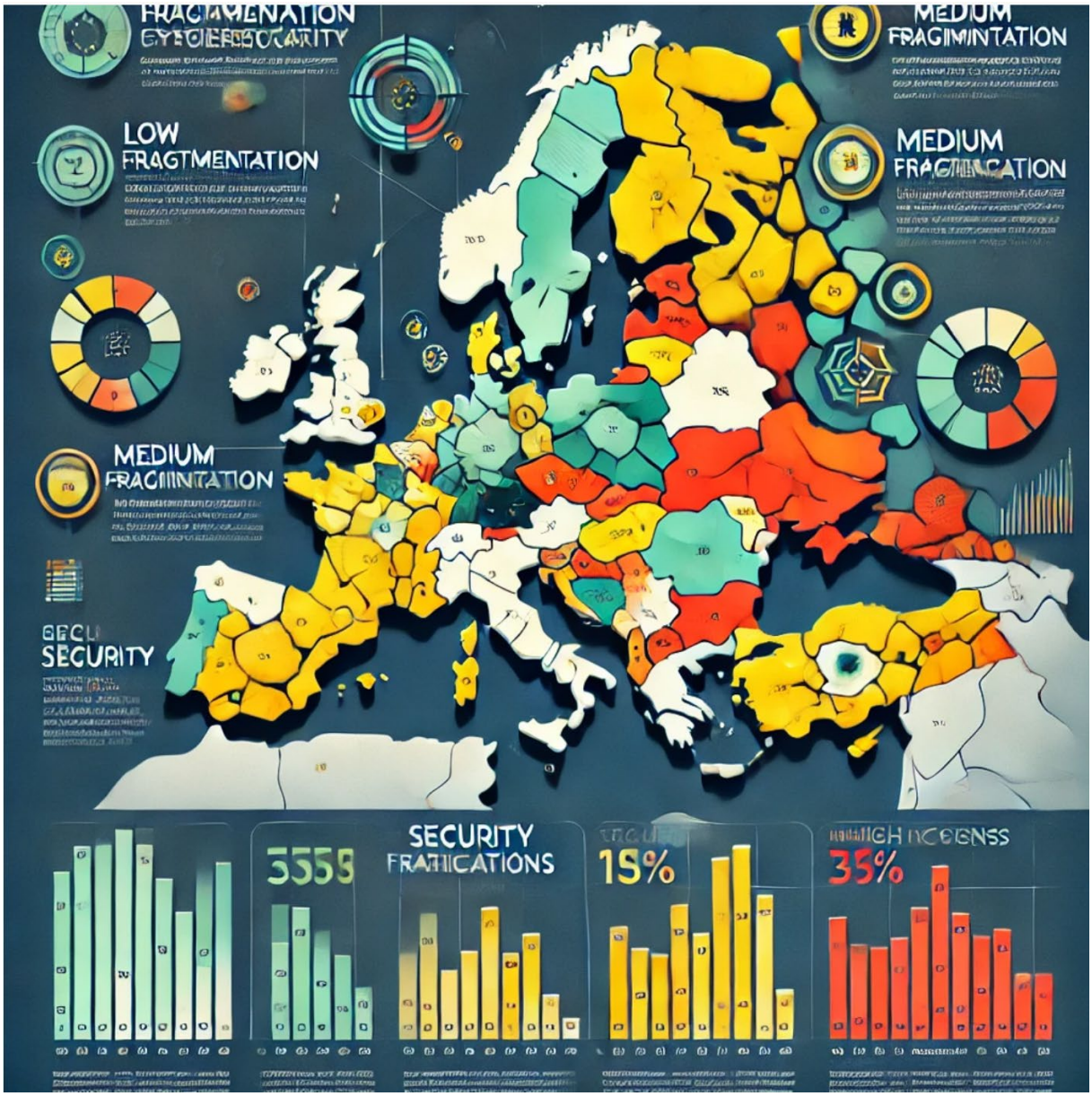


Velen zullen het erover eens zijn: Anno 2024 is de cybersecurity-infrastructuur in Europa gefragmenteerd, met uiteenlopende niveaus van volwassenheid en capaciteit tussen de lidstaten. Deze fragmentatie belemmert een uniforme reactie op cyberdreigingen en bemoeilijkt grensoverschrijdende samenwerking.. Daarnaast worden cyberdreigingen steeds complexer, met telkens geavanceerdere technieken zoals ransomware en phishing. Een ander groot probleem is het tekort aan gekwalificeerde cybersecurityprofessionals, wat de capaciteit van organisaties om zich adequaat te beschermen, vermindert.

In elk aspect van de informatiebeveiligingscyclus, van risicobeoordeling tot incidentbeheer, is de samenwerking tussen publieke en private sectoren van cruciaal belang. Deze samenwerking bevordert de uitwisseling van informatie, versterkt de responsmogelijkheden en zorgt voor een alomvattende beveiligingsstrategie die bestand is tegen de steeds complexere dreigingen in de digitale wereld. Dit uitgangspunt dient als een rode draad door alle fasen van de informatiebeveiligingscyclus en dus hoort overal in dit paper in het achterhoofd gehouden te worden.

1.1 Bestrijding van cyberaanvallen

Voorbeeld van wat goed ging: In 2022 heeft Estland, een koploper op het gebied van digitale transformatie, succesvol een grootschalige DDoS-aanval afgeslagen door gebruik te maken van een geavanceerde combinatie van AI-gestuurde detectie en responsmechanismen. Deze aanpak resulteerde in minimale verstoring van diensten en werd een best practice binnen de EU.



Deze tekst is gecreëerd door Dalle-e op basis van de volgende bronnen:

- Bron 1: European Cybersecurity Agency (ECA), Rapport over Europese cybersecurity-infrastructuur, 2023
- Bron 2: Nationaal Cyber Security Centrum (NCSC), Jaarverslag 2023

Uitleg

De hierboven geplaatste visual maakt het makkelijker om de huidige staat van cybersecurity in Europa te begrijpen, met kleur-gecodeerde secties die verschillende niveaus van fragmentatie aangeven (groen voor laag, geel voor middel, en rood voor hoog) en bar charts die het aantal beveiligingsincidenten in verschillende landen weergeven. Deze infographic helpt bij het begrijpen van de diverse uitdagingen die Europese landen tegenkomen op het gebied van cybersecurity.

Voorbeeld van wat niet goed ging: Een groot Europees bedrijf leed in 2023 aanzienlijke verliezen na een ransomware-aanval. Ondanks waarschuwingen en beschikbaar gestelde middelen, had de organisatie nagelaten een robuuste back-upstrategie en training voor medewerkers te implementeren, wat leidde tot een trage response en lange herstelperiode.

1.2 Samenwerkingsinitiatieven en betrokken organisaties

Sinds de implementatie van de NIS2-richtlijn hebben verschillende Europese landen initiatieven genomen om de samenwerking op het gebied van cybersecurity te verbeteren.

Bijvoorbeeld, de EU heeft het European Cybersecurity Competence Centre (ECCC) opgericht om de ontwikkeling van technologieën en industriële capaciteiten in cybersecurity te bevorderen.

Daarnaast spelen nationale instanties zoals het National Cyber Security Centre (NCSC) in Nederland en het Bundesamt für Sicherheit in der Informationstechnik (BSI) in Duitsland een cruciale rol in het faciliteren van samenwerking en informatie-uitwisseling tussen overheden en private sectoren.

1.3 Specifieke cybersecurity-initiatieven en richtlijnen

Europese Initiatieven

Harmonisatie van regelgeving: De EU werkt aan het verder harmoniseren van cybersecurityregels tussen lidstaten om een uniform niveau van beveiliging te garanderen en grensoverschrijdende samenwerking te vergemakkelijken.
Opleidingsprogramma's: Er wordt geïnvesteerd in Europese opleidingsprogramma's voor cybersecurityprofessionals om het tekort aan gekwalificeerd personeel aan te pakken.

Bron:

- *ENISA - Cybersecurity Skills*
- *EU Cybersecurity Strategy*
- *ECCC Official Website*
- *Digital Europe Programme*

Zoals:

NIS2 (Network and Information Systems Directive):

De NIS2-richtlijn (Network and Information Systems Directive) is een Europese Richtlijn die is gericht op het verbeteren van de beveiliging van netwerk- en informatiesystemen binnen de lidstaten van de Europese Unie. Deze richtlijn is een uitbreiding van de oorspronkelijke NIS1-richtlijn en legt strengere eisen op aan zowel publieke als private organisaties die als zeer kritiek of kritiek worden beschouwd voor de economie en samenleving, zoals in de sectoren energie, transport, gezondheid en digitale infrastructuur.

Het doel van NIS2 is om een uniform niveau van cyberbeveiliging in de hele EU te garanderen, door organisaties te verplichten om passende technische en organisatorische maatregelen te nemen om cyberincidenten te voorkomen en aan te pakken. De belangrijkste vereisten van NIS2 zijn:

- **Risicomanagement**: Organisaties moeten een risico-gebaseerde aanpak hanteren voor informatiebeveiliging en incidentbeheer.
- **Incidentrapportage**: Organisaties zijn verplicht om ernstige incidenten binnen 24 uur na ontdekking te melden bij de bevoegde nationale autoriteit.
- **Beveiligingsmaatregelen**: De richtlijn vereist de implementatie van maatregelen die de integriteit, vertrouwelijkheid en beschikbaarheid van netwerk- en informatiesystemen waarborgen.
- **Compliance en sancties**: Niet-naleving van NIS2 kan leiden tot strenge boetes en andere sancties, afhankelijk van de ernst van de overtreding.

De richtlijn legt ook de basis voor een betere samenwerking tussen lidstaten, met als doel grensoverschrijdende cyberdreigingen effectiever aan te pakken.

DORA (Digital Operational Resilience Act):

De **Digital Operational Resilience Act (DORA)** is Europese Verordening die specifiek gericht is op het versterken van de digitale weerbaarheid binnen de financiële sector. DORA zorgt ervoor dat financiële instellingen, zoals banken, verzekeraars en beleggingsbedrijven, beter beschermd zijn tegen digitale dreigingen en dat zij in staat zijn om snel en effectief te reageren op cyberincidenten. Deze wetgeving is een aanvulling op bestaande Europese richtlijnen, zoals de NIS2-richtlijn, maar richt zich specifiek op de unieke uitdagingen in de financiële sector (het is een ‘lex specialis’ bij de NIS2).

De belangrijkste focus van DORA ligt op:

- **Operationele continuïteit**: Financiële instellingen moeten ervoor zorgen dat hun IT-systemen en processen bestand zijn tegen verstoringen. Dit omvat robuuste back-upsystemen, herstelplannen en continue monitoring van kritieke systemen.

- **Risicobeheer van derde partijen**: DORA verplicht financiële instellingen om de digitale weerbaarheid van hun externe leveranciers, zoals cloud providers en IT-dienstverleners, te evalueren en te beheren. Dit voorkomt dat kwetsbaarheden in de toeleveringsketen leiden tot grote verstoringen.
- **Incidentrapportage en testvereisten**: Financiële instellingen moeten cyberincidenten melden en regelmatig hun systemen testen op kwetsbaarheden, om de weerbaarheid tegen cyberdreigingen te verbeteren.

Aanvulling op NIS2: DORA gaat specifiek in op de financiële sector. DORA zorgt voor strengere eisen op het gebied van risico's in toeleveringsketens en verplicht tot uitgebreide testen en incidentrapportages binnen deze sector. Waar NIS2 algemene richtlijnen biedt voor netwerk- en informatiesystemen, biedt DORA gedetailleerde voorschriften die specifiek zijn afgestemd op de financiële infrastructuur, waardoor deze richtlijnen elkaar aanvullen en versterken.

EU Verordening Cyberweerbaarheid:

De **EU Verordening Cyberweerbaarheid** is een belangrijke Europese Verordening die is ingevoerd om de cyberweerbaarheid binnen de Europese Unie te versterken. Deze verordening heeft twee belangrijke doelen: het versterken van het mandaat van ENISA (het Europese agentschap voor cyberbeveiliging) en het opzetten van een EU-breed certificeringskader voor ICT-producten, diensten en processen. De EU Verordening Cyberweerbaarheid is bedoeld om de algehele cyberbeveiligingsstandaarden in Europa te verhogen en een meer uniforme benadering van cyberveiligheid te bevorderen.

De belangrijkste onderdelen van de **EU Verordening Cyberweerbaarheid** zijn:

- **Versterking van ENISA**: De Verordening Cyberweerbaarheid geeft ENISA een permanente rol en een sterker mandaat om lidstaten te ondersteunen bij het voorkomen, detecteren en reageren op cyberdreigingen. ENISA fungeert nu als de coördinerende instantie voor cyberbeveiliging op EU-niveau en biedt expertise en advies.
- **Cybersecuritycertificering**: De wetgeving introduceert een uniform certificeringskader voor ICT-producten, diensten en processen in de hele EU. Deze certificeringen zijn bedoeld om het vertrouwen te vergroten in de veiligheid van digitale producten en diensten die binnen de EU worden gebruikt. Bedrijven kunnen door deze certificeringen aantonen dat hun producten voldoen aan strenge cyberbeveiligingseisen.

Aanvulling op NIS2: Terwijl de NIS2-richtlijn zich richt op het versterken van de weerbaarheid van essentiële sectoren door middel van risicobeheer en incidentrapportage, biedt de EU Verordening Cyberweerbaarheid een aanvulling door een certificeringssysteem te introduceren dat de veiligheid van producten en diensten garandeert. Dit helpt om een hoger niveau van cyberbeveiliging te waarborgen binnen de hele digitale infrastructuur van de EU. Samen zorgen NIS2 en de Verordening Cyberweerbaarheid voor een holistische benadering van cyberveiligheid, waarbij zowel de veiligheid van kritieke infrastructuren als de betrouwbaarheid van digitale producten centraal staat.

Initiatieven in de VS, CISA, NIST en CIS

CISA's Cybersecurity Framework

De **Cybersecurity and Infrastructure Security Agency (CISA)**, een Amerikaanse overheidsinstantie, heeft een framework ontwikkeld dat als leidraad dient voor organisaties om hun cyberweerbaarheid te versterken. Dit framework is ontworpen om een risico-gebaseerde benadering van cybersecurity te ondersteunen, waarbij organisaties worden geholpen om bedreigingen te identificeren, te beschermen tegen cyberincidenten, snel te reageren op incidenten en zich te herstellen na aanvallen.

Het CISA Cybersecurity Framework bestaat uit vijf kernfuncties:

1. **Identificeren**: Het in kaart brengen van kritieke activa, gegevens en systemen binnen de organisatie om potentiële risico's te begrijpen.
2. **Beschermen**: Het implementeren van maatregelen zoals toegangscontrole, gegevensbeveiliging en training om de kans op een cyberaanval te verminderen.
3. **Detecteren**: Het tijdig opsporen van cyberdreigingen en afwijkende activiteiten in de systemen.
4. **Reageren**: Het ontwikkelen van responsplannen om adequaat op cyberincidenten te kunnen reageren.
5. **Herstellen**: Het vermogen om snel te herstellen van cyberaanvallen en de normale bedrijfsvoering te hervatten.

Model voor Europese bedrijven: Europese bedrijven kunnen dit framework gebruiken als model voor hun eigen cybersecuritymaatregelen door de gestructureerde aanpak en de nadruk op risicomanagement. Het biedt een flexibele en schaalbare manier om cyberdreigingen te beheren, wat ook toepasbaar is binnen de Europese context.

NIST Frameworks (zoals NIST SP 800-53)

Het **NIST Cybersecurity Framework**, ontwikkeld door het National Institute of Standards and Technology (NIST), biedt uitgebreide richtlijnen voor het verbeteren van de cyberveiligheid binnen organisaties. Vooral het **NIST SP 800-53** framework is een belangrijke referentie voor Amerikaanse organisaties om hun informatiesystemen en netwerken te beveiligen.

Dit framework richt zich op:

- **Risicobeheer**: Het beoordelen van risico's en het implementeren van beheersmaatregelen om die risico's te beperken.
- **Beveiligingscontroles**: Er worden specifieke beveiligingscontroles beschreven, zoals het beveiligen van gegevens en systemen, het beheren van toegang en het ontwikkelen van herstelplannen.
- **Compliance**: Het NIST framework helpt organisaties om te voldoen aan wettelijke eisen, vooral op het gebied van privacy en informatiebeveiliging.

Het **NIST SP 800-53** framework wordt breed toegepast in de VS, en Europese organisaties kunnen hiervan profiteren door de best practices over te nemen, vooral als ze werken met Amerikaanse partners of binnen sterk gereguleerde sectoren zoals financiën of gezondheidszorg.

CIS Controls

De **Center for Internet Security (CIS) Controls** zijn een set van best practices voor cybersecurity die wereldwijd worden toegepast om cyberdreigingen te verminderen. CIS biedt een overzichtelijke lijst van 18 kritieke beveiligingsmaatregelen die organisaties helpen om hun systemen te beschermen tegen de meest voorkomende cyberdreigingen. Deze maatregelen zijn praktisch en worden regelmatig bijgewerkt op basis van de laatste ontwikkelingen in cyberbeveiliging.

De CIS Controls zijn ontworpen om te worden toegepast door organisaties van verschillende groottes en uit diverse sectoren, en richten zich op de volgende punten:

- **Inventory and Control of Hardware Assets**: Het nauwkeurig bijhouden van alle hardware die toegang heeft tot de netwerken.
- **Continuous Vulnerability Management**: Het doorlopend identificeren en verhelpen van kwetsbaarheden in systemen en netwerken.
- **Security Awareness and Training**: Het bewustmaken van medewerkers en hen trainen in het herkennen van en reageren op cyberdreigingen.

