Cyberweerbaarheidsgids

voor de leveranciers van Infrabel

INFRABEL

Gids voor Cybersecurity
voor leveranciers van Infrabel

Bewustwording en oriëntatie op het gebied van cyberbeveiliging en cyberweerbaarheid
Infrabel beheert kritieke spoorweginfrastructuren en moet voldoen aan meerdere kaders en normen voor cyberbeveiliging.

KADERS & NORMEN

- Wet CER
- Wet NIS2
- Cyber Resilience Act
- RED-richtlijn
- ISO 27001
- CyFun
- NIST CSF
- IEC 62443 / IEC 63452

UW VERPLICHTINGEN ALS LEVERANCIER

Risicobeheer
Kwetsbaarheden beoordelen en verminderen

Gegevensbescherming
Uw systemen en informatie beveiligen

Detectie & Respons
Incidenten bewaken en erop reageren

Levenscyclus
Beveiliging gedurende de volledige levenscyclus waarborgen

INFRABEL

Inhoudstafel

CYBERWEERBAARHEIDSGIDS VOOR INFRABEL-LEVERANCIERS

Het doel van deze gids is om de leveranciers van Infrabel bewust te maken van de praktische vereisten op het vlak van cyberbeveiliging en cyberweerbaarheid. Het doel is om ervoor te zorgen dat uw diensten en producten voldoen aan de huidige wettelijke en reglementaire verplichtingen en tegelijkertijd de continuïteit van de bedrijfsactiviteiten te beschermen.

Als beheerder van kritieke spoorweginfrastructuur moet Infrabel verschillende kaders naleven:

- de CER-wet,
- de NIS2-wet,
- de Cyber Resilience Act (CRA),
- deRadio Equipment Directive (RED),
- evenals erkende normen en benchmarks zoals
    - ISO 27001
    - nationaal kader cCB CyberFundamentals (CyFun)
    - NIST-CDF
    - IEC 62443
    - en de toekomstige spoornorm IEC 63452.

Als leverancier bent u daarom verplicht om robuuste veiligheidsmaatregelen te nemen die betrekking hebben op risicobeheer, bescherming van uw gegevens en diensten, detectie van en reactie op incidenten, gedurende de hele levenscyclus van de producten of diensten die Infrabel van u koopt.

Een wettelijke en strategische verplichting

Cyberbeveiliging is niet langer optioneel: Europese regelgeving zoals NIS2 legt de verantwoordelijkheid direct bij kritieke operatoren en hun leveranciers, met daarbijhorende controles en sancties. Cyberweerbaarheid is ook essentieel om de continuïteit van uw bedrijfsactiviteit en het vertrouwen van Infrabel te garanderen.

Concrete vereisten en best practices

Deze gids is gestructureerd per praktisch domein (toegangsbeheer, reactie op incidenten, beveiliging van de toeleveringsketen, enz.) en illustreert de verwachte maatregelen voor elk domein, samen met voorbeelden van beproefde en geteste goede praktijken, in het bijzonder aangepast aan de spoorwegcontext.

Afstemming op erkende normen

De aanbevelingen die hier worden gedaan, zijn gebaseerd op internationale normen (ISO/IEC 27001, NIST CSF v2.0, IEC 62443, enz.) en op het Belgische nationale CyberFundamentals framework (CyFun). Door ze te volgen, kunt u makkelijker uw conformiteit aantonen en op het vlak van beveiliging met Infrabel een gemeenschappelijke taal hanteren.

Overzicht van regelgevings- en normenkaders

De eisen die Infrabel stelt aan zijn leveranciers op het vlak van cyberweerbaarheid vloeien voort uit een aantal Belgische wetten, recente Europese richtlijnen en referentienormen.

De onderstaande tabel vat de belangrijkste punten samen:

Kader/Norm	Reikwijdte en rol voor leveranciers
Critical Entities Resilience (CER)	Regelgeving die is ontworpen om de veerkracht en de beveiliging van de kritieke infrastructuur in Europa te versterken tegen risico's, of die nu door de natuur of door de mens worden veroorzaakt. Het legt operatoren in kritieke sectoren (vervoer, energie, gezondheidszorg, enz.) verplichtingen op op het gebied van preventie, crisisbeheer en bedrijfscontinuïteit om de beschikbaarheid en betrouwbaarheid van essentiële diensten te garanderen.
NIS2-richtlijn	Regelgeving die een minimumset cyberbeveiligingsmaatregelen oplegt aan essentiële en belangrijke entiteiten (vervoer, energie, enz.). NIS2 vereist met name risicobeheer, toegangscontrole, incidentafhandeling, beveiliging van de toeleveringsketen en de implementatie van continuïteitsplannen. De kritieke leveranciers van Infrabel worden onrechtstreeks getroffen (en soms rechtstreeks als ze zelf onder NIS2 vallen) en moeten even strenge normen toepassen om te vermijden dat ze de zwakke schakel worden.
Cyber Resilience Act (CRA)	Europese regelgeving (Verordening 2024/2847) tot vaststelling van de cyberbeveiligingsverseisten voor producten met digitale elementen (software, verbonden objecten, hardware). Vanaf 2026 zullen fabrikanten en leveranciers van dergelijke producten moeten aantonen dat ze van bij het ontwerp beveiligd zijn (bv. geen bekende kwetsbaarheden op het moment dat ze op de markt worden gebracht), dat ze regelmatig beveiligingspatches bijwerken en dat ze een formeel proces hebben voor het kwetsbaarheids- en incidentbeheer (kennisgeving binnen 24 uur, gedetailleerd rapport binnen 72 uur als een kwetsbaarheid wordt uitgebuit). Voorbeeld: als u software of verbonden hardware aan Infrabel levert, moet u een controleproces voor kwetsbaarheden hebben en beveiligingsupdates leveren tijdens de hele levenscyclus van het product.
RED Richtlijn	EU-richtlijn 2014/53/EU (bekend als RED) regelt radioapparatuur. Een gedelegeerde verordening introduceerde cyberbeveiligingseisen die van

	toepassing zijn op bepaalde categorieën draadloze of verbonden apparaten (bijv. IoT-objecten voor het groot publiek, industriële radiomodules). In de praktijk betekent dit dat er beveiligingsfuncties moeten worden ingebouwd zoals het voorkomen van ongeautoriseerde toegang, het beschermen van persoonsgegevens en privacy, en het voorkomen van het risico op fraude met de betreffende apparatuur. De naleving moet worden aangetoond via geharmoniseerde technische normen (bijv. de nieuwe EN 303 645 en EN 18031-x normen gebaseerd op IEC 62443). Als je bijvoorbeeld aan Infrabel een draadloze sensor voor de infrastructuur verkoopt, moet die sensor netwerkbeveiligingscontroles bevatten en aan deze normen voldoen.
ISO/IEC 27001:2022	Internationale norm voor informatiebeveiligingsbeheersystemen (ISMS). Deze norm biedt een compleet raamwerk om een beleid, processen en controles op te zetten voor het beheer van de informatiebeveiliging. Infrabel gebruikt ISO 27001 als centrale referentie voor zijn eigen ISMS. De Belgische omzetting van NIS2 erkent ISO 27001 (versie 2022) als gelijkwaardig aan het CyFun-kader om de naleving van de minimumvereisten aan te tonen. Een ISO 27001 certificering van uw bedrijf zou een sterke blijk van vertrouwen zijn.
CyberFundamentals (CyFun)	Cyberbeveiligingskader uitgewerkt door het Centrum voor Cybersecurity België, ontworpen voor de NIS2-beoordeling. In het raamwerk worden minimumbeveiligingsmaatregelen uiteengezet in drie zekerheidsniveaus (Basic, Important, Essential) die in verhouding staan tot de omvang/kritieke aard van de organisatie. Van een Infrabel-leverancier kan worden geëist dat hij de CyFun-beoordeling ondergaat (of een gelijkwaardige ISO 27001-certificering afgeeft) in het kader van de periodieke conformiteitscontroles die in België van essentiële operatoren worden geëist.
NIST Cybersecurity Framework 2.0	Vrijwillig raamwerk voor het beheer van cyberrisico's, dat internationaal breed wordt toegepast. Versie 2.0 van de NIST CSF structureert veiligheid in 6 functies: Beheren, Identificeren, Beschermen, Detecteren, Reageren, Herstellen, elk met verschillende categorieën van controle (bijv. identiteitsbeheer, gegevensbescherming, continue monitoring, incidentrespons, etc.).

