



**VERDONCK
KLOOSTER &
ASSOCIATES**

A HIGHBERG COMPANY

 **JPR**
advocaten

Webinar NIS2

Koos van der Spek
Yaşar Bayram
Luuk Wassink
Dorus-Jan ten Boom

Webinar NIS 2

Yaşar Bayram & Luuk Wassink
8 juni 2023



Overzicht

1. Waarom de NIS 2 als opvolger van de NIS 1?
2. Toepassingsbereik
3. Beveiligingsplicht
4. Meldplicht
5. Informatieplicht
6. Handhaving & toezicht
7. Boetes
8. De toekomst



Netwerk- en Informatiebeveiligingsrichtlijn

Betrekking op cybersecurity of cyberveiligheid

In Nederland geïmplementeerd in de:

1. Wet beveiliging netwerk- en informatiesystemen (Wbni)
2. Besluit beveiliging netwerk- en informatiesystemen (Bbni)



Waarom de NIS 2?

Aanleiding NIS 1:

- Toenemende digitalisering
- Toename cyberincidenten
- Maatschappelijke ontwrichting
- Schade economie

Aanleiding NIS 2:

- Implementatieverschillen NIS 1
- Uitbreiding cyberdreigingslandschap
- Implementatie uiterlijk 17 oktober 2024



Door NU.nl

13 mei 2021 om 09:17

14 reacties



Het Amerikaanse oliebedrijf Colonial Pipeline heeft zijn systemen herstart, nadat het vorige week door een cyberaanval werd getroffen. Dat meldt onder meer [CNBC](#). Volgens Colonial duurt het nog enkele dagen voordat de pijplijnen weer naar behoren functioneren.



Door Elisa Heisen

03 feb 2022 om 10:17
Update: een jaar geleden

137 reacties



Opslagbedrijf EVOS kampt met problemen in de haven van Terneuzen na een cyberaanval. Het laden en lossen van olie loopt vertraging op, zegt een woordvoerder van het bedrijf donderdag in reactie op vragen van NU.nl.

Toepassingsbereik 1/4

NIS 2 van toepassing op:

1. Publieke of particuliere entiteiten;
2. Uit de zeer kritieke of andere kritieke sector;
3. Zijnde middelgrote organisaties of groter;
4. Die diensten verlenen of activiteiten verrichten in de EU



Toepassingsbereik 2/4

| | | |
|-----------------------|--|---|
| Essentiële entiteiten | Grote organisaties Meer dan 250 werkzame personen of jaaromzet hoger dan 50 miljoen Euro of balanstotaal hoger dan 43 miljoen Euro | Middelgrote organisaties <ol style="list-style-type: none">1. 50 tot 250 werkzame personen; en2. Jaaromzet tussen de 10 en 50 miljoen Euro; en3. Balanstotaal tussen de 10 en 43 miljoen Euro |
| | Zeer kritieke sectoren Bijvoorbeeld de sectoren: Energie, vervoer, bankwezen, gezondheidszorg en overheid | Andere kritieke sectoren Bijvoorbeeld de sectoren: Post- en koeriersdiensten, Afvalstoffenbeheer, vervaardiging chemische stoffen en productie levensmiddelen |