Aanvulling op NIST en CISA: Hoewel CIS Controls complementair zijn aan frameworks zoals NIST en CISA, is het bijzonder toegankelijk voor organisaties die behoefte hebben aan praktische, onmiddellijk toepasbare maatregelen. CIS is daarnaast minder complex dan sommige andere frameworks en biedt een schaalbare oplossing voor zowel kleine als grote organisaties.

Platforms en artikelen

ENISA's jaarlijkse rapporten: Deze rapporten bieden diepgaande analyses van de huidige staat van cybersecurity in Europa en zijn een waardevolle bron voor best practices en opkomende dreigingen.

UpGuard Blog: Actuele artikelen en analyses over de impact van nieuwe regelgeving en technologieën op het gebied van cybersecurity.

1.4 Slotbeschouwing

De gefragmenteerde aard van de Europese cybersecurity-infrastructuur en de complexiteit van dreigingen vormen aanzienlijke uitdagingen voor organisaties. Ondanks deze uitdagingen bieden best practices en samenwerkingsinitiatieven, zoals beschreven in recente ENISA-rapporten, waardevolle inzichten. Organisaties kunnen deze inzichten benutten om hun eigen cyberbeveiligingsstrategieën te versterken en beter voorbereid te zijn op toekomstige dreigingen.

Een voorbeeld hiervan is te vinden in het rapport van de European Cybersecurity Agency (ENISA) uit 2023, waarin succesvolle samenwerking tussen Europese lidstaten werd gedocumenteerd. Deze samenwerking heeft geleid tot verbeterde harmonisatie van cybersecuritybeleid en effectievere grensoverschrijdende respons op dreigingen. Organisaties kunnen lering trekken uit deze voorbeelden door de aanbevelingen toe te passen op hun eigen cyberbeveiligingsstrategieën.

2. Leiderschap

2.1 Beleidsverklaring en verantwoordelijkheden

Een effectieve informatiebeveiligingsstrategie is essentieel, met duidelijke rollen en verantwoordelijkheden binnen de organisatie. Het topmanagement moet actief betrokken zijn bij het goedkeuren en superviseren van cybersecuritymaatregelen.

Specifiek voor de Nederlandse overheden

BIO (Baseline Informatiebeveiliging Overheden): Deze richtlijn is ontwikkeld voor de Nederlandse overheid en is afgeleid van de ISO 27001, met specifieke aandacht voor de Nederlandse wetgeving en context. BIO is het basisnormenkader voor informatiebeveiliging van de Rijksoverheid, wat betekent dat het sterk leunt op de principes van ISO 27001.

De BIO2-versie kan meer details geven voor specifieke sectoren zoals gemeenten, waterschappen, en provincies. De verwachting is dat deze nieuwe versie van de Baseline Informatiebeveiliging Overheid (BIO) tegen het einde van 2024 formeel wordt ingevoerd. De BIO2.0 zal via de implementatie van de NIS2-richtlijn worden verankerd in de Nederlandse wetgeving, specifiek in de Wet beveiliging netwerk- en informatiesystemen (Wbni). Dit betekent dat overheidsinstellingen die onder de NIS2 vallen verplicht zullen zijn om aan deze richtlijnen te voldoen, waardoor de BIO2.0 op termijn bindend zal worden.

ISO 27001:2022: Dit is de internationale norm voor informatiebeveiliging, en de nieuwe versie (2022) richt zich nog sterker op risicobeheer en de beveiliging van informatie in een organisatie. Deze norm vormt de basis voor andere frameworks zoals de NEN7510 voor de zorgsector, wat in Nederland cruciaal is voor compliance met nationale wetgeving.

NEN 7510: Specifiek voor de zorg in Nederland, deze norm is afgeleid van ISO 27001 en focust op de bescherming van patiëntgegevens. Dit geeft aan hoe sector-specifieke aanpassingen aan de ISO 27001 worden gemaakt om te voldoen aan nationale regelgeving. De integratie van ISO 27001:2022 met de Nederlandse BIO-richtlijnen biedt een holistisch framework voor overheidsinstellingen om hun informatiebeveiliging te beheren volgens zowel internationale als nationale eisen, zoals beschreven in de BIO en gebaseerd op de internationale standaard ISO 27001. De nieuwe versie van de NEN7510 komt eind 2024 of begin 2025, maar is momenteel (september 2024) in consultatie in de Nederlandse zorgmarkt.

2.2 Aanhaken op kennisgebieden die aandacht besteden aan leiderschap

Leiderschap in cybersecurity vereist kennis van projectmanagement en organisatiekunde. Het boek *CIO 3.0 - Leiden met digitale transformatie* van Karin Zwiggelaar en Antoon van Luxemburg benadrukt de veranderende rol van de CIO

in de digitale transformatie. Hedendaagse CIO's moeten niet alleen IT-experts zijn, maar ook changemanagers die de digitale strategie van de organisatie kunnen vormgeven en implementeren. Agile werkwijzen zijn hierbij essentieel, omdat ze flexibiliteit en snelle aanpassing aan veranderingen in de dreigingsomgeving mogelijk maken. In par. 2.3 wordt verder ingegaan op veranderende rol van de CIO bij digitale transformatie.

2.3 Veranderende rol van de CIO bij digitale transformatie

De CIO van vandaag, vaak aangeduid als CIO 3.0, speelt een cruciale rol in de herdefinitie van de bedrijfsstrategie door middel van technologie. Hierbij is het belangrijk dat de CIO fungeert als coach voor het senior management en als changemanager die nieuwe digitale kansen exploiteert en agile methodieken binnen de organisatie implementeert. Dit zorgt voor een naadloze integratie van technologie in alle bedrijfsprocessen, wat essentieel is voor succes in de digitale economie.

De rol van de Chief Information Officer (CIO) is de afgelopen jaren sterk veranderd door de toenemende snelheid van digitale transformatie binnen organisaties. Waar de CIO traditioneel verantwoordelijk was voor IT-beheer en infrastructuur, is deze functie nu veel meer gericht op strategische besluitvorming en organisatieverandering. De moderne CIO fungeert als een changemanager, waarbij technologie niet alleen wordt ingezet om operationele efficiëntie te verbeteren, maar ook om nieuwe kansen voor groei en innovatie te creëren.

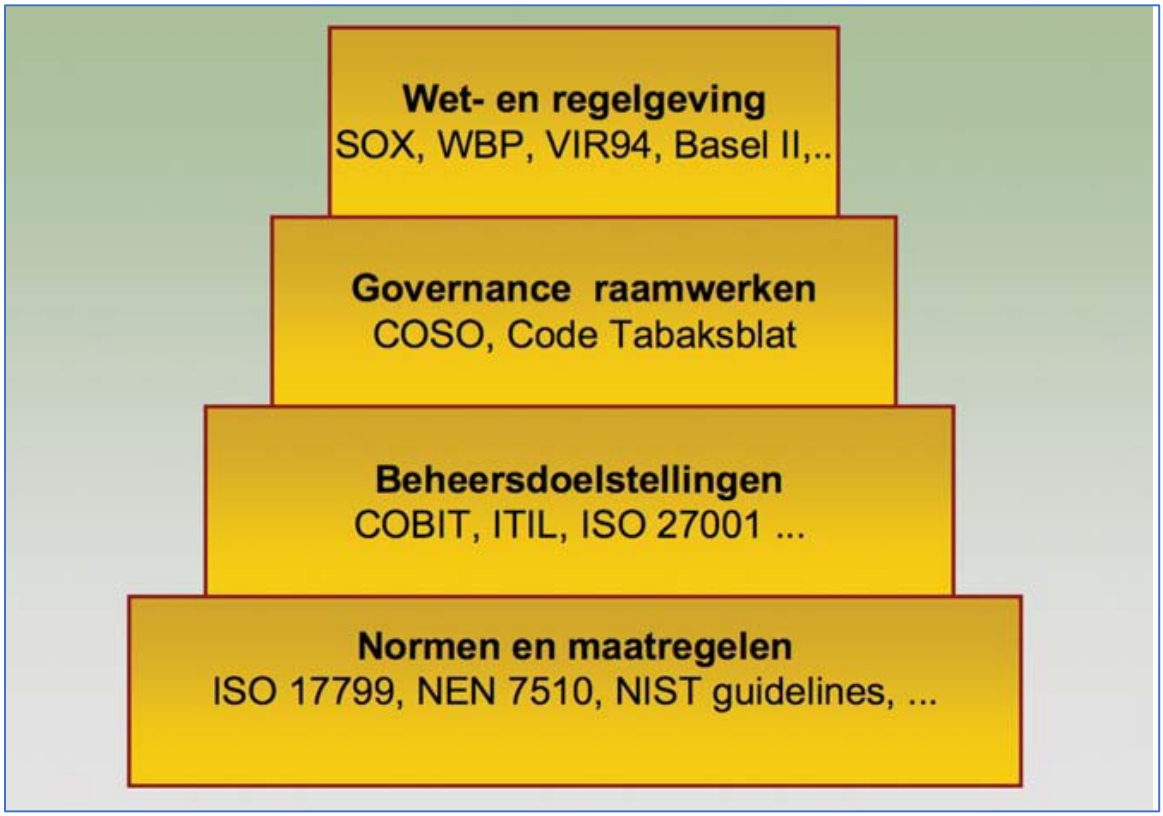
In de huidige digitale economie wordt van de CIO verwacht dat hij of zij een leidende rol speelt in het vormgeven van de digitale strategie van de organisatie. Dit houdt in dat de CIO nauw samenwerkt met andere leden van het topmanagement om technologie te integreren in alle aspecten van de bedrijfsvoering. Een belangrijke verschuiving is dat de CIO niet alleen verantwoordelijk is voor IT-systemen, maar ook voor het ondersteunen van veranderprocessen binnen de organisatie, zoals het implementeren van agile werkwijzen en het bevorderen van een cultuur die flexibel kan inspelen op veranderingen in de markt en technologische innovaties.

Daarnaast ligt er meer nadruk op samenwerking en communicatie. De CIO moet in staat zijn om complexe technologische concepten in begrijpelijke taal uit te leggen aan niet-technische stakeholders, zoals het management en andere afdelingen, om draagvlak te creëren voor digitale transformatie-initiatieven. Dit maakt de CIO van vandaag een cruciale speler in het succes van de organisatie op lange termijn.

2.4 De rol van CISO

In de paper '*Functies-in-de-informatiebeveiliging-nl van 2017 - een visiedocument*' staan vele functieprofielen zoals deze in de informatiebeveiliging heden ten dage nog steeds voorkomen. De rol van CISO is er in mijn opinie in twee hoedanigheden, namelijk de fulltime CISO en de virtuele CISO die in deeltijd binnen het met name kleinere MKB-organisaties opereert.

Onderstaande afbeelding biedt een weergave van de hiërarchie voor informatiebeveiliging, zoals gepubliceerd door Gartner.



Bron: *Gartner, Functies-in-de-informatiebeveiliging-nl van 2017*[1]

De (v)CISO-functie inhoudelijk

De CISO ontwikkelt de strategie en het beleid gericht op informatiebeveiliging. Bevorderen en coördineren van de ontwikkeling van uitvoeringsrichtlijnen en toezien op de realisatie van het beleid.

De CISO functioneert als zelfstandig opererend intern beleidsadviseur, ressorterend onder het lid van het concern managementteam verantwoordelijk voor informatiebeveiliging of zit, zoals de C van Chief aangeeft, in de directie en/of het managementteam van een organisatie. Hij of zij geeft functioneel leiding aan informatiebeveiligingsmedewerkers in de gehele organisatie door het geven van richtlijnen en sturing op interne rapportages over de uitvoering van het informatiebeveiligingsbeleid en het naleven van uitvoeringsrichtlijnen. Hij of zij moet weerstand overwinnen om het beleid en richtlijnen te laten naleven, die vaak als belemmerend worden ervaren in de uitvoering van het werk.

Onderdelen:

- Beleid
- Leidinggeven
- Implementeren

[1] De ISO 17799:2005 is nu de ISO 27002:2022

- Evalueren
- Onderhouden
- Contacten CSIRT en/of ZCERT

Fulltime CISO (1ste lijn):

- Werkt binnen een grotere organisatie en is verantwoordelijk voor de volledige uitvoering van het informatiebeveiligingsbeleid. Dit omvat beleidsontwikkeling, leidinggeven aan beveiligingsteams, en toezicht houden op interne rapportages.
- Deze CISO zit vaak in het managementteam en geeft leiding aan informatiebeveiligingsmedewerkers.

Virtuele CISO (vCISO) (2de lijn):

- Dit type CISO werkt deeltijds, meestal binnen MKB-organisaties. De virtuele CISO heeft dezelfde verantwoordelijkheden als de fulltime CISO, maar vervult deze op een minder intensieve basis.
- De vCISO biedt een flexibele oplossing voor kleinere bedrijven, waarbij dezelfde strategische doelen worden bereikt zonder dat er een fulltime functie nodig is

Verschillen tussen CISO 1ste lijn en CISO 2de lijn

Met deze verbeteringen en toevoegingen kun je de documenten verrijken en ze beter afstemmen op de specifieke behoeften en rollen binnen de organisatie. Door de verschillen tussen de CISO 1ste lijn en 2de lijn duidelijk in een tabel weer te geven, wordt het makkelijker om de rol en verantwoordelijkheden van elke positie te begrijpen.

Aspect	**CISO 1ste Lijn (fulltime)**	**CISO 2de Lijn (partime)**
Roldefinitie	Definieert, organiseert en stuurt de informatiebeveiliging.	Definieert en bewaakt de informatiebeveiliging.
Budgetverantwoor-delijkheid	Heeft budget-verantwoordelijkheid.	Heeft geen budgetverantwoordelijkheid.
Implementatie van beveiliging	Initieert en coördineert de implementatie van informatiebeveiliging.	Beoordeelt de implementatie van informatiebeveiliging en geeft advies.
Calamiteitenorga-nisatie	Zet een informatiebeveiligings-calamiteitenorganisatie op.	Helpt bij het opzetten van een informatiebeveiligingscalamiteit enorganisatie.
Projectportfolio	Zorgt voor een projectportfolio voor informatiebeveiliging.	Beoordeelt het projectportfolio voor informatiebeveiliging.

Compliance monitoring	Monitort compliance van de wet- en regelgeving ten opzichte van het beleid.	Monitort en borgt compliance op basis van assessments, tests, reviews en audits.
Stakeholder-interactie	Communiceert met senior management over de status van informatiebeveiliging.	Informeert senior management over de status van informatiebeveiliging en presenteert adviezen.
Expertise en advies	Zorgt voor de benodigde expertise en afstemming tussen verschillende beveiligingsdomeinen.	Geeft advies over afstemming tussen verschillende beveiligingsdomeinen en benodigde expertise.

2.5 Slotbeschouwing

Sterk leiderschap en betrokkenheid van het topmanagement zijn essentieel voor het succes van cybersecurity-initiatieven. Het vermogen om een duidelijke beleidsverklaring op te stellen, verantwoordelijkheden te definiëren, en het implementeren van een cultuur van veiligheid binnen de organisatie, vormen de hoekstenen van een effectieve cyberbeveiligingsstrategie. Door leiderschap te koppelen aan technische en organisatorische structuren, kunnen organisaties de uitdagingen van NIS2 effectief aanpakken.

3. Planning

In dit hoofdstuk geven we een overzicht van de methodes voor risicobeoordeling en -beheer, inclusief het stellen van SMART-doelen voor IT en OT.

3.1 Acties om risico's en kansen aan te pakken

3.1.1 Methodes voor risicobeoordeling en -beheer

Het identificeren, analyseren en evalueren van risico's is cruciaal voor een effectieve informatiebeveiliging. Het opstellen van SMART-doelen (Specifiek, Meetbaar, Acceptabel, Realistisch en Tijdgebonden) helpt organisaties om duidelijke en haalbare veiligheidsdoelstellingen te formuleren. Risicobeoordeling moet regelmatig plaatsvinden en gebaseerd zijn op standaarden zoals ISO/IEC 27005 en NIST SP 800-30.

3.1.2 Beoordeling van informatiebeveiligingsrisico's

In een wereld waar digitale en fysieke systemen steeds meer met elkaar verweven zijn, vormt cyberweerbaarheid een cruciaal element voor zowel IT (Information Technology) als OT (Operational Technology). Terwijl IT de digitale ruggengraat van een organisatie verzorgt, beheert OT de fysieke operaties en infrastructuren die het dagelijks functioneren ondersteunen. De naadloze integratie van deze twee domeinen is essentieel voor de veiligheid en efficiëntie van moderne organisaties.

Information Technology (IT) verwijst naar het gebruik van computers, opslag, netwerken en andere fysieke apparaten, infrastructuren en processen om alle vormen van elektronische data te creëren, verwerken, opslaan, beveiligen en uit te wisselen. IT is de hoeksteen van digitale informatieverwerking en communicatie binnen organisaties, die zich bezighoudt met data-analyse, softwareontwikkeling, netwerkbeheer en cybersecurity.

Operational Technology (OT) betreft hardware en software die industriële apparatuur en processen detecteert of veroorzaakt veranderingen door middel van directe monitoring en controle. OT omvat systemen zoals SCADA (Supervisory Control and Data Acquisition), PLC's (Programmable Logic Controllers), en DCS (Distributed Control Systems) die cruciaal zijn voor het beheer van fysieke processen in industrieën zoals energie, waterbeheer, productie en transport.