	Deze gemeenschappelijke woordenschat wordt door Infrabel gebruikt om zijn cyberbeveiligingsstrategie (pijlers Identify, Protect, Detect, Respond, Recover, Govern) te formuleren. De afstemming op deze categorieën vergemakkelijkt de communicatie en exhaustieve risicodekking.
IEC 62443	Een reeks internationale normen die gespecialiseerd zijn in de beveiliging van industriële systemen en SCADA/OT. Ze definiëren zowel technische vereisten (bijv. 7 fundamentele vereisten van IEC 62443-1-1 met betrekking tot authenticatie, communicatiebeveiliging, integriteit, beschikbaarheid, toegangsbeheer, enz.) als levenscyclusprocessen (bijv. IEC 62443-4-1 voor beveiligde ontwikkeling, 62443-2-1 voor industriële beveiligingsbeheerprogramma's). Voor leveranciers van industriële oplossingen aan Infrabel dient IEC 62443 als een technisch referentiekader dat is afgestemd op wettelijke verplichtingen (de principes van IEC 62443 zijn impliciet opgenomen in NIS2, CRA en RED).
AI Act	De AI Act, de Europese verordening over kunstmatige intelligentie, introduceert nieuwe verplichtingen voor leveranciers van AI-oplossingen en hun klanten. Dit kader legt een classificatie van AI-systemen op volgens hun risiconiveau, met strengere eisen voor systemen met een hoog risico (zoals systemen die worden gebruikt voor het beheer van kritieke infrastructuur, beveiliging of transport). De AI Act legt de lat hoger in de relatie met leveranciers. Zo verplicht hij tot nauwe samenwerking om de naleving, veiligheid en het beheer van de risico's met betrekking tot kunstmatige intelligentie te waarborgen, en bevordert hij een proactieve en transparante aanpak gedurende de hele levenscyclus van AI-systemen.
IEC 63452 **(In voorbereiding)**	Toekomstige internationale norm voor cyberbeveiliging op het spoor. IEC 63452, waaraan momenteel de laatste hand wordt gelegd door het TC9-comité van het IEC, zal de principes van IEC 62443 aanpassen aan de specifieke kenmerken van spoorwegsystemen (seinen, rollend materieel, grondapparatuur, enz.), waarbij de hele levenscyclus (ontwerp, exploitatie, onderhoud) wordt bestreken en de verantwoordelijkheden van de verschillende spelers (exploitant, integrator, leverancier, onderhouder) duidelijk worden gedefinieerd. Deze norm, die naar verwachting vanaf 2026 in Europa zal worden aangenomen, zal de huidige spoorwegspecificatie CLC/TS 50701

	vervangen en wordt de nieuwe basis voor naleving in de spoorwegsector, in overeenstemming met NIS2 en de CRA. Leveranciers die werkzaam zijn in het spoorwegsysteem zullen er dus snel aan moeten voldoen.

Niet elke Infrabel-leverancier heeft met al deze normen en wetten te maken, maar u moet wel nagaan welke van toepassing zijn op uw producten/diensten en uw rol.

Zo vallen bijvoorbeeld software-uitgevers of fabrikanten van verbonden objecten rechtstreeks onder de CRA en de RED, terwijl een bedrijf dat systeemonderhoud levert meer te maken heeft met NIS2 en ISO 27001.

In elk geval verwacht Infrabel van al zijn partners dat ze een proactieve houding aannemen door de concrete maatregelen die hieronder worden beschreven en die de gemeenschappelijke vereisten van deze normen samenvatten, te implementeren.

Cyberbeveiligingsbeheer en risicobeheer

Waarom?

Een goed cyberbeveiligingsbeheer is de hoeksteen van een efficiënte cyberweerbaarheid. Infrabel verwacht van zijn leveranciers dat ze informatiebeveiliging integreren in hun beheer en dat ze een risicogebaseerde aanpak hanteren om de passende beveiligingsmaatregelen te bepalen.

Dit is niet alleen een goede praktijk (in lijn met de geest van ISO 27001 en NIST CSF), maar ook een impliciete wettelijke verplichting: NIS2 legt bijvoorbeeld aan leidinggevenden van kritieke entiteiten de verplichting op om toezicht te houden op het cyberrisicobeheer en om bedrijfscontinuïteitsplannen goed te keuren.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Beveiligingsbeleid en vastgestelde verantwoordelijkheden	U moet formeel verantwoordelijke voor cyberbeveiliging of een team dat hiervoor instaat aanstellen en een intern cyberbeveiligingsbeleid laten goedkeuren door uw management. Dit beleid moet uw belangrijkste uitdagingen (vertrouwelijkheid van gegevens, beschikbaarheid van systemen, enz.) omvatten en in overeenstemming zijn met de geldende Belgische wetgeving en de contractuele verplichtingen van Infrabel. Het definieert de rollen en verantwoordelijkheden van iedereen op het gebied van informatiebeveiliging. Voorbeeld: een leverancier die een kmo is, heeft intern een 'CISO' aangesteld, een praktijk die door Infrabel wordt aangemoedigd.
Regelmatige risicoanalyses	Voer een gedocumenteerd proces in voor de risicobeoordeling van uw assets en diensten, in het bijzonder die welke verband houden met de perimeter van Infrabel. Identificeer vóór elk nieuw project of contract de relevante dreigingsscenario's, beoordeel de potentiële impact (inclusief op de spoorwegveiligheid waar van toepassing) en selecteer beveiligingsmaatregelen die in verhouding staan tot de geïdentificeerde risico's. Voorbeeld: alvorens een systeem aan te sluiten op het Infrabel-netwerk voert een leverancier een risicoanalyse uit aan de hand van de EBIOS-methode van ANSSI en in overeenstemming met IEC 62443-3-2 om het vereiste beveiligingsniveau (SL 1, 2 of hoger) te rechtvaardigen op basis van de te voorziene dreigingen.
Naleving van de regelgeving en opvolging van de vereisten	Blijf op de hoogte van de wetten en normen die van toepassing zijn in uw sector en zorg dat u eraan voldoet. In België hebben de autoriteiten (CCB) de referentiegids CyberFundamentals gepubliceerd, waarin de minimale maatregelen staan die worden verwacht onder NIS2. Zorg ervoor dat u voldoet aan deze maatregelen of die van een gelijkwaardige norm (ISO 27001:2022) om aan te tonen dat u de risico's goed beheert. Opmerking: Infrabel kan u in het kader van de kwalificatie of de controle van uw opdracht om een bewijs van deze conformiteit vragen (bijvoorbeeld een extern auditverslag of een certificaat).

Documentbeheerproces en voortdurende verbetering	Zet een ISMS op maat van uw organisatie op, ook al is het vereenvoudigd, inclusief het bijhouden van documentatie (beleid, procedures, inventarissen van bedrijfsmiddelen, actieplannen) en periodieke interne audits. Het doel is om beveiliging onderdeel te maken van een Plan-Do-Check-Act continue verbetercyclus, overeenkomstig ISO 27001. Voorbeeld: een Infrabel-leverancier houdt een register bij van beveiligingsincidenten die zich binnen zijn perimeter hebben voorgedaan en voert jaarlijks een interne audit van zijn systeem uit om verbeterpunten te identificeren en zo zijn maturiteit op het vlak van governance aan te tonen.

Digitale, technologische en strategische soevereiniteit

Waarom?

Als kritieke spoorweginfrastructuur moet Infrabel zijn soevereiniteit waarborgen tegenover digitale risico's en risico's in zijn Supply Chain. Dit betekent dat het de controle moet behouden over zijn gevoelige gegevens, de gebruikte technologieën en belangrijkste componenten en zijn strategische beslissingen, zonder buitensporige afhankelijkheid of inmenging van buitenaf.

Dit is een pijler van de nationale cyberweerbaarheid: een verlies van controle over kritieke gegevens of systemen zou Infrabel blootstellen aan grote risico's en het bedrijf zou een geopolitieke hefboom kunnen worden voor kwaadwillende actoren. Deze vereiste wordt overigens versterkt door recente regelgevingskaders: de NIS2-richtlijn legt essentiële operatoren een strikt risicobeheer op, inclusief de risico's in de toeleveringsketen en het beveiligingsbeheer; de CER-verordening is gericht op de weerbaarheid van kritieke entiteiten en verplicht hen te anticiperen op het falen van leveranciers om de continuïteit van diensten te waarborgen.

Evenzo introduceert de Cyber Resilience Act (CRA) (EU-verordening 2024/2847) vanaf 2026 cyberbeveiligingseisen voor digitale producten (beveiliging van bij het ontwerp, snelle patching, openbaarmaking van kwetsbaarheden) om de technologische transparantie te verbeteren - er mogen bijvoorbeeld geen bekende kwetsbaarheden overblijven wanneer een product op de markt wordt gebracht.

Deze verplichtingen sluiten aan bij de geest van de sectorale normen: de IEC 62443-reeks over industriële beveiliging beschrijft technische en organisatorische principes die impliciet zijn opgenomen in NIS2, de CRA en de RED-richtlijn, en de toekomstige spoorwegnorm IEC 63452 (verwacht in 2026) zal deze principes aanpassen aan het spoor door de verantwoordelijkheden van elke speler (exploitant, integrator, leverancier, enz.) te verduidelijken, in overeenstemming met NIS2 en de CRA. Concreet houdt soevereiniteit voor de leveranciers van Infrabel in: gevoelige gegevens onder een vertrouwde jurisdictie lokaliseren en beschermen, de kritieke technologische componenten (software, hardware) gedurende hun hele levenscyclus beheersen, en anticiperen op geopolitieke risico's die verband houden met mogelijke afhankelijkheden buiten de EU.

Deze aanpak vermindert de systeemrisico's aanzienlijk: NIS2 bepaalt bijvoorbeeld dat operatoren een contract met een leverancier met een te hoog cyberrisico kunnen beëindigen.

Infrabel verwacht van zijn partners dan ook een proactieve aanpak op dit vlak. De uitdaging is er een van gedeelde verantwoordelijkheid: elke schakel in de Supply Chain moet nauw samenwerken, transparantie tonen en gemeenschappelijke normen aannemen (zoals IEC 62443) om de algehele veerkracht te versterken.