Toepassingsbereik 3/4

| Zeer kritieke sectoren | Andere kritieke sectoren |
|---|---|
| Energie (elektriciteit (waaronder elektriciteitsbedrijven, elektriciteitsproducenten, energieopslagdiensten, elektriciteitsmarktbeheerders en laaddiensten); stadsverwarming en -koeling; aardolie; aardgas en waterstof) | Post- en koeriersdiensten |
| Vervoer (lucht, spoor, water en weg) | Afvalstoffenbeheer |
| Bankwezen | Vervaardiging, productie en distributie van chemische stoffen |
| Infrastructuur voor de financiële markt | Productie, verwerking en distributie van levensmiddelen |
| Gezondheidszorg (zorgaanbieders, EU-referentielaboratoria, onderzoeks- en ontwikkelingsactiviteiten m.b.t. geneesmiddelen, farmaceutische basisproducten en bereidingen, medische hulpmiddelen voor volksgezondheid noodsituaties) | Vervaardiging van medische hulpmiddelen, informatica-, elektronische en optische producten, elektrische apparatuur, machines, apparaten en werktuigen, motorvoertuigen, aanhangers en opleggers en andere transportmiddelen |
| Levering en distributie van drinkwater | Digitale aanbieders van online marktplaatsen, onlinezoekmachines en platforms voor socialenetwerkdiensten |
| Afvalwater | Onderzoeksorganisaties |
| Digitale infrastructuur (internetknooppunten, DNS-dienstverleners, topleveldomeinnamen registers, cloudcomputingdiensten, datacenterdiensten, netwerken voor levering inhoud, vertrouwensdiensten, openbare elektronischecommunicatienetwerken, openbare elektronischecommunicatiediensten) | |
| Beheer ICT-diensten (beheerde diensten, beheerde beveiligingsdiensten) | |
| Overheid (centraal en regionaal) | |
| Ruimtevaart | |

Roodgekleurde sectoren zijn nieuw ten opzichte van de NIS 1. Dit is een versimpelde weergave van Bijlage 1 en 2 van de NIS 2



Toepassingsbereik 4/4

NIS 2 is in ieder geval van toepassing op:

- Aanbieders van elektronische communicatienetwerken of –diensten
- Aanbieders van vertrouwensdiensten
- Registers voor topleveldomeinnamen
- Verleners van domeinnaamregistratiediensten
- Aanbieders van diensten essentieel voor instandhouding kritieke maatschappelijke of economische activiteiten
- Specifiek aangewezen overheidsinstanties



Beveiligingsplicht

NIS 1 eisen:

- Passende en evenredige technische en organisatorische maatregelen betreffende risicobeheersing
- Voorkomen en minimaliseren van gevolgen van incidenten

NIS 2 voegt daaraan toe:

- Governance = verantwoordelijk bestuur
- Risicogebaseerde maatregelen rekening houdend met de stand v.d. techniek, normen en uitvoeringskosten
- Beveiliging fysieke omgeving
- Concrete basismaatregelen
- Beveiliging toeleveringsketen



Meldplicht

NIS 1 eisen:

- Alleen incidenten melden met daadwerkelijke schade
- Onverwijld melden aanzienlijke en substantiële gevolgen
- Geen verhoogde aansprakelijkheid door melding

NIS 2:

- Reikwijdte **incident** verruimd: gebeurtenis die authenticiteit, integriteit, vertrouwelijkheid of beschikbaarheid van gegevens of diensten in gevaar brengt
- **Significant** indien:
 - 1) ernstige operationele verstoring van diensten of financiële verliezen voor betrokken entiteit veroorzaakt of kan veroorzaken; of
 - 2) andere (rechts)personen heeft getroffen of kan treffen via aanzienlijke (im)materiële schade
- Eerste melding binnen 24 uur, tweede binnen 72 uur en een eindverslag binnen een maand
- Ieder significant incident melden aan CSIRT of bevoegde autoriteit



Informatieplicht

Essentiële en belangrijke entiteiten moeten ontvangers van hun diensten informeren over:

1. Alle maatregelen of voorzieningen die hun ter beschikking staan om risico's die voortvloeien uit een significante cyberdreiging te beperken
2. De dreiging zelf, als de significante cyberdreiging waarschijnlijk tot incidenten zullen leiden

Significante cyberdreiging:

een cyberdreiging waarvan op basis van de technische kenmerken kan worden aangenomen dat zij ernstige gevolgen kan hebben voor de **netwerk- en informatiesystemen** van een entiteit of de gebruikers van de diensten van de entiteit door het veroorzaken van **aanzienlijke materiële of immateriële schade**;



Handhaving & toezicht

NIS 1 eisen:

- Bevoegdheden en middelen voor bevoegde autoriteiten
 - Informatie opvragen, audits, bindende aanwijzingen, publiek informeren over incident
 - Doeltreffende, evenredige en afschrikwekkende sancties
- Sectoraal toezicht met bestuursrechtelijke handhaving