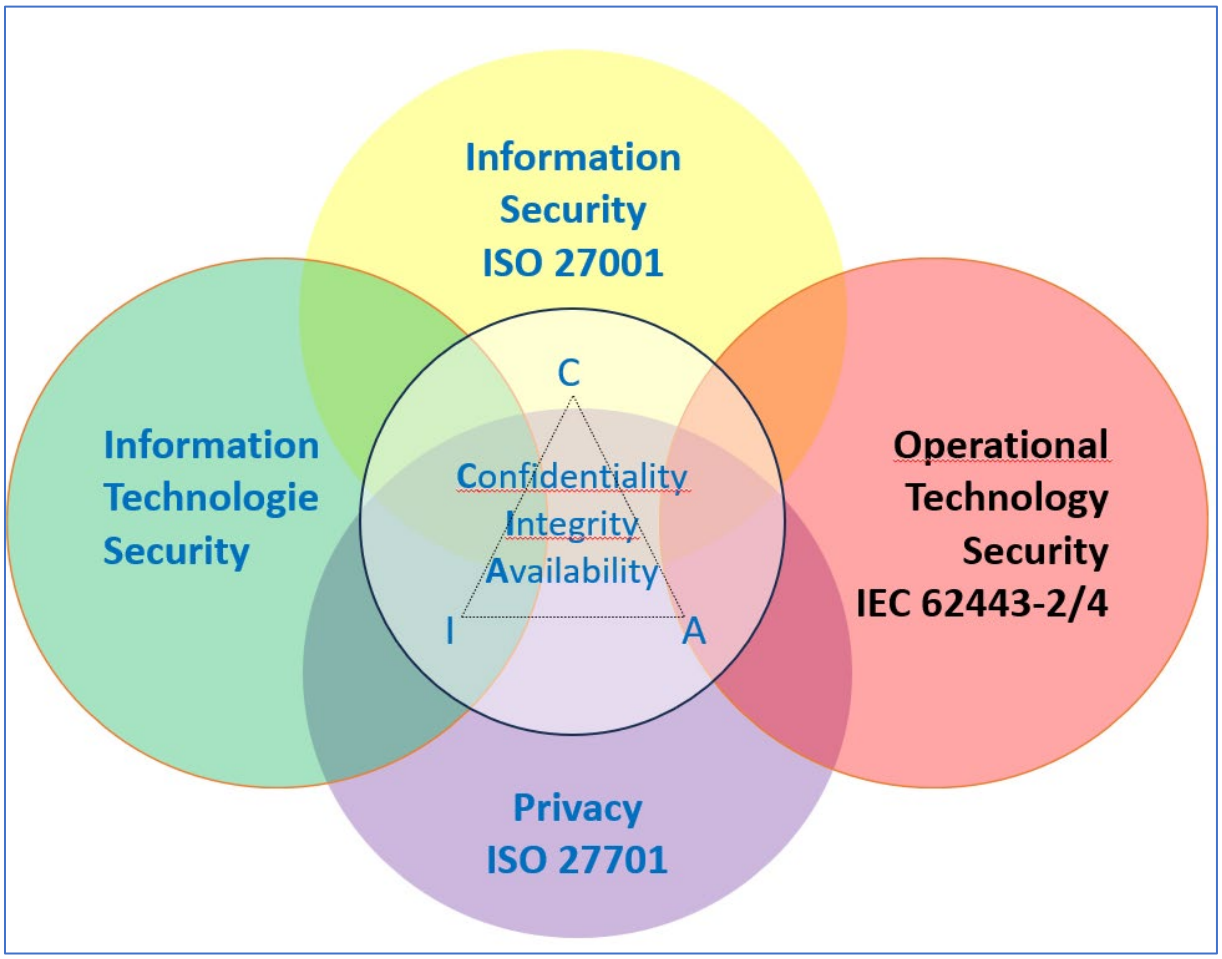
3.2 IT en OT: de verbinding

De traditionele scheiding tussen IT en OT wordt steeds meer vervaagd door de opkomst van het Industrial Internet of Things (IIoT) en digitale transformatie. De verbinding tussen IT en OT biedt talloze voordelen, zoals verbeterde efficiëntie, real-time data-analyse en proactief onderhoud. Echter, deze integratie brengt

ook nieuwe uitdagingen met zich mee, vooral op het gebied van cyberweerbaarheid.

3.2.1 SMART-doelen voor IT en OT

De integratie van IT en OT is essentieel voor de veiligheid en efficiëntie van moderne organisaties. Een goed voorbeeld van een SMART-doel voor IT en OT is: "Binnen zes maanden een geïntegreerd beveiligingsbeleid ontwikkelen en implementeren dat voldoet aan zowel ISO 27001 voor IT als IEC 62443 voor OT, met maandelijkse evaluaties en bijstellingen op basis van nieuwe dreigingen."



Bron: *MPbv Venndiagram cybersecurity*

3.2.2 Behandeling van informatiebeveiligingsrisico's

Bij steeds meer organisaties wordt de traditionele scheiding tussen IT en OT steeds meer vervaagd door de opkomst van het Industrial Internet of Things (IIoT) en digitale transformatie. De verbinding tussen IT en OT biedt talloze voordelen, zoals verbeterde efficiëntie, real-time data-analyse en proactief onderhoud. Echter, deze integratie brengt ook nieuwe uitdagingen met zich mee, vooral op het gebied van cyberweerbaarheid.

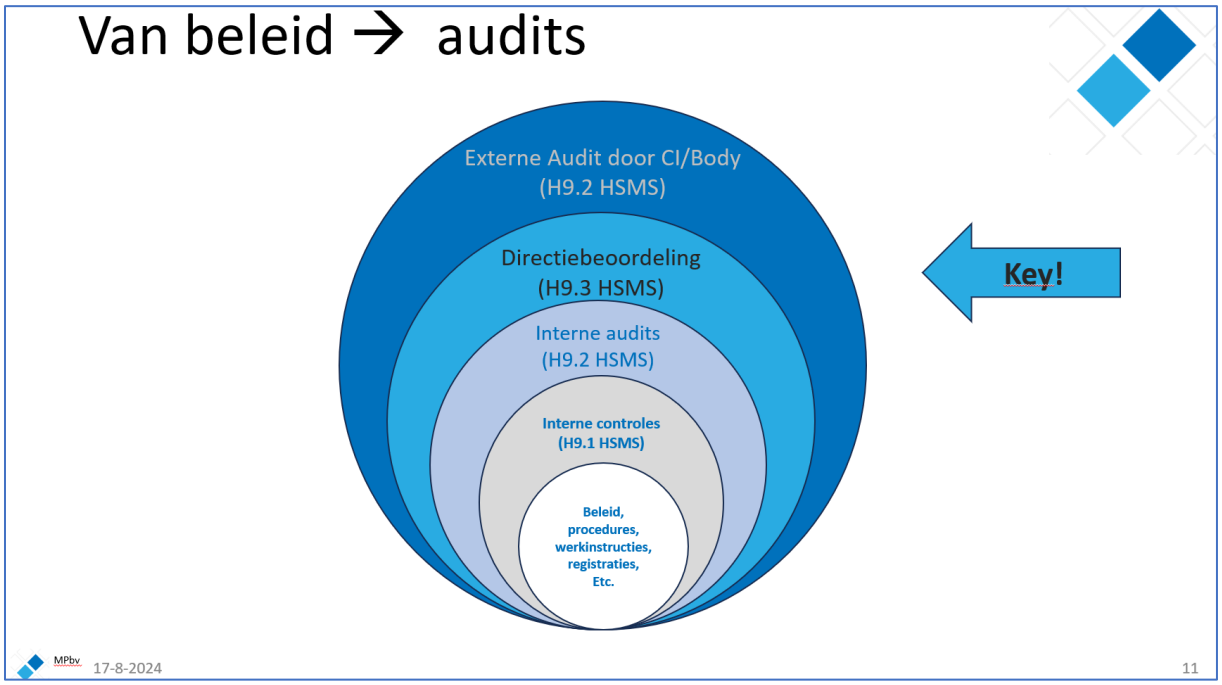
Door gebruik te maken van gedetailleerde risicoanalyses, geïntegreerde beveiligingsbeleid, bewustwordingstrainingen, robuuste incidentresponsplannen

en nauwe samenwerking tussen IT- en OT-teams, kunnen organisaties hun weerbaarheid tegen cyberdreigingen aanzienlijk vergroten en zo de continuïteit en veiligheid van hun operaties waarborgen.

Geïntegreerd beveiligingsbeleid: Het ontwikkelen van een geïntegreerd beveiligingsbeleid dat rekening houdt met zowel IT- als OT-vereisten is essentieel. Dit beleid moet conform zijn aan standaarden zoals de ISO 27001 voor IT en IEC 62443 voor OT.

Samenwerking tussen IT en OT: Het bevorderen van samenwerking tussen IT- en OT-teams is cruciaal. Dit omvat regelmatige communicatie, gezamenlijke beveiligingsinitiatieven en het delen van best practices om een verenigde verdediging te vormen tegen cyberdreigingen.

3.3 Van beleid en procedures . . . naar audits



Bron: *MPbv*

3.3.1 Gelaagdheid en communicatie in een organisatie binnen de context van NIS2

Bij de implementatie van een Harmonized Structured Management System (HSMS) onder de NIS2-richtlijn, speelt de gelaagdheid en communicatie binnen een organisatie een cruciale rol. De toepassing van het Three Lines of Defense (3LoD, zie afbeelding in par. 6.1) model biedt een robuuste aanpak voor het beheer van risico's, inclusief cyberrisico's, door duidelijke verantwoordelijkheden vast te stellen en effectieve interne controles te waarborgen. Deze lagen werken samen om de cyberweerbaarheid van een organisatie te versterken en om ervoor te zorgen dat risico's op een systematische manier worden beheerd en gecontroleerd.

3.3.2 Three Lines of Defense Model (3LoD)

Eerste Lijn: Operationeel management

Operationeel management is verantwoordelijk voor het dagelijks risicobeheer en het naleven van de beveiligingsbeleid en -procedures. Dit omvat de implementatie van beveiligingsmaatregelen, het monitoren van compliance, en het reageren op incidenten. Ze zijn de "risico-eigenaren" en werken nauw samen met andere afdelingen om ervoor te zorgen dat de operationele activiteiten in lijn zijn met de vastgestelde beveiligingsnormen.

Tweede Lijn: Risicobeheer en compliance

Deze lijn fungeert als de toezichthouder van de eerste lijn. Ze ontwikkelen en implementeren risicobeheerkaders en compliance-programma's, voeren onafhankelijke monitoring en evaluatie uit, en bieden advies en ondersteuning aan de eerste lijn. Ze zorgen ervoor dat het beveiligingsbeleid consistent wordt toegepast en dat de risicoprofielen van de organisatie goed worden begrepen en beheerd.

Derde Lijn: Interne en externe audit

De derde lijn biedt onafhankelijke zekerheid over de effectiviteit van het risicobeheer en de interne controles. Interne audits beoordelen regelmatig de naleving van het beleid en de effectiviteit van de beheersmaatregelen. Externe audits, uitgevoerd door gecertificeerde instanties, zijn cruciaal voor de formele toetsing van de implementatie van NIS2 en andere relevante normen zoals ISO 27001. Deze audits controleren niet alleen op compliance, maar ook op de mate waarin de organisatie haar beveiligingsdoelstellingen bereikt en risico's effectief beheert.

3.3.3 Verantwoording en communicatie

Effectieve communicatie is essentieel om ervoor te zorgen dat het management en de medewerkers betrokken en geïnformeerd blijven over de cybersecurity-initiatieven. Dit houdt in dat het topmanagement duidelijke richtlijnen en verwachtingen uitzet, en dat er een transparante rapportagestructuur wordt gehandhaafd. Het is belangrijk dat er een regelmatige terugkoppeling plaatsvindt tussen de verschillende verdedigingslinies om ervoor te zorgen dat alle lagen binnen de organisatie werken aan gemeenschappelijke doelen.

3.3.4 Betrokkenheid van het topmanagement

De betrokkenheid van het topmanagement is essentieel voor het succes van cybersecurity-initiatieven. Het topmanagement moet niet alleen zorgen voor de nodige middelen en ondersteuning, maar ook actief deelnemen aan het toezicht op de implementatie van beveiligingsmaatregelen en de naleving van de NIS2-richtlijn. De directie moet regelmatig de resultaten van interne en externe audits

beoordelen en de nodige corrigerende maatregelen nemen om eventuele tekortkomingen aan te pakken.

3.3.5 Noodzaak van interne en externe audits

Interne en externe audits spelen een cruciale rol in het waarborgen van de effectiviteit van het HSMS en de naleving van NIS2. Interne audits bieden inzicht in de dagelijkse uitvoering van beveiligingsmaatregelen en helpen bij het identificeren van verbeterpunten. Externe audits zorgen voor een objectieve evaluatie van de compliance en geven organisaties een formele bevestiging van hun beveiligingsstatus. Deze audits zijn ook belangrijk voor het handhaven van certificeringen zoals ISO 27001 en voor het voldoen aan de wettelijke vereisten die door de NIS2-richtlijn worden opgelegd.

3.3.6 Multidisciplinaire benadering van digitale veiligheid

In aanvulling op de gelaagde benadering van risicobeheer, zoals geïllustreerd in het Three Lines of Defense model, benadrukt recent onderzoek de noodzaak van een bredere, multidisciplinaire benadering van digitale veiligheid.

Het boek *Multidisciplinaire aspecten van digital security* (2022), samengesteld door de KNVI en deLex, biedt diepgaande inzichten in hoe technische, juridische en organisatorische aspecten integraal met elkaar verweven zijn bij het ontwikkelen van een effectieve cybersecuritystrategie.

Dit boek benadrukt dat digitale veiligheid niet alleen een technische uitdaging is, maar ook juridische, ethische en organisatorische implicaties heeft. Deze bredere aanpak is cruciaal om te kunnen anticiperen op en reageren op de complexe cyberdreigingen waarmee moderne organisaties worden geconfronteerd. De combinatie van verschillende disciplines helpt bij het creëren van een holistische benadering, die niet alleen gericht is op het beschermen van technische systemen, maar ook op het waarborgen van naleving van regelgeving, het beheren van reputatierisico's, en het verzekeren van operationele continuïteit.

Toepassing in NIS2-implementatie: Het integreren van deze multidisciplinaire inzichten in de implementatie van NIS2 binnen een organisatie kan de effectiviteit van het HSMS (Harmonized Structured Management System) verder vergroten. Door niet alleen te focussen op technische controles, maar ook op juridische naleving en organisatorische structuren, kunnen organisaties een meer robuuste en veerkrachtige beveiligingsstrategie ontwikkelen.

3.4 Slotbeschouwing

Het combineren van het 3LoD-model met robuuste communicatie- en auditprocessen tezamen met de multidisciplinaire inzichten, creëert een sterke basis voor de cyberweerbaarheid van organisaties. Door het integreren van deze elementen binnen een HSMS, kunnen organisaties niet alleen voldoen aan de vereisten van NIS2, maar ook hun algehele beveiligingsstatus versterken en voorbereid zijn op toekomstige uitdagingen in het cybersecurity-landschap.

Een gestructureerde benadering van risicobeheer en het stellen van SMART-doelen is cruciaal voor het waarborgen van cyberveiligheid binnen organisaties. Door regelmatig risico's te evalueren en doelstellingen aan te passen aan veranderende dreigingslandschappen, kunnen organisaties hun weerbaarheid verbeteren. Deze planning moet zowel IT- als OT-omgevingen omvatten, wat de basis legt voor een geïntegreerde en holistische cyberbeveiligingsstrategie.

4. Ondersteuning

In dit hoofdstuk geven we een overzicht van de beschikbare middelen, training en bewustwordingsprogramma's, alsmede communicatieplannen op het gebied van cybersecurity.

Middelen en bewustzijn: Er moeten voldoende middelen beschikbaar zijn voor cybersecurity, inclusief personeel, technologie en financiën. Training en bewustwordingsprogramma's zijn essentieel om een cultuur van veiligheid te bevorderen binnen de organisatie.

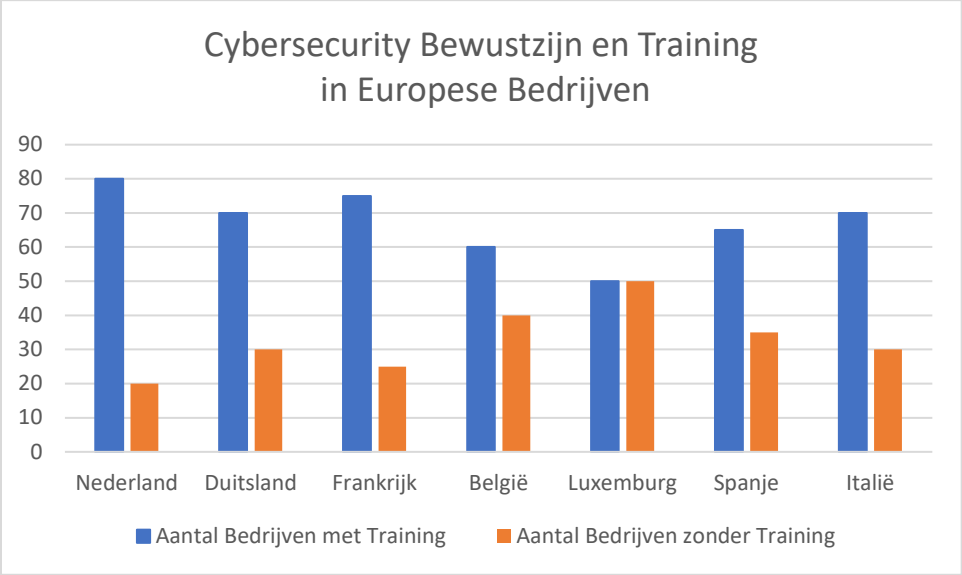
Casestudy: Het SANS Security Awareness Program biedt een effectief model voor het implementeren van bewustwordingsprogramma's binnen organisaties. Verschillende organisaties hebben met succes deze aanpak gebruikt om hun cyberweerbaarheid te vergroten, zoals gedocumenteerd in de SANS case study van 2022

4.1 Training

ENISA biedt richtlijnen en tools om de trainingsprogramma's effectief te implementeren. Daarnaast kunnen organisaties gebruik maken van frameworks zoals het SANS Security Awareness Program en anderen om hun personeel te trainen.