Kortom, de soevereiniteit van gegevens, technologieën en beslissingen is voortaan onlosmakelijk verbonden met de cyberweerbaarheid van Infrabel en zijn leveranciers.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Beleid en principes inzake soevereiniteit	Door deze soevereiniteitsprincipes toe te passen, draagt u bij aan de duurzaamheid van de veiligheid en veerkracht van Infrabel en versterkt u tegelijkertijd uw eigen positie in een steeds veeleisender wordende markt Soevereiniteit is een operationele voorwaarde voor elke leverancier van essentiële infrastructuur zoals Infrabel. Om dit te bereiken rekent Infrabel erop dat al zijn partners innoveren en zich dienovereenkomstig organiseren, van governance tot technische keuzes, zodat de spoorwegwaardeketen onder controle blijft, bestand is tegen externe schokken en in lijn is met de nationale en Europese strategische belangen.

Toegangscontrole en bescherming van kritieke systemen

Waarom?

Het beheren van de toegang tot gevoelige systemen en gegevens is een van de meest cruciale gebieden (en vaak het eerste dat onder NIS2, ISO 27001 en NIST CSF valt). Als een aanvaller uw identifiers compromitteert of via een leverancier een kritiek netwerk binnendringt, kan hij ernstige schade aanrichten.

Daarom verwacht Infrabel van zijn leveranciers dat ze de toegang tot hun systemen streng beveiligen, zeker als deze gekoppeld zijn aan de infrastructuur van Infrabel.

De NIS2-richtlijn benadrukt het belang van "bescherming van de kritieke systemen en toegangscontrole" als een prioritaire maatregel.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Identiteitscontrole en sterke authenticatie	Zorg ervoor dat alleen geautoriseerde gebruikers toegang hebben tot bronnen en alleen tot de informatie die ze nodig hebben om hun taken uit te voeren (least-privilege-principe of principe van minimale rechten). Stel multi-factor authenticatie (MFA) in voor alle gevoelige verbindingen, vooral voor externe toegang en accounts met privileges. NIS2 en beste praktijken schrijven nu het algemene gebruik van MFA voor om het risico op identiteitsdiefstal te verminderen. Voorbeeld: een leverancier die op afstand ondersteuning biedt op Infrabel-systemen heeft een MFA-oplossing van de nieuwste generatie geïmplementeerd, zodat elke technicus zich kan authenticeren op het beveiligde VPN. Bovendien worden er voor elke deelnemer unieke en op naam gestelde accounts aangemaakt (geen algemene gedeelde account) om de traceerbaarheid te garanderen.
Beheer van geprivilegieerde toegangen (PAM)	Identificeer uw beheerdersaccounts of accounts met verhoogde rechten (op uw interne systemen of die van Infrabel) en beveilig ze met een systeem voor het beheer van geprivilegieerde toegang. Dit omvat het opslaan van beheerderswachtwoorden in een beveiligde elektronische kluis, het activeren van logs/waarschuwingen over het gebruik van deze accounts, en eventueel dubbele goedkeuring voor de meest gevoelige acties Voorbeeld: een IT-dienstverlener van Infrabel heeft CyberArk (PAM) ingesteld om de bij Infrabel gebruikte beheeraccounts te centraliseren, waarbij wachtwoorden regelmatig worden vernieuwd en beheersessies worden geregistreerd. Dit soort maatregelen beantwoordt aan de verwachtingen van Infrabel op het gebied van controle van geprivilegieerde toegangen.
Netwerksegmentatie en bescherming van werkstations	Als u gegevens met betrekking tot Infrabel binnen uw infrastructuur host of verwerkt, moeten deze zich op beveiligde en afgeschermde systemen en netwerken bevinden. Scheid gevoelige omgevingen (bijv. servers aangesloten op Infrabel-systemen) van de rest van uw bedrijfsnetwerk door middel van speciale beveiligingszones (zie de principes van IEC 62443 voor zones en pipelines). Bescherm ook je werkposten en servers met anti-malware en patch management tools (zie volgende sectie). Voorbeeld: een consultancybedrijf, leverancier van Infrabel, heeft een geïsoleerd netwerk opgezet voor Infrabel-projecten, dat alleen

	toegankelijk is voor bevoegde consultants, en met geharde werkstations (antivirus up-to-date, schijfversleuteling geactiveerd, enz.) Zo blijft zelfs bij een intern incident het risico op verspreiding naar Infrabel zo veel mogelijk beperkt.
Toegangsbewaking en logboeken	Toegangs- en activiteitenlogboeken bijhouden op uw kritieke systemen (verbindingslogboeken, beheeracties, gevoelige netwerkstromen). Deze logs moeten lang genoeg worden bewaard en regelmatig worden bekeken om verdachte pogingen te detecteren. Correlatietools (SIEM) of periodieke analyses kunnen u helpen afwijkingen op te sporen. Dit is een impliciete vereiste van NIS2 en ISO 27001 (loggingcontroles, continue monitoring). Voorbeeld: na een aanbeveling van Infrabel heeft een leverancier gedetailleerde logging geactiveerd op zijn SFTP-bestandsuitwisselingsserver en controleert hij wekelijks de verbindingen om na te gaan of er geen onverwachte of buiten de kantooruren tot stand gekomen verbindingen zijn.
Versleuteling van gevoelige gegevens	Als u Infrabel-gegevens (plannen, bedrijfsgegevens, persoonlijke informatie, enz.) opslaat of uitwisselt, moeten deze zowel in rust (op uw servers, pc's, back-ups) als in transit (communicatie versleuteld via VPN, TLS, enz.) worden versleuteld. Versleutel bijvoorbeeld harde schijven met Infrabel-gegevens en verstuur gevoelige gegevens nooit onversleuteld per e-mail. Voorbeeld: een leverancier die treinverkeersgegevens verwerkt voor Infrabel, gebruikt 256-bit AES-versleuteling aan de kant van de databaseserver en geeft gegevens alleen door aan Infrabel via goedgekeurde IPsec VPN-tunnels, in overeenstemming met het Infrabel-beleid. Doel: vertrouwelijkheid en integriteit garanderen, zoals vereist door RED en CRA voor communicatie en gegevens.

Door deze maatregelen toe te passen, kunt u de risico's op inbraken en datalekken aanzienlijk beperken.

NIS2 legt in het bijzonder de nadruk op toegangsbeheer en de bescherming van kritieke systemen, omdat dit vaak de routes zijn waarlangs grote incidenten plaatsvinden (bijv. aanvallen met gestolen wachtwoorden of verkeerde netwerkconfiguratie).

Infrabel controleert regelmatig zijn eigen toegangscontroles en verwacht een gelijkwaardige waakzaamheid van zijn leveranciers.

Beveiliging van bij het ontwerp en beheer van kwetsbaarheden

Waarom?

Cyberweerbaarheid houdt in dat men op aanvallen anticipeert door systemen vanaf het ontwerp te versterken en kwetsbaarheden snel te verhelpen.

Twee recente ontwikkelingen maken dit essentieel: ten eerste verplicht de Cyber Resilience Act fabrikanten van digitale producten om beveiligde ontwikkelingspraktijken en proactief patchonderhoud te volgen; ten tweede verplicht de NIS2-richtlijn operatoren en hun waardeketen om een continu proces voor kwetsbaarheidsbeheer in te voeren (monitoring, patching, patch tracking).

Infrabel verwacht van zijn leveranciers dat ze blijk geven van een "Cyber-Resilience-by-Design"-aanpak en voorbeeldig reageren op beveiligingslekken.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Beveiligde ontwikkelingscyclus (SDLC)	Als u software of een toepassing ontwikkelt of een systeem ontwerpt voor Infrabel, integreer veiligheid dan in elke fase van uw ontwikkelingscyclus. Dit omvat een dreigingsanalyse voorafgaand aan het ontwerp (het beoordelen van potentiële aanvalsscenario's), de integratie van beveiligingsmaatregelen in de code en architectuur (bijv. robuust foutbeheer, bescherming tegen injectie, enz.), systematische beveiligingstests (statische codeanalyse, penetratietests tijdens de acceptatiefase) en het beheer van kwetsbaarheden die na oplevering worden ontdekt. Voorbeeld: een software-uitgever die software aan Infrabel levert, heeft de IEC 62443-4-1 standaard (veilig ontwikkelingsproces) geïmplementeerd: elke versie wordt onderworpen aan een beveiligingsgerichte codereview en een automatische kwetsbaarheidsscan, en de ontwikkelaars zijn getraind in best practices voor veilig coderen. Dit betekent dat het product voldoet aan de "Secure-by-Design" criteria van de CRA (geen bekende kwetsbaarheden bij levering).
Kwetsbaarheid- en patchbeheer	Zet een beveiligingsmonitoringproces op om snel op de hoogte te zijn van nieuwe kwetsbaarheden die van invloed zijn op uw producten, systemen of afhankelijkheden (bijv. abonnementen op CERT-waarschuwingen, CVE's, enz.). Zorg voor een patchmanagementprocedure met maximale