NIS 2 voegt daaraan toe:

- Lidstaten moeten zorgen voor **effectief** toezicht en nemen van **noodzakelijke** maatregelen
- **Proactief** toezicht op essentiële entiteiten
- **Reactief** toezicht op belangrijke entiteiten
- Verzwaarde maatregelen en sancties voor essentiële entiteiten
- Bestuurdersaansprakelijkheid bij essentiële entiteiten



Boetes

- Stevige aanscherping van de boetes
- Past in de lijn van de AVG

Essentiële entiteiten:

- Maximumbedrag van ten minste 10 miljoen euro of 2% van de wereldwijde jaaromzet

Belangrijke entiteiten:

- Maximumbedrag van ten minste 7 miljoen euro of 1,4% van de wereldwijde jaaromzet



Belangrijkste veranderingen

- NIS 2 van toepassing op meer instanties
- Uitgebreidere beveiligingsmaatregelen
 - O.a. rol van bestuurders uitgebreid en beveiligen toeleveringsketen
- Geen daadwerkelijke schade meer vereist voor meldplicht
- Klanten informeren bij significante cyberdreiging
- Verzwaarde handhaving, hogere boetes en bestuurdersaansprakelijkheid



De toekomst

| | | | |
|--|-----------|-------------|----------------|
| RICHTLIJN (EU) 2022/2555 VAN HET EUROPEES PARLEMENT EN DE RAAD van 14 december 2022 betreffende maatregelen voor een hoog gezamenlijk niveau van cyberbeveiliging in de Unie, tot wijziging van Verordening (EU) nr. 910/2014 en Richtlijn (EU) 2018/1972 en tot intrekking van Richtlijn (EU) 2016/1148 (NIS 2-richtlijn) | 2022/2555 | 17-okt-2024 | Niet op schema |
|--|-----------|-------------|----------------|

- Uiterlijk 17 oktober 2024 geïmplementeerd in Nederland
- Zomer 2023 internetconsultatie
- Inwerkingtreding implementatiewet eind 2024 verwacht

Begin op tijd met de voorbereidingen op NIS 2, zodat je:

- Gegevens en systemen van de organisatie en relaties beschermt
- Het risico op dure beveiligingsincidenten vermindert
- De cyberweerbaarheid van de organisatie verbetert
- De reputatie van de organisatie beschermt





Mr. H.F. de Boerlaan 34
7417 DB Deventer
+31 (0)88 616 00 10



Koopmanslaan 4
7005 BK Doetinchem
+31 (0)88 616 00 20



Euclideslaan 1
3584 BL Utrecht
+31 (0)88 616 00 40



Mr. Yaşar Bayram
Advocaat
Bayram@jpr.nl

+31 682 09 19 96



**VERDONCK
KLOOSTER &
ASSOCIATES**

A HIGHBERG COMPANY

NIS2 implementatie

Koos van der Spek

8-6-2023

Welke maatregelen moet ik nu nemen?

Hoe pak ik dit aan?

Artikel 21 van de NIS2 geeft een globaal overzicht van cybersecurity maatregelen die minimaal genomen moeten worden.

Wat is er al?

Artikel 21

Maatregelen voor het beheer van cyberbeveiligingsrisico's

1. De lidstaten zorgen ervoor dat essentiële en belangrijke entiteiten passende en evenredige technische, operationele en organisatorische maatregelen nemen om de risico's voor de beveiliging van de netwerk- en informatiesystemen die deze entiteiten voor hun werkzaamheden of voor het verlenen van hun diensten gebruiken, te beheren en om incidenten te voorkomen of de gevolgen van incidenten voor de afnemers van hun diensten en voor andere diensten te beperken.

Rekening houdend met de stand van de techniek en, indien van toepassing, de desbetreffende Europese en internationale normen, alsook met de uitvoeringskosten, zorgen de in de eerste alinea bedoelde maatregelen voor een beveiligingsniveau van de netwerk- en informatiesystemen dat is afgestemd op de risico's die zich voordoen. Bij de beoordeling van de evenredigheid van die maatregelen wordt naar behoren rekening gehouden met de mate waarin de entiteit aan risico's is blootgesteld, de omvang van de entiteit en de kans dat zich incidenten voordoen en de ernst ervan, met inbegrip van de maatschappelijke en economische gevolgen.