4.2 Communicatieplannen cybersecurity

Een effectief communicatieplan voor cybersecurity omvat duidelijke richtlijnen voor het rapporteren van incidenten, regelmatige updates over nieuwe dreigingen en de betrokkenheid van alle niveaus binnen de organisatie.
NIST SP 800-53 biedt uitgebreide richtlijnen voor de ontwikkeling van dergelijke plannen, inclusief voorbeelden en best practices.



4.3 Slotbeschouwing

Voldoende middelen, training en bewustwording zijn onmisbaar voor een robuuste cyberveiligheidscultuur. Het succes van beveiligingsinitiatieven hangt af van de betrokkenheid van het personeel en de beschikbaarheid van de juiste tools en training. Effectieve communicatieplannen versterken deze inspanningen en zorgen ervoor dat alle niveaus binnen de organisatie op de hoogte zijn van de cyberbeveiligingsdoelstellingen en -protocollen**.**

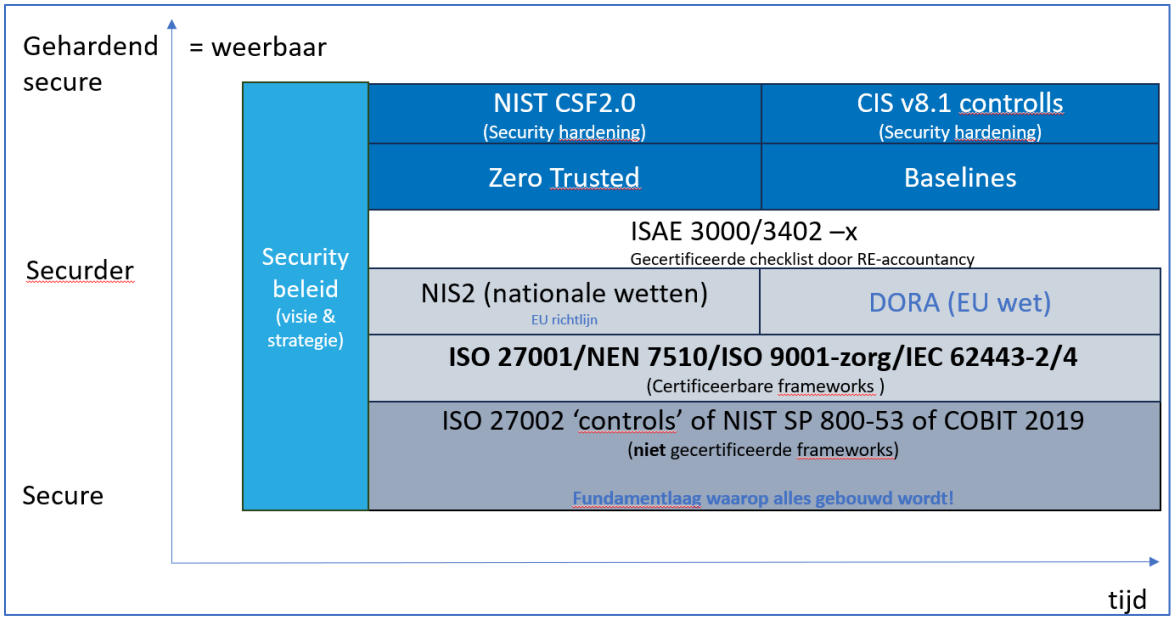
5. Operationele planning en beheersing

In dit hoofdstuk gaan we in op de implementatie van controlemaatregelen en incidentmanagement.

5.1 Beheersmaatregelen en incidentmanagement

ISO 27001:2022, BIO2, NEN7510 voor de Nederlandse overheden en de zorg

Het is verstandig bij de implementatie van controlemaatregelen standaarden te volgens zoals ISO 27001:2022, NIST SP800-53, COBIT 2019 of de BIO2 en NEN7510 welke wettelijk verplicht moeten toegepast respectievelijk bij de (semi)overheden en de NEN7510 en ISO9001-zorg binnen dé zorg in brede zin bedoeld.



Bron: *MPbv*

ISO 27001:2022 biedt een gestructureerd raamwerk voor het ontwikkelen en beheren van een Information Security Management System (ISMS), terwijl de BIO2 richtlijnen specifiek zijn voor de Nederlandse overheid en aansluiten bij de unieke wettelijke en operationele eisen van overheidsinstellingen. Door deze normen te volgen, kunnen organisaties een samenhangende en effectieve set controlemaatregelen ontwikkelen die voldoen aan zowel internationale als nationale standaarden. Dit omvat het uitvoeren van regelmatige risicobeoordelingen, het ontwikkelen van incidentresponsplannen en het implementeren van continue monitoring- en verbeteringsprocessen.

Er zijn de laatste jaren specifieke procedures en technologieën ontwikkeld om bedreigingen te detecteren, te analyseren en erop te reageren voordat ze

bedrijfsactiviteiten schade berokkenen zoals SIEM (Security Information and Event Management), SOC (Security Operations Center) en SOAR (Security Orchestration, Automation and Response). Processen voor incidentrespons moeten worden ontwikkeld om snel en effectief te kunnen reageren op cyberaanvallen .

5.2 SIEM

Security Information and Event Management, oftewel SIEM, is een oplossing die organisaties helpt bedreigingen te detecteren, te analyseren en erop te reageren voordat ze bedrijfsactiviteiten schade berokkenen. SIEM, uitgesproken als 'siem', combineert zowel SIM (Security Information Management) als SEM (Security Event Management) in één beveiligingsbeheersysteem. SIEM-technologie verzamelt gebeurtenislogboekgegevens uit een reeks bronnen, identificeert activiteit die van de norm afwijkt met real-time analyse, en onderneemt gepaste actie. Kort gezegd geeft SIEM organisaties inzicht in activiteit binnen hun netwerk, zodat ze snel op potentiële cyberaanvallen kunnen reageren en aan compliance-vereisten kunnen voldoen.

SIEM-systemen zijn zo ontwikkeld dat ze een volledig beeld geven van de beveiligingsstatus van een bedrijf of organisatie. Beveiligingsteams kunnen hierdoor snel bedreigingen identificeren en hierop reageren. Het SIEM-systeem maakt gebruik van Security Information Management (SIM) en Security Event Management (SEM) om gegevens te verzamelen en te analyseren vanuit verschillende bronnen. Activiteiten die van de norm afwijken worden real-time zichtbaar en hierop wordt op gepaste wijze actie ondernomen.

SIEM-tools verzamelen, aggregeren en analyseren in real-time grote hoeveelheden gegevens uit de toepassingen, apparaten, servers en gebruikers van een organisatie, zodat beveiligingsteams aanvallen kunnen detecteren en blokkeren. SIEM-tools gebruiken vooraf bepaalde regels om beveiligingsteams te helpen bedreigingen te definiëren en waarschuwingen te genereren.

SIEM-systemen variëren in hun mogelijkheden, maar bieden over het algemeen deze kernfuncties:

5.2.1 Logboekbeheer

SIEM-systemen verzamelen enorme hoeveelheden gegevens op één plek, organiseren ze en bepalen vervolgens of ze tekenen van een bedreiging, aanval of gegevenslek vertonen.

Gebeurteniscorrelatie: De gegevens worden vervolgens gesorteerd om relaties en patronen te identificeren om snel potentiële bedreigingen te detecteren en erop te reageren.

Incidentbewaking en reactie: SIEM-technologie bewaakt beveiligingsincidenten in het hele netwerk van een organisatie en biedt waarschuwingen en audits van alle activiteit die is gerelateerd aan een incident.

SIEM-systemen kunnen cyberrisico's mitigeren met een reeks use cases zoals het detecteren van verdachte gebruikersactiviteit, het bewaken van

gebruikersgedrag, het beperken van toegangspogingen en het genereren van compliance-rapporten.

SIEM-tools bieden veel voordelen die kunnen helpen de algehele beveiligingssituatie van een organisatie te versterken, waaronder:

- Een centraal overzicht van potentiële bedreigingen;
- Real-time bedreigingsidentificatie en reactie;
- Geavanceerde bedreigingsinformatie;
- Controle en rapportage van wettelijke compliance;
- Meer transparantie in het bewaken van gebruikers, toepassingen en apparaten.

Organisaties van elke omvang gebruiken SIEM-oplossingen om cyberbeveiligingsrisico's te mitigeren en aan wettelijke compliance-normen te voldoen. De aanbevolen procedures voor het implementeren van een SIEM-systeem omvatten:

- Definieer de vereisten voor SIEM-implementatie.
- Voer een test uit.
- Verzamel voldoende gegevens.
- Stel een incidentreactieplan op.
- Blijf je SIEM verbeteren.

5.3 SOC - Security Operations Center

Een Security Operations Center, of in het kort ook wel SOC genoemd is zoals het woord 'centrum' al aangeeft, de fysieke locatie van een informatiebeveiligingsteam. De mensen die in het SOC werken, zijn voortdurend bezig met het bewaken en verbeteren van de security status van een organisatie en tegelijkertijd met het voorkomen, opsporen, analyseren en reageren op cybersecurity-incidenten.

In een SOC maakt het security team gebruik van een combinatie van technologische oplossingen en een reeks sterke processen. Dit vakkundige team bestaat meestal uit security-analisten, engineers en managers die toezicht houden op de security-activiteiten. Het team werkt nauw samen met het incident response team, dat ervoor zorgt dat security-problemen snel na ontdekking worden aangepakt.

Niet alle organisaties zijn in staat een Security Operations Center op te zetten. Dit heeft verschillende redenen, maar heeft vaak te maken met een gebrek aan middelen, interne deskundigheid, tijd en geld om het op te zetten. Om die reden kiezen veel organisaties ervoor om SOC-diensten uit te besteden aan een externe vertrouwde IT-partner. In dat geval spreken we van een managed SOC service.

Praktijkvoorbeeld: Een succesvol voorbeeld van de implementatie van een SIEM-systeem is te vinden in het recent gepubliceerde ENISA-rapport over incidentrespons in de financiële sector, waar een toonaangevende Europese bank

erin slaagde om de detectie en respons op cyberaanvallen aanzienlijk te verbeteren

5.4 Technologie die wordt gebruikt in een Security Operations Center

Voor het opzetten van effectieve security-activiteiten heb je de juiste tooling nodig. Zonder dat word je overweldigd door een groot aantal security events. Hieronder hebben we de belangrijkste security-oplossingen geselecteerd die je helpen om veel processen te automatiseren, om te gaan met deze gebeurtenissen en ervoor te zorgen dat je de significante bedreigingen opspoort.

5.4.1 SOAR

Security Orchestration, Automation and Response (SOAR) verwijst naar een set diensten en hulpprogramma's die de preventie van en reactie op cyberaanvallen automatiseren. Deze automatisering wordt bereikt door je integraties te verenigen, te definiëren hoe taken moeten worden uitgevoerd, en een incidentreactieplan te ontwikkelen dat past bij de behoeften van je organisatie.

Met behulp van SOAR-technologie zijn SOC-teams (beveiligingscentrum) die voorheen werden overspoeld met repetitieve en tijdrovende taken, nu in staat incidenten efficiënter op te lossen, waardoor de kosten dalen, gaten in de dekking worden gedicht en de productiviteit toeneemt.

Security Orchestration, Automation and Response (SOAR) is een type software dat wordt gebruikt in beveiligingsinlichtingen- en informatiesystemen en is bedoeld om de effectiviteit van beveiligingsactiviteiten te verbeteren. Het stelt organisaties in staat om snel te reageren op beveiligingsincidenten en het proces van reageren op beveiligingsproblemen te automatiseren.

In essentie is SOAR een combinatie van automatiseringstools en responstactieken waarmee beveiligings- en incidentresponsteams sneller en effectiever kunnen reageren op beveiligingsincidenten. SOAR helpt bij het samenvoegen van gegevens uit meerdere bronnen, het automatiseren van de respons op incidenten en het stroomlijnen van de beveiligingsanalyse en -respons.

SOAR automatiseert het proces van het verzamelen en analyseren van gegevens over een incident, waarbij de gegevens uit verschillende beveiligingsbronnen (zoals SIEM-oplossingen, Endpoint Detection and Response-oplossingen, IDS en firewalls) worden gecorreleerd om een beeld van het incident te krijgen. SOAR helpt organisaties ook om sneller te reageren op beveiligingsproblemen, door het automatiseren van stappen zoals het waarschuwen van personeel en het indammen van de inbreuk op het netwerk. Het doel van SOAR is om de snelheid en doeltreffendheid van een beveiligingsorganisatie te verhogen en tegelijkertijd de operationele kosten te verlagen die gepaard gaan met het reageren op incidenten.

SOAR kan ook worden gebruikt voor threat hunting, waarbij proactief wordt gezocht naar tekenen van compromittering en kwaadaardige activiteiten. Schaalbaarheid en betrouwbaarheid zijn belangrijke voordelen van SOAR. Daarnaast bieden SOAR-oplossingen een beter inzicht in de beveiligingsomgeving, wat helpt bij het reageren op incidenten en het opsporen van bedreigingen.

SOAR's worden in veel industrieën en organisaties gebruikt om de beveiliging van hun netwerken te verbeteren. SOAR's bieden organisaties krachtige hulpmiddelen om te reageren op beveiligingsincidenten en geven waardevolle inzichten in hun beveiligingsstatus. Nu organisaties steeds meer vertrouwen op automatisering en analyse-gestuurde beveiligingsactiviteiten, wordt SOAR een steeds belangrijker hulpmiddel voor elke organisatie.

Hoe werkt SOAR?

SOAR bestaat doorgaans uit drie componenten die samenwerken om aanvallen te zoeken en te stoppen: indeling, automatisering en incidentreactie.

Indeling verbindt interne en externe hulpprogramma's, inclusief gebruiksklare en aangepaste integraties, zodat ze kunnen worden geopend vanaf één centrale plaats. Hierdoor kun je gegevens consolideren en processen stroomlijnen, waarmee je de weg vrijmaakt voor automatisering.

Automatisering programmeert taken zodat ze zelfstandig worden uitgevoerd. Dit wordt bereikt door playbooks of verzamelingen van workflows die automatisch worden uitgevoerd als ze door een regel of incident worden geactiveerd. Met playbooks kun je taken automatiseren, waarschuwingen beheren en reacties op bedreigingen en incidenten creëren.

Indeling en automatisering leggen de basis voor AI-aangedreven incidentreactie, wat resulteert in snellere, nauwkeurigere reacties en minder beveiligingsproblemen om te herstellen.

Automatisering en indeling

Laten we dieper ingaan op de twee basisonderdelen die SOAR mogelijk maken, automatisering van de beveiliging en indeling, en hoe ze van elkaar verschillen en elkaar aanvullen.

Automatisering van beveiliging biedt de mogelijkheid om de juiste acties voor te schrijven die vanzelf werken. Je zou bijvoorbeeld automatisering kunnen gebruiken om taken, waarschuwingen of reacties op incidenten te programmeren. Automatisering helpt ook beveiligingsprocessen zoals bedreigingsopsporing en herstel te versnellen, zodat potentiële bedreigingen in je omgeving in minder stappen worden opgelost. Door taken en processen te stroomlijnen, zijn SOC-teams minder tijd kwijt aan het sorteren van eindeloze waarschuwingen en kunnen ze zich richten op de signalen die ertoe doen.

Indeling van beveiliging biedt de mogelijkheid om verbinding te maken met een grote verscheidenheid aan hulpprogramma's en integraties, zodat informatie

kan worden gecentraliseerd en gedeeld. Met indeling kunnen deze hulpprogramma's ook als groep reageren op incidenten in de hele omgeving, zelfs als gegevens over het netwerk zijn verspreid. Vanwege deze mogelijkheden is indeling doorslaggevend voor het coördineren van grootschalige automatisering.

Beveiligingsautomatisering vereenvoudigt taken zodat ze soepeler verlopen, terwijl beveiligingsindeling hulpprogramma's met elkaar verbindt zodat ze samenwerken. Beide SOAR-onderdelen werken samen om een meer samenhangend systeem te vormen, waardoor de efficiëntie van begin tot eind wordt gemaximaliseerd.

Waarom is SOAR belangrijk?

Cyberaanvallen komen vaker voor dan ooit en ze worden alleen maar geavanceerder. Daarom geven veel organisaties nu prioriteit aan cyberbeveiliging en geven zowel bedrijven als consumenten elk jaar meer uit aan beveiligingsoplossingen.

Desondanks zijn cybercriminelen niet minder actief geworden. Het aantal gegevenslekken neemt toe, wat bijdraagt aan het enorme aantal waarschuwingen die SOC-teams dagelijks onder druk zetten. Handmatig reageren op deze waarschuwingen kan tijdrovend, lastig en onnauwkeurig zijn. En met de enorme hoeveelheid meldingen die via verschillende systemen binnenkomen, wordt het steeds moeilijker om door de ruis heen een duidelijk en samenhangend beeld te krijgen van je beveiligingslandschap.

Daar komt SOAR om de hoek kijken. De SOAR-technologie biedt een end-to-end-systeem dat automatisch kwetsbaarheden opspoort en daarop reageert zonder menselijke tussenkomst. Met SOAR-hulpprogramma's kan een organisatie bepalen en instellen hoe ze op een gebeurtenis reageren, waardoor tijd en budget vrijkomen om de focus te leggen op projecten met een hogere prioriteit.