	termijnen voor het toepassen van patches: kritieke kwetsbaarheden moeten idealiter binnen een paar dagen worden verholpen. Documenteer dit proces duidelijk en, indien een belangrijke kwetsbaarheid een door Infrabel gebruikt onderdeel treft, breng de betrokken Infrabel-contactpersonen onmiddellijk op de hoogte. Voorbeeld: een leverancier die verantwoordelijk is voor het onderhoud van een industrieel SCADA-systeem voor Infrabel heeft een timing opgesteld met maandelijkse updates (voor standaardpatches) en een hotfix-proces van 48 uur voor kritieke fouten. Toen Log4Shell eind 2021 werd onthuld, identificeerde deze leverancier binnen 24 uur kwetsbare toepassingen binnen zijn Infrabel-perimeter en implementeerde corrigerende patches in minder dan 4 dagen, in lijn met de verwachtingen van Infrabel.
Communicatie en transparantie (Coordinated Disclosure)	De CRA introduceert een verplichting voor leveranciers van digitale producten om een gecoördineerd mechanisme voor de openbaarmaking van kwetsbaarheden (CVD) op te zetten. Praktisch gezien moet u een contactpunt voorzien (beveiligingse-mail, portaal) waar onderzoekers of klanten een kwetsbaarheid aan u kunnen melden en zich ertoe verbinden om te reageren en patches te publiceren binnen een redelijk tijdsbestek. Infrabel beloont leveranciers die blijk geven van deze transparantie. Voorbeeld: een leverancier van IoT-oplossingen heeft op zijn B2B-website een beleid voor het openbaar maken van kwetsbaarheden gepubliceerd, waarin hij zich ertoe verbindt om binnen 72 uur ontvangst te bevestigen en binnen 21 dagen een patch of workaround te bieden voor kwetsbaarheden die als kritiek worden beschouwd. Dit soort initiatieven getuigt van een volwassen veiligheidscultuur en wordt gewaardeerd bij de beoordeling van uw offertes.
Veilig onderhoud van industriële apparatuur	Voor leveranciers van operationele hardware of software (OT) die ingezet worden in de infrastructuur van Infrabel, is de fase van onderhoud in veilige omstandigheden (MCS) even belangrijk als de initiële oplevering. Firmware-updates en beveiligingspatches moeten worden geleverd voor de gehele levensduur van het product en deze toezeggingen moeten in de contracten worden vastgelegd. IEC 62443-3-3 en 62443-2-4 specificeren bijvoorbeeld de vereisten voor veilig onderhoud voor systemen en serviceproviders. Voorbeeld: een fabrikant van spoorwegautomatiseringssystemen die aan Infrabel seinposten levert, heeft zich er via een contractuele clausule toe verbonden 10 jaar lang beveiligingsondersteuning te bieden (levering van software-updates, bewaking van kwetsbaarheden in zijn componenten,

	kennisgeving aan Infrabel in geval van vroegtijdige beëindiging van de ondersteuning). Op die manier kan Infrabel deze elementen integreren in zijn eigen assetbeheerplan en ervoor zorgen dat het systeem blijft voldoen aan de eisen met betrekking tot nieuwe bedreigingen (zoals vereist door NIS2 voor kritieke systemen).

Kortom, laat zien dat er bij u geen bekende kwetsbaarheid blijft bestaan zonder dat er een actieplan voor is. Studies tonen aan dat meer dan de helft van de KMO's die het slachtoffer worden van een grote cyberaanval binnen zes maanden failliet gaan. Niet reageren op patches kan u niet alleen uw reputatie bij Infrabel kosten, het kan ook uw economische voortbestaan in gevaar brengen.

Omgekeerd zal een proactieve benadering van security by design en een flexibel kwetsbaarheidsbeheer een doorslaggevende vertrouwensfactor zijn voor Infrabel.

Monitoring, detectie en vroegtijdige waarschuwing

Waarom?

Ondanks alle preventieve maatregelen kan er toch een incident plaatsvinden. Het vermogen om een anomalie of aanval snel te detecteren is daarom cruciaal om de impact te beperken.

NIS2 en standaarden zoals ISO 27001 vereisen dat er systemen voor beveiligingsmonitoring en incidentdetectie worden opgezet. Infrabel van zijn kant heeft een 24/7 CyberSOC om zijn kritieke activa te bewaken.

Het verwacht van zijn leveranciers, en in het bijzonder van de leveranciers die verbonden zijn met zijn systemen, een gepaste waakzaamheid: indien een incident een van uw systemen die verbonden zijn met Infrabel treft, moet u in staat zijn dit te detecteren en Infrabel onmiddellijk te waarschuwen.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Continue monitoring (CyberSOC)	Zet, afhankelijk van de grootte van uw organisatie en het kritieke karakter van uw diensten, een team of afdeling voor beveiligingsmonitoring op. Dit kan variëren van een eenvoudig systeem van automatische waarschuwingen bij ongebruikelijke gebeurtenissen tot een volwaardig in-house of uitbesteed CyberSOC dat logs en gedrag in realtime analyseert. Voorbeeld: een middelgroot bedrijf, leverancier van Infrabel, heeft zich geabonneerd op een uitbestede CyberSOC-dienst die zijn servers en firewall 24/7 bewaakt. Op een nacht werd abnormale activiteit gedetecteerd (verdachte netwerkscan) en CyberSOC waarschuwde onmiddellijk de beveiligingsmedewerker van de leverancier, waardoor

	het kwaadaardige IP-adres onmiddellijk kon worden geblokkeerd. Dit soort proactieve dienstverlening ligt in de lijn van de aanpak van Infrabel, dat ook een beroep doet op een externe CyberSOC om zijn detectie te versterken.
Intrusiedetectiesystemen (IDS/IPS)	Zet geautomatiseerde detectietools in op uw kritieke netwerken en systemen: firewalls van de nieuwe generatie met diepe inspectie, netwerk IDS sensoren, EDR (Endpoint Detection & Response) agents op werkstations/servers, enz. Deze tools sturen waarschuwingen bij activiteiten die duiden op een aanval (bekende malware, abnormaal gedrag, poging tot ongeautoriseerde toegang). Ze moeten worden geconfigureerd dat ze alle mogelijke toegangspunten tot de gegevens/systemen van Infrabel dekken. Voorbeeld: een datahost voor Infrabel heeft een IDS sensor geïnstalleerd op het netwerksegment dat de servers van het project host, geconfigureerd met de nieuwste dreigingshandtekeningen. Op een dag detecteerde de sensor een poging om een gekende kwetsbaarheid op een webserver uit te buiten: de waarschuwing werd gecorreleerd en activeerde automatisch de blokkering van het bron-IP door de firewall (IPS), waardoor een mogelijke compromittering werd voorkomen. Het doel is om niet alleen te vertrouwen op menselijke waakzaamheid, maar om permanent actieve "sensoren" te hebben.
Logbeheer en correlatie	Zorg ervoor dat logs van uw servers, applicaties, beveiligingsapparatuur, etc. op een consistente manier worden verzameld en geanalyseerd. Een SIEM (Security Information and Event Management) kan deze gegevens samenvoegen en correlaties mogelijk maken (bijvoorbeeld detecteren dat hetzelfde IP-adres 5 keer geen verbinding heeft kunnen maken met het VPN + een poort op een server heeft gescand). Als u geen SIEM hebt, zorg er dan in ieder geval voor dat een verantwoordelijke regelmatig de essentiële logs bekijkt, handmatig of met eenvoudige tools. Voorbeeld: een leverancier heeft het versturen van logs van zijn appliances (firewall, VPN) naar het logplatform van Infrabel of naar een gemeenschappelijke SIEM geconfigureerd. Op die manier zou Infrabel ook zicht krijgen op eventuele intrusiepogingen gericht tegen deze leverancier en er aan zijn kant op kunnen anticiperen - een win-winsamenwerking.

Detectie van datalekken (DLP)	Als u gevoelige Infrabel-informatie behandelt, overweeg dan oplossingen om datalekken te voorkomen en te detecteren, of ze nu het gevolg zijn van nalatigheid of interne kwaadwilligheid. DLP-systemen kunnen de uitgaande gegevens (e-mails, bestandsoverdrachten) en waarschuwingen genereren als bijvoorbeeld een vertrouwelijk document buiten het geautoriseerde domein wordt verzonden. Voorbeeld: een consultancybedrijf dat technische plannen uitvoert voor Infrabel heeft een DLP-regel geïmplementeerd voor zijn e-mailsysteem: elke uitgaande e-mail met gevoelige termen of grote bijlagen wordt gemeld aan de CISO. Op een dag probeerde een medewerker een document van Infrabel naar zichzelf te sturen (om van thuis uit te werken). Het systeem blokkeerde de e-mail en bracht het beveiligingsteam op de hoogte, waardoor een inbreuk op de vertrouwelijkheid werd vermeden.

Door te focussen op vroegtijdige detectie, vergroot u uw kansen aanzienlijk om een incident in te dammen voordat het grote schade veroorzaakt

Infrabel beschouwt continue monitoring als een essentieel onderdeel van de weerbaarheid: "Cyberdreigingen 24 uur per dag voorkomen, detecteren, onderzoeken en erop reageren" is het verklaarde doel van het CyberSOC. Het verwacht van u een soortgelijke filosofie, aangepast aan uw context.

Incidentrespons en hervatting van de activiteiten

Waarom?

Geen enkele verdediging is 100% waterdicht. De organisatie moet daarom voorbereid zijn om effectief te reageren in het geval van een incident (cyberaanval, grote storing, datalek), om de impact te beperken en snel herstel te garanderen.

Het respons- en hervattingsvermogen - de kern van cyberweerbaarheid - is een component die expliciet aan bod komt in NIS2 (crisisbeheerplannen, bedrijfscontinuïteit) en in normen voor beheersystemen (ISO 27001, ISO 22301 voor continuïteit, NIST CSF-functie Recover).