2. De in lid 1 bedoelde maatregelen zijn gebaseerd op een benadering die alle gevaren omvat en tot doel heeft netwerk- en informatiesystemen en de fysieke omgeving van die systemen tegen incidenten te beschermen, en omvatten ten minste het volgende:

- a) beleid inzake risicoanalyse en beveiliging van informatiesystemen;
- b) incidentenbehandeling;
- c) bedrijfscontinuïteit, zoals back-upbeheer en noodvoorzieningsplannen, en crisisbeheer;
- d) de beveiliging van de toeleveringsketen, met inbegrip van beveiligingsgerelateerde aspecten met betrekking tot de relaties tussen elke entiteit en haar rechtstreekse leveranciers of dienstverleners;
- e) beveiliging bij het verwerven, ontwikkelen en onderhouden van netwerk- en informatiesystemen, met inbegrip van de respons op en bekendmaking van kwetsbaarheden;
- f) beleid en procedures om de effectiviteit van maatregelen voor het beheer van cyberbeveiligingsrisico's te beoordelen;
- g) basispraktijken op het gebied van cyberhygiëne en opleiding op het gebied van cyberbeveiliging;
- h) beleid en procedures inzake het gebruik van cryptografie en, in voorkomend geval, encryptie;
- i) beveiligingsaspecten ten aanzien van personeel, toegangsbeleid en beheer van activa;
- j) wanneer gepast, het gebruik van multifactor-authenticatie- of continue-authenticatieoplossingen, beveiligde spraak-, video- en tekstcommunicatie en beveiligde noodcommunicatiesystemen binnen de entiteit.

3. De lidstaten zorgen ervoor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), van dit artikel passend zijn, rekening houden met de specifieke kwetsbaarheden van elke rechtstreekse leverancier en dienstverlener en met de algemene kwaliteit van de producten en de cyberbeveiligingspraktijken van hun leveranciers en dienstverleners, met inbegrip van hun veilige ontwikkelingsprocedures. De lidstaten zorgen er ook voor dat de entiteiten, wanneer zij overwegen welke maatregelen als bedoeld in lid 2, punt d), passend zijn, rekening moeten houden met de resultaten van de overeenkomstig artikel 22, lid 1, uitgevoerde gecoördineerde beveiligingsrisico-beoordelingen van kritieke toeleveringsketens.

4. De lidstaten zien erop toe dat een entiteit die vaststelt dat zij niet voldoet aan de in lid 2 bedoelde maatregelen, onverwijld alle noodzakelijke, passende en evenredige corrigerende maatregelen neemt.

Wat is er al – een overzicht

Vanuit de WBNI was er al een implementatieplicht voor een kleinere groep organisaties. Deze groep is nu aanzienlijk groter geworden zoals we in het voorgaande hebben gezien.

De NIS2 verwijst nadrukkelijk naar het gebruik van erkende standaarden voor de implementatie.

Onderstaand tref je een overzicht van de meest gebruikte en bekendste standaarden voor de implementatie van beveiligingsmaatregelen aan.

- ISO27001 en 2: overwegend voor kantoorautomatisering
- NEN7510: voor de zorgsector
- BIO: voor de overheid
- IEC62443: voor procesautomatisering en productiefaciliteiten
- CSIR: specifiek voor Rijkswaterstaat en Waterschappen
- NIST
- ISO31000 voor riskmanagement
- ISO22301 voor business continuïteit
- etc

Wat is vanuit de NIS2 gezien nu het belangrijkste? Hoe te beginnen?

Hoofdzaken uit NIS2

- **Basis op orde**
- **Risicogebaseerd**
- **Continuïteit**
- **Incident Respons**
- **Certificering**

Maatregelen nemen volgens de laatste stand van de techniek → trends volgen!