5.4.2 SOAR versus SIEM

SOAR-hulpprogramma's worden vooral gebruikt om de reactie op bedreigingen in te delen en te automatiseren, terwijl SIEM meer zicht biedt op activiteiten door detectie van bedreigingen, logboekbeheer, analyse van incidenten en naleving van regelgeving en normen. Deze zichtbaarheid wordt bereikt door logboekregistratie en het consolideren van meerdere datastromen uit je hele netwerk, waardoor je een overzicht krijgt van het totale beveiligingslandschap van je organisatie.

De twee systemen werken het beste samen. SIEM verzamelt en analyseert gegevens, SOAR draait op basis van die gegevens en vormt zo een complete oplossing voor risicodetectie, zichtbaarheid en reactie.

5.4.3 MISFC: Een aanvulling op SOC/SIEM/SOAR monitoringoplossingen

Naast de traditionele Security Operations Centers (SOC), Security Information and Event Management (SIEM) en Security Orchestration, Automation and

Response (SOAR) oplossingen, biedt de Multilayer Integrated Security Fusion Center (MISFC) een krachtige en innovatieve aanvulling op bestaande cybersecurity-infrastructuren. Waar een SOC en SIEM zich primair richten op het monitoren en analyseren van incidenten, en SOAR de automatisering van responsprocessen mogelijk maakt, integreert MISFC een breder scala aan beveiligingstechnologieën en strategieën voor een proactieve en geïntegreerde aanpak.

De MISFC biedt onder meer:

Diepe Integratie van Beveiligingstechnologieën: Door middel van een breed scala aan technologieën zoals endpoint detection and response (EDR), threat intelligence en netwerkbeveiligingssystemen, biedt MISFC een holistische kijk op bedreigingen.

Geavanceerde Data-analyse en Machine Learning: Met gebruik van geavanceerde analytische technieken, waaronder machine learning, kan het MISFC anomalieën en verdachte patronen identificeren die duiden op cyberaanvallen.

Continue Verbetering: Het MISFC is continu bezig met het optimaliseren van processen en procedures om mee te kunnen bewegen met veranderende dreigingslandschappen, wat het bijzonder geschikt maakt voor organisaties die veeleisende en dynamische omgevingen beheren.

Cross-functionele samenwerking: Het centrum faciliteert nauwe samenwerking tussen verschillende beveiligingsteams, waaronder IT, incident response, juridische teams, en business stakeholders, wat een gecoördineerde en efficiënte respons mogelijk maakt.

Met deze uitbreiding biedt de MISFC een gelaagde aanpak die verder gaat dan de traditionele monitoringsmethoden, door zowel preventieve als responsieve capaciteiten te versterken. Organisaties kunnen hiermee niet alleen incidenten sneller detecteren en mitigeren, maar ook proactief verdedigen tegen geavanceerde bedreigingen dankzij voortdurende verbetering en multidimensionale samenwerking.

5.5 Toepassing van cybersecurity-technologieën in verschillende contexten

Inleiding

In de snel veranderende wereld van cybersecurity speelt technologie een cruciale rol bij het beschermen van digitale assets en het beheersen van risico's. In dit hoofdstuk worden niet alleen verschillende technologieën zoals SOC, SIEM, en SOAR besproken, maar wordt ook uiteengezet in welke specifieke situaties deze technologieën het meest effectief zijn. Het doel is om organisaties te voorzien van richtlijnen en concrete aanwijzingen over wanneer en hoe ze bepaalde technologieën moeten inzetten, afhankelijk van hun unieke behoeften en uitdagingen.

I. Security Information and Event Management (SIEM)

Context en toepassing: SIEM-systemen zijn ontworpen om grote hoeveelheden beveiligingsgegevens te verzamelen, correleren en analyseren. Ze zijn vooral nuttig in complexe IT-omgevingen waar veel verschillende gegevensbronnen en systemen aanwezig zijn. SIEM biedt real-time monitoring en detectie van bedreigingen, wat het een onmisbaar instrument maakt voor organisaties die snel willen reageren op security-incidenten.

Aanbevolen situaties:

- **Grotere organisaties:** Bedrijven met een uitgebreide IT-infrastructuur en diverse systemen.
- **Regelgeving en compliance:** Bedrijven die aan strenge compliance-eisen moeten voldoen, zoals in de financiële of gezondheidszorgsector.
- **Gecompliceerde dreigingslandschappen:** Organisaties die te maken hebben met geavanceerde, persistent dreigingen (Advanced Persistent Threats, APT's).

Praktijkvoorbeeld: Een bank gebruikt een SIEM-systeem om transacties in real-time te monitoren en verdachte activiteiten onmiddellijk te signaleren, waardoor potentiële fraude wordt voorkomen voordat deze schade kan veroorzaken.

II. Security Orchestration, Automation and Response (SOAR)

Context en toepassing: SOAR-systemen zijn ontworpen om het werk van beveiligingsteams te stroomlijnen door processen te automatiseren en reacties op incidenten te coördineren. Dit helpt bij het verminderen van de werkdruk op beveiligingsanalisten en het versnellen van de tijd die nodig is om op bedreigingen te reageren.

Aanbevolen situaties:

- **Hoge incidentvolumes:** Organisaties die dagelijks een groot aantal beveiligingswaarschuwingen ontvangen.

- **Beperkte personeelscapaciteit:** Kleine of middelgrote bedrijven met beperkte beveiligingspersoneel, die efficiëntie willen vergroten door automatisering.
- **Geavanceerde beveiligingsvereisten:** Bedrijven die te maken hebben met complexe incidenten die een snelle, gecoördineerde reactie vereisen.

Praktijkvoorbeeld: Een middelgroot technologiebedrijf implementeert SOAR om de tijd die nodig is om op phishing-aanvallen te reageren met 70% te verminderen, door automatisch routines uit te voeren zoals het blokkeren van verdachte e-mails en het afsluiten van geïnfecteerde accounts.

III. Security Operations Center (SOC)

Context en toepassing: Een SOC is het zenuwcentrum van de cyberbeveiliging binnen een organisatie. Hier worden alle beveiligingsoperaties gecentraliseerd en wordt continu gemonitord op bedreigingen. Een SOC integreert de functionaliteiten van SIEM en SOAR, samen met andere tools, om een alomvattende verdediging tegen cyberdreigingen te bieden.

Aanbevolen situaties:

- **Kritieke infrastructuur:** Organisaties die vitale diensten leveren, zoals energiebedrijven of transportnetwerken, waar elke onderbreking ernstige gevolgen kan hebben.
- **Continuïteit van diensten:** Bedrijven die 24/7 operationeel zijn en een constante monitoring van hun netwerken vereisen.
- **Mature security teams:** Organisaties met voldoende middelen om een toegewijd team te ondersteunen dat zich richt op continu toezicht en incidentbeheer.

Praktijkvoorbeeld: Een energieleverancier richt een SOC op om real-time toezicht te houden op zijn netwerk van slimme meters, wat helpt om storingen snel te detecteren en te verhelpen voordat ze klanten beïnvloeden.

IV. Multilayer Integrated Security Fusion Center (MISFC)

Context en toepassing: Het Multilayer Integrated Security Fusion Center (MISFC) vertegenwoordigt een meerlaagse en geïntegreerde benadering van cybersecurity. Waar SOC-, SIEM- en SOAR-oplossingen waardevol zijn voor monitoring, correlatie en automatisering, biedt het MISFC een bredere integratie van beveiligingstechnologieën met een nadruk op proactieve detectie en respons op cyberdreigingen. Het MISFC combineert data-analyse, threat intelligence en machine learning om de effectiviteit van dreigingsdetectie en -respons te verbeteren.

Aanbevolen situaties:

- **Kritieke infrastructuur en overheden:** Organisaties met complexe dreigingslandschappen die een uitgebreide gelaagde beveiligingsaanpak vereisen.
- **Grotere bedrijven met geavanceerde dreigingsvereisten:** Bedrijven die te maken hebben met APT's en zero-day-aanvallen, waarvoor diepgaande gedragsanalyse en geautomatiseerde respons nodig zijn.
- **Organisaties met beperkte resources voor continue verbetering:** Het MISFC biedt een ingebouwde continue verbetering en optimalisatie van processen, wat het ideaal maakt voor bedrijven die evoluerende dreigingen willen voorblijven.

Praktijkvoorbeeld: Een overheidsinstantie implementeert het MISFC om een proactieve verdediging tegen APT's te ontwikkelen. Door gebruik te maken van geavanceerde dreigingsinformatie en machine learning, is de instantie in staat om potentiële bedreigingen te identificeren voordat deze zich manifesteren in netwerkactiviteiten.

V. Aanvullende technologieën en overwegingen

Naast de bovengenoemde kerntechnologieën zijn er nog andere technologieën die, afhankelijk van de context, waardevol kunnen zijn. Denk aan Data Loss Prevention (DLP) systemen in omgevingen waar dataverlies een grote zorg is, of aan Intrusion Detection Systems (IDS) voor bedrijven die hun perimeterbeveiliging willen versterken.

Context-specifieke keuzes:

- **DLP:** Vooral nuttig in omgevingen waar gevoelige informatie, zoals patiëntgegevens of financiële informatie, moet worden beschermd tegen onopzettelijk verlies of diefstal.
- **IDS:** Geschikt voor bedrijven die hun netwerken willen beschermen tegen ongeautoriseerde toegang, vooral wanneer er veel externe connecties zijn.

Besluitvorming en implementatie

Het kiezen van de juiste technologie vereist een diepgaand begrip van de specifieke bedreigingen en vereisten van de organisatie. Een beslisboom of matrix kan organisaties helpen bij het bepalen welke technologieën het meest geschikt zijn voor hun situatie. Bij het implementeren van deze technologieën moet rekening worden gehouden met de bestaande infrastructuur, de beschikbare middelen en de mate van gewenste automatisering en integratie.

In tabelvorm gepresenteerd

In de tabel hieronder zijn de technologieën SOC, SIEM, SOAR en MISFC met elkaar vergeleken op basis van hun toepasbaarheid in verschillende sectoren. De plusjes geven de geschiktheid aan, waarbij "+++" betekent dat de technologie zeer geschikt is en "---" betekent dat deze nauwelijks van toepassing is.

Sector	SOC	SIEM	SOAR	MISFC
Kritieke infrastructuur	+++	+++	++	+++
Overheid & publieke sector	+++	++	++	+++
Financiële sector	++	+++	+++	+++
Gezondheidszorg	++	+++	++	++
Commerciële sector (Retail)	++	++	++	+
Kleine en middelgrote bedrijven (MKB)	+	+	+	++
Telecommunicatie	+++	+++	++	+++
Onderwijs & onderzoek	++	+	+-	++
Manufacturing & industrie	++	+	++	+++
E-commerce	+	++	+	++

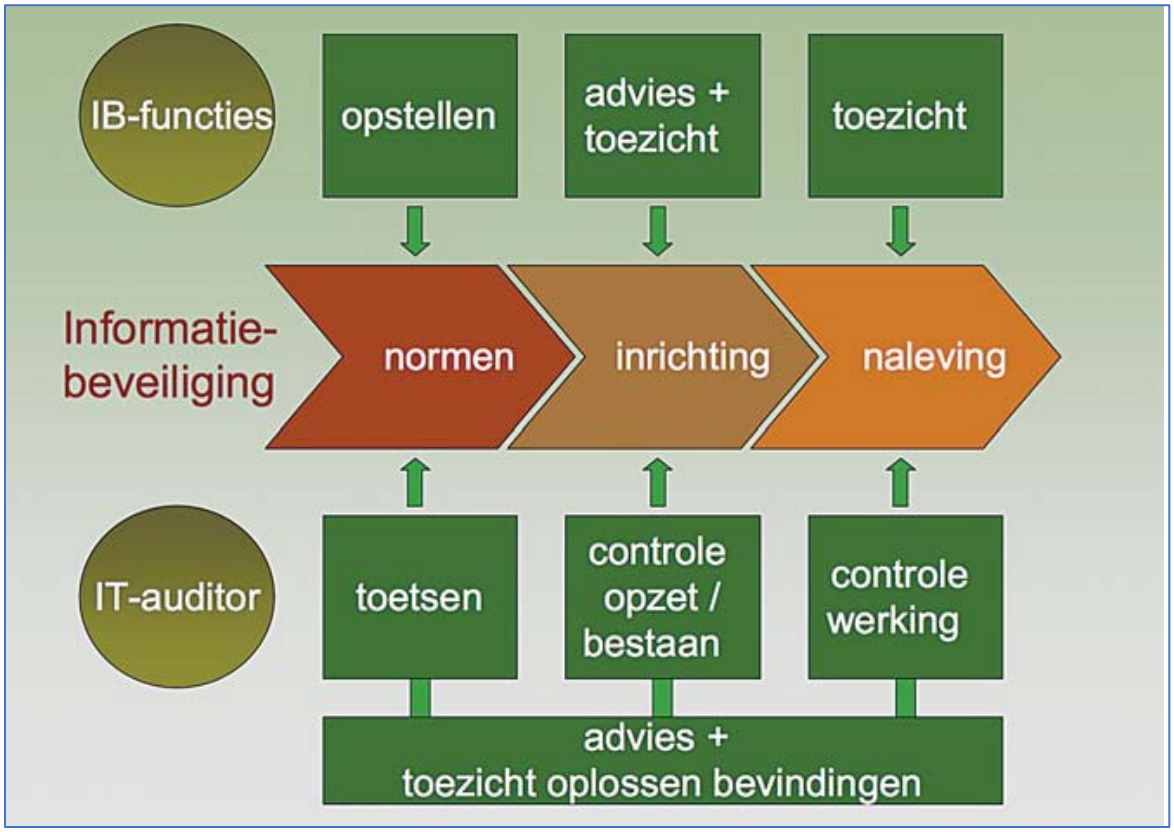
5.6 Slotbeschouwing

De implementatie van controlemaatregelen en een effectief incidentmanagementproces zijn cruciaal voor de continuïteit van de bedrijfsvoering en het minimaliseren van schade door cyberdreigingen. Door gebruik te maken van technologieën zoals SIEM, SOC, en SOAR, kunnen organisaties niet alleen dreigingen sneller detecteren, maar ook sneller en effectiever reageren. Een proactieve benadering van cyberbeveiliging is noodzakelijk om de veiligheid en weerbaarheid van de organisatie te waarborgen.

6. Prestatie-evaluatie

In dit hoofdstuk gaan we in op monitoring, interne audits en managementbeoordelingen.

Hierbij zijn betrokken, de directie oftewel het topmanagement dat de eindverantwoordelijkheid draagt en via de directiebeoordeling daarover verantwoordelijkheid aflegt aan de interne en de externe auditor. De laatste is werkzaam voor een certificeringsinstantie die onder toezicht staat van de Raad voor Accreditatie. Elk land heeft minimaal een zo'n instantie. Zij zijn geautoriseerd om certificaten uit te reiken na een succesvolle audit.



Bron: *Functies-in-de-informatiebeveiliging-nl van 2017*

Met de introductie van DORA (Europese wet) en NIS2 (Europese aanbeveling, nationale wetten), is voor het eerst geïntroduceerd in de wettekst dat de bestuurders -die de frameworks vaak aanduiden als het topmanagement- hoofdelijk aansprakelijk zijn voor de realisatie en implementatie binnen hun organisatie.

Monitoring en interne audits: Regelmatige audits en managementbeoordelingen zijn noodzakelijk om de effectiviteit van het cybersecuritybeleid te meten. Dit omvat het uitvoeren van ENISA-audits (European Network and Information Security Agency).

ENSIA, wat staat voor Eenduidige Normatiek Single Information Audit, is een specifiek verantwoordingsstelsel dat binnen de Nederlandse gemeentelijke overheden wordt gebruikt om de informatieveiligheid te waarborgen. ENSIA is in 2017 ingevoerd als een gezamenlijk initiatief van verschillende ministeries en de Vereniging van Nederlandse Gemeenten (VNG) om de verantwoordingsprocessen voor informatieveiligheid te harmoniseren en efficiënter te maken.

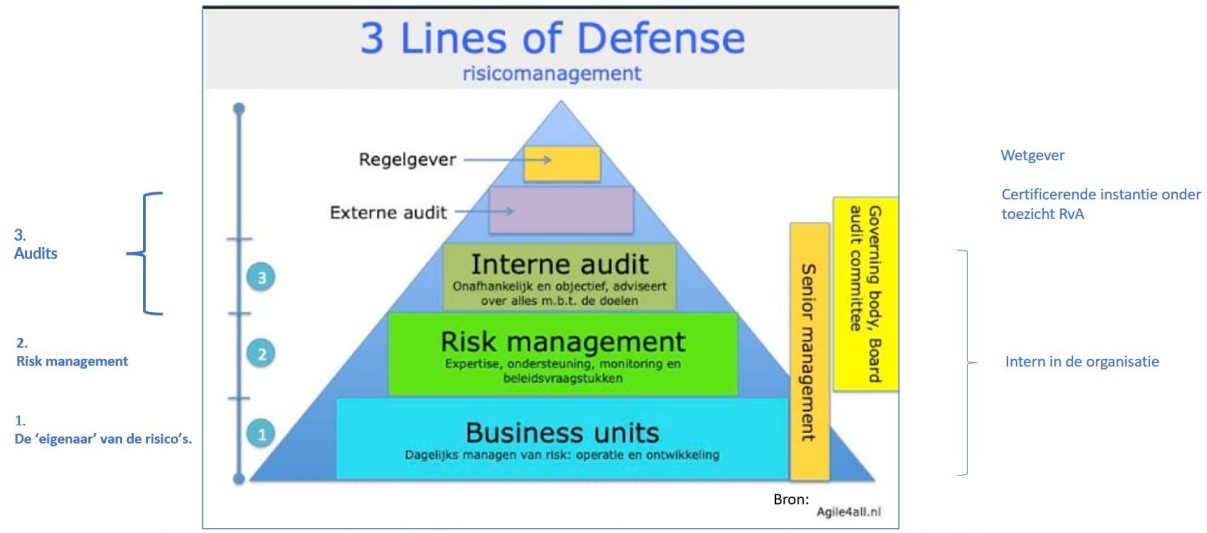
6.1 Rol van ENSIA binnen gemeenten

ENSIA helpt gemeenten om op een gestroomlijnde manier verantwoording af te leggen over hun informatieveiligheid. Dit gebeurt op basis van de Baseline Informatiebeveiliging Overheid (BIO/BIO2), een normenkader dat van toepassing is op alle overheidslagen in Nederland. Via ENSIA wordt er een horizontaal en verticaal verantwoordingsproces gehanteerd. Horizontaal betekent dat het college van B&W verantwoording aflegt aan de gemeenteraad, terwijl verticaal verwijst naar de verantwoording aan centrale toezichthouders, zoals die van DigiD en Suwinet.