Een Infrabel-leverancier moet niet alleen in staat zijn om zijn eigen incidenten te behandelen, maar ook om samen te werken met Infrabel in geval van een incident dat zijn centrales of de gedeelde infrastructuur treft.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Incidentresponsplan (CSIRT)	Stel een plan op voor het beheer van beveiligingsincidenten waarin de te volgen stappen bij een bewezen aanval of ernstig vermoeden van een aanval gedetailleerd worden beschreven (CSIRT-procedure). Dit plan moet het volgende specificeren: de rol van elke persoon (wie coördineert, wie onderzoekt, wie communiceert), de inzetbare noodmiddelen, de technische middelen om het incident in te dammen (servers isoleren, accounts blokkeren, enz.), alsook de te waarschuwen contactpersonen (inclusief Infrabel indien nodig). Oefen minstens één keer per jaar via oefeningen of simulaties, zodat uw team vertrouwd raakt met het proces Voorbeeld: een dienstverlenend bedrijf, een leverancier van Infrabel, heeft een draaiboek voor incidenten geformaliseerd: "Als ransomware wordt gedetecteerd op een server: 1) de noodmodus activeren, 2) de server isoleren van het netwerk, 3) onmiddellijk de IT-manager en de CISO waarschuwen, 4) Infrabel informeren als gedeelde gegevens of diensten worden beïnvloed, 5) de omvang analyseren, enz. Dankzij dit plan, dat elk jaar wordt herzien, heeft ons in staat gesteld om snel en kalm te reageren op de dag van een aanval door een cryptovirus, waardoor verspreiding werd voorkomen.
Melding en communicatie van incidenten	Breng Infrabel onmiddellijk op de hoogte als zich een beveiligingsincident voordoet dat verband houdt met de activiteiten die u voor Infrabel uitvoert. Als bijvoorbeeld uw systemen die Infrabel-gegevens hosten of die verbonden zijn met het Infrabel-netwerk gecompromitteerd zijn, of als u een aanval detecteert die zich zou kunnen verspreiden naar Infrabel, moet u ons onmiddellijk op de hoogte brengen. Transparantie is cruciaal: Infrabel hoort liever snel van u dan via de media. Bovendien vereist NIS2 dat essentiële entiteiten hun autoriteit binnen 24 uur na de detectie van een ernstig incident op de hoogte stellen, dus deze ultrakorte deadline heeft gevolgen voor kritieke leveranciers. Voorbeeld: in 2025 werd een Infrabel-dienstenleverancier het slachtoffer van een diefstal van hardware met gevoelige gegevens. In overeenstemming met zijn contract en de goede praktijken heeft hij Infrabel onmiddellijk op de hoogte gebracht, waardoor samen maatregelen konden worden genomen (wijziging van

	gecompromitteerde wachtwoorden, gezamenlijke communicatie indien nodig naar de geïmpacteerde personen, enz.). Denk eraan: in het geval van een lek in persoonsgegevens vereist de GDPR ook dat de autoriteiten binnen 72 uur op de hoogte worden gesteld.
Bedrijfscontinuïteitsplan (BCP)	Ontwikkel en test een continuïteitsplan voor uw kritieke diensten, inclusief cyberincidentscenario's Het doel is om zelfs in een crisissituatie een minimaal serviceniveau te garanderen en zo snel mogelijk weer normaal te functioneren (hersteltijddoelstelling, RTO). Identificeer uw essentiële Infrabel-processen en plan back-upoplossingen (reservesystemen, offline back-ups, tijdelijke handmatige capaciteiten, enz) NIS2 vereist expliciet het bestaan van continuïteits- en noodherstelplannen voor operatoren en hun dienstverleners. Voorbeeld: een belangrijke leverancier van een onlineplatform dat door Infrabel wordt gebruikt, heeft een BCP opgesteld: in het geval van een grote cyberaanval waardoor het platform niet beschikbaar is, kan binnen 4 uur een back-upsite op een andere cloud worden geactiveerd, waarbij de gegevens van de laatste back-up (D-1) worden hersteld. Om de 6 maanden worden er kanteloefeningen uitgevoerd. Op die manier weet Infrabel dat zelfs bij een ernstig incident de dienst snel weer operationeel zal zijn, wat een factor van weerbaarheid en compliance is.
Herstel en geleerde lessen	Voer na elk incident, zelfs een klein incident, een post-incidentanalyse uit om de hoofdoorzaak vast te stellen, eventuele zwakke punten te corrigeren en uw processen te verbeteren. Deel de bevindingen met Infrabel indien dit relevant is (bijvoorbeeld als het incident een systeemrisico of een aanval aan het licht brengt die ook andere partners zou kunnen treffen). Deze aanpak van voortdurende verbetering maakt deel uit van de verwachtingen van Infrabel en helpt het partnerschap te versterken. Bijvoorbeeld: na een phishing-incident waarbij een van zijn medewerkers betrokken was, ontdekte een leverancier een gebrek aan filtering op zijn e-mailsysteem. Hij implementeerde vervolgens een versterkte antispamfiltering en voerde een interne bewustmakingscampagne, terwijl hij Infrabel op de hoogte bracht van de gebruikte aanvalsvector, zodat iedereen op zijn hoede zou zijn voor dit soort e-mails.

Kortom, wees bereid om de klap op te vangen en weer op te krabbelen. Een snelle en gecoördineerde reactie beperkt de financiële, operationele en juridische schade drastisch.

Omgekeerd kan een chaotische of vertraagde reactie een matig incident veranderen in een regelrechte crisis. Infrabel investeert fors in zijn eigen responscapaciteit (CSIRT-team, crisisprocedures, enz.) en uw voorbereiding vormt een aanvulling op deze algemene weerbaarheid van de waardeketen.

Beveiliging van de toeleveringsketen en derden

Waarom?

"U bent zo sterk als uw zwakste schakel". Aanvallers zijn zich hier terdege van bewust en proberen vaak een doelwit te compromitteren via zijn leveranciers of onderaannemers (supply chain-aanvallen).

De NIS2-richtlijn legt de beveiliging van de toeleveringsketen expliciet vast: organisaties moeten de risico's van hun dienstverleners beheren en contractuele maatregelen opleggen aan kritieke leveranciers.

Voor Infrabel, dat een kritieke missie heeft, is het absoluut noodzakelijk dat alle leveranciers hoge veiligheidsnormen hanteren en dat er vanaf de aanbestedingsfase en gedurende het hele contract rekening wordt gehouden met de veiligheid.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Veiligheid integreren in contracten	Verwacht dat Infrabel specifieke vereisten voor informatiebeveiliging opneemt in zijn bestekken en contracten. Bijvoorbeeld: NIS2/CER/CRA-nalevingsclausules, technische clausules (versleuteling, patchbeheer), certificeringsvereisten (ISO 27001 of andere) of auditrechten. U moet deze clausules aanvaarden en naleven. Als u zelf onderaannemers gebruikt om een deel van het contract uit te voeren, moet u deze vereisten aan hen doorgeven. Voorbeeld: Infrabel heeft standaard veiligheidsclausules die in alle leverancierscontracten moeten worden opgenomen. Deze clausules hebben betrekking op toegangsbeheer, gegevensbescherming, melding van incidenten, enz. en worden aangepast naargelang de leverancier al dan niet toegang heeft tot Infrabel-gegevens, zijn netwerken of een clouddienst aanbiedt (hoe groter de blootstelling, hoe strenger de vereisten). Zorg dat u hiervan op de hoogte bent van zodra de aanbesteding is uitgeschreven, zodat u er op de juiste manier op kunt reageren.

Upstream veiligheidsbeoordeling van de leveranciers	Als u producten van derden uitbesteedt of gebruikt als onderdeel van het Infrabel-project, moet u hun beveiligingspraktijken beoordelen. Kies bij voorkeur gecertificeerde partners (ISO 27001, CyFun-label) of controleer via vragenlijsten/interviews of ze een adequaat beveiligingsniveau respecteren. ISO 27001:2022 heeft specifieke controles geïntroduceerd (A.5.19, A.5.22) op het beheren van de beveiliging van leveranciersrelaties, waaronder het vastleggen van beveiligingseisen in contracten, het bewaken van de implementatie ervan en het periodiek beoordelen van leveranciers. Houd u aan deze best practices. Voorbeeld: een bedrijf dat aan Infrabel levert (voor softwareontwikkeling) moest een andere dienstverlener inhuren voor een deel van de code. Het begon met de onderaannemer te vragen een veiligheidsvragenlijst in te vullen en nam de resultaten op in de risicoanalyse van het project. Het stelde Infrabel gerust dat het bedrijf zijn eigen supply chain onder controle had en zijn partners niet koos zonder de nodige voorzorgsmaatregelen te nemen.
Monitoring en audits van kritische leveranciers	Gedurende de hele looptijd van een contract is het belangrijk om de naleving door leveranciers en partners te controleren. Infrabel behoudt zich het recht voor om zijn leveranciers te controleren op veiligheidsaspecten. U moet dus bereid zijn om indien nodig informatie te verstrekken of een audit te organiseren. Aarzel van uw kant niet om uw eigen kritieke onderaannemers om regelmatige rapporten of certificaten te vragen. Zo organiseert de veiligheidsdienst van Infrabel jaarlijks controles bij bepaalde gevoelige dienstverleners: controle van de getroffen maatregelen, gezamenlijke penetratietests, enz. Een vooruitdenkende leverancier zou zelf een externe audit van zijn systeem kunnen uitvoeren en die spontaan aan Infrabel kunnen doorsturen als blijk van zijn ernst. Aandachtspunt: NIS2 bepaalt dat essentiële operatoren (zoals Infrabel) door hun overheid verplicht kunnen worden om een contract met een leverancier die een hoog cyberrisico inhoudt, op te schorten of te beëindigen. We hopen dat het nooit zover komt en uw proactieve medewerking zal ons helpen dergelijke extreme situaties te voorkomen.
Teruggave gegevens en beëindiging van het contract	Wanneer uw opdracht of contract met Infrabel ten einde loopt, zorg er dan voor dat u alle Infrabel-gegevens in uw bezit veilig teruggeeft of vernietigt, in overeenstemming met de contractuele bepalingen. Dit is

	een integraal onderdeel van de beveiligde levenscyclus van de leverancier. Voorbeeld: op het einde van het contract bezorgde een logistieke dienstverlener aan Infrabel alle operationele gegevensreeksen die hem ter beschikking waren gesteld, samen met een verwijderingscertificaat dat bewijst dat alle kopieën van deze gegevens gewist waren van zijn servers en back-ups. Dit niveau van striktheid sluit de samenwerking op een positieve manier af en zorgt ervoor dat er geen 'tijdbommen' overblijven na je vertrek.