Basis op orde

Doel: voorzien in een minimale set aan beveiligingsmaatregelen

Aanpak

- Informatiebeveiligingsbeleid
 - Voor zowel IT als OT
- Awareness training en bewustwording (ook voor bestuurders)
 - phishingcampagnes
- Identiteit en Toegangsbeheer + **MFA**: wie heeft toegang tot welke applicatie/data
 - Vaststellen van rollen en toekennen van autorisaties aan deze rollen
- Segmentering: netwerk opdelen in kleinere delen
- Malware scanning
- Monitoring: weten wie er op je netwerk, systemen en applicaties zit.
- Software updates en Patching: kwetsbaarheden wegnemen
- Encryptie: gegevens tijdens transport en bij opslag beveiligen
- Ook aandacht voor fysieke toegangsbeveiliging

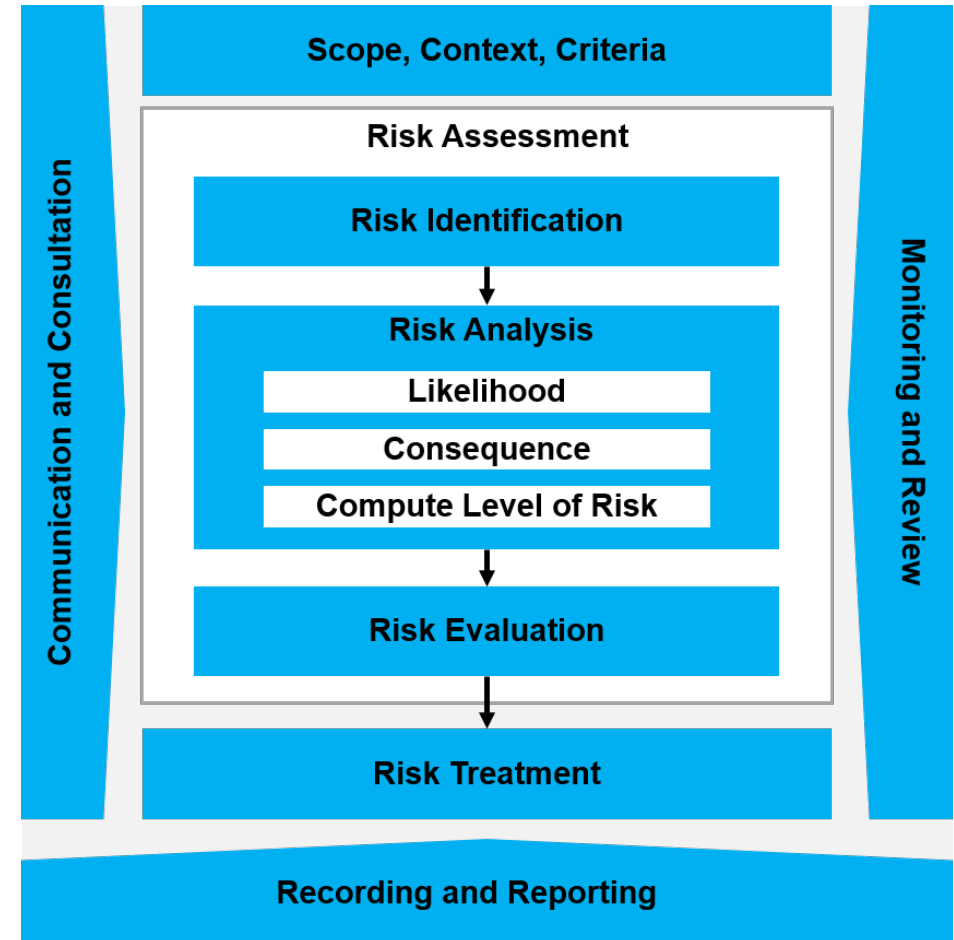


Risicogebaseerd

Doel: Inzicht in de risico's om beschikbare middelen (budget) zo efficiënt mogelijk in te zetten voor het mitigeren van de grootste risico's.