De implementatie van ENSIA heeft ervoor gezorgd dat de audits en rapportages over informatieveiligheid efficiënter kunnen verlopen, doordat alle relevante informatie wordt gebundeld en slechts één keer per jaar hoeft te worden gerapporteerd. ENSIA ondersteunt dus niet alleen de naleving van de informatieveiligheidsnormen, maar ook de bestuurlijke transparantie en het toezicht op de uitvoering van informatieveiligheidsbeleid.

ENISA (European Union Agency for Cybersecurity), de Europese dienst voor cybersecurity, publiceert regelmatig rapporten die best practices bevatten voor zelfbeoordeling en auditprocessen. Deze rapporten richten zich op nationale bevoegde autoriteiten (National Competent Authorities, NCA's), digitale dienstverleners (Digital Service Providers, DSP's), en operators van essentiële diensten (Operators of Essential Services, OES). Het doel van deze publicaties is om deze entiteiten te ondersteunen bij het naleven van de NIS2-richtlijn (Network and Information Security Directive), door hen te voorzien van richtlijnen en methodologieën voor het uitvoeren van effectieve zelfbeoordelingen en audits.

Deze rapporten bevatten onder andere aanbevelingen over hoe deze organisaties hun cybersecuritymaatregelen kunnen verbeteren, hoe ze risico's kunnen beheren, en hoe ze moeten voldoen aan de wettelijke vereisten die voortvloeien uit de Europese wetgeving aldus NOREA.



Het doel van alle verdedigingslinies is het managen en mitigeren van risico's.

Bronnen: *MPbv & Agile4all*

Bewustwording bevorderen

Regelmatige beveiligingstrainingen voor personeel en bewustwordingscampagnes kunnen helpen om de naleving van beveiligingsprotocollen te verbeteren en de algehele beveiligingshouding van de organisatie te versterken.

6.2 Slotbeschouwing

Regelmatige monitoring, interne audits, en managementbeoordelingen zijn essentieel om de effectiviteit van cyberbeveiligingsstrategieën te waarborgen. Deze evaluaties helpen bij het identificeren van zwakke plekken en bieden mogelijkheden voor voortdurende verbetering. Door gebruik te maken van frameworks zoals ISO 27001 en NIST, en het implementeren van auditprocessen zoals ENSIA voor overheidsorganisaties, kunnen organisaties ervoor zorgen dat hun beveiligingsmaatregelen voldoen aan de hoogste normen. Deze aanpak versterkt niet alleen de compliance maar ook de algehele cyberweerbaarheid van de organisatie, waardoor ze beter voorbereid is op toekomstige dreigingen en uitdagingen.

7. Verbetering

In dit hoofdstuk geven we een overzicht van de corrigerende maatregelen en aanpak voor voortdurende verbetering van het managementsysteem.

Corrigerende maatregelen en voortdurende verbetering: Procedures voor het identificeren en corrigeren van niet-conformiteiten moeten worden ingesteld, evenals methoden voor voortdurende verbetering van het ISMS (Information Security Management System).

Effectieve cybersecurity vereist voortdurende verbetering en het snel corrigeren van niet-conformiteiten. ISO/IEC 27001:2022 biedt een raamwerk voor het implementeren van corrigerende maatregelen en het bevorderen van voortdurende verbetering. NIST SP 800-137 beschrijft methoden voor Information Security Continuous Monitoring (ISCM) die organisaties helpen om constant hun beveiligingsstatus te verbeteren.

7.1 Baselines en lifecycle management

Effectieve cybersecurity vereist niet alleen naleving van wetgeving, maar ook de implementatie van robuuste baselines voor onder ander security hardening en lifecycle management van apparatuur, software, database, applicaties en firmware.

7.1.1 Baselines

- **Beveiligingsbaselines** definiëren de minimale beveiligingscontroles die moeten worden geïmplementeerd om de vertrouwelijkheid, integriteit en beschikbaarheid van systemen en gegevens te waarborgen, zoals het NIST CSF2.0-framework of de CIS v8 Controls naast ISO 27001:2022 of NIST SP800-53.
- Deze baselines moeten vanuit de PCDA-cyclus frequent worden bijgewerkt om te blijven voldoen aan nieuwe dreigingen en technologische ontwikkelingen.

7.1.2 Lifecycle management

- **Lifecycle management** omvat de planning, ontwikkeling, implementatie, onderhoud en uiteindelijke verwijdering van apparatuur, software, database, applicaties en OT-firmware.
- Het is essentieel om gedurende de hele levenscyclus van deze componenten beveiligingsmaatregelen te implementeren, inclusief regelmatige updates en patches, kwetsbaarheidsbeheer en beveiligingstrainingen voor personeel.

De NIS2-richtlijn legt extra nadruk op geavanceerde netwerkbeveiliging en monitoring. Organisaties moeten geavanceerde beveiligingstechnieken zoals

continue netwerkanalyse en automatische dreigingsdetectie implementeren om te voldoen aan de NIS2-vereisten en proactief cyberdreigingen aan te pakken.

7.2 Slotbeschouwing

Voortdurende verbetering is de sleutel tot een effectieve cybersecuritystrategie. Het snel en efficiënt aanpakken van niet-conformiteiten, gecombineerd met het gebruik van corrigerende maatregelen, zorgt ervoor dat de organisatie blijft voldoen aan de steeds veranderende dreigingslandschappen en wettelijke vereisten. Door een cultuur van voortdurende verbetering te bevorderen, kunnen organisaties hun ISMS (Information Security Management System) versterken en beter voorbereid zijn op toekomstige uitdagingen.

8. Kritieke infrastructuur en cyberweerbaarheid

In dit hoofdstuk geven we een overzicht van de specifieke uitdagingen en maatregelen voor kritieke sectoren zoals energie, telecommunicatie, datacenters en transport.

Verschillende sectoren hebben unieke uitdagingen op het gebied van cyberweerbaarheid. Voor de energiesector is het bijvoorbeeld cruciaal om SCADA-systemen te beschermen tegen aanvallen. In de gezondheidszorg is het belangrijk om medische apparaten en patiëntgegevens te beveiligen. ENISA biedt gedetailleerde richtlijnen voor het beschermen van kritieke infrastructuur in diverse sectoren, zoals energie, telecommunicatie, datacenters, transport, en gezondheidszorg.

In dit paper onderscheiden we zeven **sectoren van kritieke infrastructuur**:

1. **Energie**: Stroomnetwerken en olie- en gasfaciliteiten zijn van cruciaal belang. Cyberaanvallen kunnen leiden tot stroomuitval of verstoringen in de energievoorziening.
2. **Telecommunicatie**: Dark Fiber, belichte Dark Fiber en mobiele netwerken vormen de backbone van de communicatie-infrastructuur.
3. **Datacenters en cloud applicaties**: Bescherming van fysieke datacenters en cloud services zoals AWS, Azure en Google Cloud tegen cyberdreigingen is essentieel.
4. **Transport**: Systemen voor luchtvaart, spoorwegen en maritieme operaties zijn kwetsbaar voor cyberaanvallen die de logistiek en veiligheid kunnen verstoren.
5. **Water en afvalbeheer**: Beheer van drinkwater en afvalwaterzuiveringsinstallaties moet worden beschermd om de waterkwaliteit en beschikbaarheid te waarborgen.
6. **Gezondheidszorg**: Ziekenhuizen, klinieken en farmaceutische bedrijven moeten beschermd worden tegen aanvallen die de patiëntenzorg kunnen verstoren.
7. **Financiële sector**: Banken, verzekeringen en financiële markten moeten worden beveiligd tegen aanvallen die financiële verliezen kunnen veroorzaken.

Cyberbeveiligingsuitdagingen:

1. **Operationele technologie (OT):** Beheer van industriële controlesystemen, risicobeheer en incidentrespons.
2. **Informatietechnologie (IT):** Gegevensbescherming, netwerkbeveiliging en naleving van regelgeving Huidige stand van cybersecurity in Europa.

Europa heeft aanzienlijke vooruitgang geboekt met de implementatie van diverse wetgevingen en richtlijnen om de cyberveiligheid te waarborgen. Belangrijke initiatieven zijn onder andere de Algemene Verordening Gegevensbescherming

(AVG), de Netwerk- en Informatiesystemenrichtlijn (NIS1 en NIS2), de EU Cybersecurity Act, en de Digital Operational Resilience Act (DORA).

8.1 Belangrijkste Nederlandse en Europese wetten en richtlijnen

1. **General Data Protection Regulation (GDPR)**: Reguleert gegevensbescherming en privacy binnen de EU, met strikte eisen voor gegevensverwerking en meldingsprocedures bij datalekken.
2. **Network and Information Systems Directive (NIS2)**: Richt zich op de beveiliging van essentiële en belangrijke entiteiten, met verhoogde eisen voor risicobeheer, incidentrespons en samenwerking tussen lidstaten. Er ligt inmiddels een wetsvoorstel Cyberbeveiligingswet.
3. **EU Verordening Cyberweerbaarheid** Versterkt de rol van ENISA en introduceert een EU-breed certificeringskader voor ICT-producten, diensten en processen).
4. **Digital Operational Resilience Act (DORA)**: Specifiek gericht op de financiële sector, met nadruk op digitale weerbaarheid, risicobeheer en incidentrespons.
5. Het wetsvoorstel **Wet bevordering digitale weerbaarheid bedrijven** van 19 maart 2024 legt de taken en bevoegdheden van de minister van Economische Zaken en Klimaat (EZK) vast op het terrein van digitale weerbaarheid van niet-vitale bedrijven in Nederland, zoals het verwerken en verspreiden van informatie over kwetsbaarheden, dreigingen en incidenten en het samenwerken met andere bestuursorganen en organisaties.

8.2 Integratie van DORA en NIS2

Het naleven van zowel DORA als NIS2 is van cruciaal belang voor Nederlandse bedrijven die onder deze wetgevingen vallen. DORA kent een niveau van ICT-risicobeheer en ICT-gerelateerde incidentenrapportage dat strenger is dan NIS2, daarom vormt DORA een ‘lex specialis’ met betrekking tot NIS2, hetgeen betekent dat financiële entiteiten, bovenop NIS2, zullen moeten voldoen aan de strengere eisen van DORA.

8.3 Slotbeschouwing

Kritieke sectoren zoals energie, transport, en gezondheidszorg staan voor unieke uitdagingen op het gebied van cyberweerbaarheid. Het beschermen van deze sectoren tegen cyberdreigingen is essentieel voor de continuïteit en veiligheid van vitale diensten. Door gebruik te maken van specifieke richtlijnen en best practices, zoals die van ENISA, kunnen organisaties in deze sectoren hun cyberbeveiligingsmaatregelen versterken en de operationele continuïteit waarborgen

9. Cyberweerbaarheid in de keten van IT-leveranciers en partners

Om ervoor te zorgen dat ook leveranciers en andersoortige partners voldoen aan de vereisten van ketencyberweerbaarheid zonder dat ze zelf gecertificeerd zijn volgens NIS2 of ISO 27001, zullen organisaties een reeks aan maatregelen en benaderingen hiervoor moeten gaan hanteren, zoals gedetailleerde vragenlijsten en zelfbeoordelingen (denk o.a. in Nederland aan CYRA of Quality MARK die dat gecertificeerd bieden) initiatieven, ontwikkelen en/of laten invullen, periodieke beoordelingen en audits uitvoeren, en specifieke beveiligingsclausules opnemen in contracten. NIST SP 800-161 biedt uitgebreide richtlijnen voor Supply Chain Risk Management, die nuttig kunnen zijn voor het opzetten van dergelijke evaluatieprocessen. We beschrijven hierna enkele belangrijke stappen en methoden die kunnen worden gebruikt om leveranciers te evalueren en hun cyberveiligheidspraktijken te waarborgen:

9.1 Toetsing van leveranciers

I. **Leveranciersbeoordeling en due diligence**: In de hedendaagse digitale economie zijn organisaties steeds afhankelijker van hun leveranciers en partners voor het leveren van kritieke IT-diensten en -producten. Deze afhankelijkheid brengt echter ook aanzienlijke risico's met zich mee, vooral als het gaat om cyberveiligheid. Een zwakke schakel in de keten kan leiden tot ernstige beveiligingsincidenten die niet alleen de betrokken leverancier, maar ook de gehele keten en uiteindelijk de organisatie zelf treffen.

   Het waarborgen van cyberweerbaarheid binnen de toeleveringsketen is daarom essentieel. Dit begint bij een grondige leveranciersbeoordeling en due diligence-proces, wat ook contractueel is (in)geregeld. Hierbij zijn meerdere stakeholders binnen de organisatie betrokken, waaronder het inkoopteam, de IT-afdeling, en de compliance-afdeling. Het proces omvat het selecteren van leveranciers die voldoen aan de vastgestelde beveiligingseisen, evenals het continu monitoren en beoordelen van hun prestaties gedurende de gehele samenwerking.

II. Het antwoord op de vraag wie is verantwoordelijk voor de leveranciersbeoordeling is helder, dat is de leverancier zelf.

III. Welke vormen van inkoop/uitbesteding zijn er?
Als je de leveranciers niet wil dwingen tot externe assessments, dan zul je als klant zelf de gedetailleerde vragenlijsten moeten ontwikkelen en periodieke beoordelingen en audits uit moeten voeren, om de cyberveiligheidspraktijken van leveranciers te beoordelen en te evalueren. Binnen DORA is zelfs bepaald aan welke eisen deze assessments moeten voldoen.

IV. **a) Informatievragenlijst en zelfbeoordeling (self assessment)**:
Op basis van onze uitgebreide expertise in samenwerking met verschillende stakeholders, hebben wij een gedetailleerde vragenlijst ontwikkeld die leveranciers zouden kunnen invullen. Deze vragenlijst is ontworpen om ook te voldoen aan de eisen van NIS2 en DORA en behandelt de onder andere volgende aspecten:

- **Beveiligingsbeleid en -procedures**: Vraag naar de aanwezigheid van interne cyberveiligheidsbeleid en procedures.
- **Risicobeheer**: Informeer naar de methoden die worden gebruikt voor risicobeoordeling en -beheer.
- **Incidentbeheer**: Vraag naar de protocollen en processen voor incidentrespons.
- **Toegangscontrole**: Controleer op de aanwezigheid van maatregelen zoals Autorisatie matrixen, multifactor-authenticatie (MFA) en eventueel role-based access control (RBAC) implementatie.

Alternatief is dat leveranciers het self assessement doen bij bijvoorbeeld CYRA of Quality Mark en dat zij dan ook de audit op het assessment verzorgen. Of men kiest voor een IOS 27001 implementatietraject.

b) Training en bewustwording: Er is een groot aanbod aan examens en trainingen op het gebied van IT security. De belangrijkste zijn: TCSC, Firebrand, PECB, EC-Council, ISC2, SANS etc. In een aantal wordt ook aandacht besteed aan Cyberveiligheid, o.a.: CCISO, ISO, NIS2, Lead Auditor, etc. Informeer naar de trainingsprogramma's voor medewerkers op het gebied van cyberveiligheid.

V. Leveranciersbeoordelingsbezoeken en audits:

- Voer periodieke beoordelingen en audits uit bij leveranciers om de antwoorden in de vragenlijst te verifiëren en een grondige beoordeling van hun beveiligingspraktijken te krijgen.
- Besteed speciale aandacht aan fysieke beveiliging, netwerkbeveiliging en gegevensbescherming.

Contractuele vereisten en SLA's: voeg specifieke beveiligingsclausules toe aan contracten en stel duidelijke SLA's op die de verwachtingen rond cyberveiligheid specificeren .

Beveiligingsclausules in contracten:

- Voeg specifieke beveiligingsclausules toe aan contracten met leveranciers, waarin minimumeisen voor cyberveiligheid worden vastgelegd.
- Vereis dat leveranciers voldoen aan industriestandaarden en best practices, zelfs als ze niet gecertificeerd zijn.

Bron: *CIPS Contract Management Guide*.

Service Level Agreements (SLAs) & DAP's:

- Stel duidelijke SLA's op die de verwachtingen rond cyberveiligheid specificeren, inclusief reactie- en herstelacties bij incidenten.
- Definieer boetes of sancties bij niet-naleving van de afgesproken beveiligingsmaatregelen.

Bron: *ISACA Guidance on SLAs*.

1. **Continue monitoring en evaluatie**: Implementeer een proces voor continue risicobeoordeling en gebruik tools voor risicoanalyse en monitoring.
2. **Beoordeling van beveiligingsincidenten**: Vereis dat leveranciers beveiligingsincidenten onmiddellijk melden en voer post-incident evaluaties uit.