Kortom, de hele keten werkt mee aan de veiligheid. Infrabel integreert nu systematisch beveiligingsoverwegingen in zijn aankoopproces (risicobeoordeling voor, tijdens en na het contract). Leveranciers moeten actief meewerken aan dit proces. Door maturiteit te tonen in het beheren van uw eigen ecosysteem van onderaannemers, positioneert u uzelf als een betrouwbare partner.

Omgekeerd kan elke kenbare zwakte van een leverancier de commerciële relatie in vraag stellen (door wettelijke verplichting voor Infrabel).

Sensibilisering van het personeel en veiligheidscultuur

Waarom?

Het menselijke aspect is vaak de zwakste schakel in cyberbeveiliging. Beleid en technologieën zijn niet voldoende als de medewerkers of partners die ze gebruiken niet bewust worden gemaakt van de risico's. Veel aanvallen (phishing, social engineering) richten zich rechtstreeks op individuen.

De NIS2-richtlijn dringt aan op beveiligingstraining voor het personeel en ISO 27001 wijdt verschillende controles aan bewustwording en vaardigheden. Infrabel voert regelmatig interne campagnes over deze onderwerpen (e-learning, phishingtests, communicatie).

Van de leveranciers wordt verwacht dat ze hetzelfde doen met hun eigen teams, vooral als ze werken met informatie of systemen van Infrabel.

Verwachte maatregelen

Verwachte maatregelen	Beschrijving
Basisopleidingen en voortgezette opleidingen	Zorg ervoor dat elke medewerker in uw bedrijf, en vooral de medewerkers die Infrabel-projecten uitvoeren, een basisopleiding in cyberbeveiliging krijgt. Dit moet gaan over goede beschermingspraktijken en bewustmaking van veelvoorkomende dreigingen (phishing, malware,

	fraude). Versterk deze concepten door regelmatige (bijv. jaarlijkse) sessies of korte e-learningmodules. Voorbeeld: een onderhoudsprovider heeft al zijn technici ingeschreven voor een online training "Cybersecurity", waarin best practices, risicobeheer, leveranciersbeheer en "Security by Design" aan bod komen. Deze technici kennen dus het essentiële en integreren veiligheid op natuurlijke wijze in hun werk.
Gerichte bewustmaking (phishing, fraude)	Zet simulatieoefeningen op (bijvoorbeeld het versturen van nep phishing e-mails om reactie te testen) en deel regelmatig waarschuwingen of anekdotes over cyberbedreigingen die jouw doelwit kunnen zijn. Stimuleer een cultuur waarin mensen een incident of een verdachte e-mail durven te melden zonder bang te zijn dat ze de schuld krijgen - een vals alarm is beter dan malware doorlaten. Zo heeft een toeleveringsbedrijf in Outlook voor zijn medewerkers een knop "Verdachte e-mail melden" ingesteld, die gekoppeld is aan het beveiligingsteam en gebaseerd is op een initiatief van Infrabel. Als gevolg hiervan is het aantal klikken op e-mails dat wordt onderschept tijdens interne phishing-oefeningen in een jaar tijd gedaald van 15% naar 3%, een teken dat het personeel waakzamer is geworden.
Interne communicatie over de veiligheid	Geef belangrijke informatie over informatiebeveiliging door via uw interne kanalen (vergaderingen, posters, nieuwsbrieven). Benadruk dat iedereen een rol speelt in de beveiliging, niet alleen de IT-afdeling. Erken goed gedrag en proactieve mensen (bijvoorbeeld een medewerker die een zwendel heeft vermeden, moet publiekelijk worden gefeliciteerd, omdat dit anderen aanmoedigt om op te letten). Tijdens de Europese Cyber Security Maand in oktober organiseren veel medewerkers bijvoorbeeld leuke bewustmakingsactiviteiten (quizzen, uitdagingen). Een leverancier nodigde het I-ICT.14-team van Infrabel uit om zijn medewerkers een presentatie te geven over de nieuwste dreigingen in de spoorwegsector en de juiste reflexen. Deze interactieve sessie was een groot succes en versterkte de vertrouwensrelatie tussen Infrabel en de leverancier, terwijl iedereen bewuster werd gemaakt.
Interne communicatie over de veiligheid	Door een echte cyberbeveiligingscultuur binnen uw organisatie te ontwikkelen, verkleint u de kans op kostbare menselijke fouten en voldoet u aan de verwachtingen op het gebied van regelgeving (NIS2 vereist bijvoorbeeld dat "werknemers een gedegen kennis hebben van informatiebeveiliging").

Infrabel hecht veel belang aan dit menselijke aspect van veiligheid. Uw inspanningen op dit gebied worden daarom bijzonder gewaardeerd.

We nodigen al onze leveranciers uit om contact op te nemen met ons team om deel te nemen aan een informatiesessie of om een van onze speciale cyberbeveiligingsopleidingen bij te wonen. Deze bijeenkomsten bieden de gelegenheid om de vereisten van Infrabel grondiger te bestuderen, beste praktijken uit te wisselen en samen te werken om de veiligheid van het spoorecosysteem te verbeteren.

Contractuele bepalingen en governancevereisten

Infrabel zal zijn marktmacht en wettelijke verplichtingen gebruiken om in al zijn nieuwe contracten strenge cyberbeveiligingsclausules op te nemen. De vijf essentiële clausules voor een leverancier zijn :

1. **Auditclausule :** Infrabel behoudt zich het recht voor om jaarlijks veiligheidsaudits of penetratietests uit te voeren op de geleverde oplossingen.
2. **Transparantie van de onderaanneming:** De leverancier moet zijn eigen onderaannemers aangeven en ervoor zorgen dat zij aan dezelfde beveiligingsniveaus voldoen.
3. **Behoud van de beveiliging (MCS) :** De leverancier verplicht zich om de beveiligingspatches gedurende de gehele contractuele levensduur van het product te onderhouden, met strikte SLA's voor correctie (bv. 48 uur voor een kritieke fout).
4. **Cyberverzekering :** Bewijs dat de leverancier gedekt is door een adequate cyberverzekeringspolis om de financiële gevolgen van een inbreuk op te vangen.
5. **Eindelevensbeheer** Procedure voor beveiligde gegevensvernietiging en herstel van de configuraties in geval van beëindiging.

Besluit : Naar een weerbare en conforme samenwerking

Door de hierboven beschreven concrete vereisten te implementeren, van governance tot beveiligingstechnieken, met inbegrip van detectie, reactie en beheer van uw eigen onderaannemers, versterkt u niet alleen de beveiliging van Infrabel, maar ook die van uzelf. Regelgevingskaders zoals NIS2 en de CRA hebben tot doel het niveau van cyberbeveiliging in het hele ecosysteem te verhogen: Infrabel en zijn leveranciers.

In de praktijk moedigen we u aan om de naleving van deze vereisten te formaliseren. Het verkrijgen van een ISO/IEC 27001-certificering of een verklaring van overeenstemming met het CyberFundamentals-programma van de CCB (afhankelijk van uw categorie) is een zeer gewaardeerde aanpak, die een vermoeden van overeenstemming biedt in de ogen van de NIS2-autoriteiten en uw belangrijkste klanten. Ook de deelname aan wederzijdse veiligheidsaudits of de uitwisseling van beste praktijken met Infrabel zal het vertrouwen en de doeltreffendheid van ons partnerschap versterken.