Aanpak

- Risk Appetite vaststellen
 - Verwachting dat je als essentiële entiteit daar geen vrije keuze in hebt
- Risicoanalyses uitvoeren
- Stel vast waar de grootste risico's liggen en neem passende maatregelen om deze te mitigeren

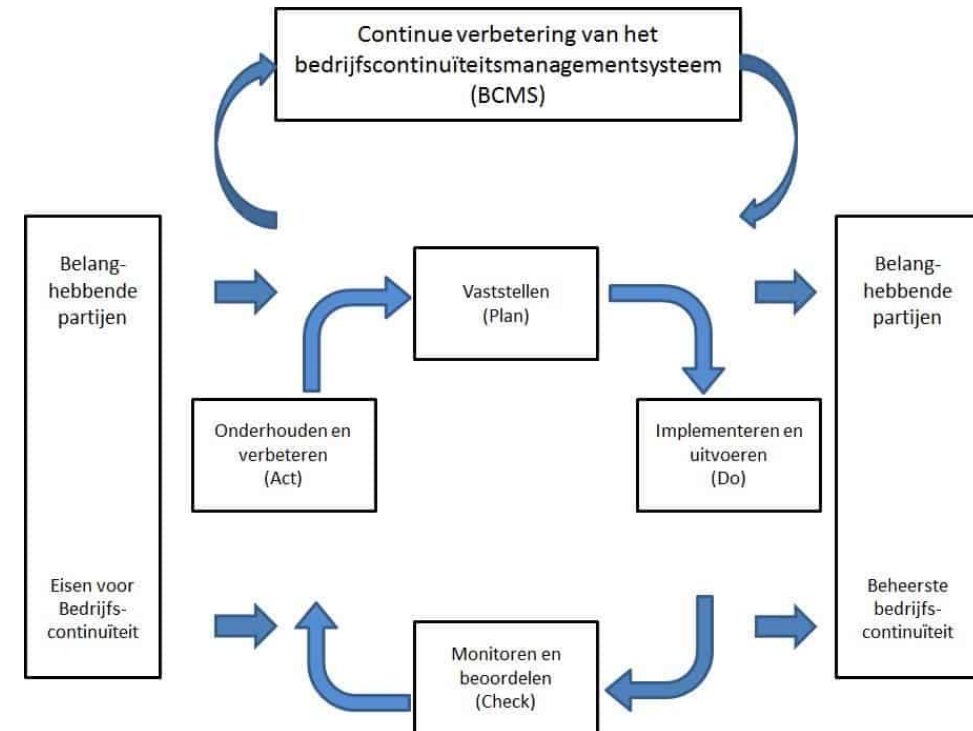


Borgen bedrijfscontinuïteit

Doel: Continuïteit van bedrijfsprocessen borgen door voorbereid te zijn op verstoringen

Aanpak

- Uitvoeren business impact analyses voor het vaststellen van kritieke bedrijfsprocessen en onderliggende kritieke systemen en applicaties
- Opstellen Business Continuity Plan
- Opstellen crisismanagementplan en inrichten crisisteams
- Oefenen cybersecurity crisis



Incident Respons



Bron: NCSC

Doel: Effectief reageren op incidenten

Stappen in het incident respons proces:

- **Preparation** (voorbereiding): Nemen van preventieve maatregelen om schade door succesvolle aanvallen te beperken
- **Identification** (identificatie): Vaststellen aard en omvang van de aanval
- **Containment** (inperking): Nemen van acties om verdere verspreiding te voorkomen
- **Eradication** (eliminatie): Wegnemen van kwetsbaarheden die de aanvallers hebben misbruikt om toegang te krijgen
- **Recovery** (herstel): Herstellen van de oude situatie
- **Lessons Learned**: Evaluatie met leerpunten van de aanval

Bovenstaande stappen kunnen, evenals monitoring, worden ondersteund door een SOC dienst: uitbesteed, hybride of zelf.

Daarnaast meldingsproces inregelen voor het verplicht melden van cybersecurity incidenten.