VI. Continue monitoring en evaluatie

1. **Continue risicobeoordeling**:
   - Implementeer een proces voor continue risicobeoordeling waarbij de beveiligingsstatus van leveranciers regelmatig wordt geëvalueerd.
   - Gebruik tools voor risicoanalyse en monitoring om real time inzicht te krijgen in de beveiligingsstatus van leveranciers.
   - **Bron**: *NIST SP800-30 Guide for Conducting Risk Assessments*, *ISO/EIC 27005 Information Security Risk Management* en *ENISA Cybersecurity Risk Management*.
2. **Threat intelligence en informatie-uitwisseling**:
   - Maak gebruik van threat intelligence-diensten om op de hoogte te blijven van potentiële dreigingen die van invloed kunnen zijn op leveranciers.
   - Neem deel aan informatie-uitwisselingsinitiatieven zoals ISACs (Information Sharing and Analysis Centers) om dreigingsinformatie te delen en te ontvangen.

   Bron: *ENISA Threat Intelligence Sharing*, *FS0ISAC* en *MITRE ATT&CK Framework*.

VII. Beoordeling van beveiligingsincidenten

1. **Incidentrapportage**:
   - Vereis dat leveranciers beveiligingsincidenten onmiddellijk melden en gedetailleerde rapporten verstrekken over de oorzaak, impact en herstelmaatregelen).
   - Analyseer incidentrapporten om patronen te identificeren en verbeteringen in het leveranciersbeoordelingsproces aan te brengen.

     Bron: *ISO/IEC 27035: Information Security Incident Management*.

2. **Post-incident evaluaties**:
    - Voer na elk incident een grondige evaluatie uit om te begrijpen wat er is gebeurd en welke maatregelen zijn genomen om toekomstige incidenten te voorkomen.
    - Werk samen met leveranciers om corrigerende maatregelen te implementeren en beveiligingslacunes te dichten.
    - Het evalueren van de cyberveiligheid van leveranciers zonder dat zij geaudit zijn volgens ISAE 3000/3402 en/of ISO 27001 vereist dus een grondige en systematische benadering. Door gebruik te maken van uitgebreide vragenlijsten, contractuele vereisten, continue monitoring en evaluatie, en incidentrapportage, kunnen organisaties ervoor zorgen dat hun leveranciers voldoen aan de noodzakelijke beveiligingsnormen en bijdragen aan de algehele cyberweerbaarheid van de keten. De integratie van de NIS2-richtlijn in nationale wetgeving legt een belangrijke basis voor het versterken van de cyberweerbaarheid binnen kritieke sectoren zoals energie, transport en digitale infrastructuur. Dit vereist een nauwe samenwerking tussen publieke en private sectoren om de continuïteit en veiligheid van de essentiële diensten te waarborgen.

      Bron: *NIST SP 800-61 Computer Security Incident Handling Guide*, *ENISA Supply Chain Security*, *ISACA Implementing the NIS2 Directive* en European Commission, *NIS2 Directive*.

9.2 Slotbeschouwing

De cyberweerbaarheid van organisaties is sterk afhankelijk van de beveiligingspraktijken van hun leveranciers en partners. Een grondige beoordeling en continue monitoring van leveranciers zijn cruciaal om te voorkomen dat zwakke schakels in de toeleveringsketen leiden tot beveiligingsincidenten. Door duidelijke beveiligingsvereisten vast te leggen in contracten en regelmatig audits uit te voeren, kunnen organisaties de risico's in hun toeleveringsketen effectief beheren en de algehele cyberweerbaarheid versterken.

10. Conclusie

10.1 De Noodzaak van geïntegreerde cyberweerbaarheid in Europa

In een tijdperk waarin digitale transformatie de ruggengraat vormt van economische en sociale ontwikkeling, staat Europa voor ongekende uitdagingen op het gebied van cyberveiligheid. De recente stortvloed aan Europese en nationale cyberwetten, waaronder de NIS2-richtlijn, de Digital Operational Resilience Act (DORA), en de EU Cybersecurity Act, benadrukt de dringende behoefte aan een samenhangende, grensoverschrijdende aanpak om de cyberweerbaarheid te versterken.

10.2 Nieuwe dreigingen en innovaties: AI en quantum computing

Het huidige landschap wordt echter verder gecompliceerd door de opkomst van nieuwe technologieën, met name kunstmatige intelligentie (AI) en quantum computing. De toenemende rol van AI in zowel offensieve als defensieve cyberoperaties roept vragen op over ethiek, regelgeving en veiligheid. De AI-wetgeving die momenteel in ontwikkeling is binnen de Europese Unie, is gericht op het reguleren van het gebruik van AI om risico's te beperken. Deze wetgeving wordt ingegeven door zorgen over de potentieel destructieve kracht van AI als deze in de verkeerde handen valt, evenals de angst voor onvoldoende beveiligde AI-systemen die kunnen worden misbruikt.

Tegelijkertijd staan we aan de vooravond van een quantum revolutie. Quantum computers hebben het potentieel om bestaande cryptografische methoden, die de basis vormen van huidige cybersecurity, te breken. Recentelijk heeft NIST (National Institute of Standards and Technology) nieuwe cryptografische standaarden gepubliceerd die bestand moeten zijn tegen aanvallen door quantum computers. Deze ontwikkelingen dwingen organisaties om vooruit te denken en hun beveiligingsstrategieën te herzien om voorbereid te zijn op een toekomst waarin quantum computers de norm worden.

10.3 De Europese reactie: harmonisatie en interoperabiliteit

Europa moet deze uitdagingen aangaan door een geïntegreerde benadering van cyberveiligheid te omarmen. Harmonisatie van regelgeving en interoperabiliteit tussen systemen zijn essentieel om te zorgen dat lidstaten effectief kunnen samenwerken. Het fragmentarische karakter van de huidige cybersecurity-infrastructuur belemmert de gezamenlijke inspanningen om cyberdreigingen het hoofd te bieden. Dit vereist niet alleen juridische uniformiteit, maar ook technologische integratie en gedeelde responsstrategieën.

10.4 De rol van technologie en topmanagement

In dit licht moeten organisaties investeren in geavanceerde technologieën, zoals Security Operations Centers (SOC), Security Information and Event Management (SIEM) en Security Orchestration, Automation and Response (SOAR). Deze systemen zijn cruciaal om proactief te kunnen reageren op bedreigingen, maar ook om snel herstel te realiseren na een incident.

Topmanagement speelt hierbij een cruciale rol. Zonder sterke leiderschap en betrokkenheid op het hoogste niveau blijven investeringen in cyberveiligheid gefragmenteerd en ineffectief. Het topmanagement moet niet alleen de middelen en strategische richting bieden, maar ook zorgen voor een cultuur van continue verbetering en bewustwording binnen de organisatie.

10.5 Conclusie: naar een veerkrachtig Europa

De toekomst van Europa's cyberweerbaarheid ligt in een geïntegreerde aanpak die nieuwe technologieën, zoals AI en quantum computing, incorporeert, terwijl ze tegelijkertijd een sterke juridische basis handhaaft. De publicaties van NIST zijn een eerste stap in de voorbereiding op de dreiging van quantum computers, maar er is nog veel werk te doen om de huidige systemen te upgraden en te beveiligen tegen deze dreiging.

10.6 Slotbeschouwing

De groeiende digitale transformatie binnen Europa biedt zowel enorme kansen als aanzienlijke risico's op het gebied van cyberveiligheid. Dit hoofdstuk heeft de noodzaak belicht van een geïntegreerde aanpak om de cyberweerbaarheid in Europa te versterken. De recente ontwikkelingen op het gebied van wet- en regelgeving, zoals de NIS2-richtlijn, DORA, en de EU Cybersecurity Act, onderstrepen de urgentie om een samenhangende en grensoverschrijdende strategie te ontwikkelen.

Daarnaast is er aandacht besteed aan de invloed van opkomende technologieën zoals kunstmatige intelligentie (AI) en quantum computing, die nieuwe uitdagingen en dreigingen met zich meebrengen. De AI-wetgeving binnen de EU probeert deze technologie te reguleren, terwijl de recente publicaties van NIST nieuwe cryptografische standaarden introduceren die bestand moeten zijn tegen de kracht van quantum computers.

Het hoofdstuk benadrukt verder het belang van harmonisatie van regelgeving, interoperabiliteit van systemen, en gezamenlijke responsstrategieën binnen de Europese Unie. Ook is de cruciale rol van geavanceerde technologieën zoals SOC, SIEM, en SOAR besproken, evenals de onmisbare betrokkenheid van het topmanagement om de veerkracht en veiligheid van de digitale infrastructuur te waarborgen.

De toekomst van Europa’s cyberweerbaarheid hangt af van een geïntegreerde en gecoördineerde inspanning, waarbij nieuwe technologieën en juridische structuren hand in hand gaan om de dreigingen van vandaag en morgen het hoofd te bieden.

Europa staat voor ongekende uitdagingen op het gebied van cyberveiligheid, vooral gezien de toenemende digitalisering en opkomst van nieuwe technologieën zoals AI en quantum computing. Een geïntegreerde en grensoverschrijdende aanpak is essentieel om de cyberweerbaarheid te versterken. Door te investeren in geavanceerde technologieën en sterke leiderschap te tonen, kunnen organisaties zich voorbereiden op de dreigingen van morgen en bijdragen aan een veiliger digitaal Europa. Het document benadrukt het belang van harmonisatie, interoperabiliteit, en de betrokkenheid van het topmanagement om de digitale infrastructuur te beschermen en veerkrachtiger te maken.

Bijlagen

B.1 NIS2 in de omringende landen

In dit overzicht staan de aanpassingen die zijn doorgevoerd voor de implementatie van de NIS2-richtlijn in de Benelux, Duitsland en Frankrijk:

Land	Aanpassingen en implementatie
België	In België is de wetgeving die NIS2 implementeert, op 26 april 2024 aangenomen en zal van kracht worden op 18 oktober 2024. Het Cyberfundamentals framework, ontwikkeld door het Centrum voor Cybersecurity België (CCB), speelt een integrale rol in de manier waarop bedrijven aan NIS2 moeten voldoen. Het framework biedt specifieke maatregelen en tools om de cyberweerbaarheid van organisaties te versterken en is afgestemd op de eisen van NIS2.
Nederland	Nederland werkt aan de transpositie van de NIS2-richtlijn door bestaande wetten aan te passen en nieuwe maatregelen te introduceren die aansluiten bij de richtlijn. Huidige status (augustus 2024): Het wetsvoorstel Cyberbeveiligingswet is al in consultatie geweest. Naar verwachting zal de Cyberbeveiligingswet in 2025 in werking treden, nadat deze door het parlement is behandeld. Organisaties die onder de Cyberbeveiligingswet vallen moeten vanaf dat moment aan de plichten voldoen. De nadruk ligt op het versterken van de cybersecurity in kritieke sectoren zoals energie, transport en digitale infrastructuur. Er wordt ook aandacht besteed aan het opstellen van richtlijnen voor de bescherming van de toeleveringsketen en de implementatie van incidentresponsprotocollen Ondertussen is ook de Wet bevordering digitale weerbaarheid bedrijven aangenomen in de eerste kamer voor die bedrijven die niet NIS2-plichting zijn. De auteur noemt dit wel “NIS2 lite”.
Luxemburg	Luxemburg volgt een soortgelijk pad als België en Nederland door bestaande nationale cybersecuritymaatregelen aan te passen aan de NIS2-richtlijn. Luxemburg richt zich op het uitbreiden van de reikwijdte van de regulering om nieuwe sectoren op te nemen en op het versterken van de samenwerking tussen publieke en private sectoren. Consultaties met belanghebbenden zijn aan de gang om een soepele transitie te garanderen
Duitsland	Duitsland heeft een conceptwet ingediend, de ‘*NIS2-Implementierungs- und Cybersicherheitsstärkungsgesetz*‘ (NIS2UmsuCG). Deze wet breidt de bestaande BSI-wet uit van 15 naar 65 secties, introduceert nieuwe categorieën van "bijzonder belangrijke" en "belangrijke" entiteiten, en specificeert uitgebreide

Land	Aanpassingen en implementatie
	maatregelen voor risicobeheer en incidentrespons. Er zijn strenge rapportageverplichtingen en hoge boetes bij niet-naleving. De wet treedt naar verwachting in werking op 1 oktober 2024
Frankrijk	Frankrijk werkt aan de transpositie van de NIS2-richtlijn door de bestaande cyberveiligheidswetten, zoals de Militaire Programmeringswet en de implementatie van NIS1, te harmoniseren met NIS2. De ANSSI (Franse nationale cyberveiligheidsautoriteit) speelt een centrale rol bij het opstellen en handhaven van de nieuwe regels. De nieuwe wetgeving zal sectorspecifieke vereisten bevatten voor onder andere energie, transport en financiële sectoren, en er worden aanvullende richtlijnen ontwikkeld voor de interactie met andere EU-wetgeving zoals de DORA-regeling).

Deze tabel geeft een overzicht van de voortgang en aanpassingen die zijn gedaan door de respectievelijke landen om de NIS2-richtlijn in hun nationale wetgeving te integreren. Elk land werkt aan specifieke aanpassingen om te voldoen aan de EU-deadline van oktober 2024.

B.2 Rationale Interessegroep Open standaarden KNVI

- **Definitie van open standaarden**: Open standaarden zijn specificaties die publiek beschikbaar zijn en ontwikkeld worden door middel van een samenwerkings- en consensusproces. Ze faciliteren interoperabiliteit en gegevensuitwisseling tussen verschillende producten en diensten en zijn bedoeld voor breed gebruik en acceptatie.

- De KNVI Interessegroep (IG) Open standaarden (KOS) zet zich in voor open management standaarden. Standaarden ondersteunen gegevensuitwisseling tussen informatiesystemen. De openheid zorgt ervoor dat iedereen de standaard kan gebruiken:

  Alle standaarden op de lijst van KOS zijn 'open'. Hiervoor hanteert de KOS vijf eisen waaraan een standaard moet voldoen om als 'open standaard' aangemerkt te worden. *(deels afkomstig van Forum van Open Standaarden):
  1. De benodigde documentatie moet laagdrempelig beschikbaar zijn.
  2. Er mogen geen hindernissen zijn op het terrein van intellectueel eigendomsrecht.
  3. Er moeten voldoende inspraakmogelijkheden zijn voor stakeholders tijdens de (door)ontwikkeling van de standaard.
  4. De onafhankelijkheid en duurzaamheid van de standaardisatieorganisatie moeten verzekerd zijn.
  5. Standaarden dienen interoperabiliteit te verbeteren.

- Het vijfde punt, dat standaarden moeten bijdragen aan **interoperabiliteit**, is specifiek toegevoegd door KOS.
  Motivatie voor de toevoeging:

  a) Interoperabiliteit is essentieel in een steeds meer gedigitaliseerde en verbonden wereld. Door dit criterium toe te voegen, benadrukt KOS dat open standaarden niet alleen vrij toegankelijk en duurzaam moeten zijn, maar ook moeten bijdragen aan de mogelijkheid om verschillende systemen en organisaties naadloos met elkaar te laten communiceren. Dit is van cruciaal belang om te voorkomen dat organisaties vast komen te zitten in silo's of afhankelijk worden van specifieke leveranciers, wat de flexibiliteit en keuzevrijheid zou beperken.
  b) KOS ziet interoperabiliteit als een hoeksteen van innovatie en samenwerking binnen de IT-sector. Door dit expliciet te maken als een eis voor open standaarden, zorgt KOS ervoor dat deze standaarden daadwerkelijk bijdragen aan een robuuste, flexibele en toekomstbestendige digitale infrastructuur.

- **Motivatie voor het Bestaansrecht van de KNVI Interessegroep Open standaarden (KOS)**
  De KNVI Interessegroep Open standaarden (KOS) vervult een cruciale rol binnen het Nederlandse en internationale landschap van

informatietechnologie door het bevorderen en ondersteunen van open standaarden. Dit bestaansrecht is gebaseerd op de volgende kernpunten:

1. **Faciliteren van interoperabiliteit en innovatie:** KOS zet zich in om interoperabiliteit tussen verschillende systemen te bevorderen, wat essentieel is in een tijd waarin de integratie van diverse IT-systemen een fundamentele vereiste is voor succesvolle digitale transformatie. Door te pleiten voor het gebruik van open standaarden, ondersteunt KOS innovatie en samenwerking tussen organisaties, zowel binnen als buiten Nederland.
2. **Toegankelijkheid en gelijkheid:** Een van de belangrijkste principes van open standaarden is dat ze publiekelijk beschikbaar en toegankelijk zijn voor iedereen. KOS bevordert deze openheid, waardoor organisaties van verschillende groottes, zonder hinder van intellectuele eigendomsrechten of hoge toegangskosten, gebruik kunnen maken van deze standaarden. Dit zorgt voor een gelijk speelveld en stimuleert inclusiviteit in de digitale economie.
3. **Inspraak en transparantie:** KOS benadrukt het belang van inspraakmogelijkheden voor stakeholders tijdens de ontwikkeling en doorontwikkeling van standaarden. Dit proces zorgt ervoor dat standaarden niet alleen technisch solide zijn, maar ook breed gedragen en toepasbaar in verschillende sectoren. Transparantie en betrokkenheid van alle belanghebbenden waarborgen dat de standaarden voortdurend evolueren om te voldoen aan de veranderende behoeften van de samenleving.
4. **Onafhankelijkheid en duurzaamheid:** KOS waarborgt dat de organisaties die verantwoordelijk zijn voor de ontwikkeling van open standaarden onafhankelijk opereren, wat cruciaal is voor het behouden van vertrouwen en het voorkomen van monopolies. De duurzaamheid van deze organisaties is eveneens van belang om ervoor te zorgen dat standaarden over de lange termijn beschikbaar blijven en worden onderhouden.
5. **Nationale en internationale relevantie:** In een tijd waarin digitale grensoverschrijdende samenwerking steeds belangrijker wordt, werkt KOS samen met nationale en internationale platforms, zoals het Forum Standaardisatie, om de adoptie en ontwikkeling van open standaarden te bevorderen. Dit versterkt de positie van Nederland als voorloper op het gebied van digitale standaarden en draagt bij aan een robuuste en interoperabele digitale infrastructuur.