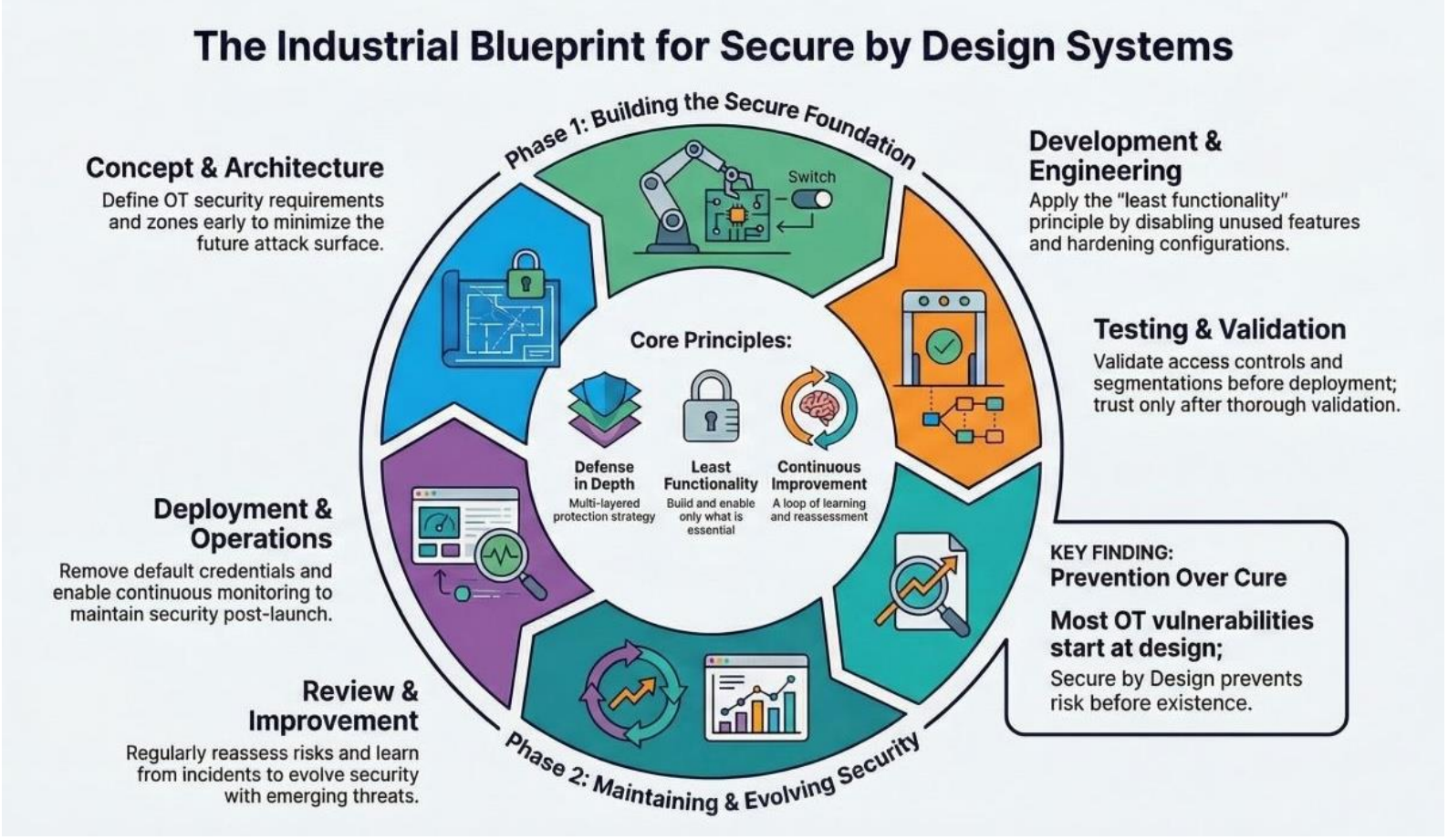
Cyberregelgeving zal zich blijven ontwikkelen (implementatie van de CRA, afronding van IEC 63452 op spoorwegniveau, enz.) De sleutel is om nu een proactieve houding aan te nemen. Door te investeren in cyberweerbaarheid verlaagt u het risico op sancties, financieel verlies of uitsluiting van de markt en positioneert u zichzelf als een betrouwbare partner voor de lange termijn. Infrabel staat klaar om u te ondersteunen bij uw groei, want onze weerbaarheid is een collectieve inspanning.

Onthoud tot slot dat cyberweerbaarheid van leveranciers is opgebouwd rond drie principes: anticiperen (risico's via governance en veilig ontwerp), monitoren/reageren (continue detectie en effectieve respons) en aanpassen/verbeteren (leren en constante evolutie). Dit is de prijs die we zullen moeten betalen als we willen samenwerken om de veiligheid en duurzaamheid van de spoorwegsector te waarborgen in het licht van de toenemende digitale dreigingen.

Nuttige contacten

Kanaal	Beschrijving
ciso@infrabel.be	Voor vragen over de veiligheidsvoorschriften van Infrabel.
csirt@infrabel.be	In geval van nood (vermoedelijke aanval) is het contactpunt van Infrabel 24/7 bereikbaar.

We willen u bedanken voor uw medewerking en uw inzet voor een veiligere digitale toekomst.



VOOR INDUSTRIËLE SYSTEMEN « SECURE-BY-DESIGN »

Dit door Infrabel aanbevolen operationele referentiemodel voor leveranciers van industriële oplossingen is gebaseerd op het „Security-by-Design“-basisprincipe.

Deze blauwdruk, verdeeld in twee grote fasen, is erop gericht om risico's te voorkomen in plaats van ze achteraf te proberen bestrijden. De kwetsbaarheidsanalyse toont aan dat de meeste kwetsbaarheden in operationele technologieën (OT) hun oorsprong vinden in de initiële ontwerpfase.

FASE 1: Een beveiligde basis bouwen

De eerste fase in de levenscyclus van een beveiligd industrieel systeem richt zich op het leggen van een solide technische en organisatorische basis. Het begint met een rigoureuze definitie van de architectuur en van de beveiligingsconcepten.

Het domein **"Concept & Architecture"** vereist dat EO veiligheidsvereisten en zonering in de vroegste stadia van het project worden gedefinieerd om het toekomstige aanvalsoppervlak zo laag mogelijk te houden. Op basis van de norm IEC 62443-3-2 moet de leverancier zijn oplossing onderverdelen in logische zones op basis van risico en kriticiteit, waarbij elke zone wordt verbonden door gecontroleerde en beveiligde 'leidingen'. Deze aanpak zorgt ervoor dat een compromis in een minder kritiek IT-gebied zich niet kan verspreiden naar de "kroonjuwelen", d.w.z. kritieke operationele systemen.

Het domein **"Development & Engineering"** implementeert het principe van de minste functionaliteit ("Least Functionality" principle). Dit omvat bijvoorbeeld het systematisch uitschakelen van alle ongebruikte functies, poorten en diensten in de standaard configuraties van de apparatuur. Daarnaast moet het hardenen (hardening) van configuraties worden gedocumenteerd zodat de essentiële entiteit de integriteit van het systeem bij oplevering kan controleren.

FASE 2: Onderhoud en evolutie van de beveiliging

Als de fundamenten eenmaal zijn gelegd, moet de beveiliging tijdens de operationele fase worden onderhouden en aangepast om het hoofd te kunnen bieden aan voortdurend veranderende dreigingen.

Het **"Tests & Validatie"** domein is het laatste filter voor de implementatie. Het vereist rigoureuze validatie van toegangscontroles en netwerksegmentaties. De leverancier moet een "Zero Trust"-houding aannemen, waarbij geen enkel onderdeel als veilig wordt beschouwd zonder grondige validatie van protocollen en identiteiten. Fabrieksacceptatietests (FAT) en siteacceptatietests (SAT) moeten cyberweerbaarheidsscenario's bevatten.

Het **"Deployment & Operations"** domein behandelt de overgang naar de effectieve productie. Een dwingende maatregel is de onmiddellijke intrekking of wijziging van alle standaard identificatiecodes en wachtwoorden die door de fabrikant worden geleverd. Tegelijkertijd moet de leverancier continue bewakingsmogelijkheden activeren om de beveiligingspositie post-productie te handhaven. Dit omvat bijvoorbeeld de integratie van industriële IDS-sondes die ongeautoriseerde logische veranderingen in OT-systemen kunnen detecteren.

Het **"Review & Improve"** -gebied sluit de cirkel met een systeem van levenslang leren. De leverancier moet de risico's regelmatig opnieuw beoordelen en lessen trekken uit eerdere incidenten om zijn oplossingen aan te passen aan nieuwe dreigingen. Deze iteratieve aanpak voldoet aan de vereisten van IEC 62443-2-1 en de NIS2-wet inzake de voortdurende verbetering van risicobeheersmaatregelen.

Implementatie van de IEC 62443-norm voor de leveranciers van Infrabel

De reeks IEC 62443, die Infrabel als referentienorm in zijn bestekken gebruikt, biedt het technische kader dat nodig is om te voldoen aan de eisen van de NIS2-wet in de industriële sector.

Elk type leverancier moet de delen van de norm identificeren die van toepassing zijn op zijn specifieke rol.

Fabrikanten van besturingssystemen, netwerkcomponenten en industriële softwaretoepassingen staan garant voor intrinsieke veiligheid van de producten (Product Suppliers - 4-1 & 4-2)

Ze moeten een veilige ontwikkelingscyclus aantonen die voldoet aan IEC 62443-4-1. Dit omvat threat modeling vanaf de ontwerpfase en een strikt beheer van de patches. Op technisch niveau (IEC 62443-4-2) moeten de componenten minimaal niveau SL 2 bereiken voor een essentiële entiteit, wat garandeert dat men bestand is tegen eenvoudige opzettelijke aanvallen.

Voor integrators en dienstverleners (Service Providers (2-4 & 3-3)

Het veiligheidsprogramma voor dienstverleners (IEC 62443-2-4) vereist een strikt beleid voor onderhoud op afstand. De integrator is er verantwoordelijk voor dat de algehele architectuur voldoet aan de systeemvereisten (IEC 62443-3-3), met name wat betreft gebruiksbeheer en beperkte gegevensstromen.

Convergentie met de Cyber Resilience Act (CRA)

Het is belangrijk om op te merken dat het Belgische regelgevingslandschap steeds meer afgestemd wordt op de toekomstige vereisten van de Europese Cyber Resilience Act (CRA), gepubliceerd op 20 november 2024. De CRA legt horizontale cyberbeveiligingsvereisten op voor alle producten met digitale onderdelen.