Certificering

Doel: Onafhankelijk beoordeling van de betrouwbaarheid van producten en diensten

Aanpak

Certificering conform bekende standaarden:

- ISO27001 voor kantoorautomatisering
- IEC62443 voor procesautomatisering
- ISO22301 voor business continuïteit
- Common Criteria
- Baseline Security Product Assessment door het Nationaal Bureau voor Verbindingsbeveiliging (NBV) van de AIVD
- Rijksinspectie Digitale Infrastructuur (RDI) als Nationale Cybersecuritycertificeringsautoriteit (NCCA)

Met name voor dienstverleners van belang om te voorkomen dat ze per opdrachtgever een eisenlijst krijgen.

Ook voor de **toeleveringsketen** en leveranciers van producten en diensten. **Ketenafhankelijkheid** is hierbij een belangrijk onderdeel.



BELANG VAN DE BESTUURDER

- SAFETY: Voorkomen levensbedreigende situaties
- CONTINUÏTEIT: Geen verstoringen productieproces
- Voldoen aan wetgeving
- Geen ongewenste modificaties
- Geen herstel- of terugoproepacties
- Geen schadeclaims
- Voorkomen reputatieschade
- Aandacht voor ketenafhankelijkheid (Supply Chain)

**MAATSCHAPPELIJKE
WAARDEN**

- Geen risico's voor mensen
- Veilige productie en productieprocessen
- Geen ongewenste modificaties in producten; voorkomen gezondheidsrisico's
- Voorkomen groot schalige economische schade
- Voorkomen maatschappelijk ontwrichting als gevolg van uitval vitale sectoren



Cybersecurity voor Industriële Automatisering

waar de fysieke en digitale wereld samenkomen

VISIE OP BEVEILIGING VAN INDUSTRIËLE SYSTEMEN

- Risico gebaseerde aanpak
- Focus op Assets: beveiliging van objecten
- Focus op informatie: bij integratie van OT met andere omgevingen
- Zorg voor een integrale aanpak van fysieke beveiliging en logische toegangsbeveiliging
- Scherm industriële systemen af:
 - Zonering en Segmentatie
 - Unidirectional Security Gateways
 - Defence in Depth
- Richt life-cycle management in; vervang zo mogelijk oude en kwetsbare systemen/applicaties
- Pas best practices uit ICT beveiliging toe waar dit mogelijk is:
 - Ken de beperkingen van OT-systemen
 - Richt beheerprocessen, verantwoordelijkheden en governance in
 - Voer 'threat intelligence' in
- Zorg voor regulering van de verkeerstromen tussen de domeinen IT, OT en IIOT: werk een datamanagement strategie uit



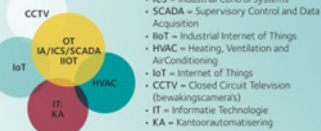
CYBERSECURITY FOCUS

- In procesautomatisering van oudsher veel nadruk op fysieke (toegangs)beveiliging. (Toegangscontrole is ook digitaal)
- Koppeling OT - IT (kantooromgeving) geeft verhoogde kans op cybersecurity risico's
- Groeiend aantal verbindingen / connecties doet complexiteit toenemen
- Risico procesautomatisering is risico IT plus risico OT (optisim risico)
- Menselijke factor is ook in OT omgevingen het grootste risico
- Verschuiving Safety naar Security (kan ook safety mee genoemd zijn)

Actieplan

1. Bepaal risico's op Assets en Informatie (prioritering, Quick Wins)
2. Zorg voor draagvlak bij het management (sponsorship)
3. Zorg voor Cybersecurity Awareness bij alle medewerkers
4. Stel een toetskader op met cybersecurity eisen waaraan de OT omgeving moet voldoen
5. Check de OT omgeving op het toetskader en verwerk tekortkomingen in een implementatieplan
6. Denk vanuit een architectuur gedachte aan de mens, processen en technologie
7. Scherm OT omgevingen zo goed mogelijk af (Zonering en Segmentatie, Defence in Depth)
8. Voer Patchmanagement waar mogelijk uit
9. Vervang zonodig 'oude' systemen/applicaties waarmee een hoog risico gelopen wordt
10. Maak offline backups en richt restore in
11. Implementeer actieve monitoring
12. Zorg voor een goed ingeredeld storingsmeldings- en respons proces
13. Richt crisismanagement in
14. Leg relatie met business continuity management
15. Oefen het storingsmeldings- en respons proces (en crisismanagement)