B.3 De top 24 essentiële ‘cybersecurity frameworks’

In het dynamische digitale landschap van vandaag is het beschermen van gegevens en systemen van het grootste belang. @Andrey Prozorov van Patreon.com, heeft een lijst samengesteld met de 24 belangrijkste cyberframeworks die organisaties kunnen gebruiken om hun verdediging te versterken (lees hardenen) en veerkrachtige en wendbare operaties te garanderen. Deze verschillende frameworks bieden richtlijnen en ‘best practices’ om veilige informatiesystemen te onderhouden m.b.v. de PDCA-methodologie.

- NIST Cybersecurity Framework (CSF2.0)
- ISO/IEC 27001:2022
- COBIT (2019, Control Objectives for Information and Related Technologies)
- CIS Controls v8 (Center for Internet Security Controls)
- GDPR (General Data Protection Regulation, AVG in the Netherlands)
- HIPAA (Health Insurance Portability and Accountability Act, NEN 7510 in the Netherlands)
- PCI DSS (Payment Card Industry Data Security Standard)
- FISMA (Federal Information Security Management Act)
- SOX (Sarbanes-Oxley Act)
- NERC CIP (North American Electric Reliability Corporation Critical Infrastructure Protection)
- FedRAMP (Federal Risk and Authorization Management Program)
- ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection — Information security controls - essentially a detailed catalog of information security controls that might be managed through the ISMS (controls framework)
- ISO/IEC 27701, 27017 and 27018 are also important
- ISO/IEC 27032 — Guideline for cybersecurity
- ISO/IEC TS 27110 — Information technology, cybersecurity and privacy protection — Cybersecurity framework development guidelines
- ISO/IEC 27557 — Information security, cybersecurity and privacy protection — Application of ISO 31000:2018 for organizational privacy risk management
- ITIL (Information Technology Infrastructure Library)
- SWIFT Customer Security Programme (CSP)
- CMMC (Cybersecurity Maturity Model Certification)
- CSA (Cloud Security Alliance) STAR
- SANS Institute Security Policy Templates
- TISAX (Trusted Information Security Assessment Exchange)
- MITRE ATT&CK
- ANSSI (Agence nationale de la sécurité des systèmes d'information) Cybersecurity Guidelines
- BSIMM (Building Security In Maturity Model)

- SCF (Secure Controls Framework)
- OGC's IT4IT
- NIST SP 800-53
- IEC 62443 (operational technology)

B.3.1 Overige bronnen

Een stortvloed aan Europese en nationale cyberwetten!

Volgens de schrijver AE werkzaam bij ICT Recht te Utrecht (zie link hierboven naar het artikel) van het artikel op LinkedIn zijn er acht aspecten te onderscheiden waarmee hij de Digital Decade in het kader van cyberweerbaarheid nader uitwerkt:

- Mensgericht en inclusief
- Digitale identiteit
- Inhoud en expressie
- Infrastructuur en toegang
- Digitale economie en markten
- Data en privacy
- Cyber en weerbaarheid
- Digitale soevereiniteit

Bronnenoverzicht:

Er is gestreefd naar volledigheid echter gezien de inhoud van het stuk kan het zijn da we er inmiddels vergeten hebben te vermelden, waarvoor excuses.

1. **Internationale Voorbeelden van Cybersecurity**
   - NCSC rapporten en voorbeelden
   - ENISA Threat Landscape Reports
   - Ziegler, S. (2022). "Global Lessons in Cybersecurity"
2. **Samenwerkingsinitiatieven en Betrokken Organisaties**
   - European Union Agency for Cybersecurity (ENISA)
   - National Cyber Security Centre (NCSC)
3. **Verbeteringsvoorstellen voor Europese Cybersecurity**
   - Digital Operational Resilience Act (DORA)
   - Network and Information Systems Directive (NIS2)
4. **Platforms en Artikelen**
   - ENISA's jaarlijkse rapporten
   - UpGuard Blog: Cybersecurity Regulations in the European Union
   - Simpliant: NIST Cyber Supply Chain Risk Management Practices
5. **Leiderschap**
   - Zwiggelaar, "CIO 3.0"
   - Denning, S. (2018). "The Agile Organization"
6. **Planning**
   - ISO/IEC 27005 - Information Security Risk Management
   - NIST SP 800-30 - Guide for Conducting Risk Assessments
   - IEC 62443 - Security for Industrial Automation and Control Systems

7. **Ondersteuning**
    - ENISA richtlijnen en tools
    - SANS Institute, "Building a Security Awareness Program"
8. **Communicatieplannen Cybersecurity**
    - NIST SP 800-53 - Security and Privacy Controls for Information Systems and Organizations
9. **Operationele Planning en Beheersing**
    - Young, D. (2019). "The SIEM Handbook"
    - Collins, J. (2020). "Building a Modern Security Operations Center"
    - Cisco, "SOAR Implementation Guide" (2021)
10. **Prestatie-evaluatie**
    - ISO/IEC 27004 - Information Security Management - Monitoring, Measurement, Analysis, and Evaluation
    - ENISA audit frameworks
11. **Verbetering**
    - Boek **"Multidisciplinaire aspecten van digital security"**
    - ISO/IEC 27001:2022 - Continual Improvement
    - BIO2 en NEN7510 als specifieke normenkaders voor overheden en de zorg
    - ISO?IEC 27002:2022 – framework of controls as the basis for the IT architectuur
    - NIST SP 800-137 - Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
12. **Kritieke Infrastructuur en Cyberweerbaarheid**
    - Stouffer, K. (2021). "Critical Infrastructure Protection"
    - Health Sector Cybersecurity Coordination Center (HC3) Reports
13. **Cyberweerbaarheid in de Keten van IT-leveranciers**
    - NIST SP 800-161 - Supply Chain Risk Management Practices for Federal Information Systems and Organizations
    - ISACA's Guide to IT Supplier Relationships
14. **Conclusie**
    - ENISA's jaarlijkse rapporten
    - World Economic Forum's publicaties

De hoofdbronnen in APA format:

1. ENISA. (z.j.). *Supply Chain Security*. Geraadpleegd van [ENISA website] (https://www.enisa.europa.eu/)

2. ENISA. (z.j.). *Cybersecurity Risk Management*. Geraadpleegd van [ENISA website] (https://www.enisa.europa.eu/)

3. ENISA. (z.j.). *Threat Intelligence Sharing*. Geraadpleegd van [ENISA website] (https://www.enisa.europa.eu/)

4. European Commission. (2024). *NIS2 Directive*. Geraadpleegd van [European Commission website] (https://ec.europa.eu/)

5. ISO/IEC. (2016). *ISO/IEC 27035: Information Security Incident Management*. International Organization for Standardization.

6. ISO/EIC. (z.j.). *Information Security Risk Management (ISO/EIC 27005)*. Geraadpleegd van [ISO website] (https://www.iso.org/)

7. ISACA. (2023). *Implementing the NIS2 Directive*. ISACA Publications.

8. ISACA. (2023). *Guidance on SLAs*. ISACA Publications.

9. MITRE Corporation. (z.j.). *ATT&CK Framework*. Geraadpleegd van [MITRE website] (https://attack.mitre.org/)

10. NIST. (2022). *SP 800-30: Guide for Conducting Risk Assessments*. National Institute of Standards and Technology.

11. NIST. (2022). *SP 800-61: Computer Security Incident Handling Guide*. National Institute of Standards and Technology.

12. CIPS. (2023). *Contract Management Guide*. Chartered Institute of Procurement & Supply.

13. FS0ISAC. (z.j.). *FS0ISAC Resources*. Geraadpleegd van [FS0ISAC website] (https://www.fs0isac.com/)

B.4 Casestudies

Inleiding

In de huidige digitale wereld is cyberweerbaarheid niet alleen een vereiste, maar een strategische noodzaak voor organisaties die hun continuïteit willen waarborgen. Om de praktische toepassing van de aanbevelingen in dit paper te illustreren, presenteren we twee casestudies. Deze casestudies zijn geselecteerd om te laten zien hoe organisaties in verschillende sectoren succesvol hun cyberweerbaarheid hebben verbeterd door middel van gerichte strategieën en implementaties.

Doel van de casestudies:
Het hogere doel van deze casestudies is om praktische voorbeelden te bieden van hoe organisaties uitdagingen op het gebied van cybersecurity hebben aangepakt. Door deze voorbeelden te analyseren, willen we andere organisaties inspireren en richting geven bij het ontwikkelen en implementeren van hun eigen cybersecurity-strategieën. De casestudies benadrukken het belang van een proactieve en systematische aanpak om bedreigingen het hoofd te bieden en de algehele beveiligingsstatus te verbeteren.

Casestudy 1: Implementatie van ISO 27001 bij Bedrijf X

Context en doel:
Bedrijf X, een middelgrote organisatie in de financiële sector, kampte met een gebrek aan gestructureerde beveiligingsprocessen. Dit vormde een risico voor de vertrouwelijkheid, integriteit, en beschikbaarheid van gevoelige klantinformatie. Het hogere doel van deze casestudy is om te laten zien hoe de implementatie van ISO 27001 niet alleen de compliance met regelgeving kan verbeteren, maar ook de operationele efficiëntie en de algehele weerbaarheid van een organisatie tegen cyberdreigingen kan verhogen.

Uitdaging:
Voor de implementatie van ISO 27001 had Bedrijf X geen gestructureerde aanpak voor risicobeheer en incidentrespons. Dit leidde tot langere responstijden bij incidenten en een verhoogd risico op datalekken.

Oplossing:
Door een Information Security Management System (ISMS) op te zetten volgens de ISO 27001-normen, kon Bedrijf X duidelijke procedures ontwikkelen voor risicobeheer, incidentrespons en continue monitoring.

Resultaat:
Binnen zes maanden behaalde Bedrijf X de ISO 27001-certificering en verbeterde het de responstijd bij beveiligingsincidenten met 40%. Dit zorgde voor een aanzienlijke vermindering van risico's en verhoogde het vertrouwen van klanten in de organisatie.

Casestudy 2: Opzetten van een SOC bij Organisatie Y

Context en doel:
Organisatie Y, een belangrijke speler in de energiesector, zag zich geconfronteerd met een fragmentarische en reactieve incidentrespons, wat hun operationele continuïteit in gevaar bracht. Deze casestudy illustreert hoe het opzetten van een Security Operations Center (SOC) organisaties kan helpen om een proactieve benadering van cybersecurity te ontwikkelen. Het hogere doel is om te laten zien hoe een centraal SOC niet alleen de incidentrespons kan verbeteren, maar ook de algehele cyberweerbaarheid kan versterken.

Uitdaging:
Voor de oprichting van het SOC reageerde Organisatie Y vaak te traag op cyberdreigingen, waardoor het risico op schade aan kritieke infrastructuur toenam.

Oplossing:
Organisatie Y implementeerde een SOC met een volledig zicht op hun netwerkactiviteiten, waardoor bedreigingen in real-time konden worden gedetecteerd en aangepakt. Het SOC werd uitgerust met geavanceerde SIEM- en SOAR-tools om de dreigingsinformatie te verzamelen, analyseren en erop te reageren.

Resultaat:
De oprichting van het SOC leidde tot een vermindering van de incidentresponstijd met 50%, waardoor de beveiligingsstatus van de organisatie aanzienlijk verbeterde. Hierdoor kon Organisatie Y de impact van cyberaanvallen minimaliseren en de continuïteit van de kritieke infrastructuur waarborgen.

Conclusie:

Deze casestudies benadrukken het belang van een gestructureerde en proactieve aanpak van cybersecurity. Ze tonen aan dat met de juiste strategieën en tools, organisaties niet alleen hun compliance kunnen verbeteren, maar ook hun operationele veerkracht en beveiligingsstatus aanzienlijk kunnen versterken.

De achtergrond bij dit paper

Over Management Projects

De auteur Harry van der Plas heeft deze white paper geschreven vanuit zijn kennis zoals opgedaan bij Management projects, de werkmaatschappij van waaruit hij sinds 1989 zijn diensten aanbiedt op het gebied van security voor het MKB:

- ISO-lead implementator
- ISO-lead auditor (interne en externe audits)
- ISO 27001-transitie
- NIS2-begeleiding
- Virtuele CISO
- Interim IT manager

Over KNVI

De KNVI ondersteunt professionals met het ontwikkelen van hun kennis en het delen van kennis. De vereniging stimuleert professionals deze kennis te delen, onder meer via het schrijven van white papers. Dit white paper wordt gedeeld vanuit de Interessegroep Open Standaarden, en komt daarmee voor alle professionals beschikbaar.

KNVI, de Koninklijke Nederlandse Vereniging van Informatieprofessionals, is in Nederland hét platform voor Professionals in Informatiemanagement, Informatietechnologie en Informatievoorziening, waar iedere professional in deze disciplines zich thuis voelt. Informatie speelt een leidende rol speelt in de ontwikkeling van mens en maatschappij. Wij zien het dan ook als onze taak om de ontwikkeling van informatieprofessionals te bevorderen, door samen te werken, te faciliteren, elkaar te ontmoeten, focus aan te brengen en voorop te lopen. Daarbij houden we rekening met onze kernwaarden onafhankelijkheid, integriteit, professionaliteit.[2]

Over de interessegroep Open standaarden

Het doel van de interessegroep Open standaarden is om de professionals van KNVI te ondersteunen door een onafhankelijke verzameling van aanbevolen standaarden aan te bieden welke ook voldoen aan vooraf opgestelde criteria. Deze interessegroep sluit ook perfect aan op de overige interessegroepen omdat er standaarden van die onderwerpen in de lijst zullen staan zoals Architectuur, Beheer en servicemanagement, Informatiemanagement, Governance, etc. Daarnaast is het doel van de interessegroep om een open standaarden lijst te publiceren die open en vrij toegankelijk is om te raadplegen.

[2] https://www.knvi.nl/over-knvi

De ambitie van deze interessegroep is om het go-to punt te zijn voor professionals die op zoek zijn naar nieuwe standaarden in zijn of haar vakgebied maar goedgekeurd en aanbevolen door de KNVI.[3]

We werken altijd nauw samen met onze opdrachtgevers. Zo dragen we bij aan hun aanhoudende succes en maatschappelijke impact.

Over de ISO.org

Doelstellingen internationaal

De International Organization for Standardization (ISO) is een onafhankelijke, niet-gouvernementele internationale organisatie die normen ontwikkelt en publiceert om de wereldwijde handel te vergemakkelijken en te verbeteren. ISO heeft als doel om consensus te bereiken tussen belanghebbenden in verschillende sectoren, waaronder industrie, overheid, en consumenten, om zo normen te creëren die de kwaliteit, veiligheid, en efficiëntie van producten, diensten en systemen verhogen. Met meer dan 24.000 gepubliceerde normen bestrijkt ISO een breed scala aan onderwerpen, van technologie en energiebeheer tot voedselveiligheid en gezondheidszorg. De normen van ISO helpen bedrijven wereldwijd om best practices te implementeren, innovatie te bevorderen, en de toegang tot internationale markten te verbeteren.

Bron: ISO.org - About Us

Over NEN in Nederland

In Nederland vertegenwoordigt de NEN (Nederlandse Norm) ISO op nationaal niveau. NEN is de Nederlandse organisatie die verantwoordelijk is voor de ontwikkeling en implementatie van nationale en internationale normen. NEN werkt nauw samen met bedrijven, overheid, en maatschappelijke organisaties om normen te ontwikkelen die relevant zijn voor de Nederlandse context, terwijl ze ook bijdragen aan de harmonisatie van normen op internationaal niveau. De doelstellingen van NEN omvatten het ondersteunen van de concurrentiekracht van Nederlandse bedrijven, het bevorderen van duurzaamheid, en het verbeteren van de kwaliteit van producten en diensten. NEN is tevens betrokken bij de implementatie van Europese richtlijnen en speelt een sleutelrol in het bevorderen van de adoptie van ISO-normen in Nederland, zodat Nederlandse bedrijven internationaal concurrerend blijven.

Bron: NEN - *Over NEN*

[3] https://www.knvi.nl/interessegroep/open-standaarden

Over de auteur

Professionele Samenvatting: *Harry van der Plas*

Eigenaar van Management Projects bv en voorzitter van de KNVI-interessegroep Open standaarden (waaronder ook BiSL valt).

Naast echtgenoot van Rianne, vader van vier zonen, en grootvader van momenteel vijf kleinkinderen, is Harry momenteel als zelfstandige werkzaam als vCISO, ISO lead en ISO auditor (intern & extern) en in de rol CliëntISO - een soort security bruggenbouwer - voor een grote retailer en zijn opdrachtgever de IT-dienstverlener. Daarnaast beschikt hij over een indrukwekkende ervaring in 38 jaar IT waarvan o.a. 30 jaar als CIO en CEO van Newway, een Retail-ERP-softwarebedrijf. Als initiator van het Keurmerk Betrouwbare Afrekensystemen is Harry gevraagd om voorzitter te worden van de KNVI-interessegroep Open standaarden. Hij heeft deze rol met verve op zich genomen en heeft actief gewerkt aan het samenbrengen van alle relevante partijen. Zijn aanpak is resultaatgericht, waarbij hij de kwaliteiten binnen organisaties optimaal inzet om succesvolle projecten te realiseren.