SAMENHANG



- OT = Operational Technology
- IA = Industriële Automatisering
- ICS = Industrial Control Systems
- SCADA = Supervisory Control and Data Acquisition
- IIoT = Industrial Internet of Things
- HVAC = Heating, Ventilation and AirConditioning
- IIoT = Internet of Things
- CCTV = Closed Circuit Television (bewakingscamera's)
- IT = Informatie Technologie
- KA = Kantoorautomatisering

NORMEN, STANDAARDEN EN HANDREIKINGEN

- NIST SP 800-82 - Guide to Industrial Control Systems (ICS) Security
- ISO27018 - Information Security for the Energy Utility Industry
- ISA99 - Industrial Automation and Control Systems Security
- IEC 62351 - Security Standards for the Power System Information Infrastructure
- IEC 62443 - Cybersecurity for Industrial Automation and Control Systems (IACS)
- NCSG - Checklist beveiliging van ICS / SCADA systemen
- NCSG - Uw ICS/SCADA- en gebouwbeheersystemen online
- ENISA - Communication network dependencies for ICS/SCADA Systems

IT VERSCHILLEN IT EN OT OMGEVINGEN

| | | |
|-----------------------|----------------------------------|--|
| 1,5 tot 4 jaar | levensduur | 10 tot 30 jaar |
| informatieverwerking | focus op | fysieke industriële systemen |
| kantoorwerkplekken | in bedrijf | real time, 7x24 uur |
| generiek en vaak | hackaantallen | specifiek/doelgericht |
| dataverlies | gevolgen hackaanval | fysieke schade / kans op slachtoffers / economische schade |
| persoonlijk | gebruikersaccount | geen of gemeenschappelijk blijft lang(er) onontdekt |
| wordt sneller ontdekt | malware | bijna geen updates of patches zelden afzonderlijke OTAP |
| vaak | updates en patches | veel maatwerk |
| afzonderlijke OTAP | ontwikkel en testomgeving (OTAP) | veel leveranciers |
| hoge mate | standaardisatie | veel leveranciers |
| veel | leveranciers | veel beperkt |
| veel | beschikbare kennis | neemt toe |
| veel | internetconnectiviteit | op locatie |
| datacenter / cloud | dataverwerking | |

TOEKOMST

- Ontwikkelingen die impact hebben op cybersecurity:
- Toename genestwerkte omgevingen:
 - "always connected": anywhere, anytime, anything
 - Industry 4.0, OT, IIoT en Cloud Computing
 - Nieuwe toepassingen
 - IIoT: contactloze sloten, (bewakings)camera's, temperatuursensoren etc. gekoppeld aan de kantooromgeving en/of internet
 - IIoT: sensoren en connecties van de fysieke productieomgevingen (OT) naar de informatieverwerkende (IT) omgevingen
 - Integratie van bediening en besturingsplakaten (van ERP /m machine niveau)
 - Toename ketenleveranciers en security risico's in de keten
 - Commodity: nieuwe technologieën worden steeds meer gemeengoed, bijv. in de medische wereld
 - In-control zijn/governance: voldoen aan (nieuwe) wetgeving en dit zowel in beleid als in de praktijk laten zien
 - IT - OT Big Data analytics, GS, Forecasting, bijv. ook: weersvoorspelling

Meer info:

<https://www.vka.nl/publicaties/poster-cybersecurity-voor-industriële-automatisering/>

**VERDONCK
KLOOSTER &
ASSOCIATES**

Koos van der Spek MSc CISSP CPP CISA
Management Consultant Cybersecurity

+31 6 22 19 70 31
koos.vanderspek@vka.nl

Baron de Coubertinlaan 1
2719 EN Zoetermeer
Tel 079 368 1000
www.vka.nl

Promotieonderzoek naar de impact van de NIS2 Directive op organisaties

Amsterdam Business Research Instituut van de Vrije Universiteit Amsterdam



School of Business and Economics
Vrije Universiteit Amsterdam