IEC 62443-4-2 zal naar verwachting een geharmoniseerde norm worden onder de CRA. Een industriële leverancier die vandaag IEC 62443-4-2-gecertificeerd is, zal dus vanzelfsprekend klaar zijn voor de verplichtingen van de CRA, die tegen 2027 volledig van kracht zullen zijn Deze convergentie vergemakkelijkt het compliancebeheer aanzienlijk: één enkele certificeringsinspanning volstaat om zowel te voldoen aan de contractuele NIS2-vereisten van essentiële klanten, zoals Infrabel, als aan de Europese regelgevende verplichtingen voor het op de markt brengen van producten.

Voorbeelden van maatregelen

Toepassingsdomein	Industriële maatregel (voorbeelden)	Normatieve / Wettelijke referentie
Toegang op afstand	IPsec/TLS-VPN met verplichte MFA en Privileged Access Gateway (PAM).	IEC 62443-2-4 NIS2 Art. 21
Verharding	Uitschakeling van onnodige diensten (FTP, onversleuteld HTTP) en vergrendeling van fysieke USB-poorten	IEC 62443-4-2 CRA Essential Req.
Integriteit	Cryptografische ondertekening van firmware en activering van Secure Boot op de automaten.	IEC 62443-4-2 CRA Bijlage I
SBOM	Dynamische inventaris van softwarecomponenten (open source en bedrijfseigen) die bij elke release wordt bijgewerkt.	IEC 62443-4-1 CRA Article 6
Monitoring	Integratie van OT-IDS-sensoren en export van auditlogs met tijdstempel naar het CyberSOC van Infrabel	IEC 62443-3-3 NIS2 Defensie
CVD	Publicatie van een gecoördineerd beleid voor het melden van kwetsbaarheden op de website van de leverancier.	NIS2 België CRA Deel II

Conclusie

Kortom, cyberbeveiliging van industriële oplossingen voor een essentiële Belgische entiteit als Infrabel is niet langer louter een technische optie, maar een dwingende wettelijke en contractuele verplichting

Door zich te baseren op het "Secure-by-Design"-principe en de IEC 62443-normen te respecteren, garanderen de leveranciers van Infrabel niet alleen de weerbaarheid van de kritieke nationale infrastructuren van Infrabel, maar verzekeren ze ook hun eigen voortbestaan in een steeds sterker gereguleerde markt

De inspanningen die we vandaag leveren om onze processen te structureren en onze producten te verharden, zijn de beste investering die we kunnen doen om de cyberuitdagingen van morgen het hoofd te bieden.

CRA-CONFORME PRODUCTEN

De Cyber Resilience Act (CRA) is een horizontale verordening van de Europese Unie, aangenomen in oktober 2024, die de verplichtingen vastlegt van leveranciers die producten met digitale elementen (PDE) aanbieden op de Europese markt.

De CRA legt de basisveiligheidseisen vast voor alle digitale producten die op de EU-markt worden gebracht. De verordening is van toepassing op alle soorten producten, van slimme apparaten en ingebedde systemen tot pure softwaretools. Als uw product verbinding maakt met een netwerk, is de kans groot dat het hieronder valt.

De CRA-verordening introduceert ook een nieuw niveau van verantwoordelijkheid in de toeleveringsketen van digitale producten. U bent verplicht om cyberbeveiliging te beschouwen als een fundamentele vereiste van het product, en niet als een extra functionaliteit. Deze verordening integreert beveiliging vanaf de eerste fasen van de ontwikkeling en de aankoop.

Doelstelling en wetgevende context

Vóór de inwerkingtreding van de CRA verschilden de regels op het gebied van cyberbeveiliging van land tot land. Dit leidde tot enige verwarring en liet hiaten achter in het totale productlandschap.

De CRA vervangt deze lappendeken door een duidelijk kader dat geldt voor alle EU-lidstaten

Waarom is dit belangrijk voor productbeveiligingsverantwoordelijken?

Uw rol beperkt zich niet tot het afvinken van vakjes: het gaat om het beschermen van gebruikers en het ondersteunen van de doelstellingen van het bedrijf. De CRA biedt u een duidelijk pad om deze twee doelstellingen te bereiken. Vroegtijdige voorbereiding helpt uw team om veilig, compliant en concurrerend te blijven

De CRA vanuit het perspectief van de EIM (European Infrastructure Managers)

De EIM, waarvan Infrabel een actief lid is, juicht de CRA en de fundamentele paradigmaverschuiving op het gebied van digitale veiligheid die deze binnen de EU teweegbrengt, toe : het huidige niveau van cyberbeveiliging van PDE's is laag en moet worden versterkt om cyberrisico's in alle sectoren te verminderen. De CRA bestrijkt de volledige levenscyclus van het product, van planning, ontwerp, ontwikkeling of productie, testen en onderhoud tot buitendienststelling

Hoewel het om horizontale wetgeving gaat die op talrijke sectoren van toepassing is, bevat de CRA specifieke bepalingen die erkennen dat bepaalde EDP's moeten voldoen aan sectorspecifieke wetgeving (zoals de technische specificaties voor interoperabiliteit (TSI)) en bijgevolg mogelijk moeten afwijken van bepaalde essentiële eisen van de CRA. Daartoe voorziet de CRA in duidelijke mechanismen om met dergelijke situaties rekening te houden

Bovendien is de CRA, zoals aangegeven in de preambule, bedoeld als aanvulling op het door de NIS2-richtlijn vastgestelde rechtskader door te waarborgen dat de hardware- en softwareproducten die door infrastructuurbeheerders worden gebruikt, aan bepaalde essentiële cyberbeveiligingseisen voldoen

Beveilig uw producten in overeenstemming met de Europese Cyber Resilience Act (CRA) dankzij SBOM's

Elk PDE dat vanaf 11 december 2027 op de markt wordt gebracht, moet voldoen aan de essentiële cyberbeveiligingsverseisten van de CRA, en de fabrikant moet gedurende de gehele verwachte levensduur van dat PDE ondersteuning bieden op het gebied van kwetsbaarheden.

Voor teams die verbonden apparaten ontwikkelen, gaat het niet langer alleen om innovatie. De CRA voert de eerste uniforme regelgeving op het gebied van cyberbeveiliging in. De "Software Bill of Material" (SBOM) is voortaan een verplichting, en niet langer slechts een troef.

Wat is de Europese Cyber Resilience Act (CRA)?

Waarom zijn SBOM's essentieel om aan de CRA te voldoen?

SBOM's geven gedetailleerde informatie over alle softwarecomponenten die in uw product worden gebruikt. Deze zichtbaarheid is essentieel om kwetsbaarheden te identificeren en daar snel op te reageren. De SBOM-vereisten van de CRA zijn gebaseerd op het idee dat volledig inzicht noodzakelijk is om de veiligheid en naleving te waarborgen.

Onder de CRA zijn SBOM's niet alleen bedoeld voor intern gebruik; ze maken deel uit van het officiële technische dossier van uw product. Als de markttoezichtautoriteiten daarom vragen, moet u een actuele SBOM met traceerbare softwareherkomst verstrekken. Met dit document laat u toezichthouders zien dat u transparantie en veiligheid serieus neemt.

De rol van SBOM's in productveiligheid

Een SBOM werkt als een numerieke nomenclatuur, die aangeeft wat uw code bevat. Het bevat bibliotheken, pakketten en componenten van derden die beveiligingsrisico's kunnen inhouden. Met deze informatie kunt u problemen in de gaten houden en snel handelen wanneer er dreigingen opduiken.

Voordelen voor fabrikanten en ontwikkelaars

SBOM's bieden uw team een concreet voordeel, ongeacht de functie. Bijvoorbeeld:

- Ontwikkelaars kunnen afhankelijkheden bijhouden en risico's vroegtijdig identificeren
- Beveiligingsmanagers kunnen bekende kwetsbaarheden koppelen aan effectieve componenten
- Compliance verantwoordelijken beschikken over duidelijke en actuele documentatie voor audits

Wie moet de CRA naleven?

De CRA is niet alleen van toepassing op fabrikanten. Hieronder vallen ook importeurs, distributeurs en verschillende actoren binnen de product- en beveiligingsteams.

Elke speler in de toeleveringsketen moet ook begrijpen hoe naleving van de CRA zich verhoudt tot andere EU-regelgeving, zoals de NIS2-richtlijn. Afhankelijk van uw sector of uw implementatiemodel ( ) kunt u onderworpen zijn aan meerdere regelgevingskaders. Een geharmoniseerde aanpak tussen de teams voorkomt dubbel werk en niet-nakoming van verplichtingen.

Fabrikanten

U bent verplicht om cyberbeveiliging vanaf het begin in het product in te bouwen. Dit omvat het opstellen en bijwerken van een SBOM, het uitvoeren van risicobeoordelingen en het documenteren van incidentrespons.

Voor sommige producten kan een conformiteitsbeoordeling door een derde partij nodig zijn, afhankelijk van hun kriticiteitsniveau.

Importeurs

U moet ervoor zorgen dat de producten die u in de EU invoert, voldoen aan de CRA-vereisten. Dit houdt onder meer in dat u controleert:

- Of de fabrikant een risicobeoordeling heeft uitgevoerd
- Of er een actuele lijst van softwarecomponenten (SBOM) en de bijbehorende documentatie beschikbaar is
- Of het product de juiste conformiteitsmarkeringen draagt

Het niet naleven van deze controles kan leiden tot juridische problemen of moeilijkheden bij de toegang tot de markt.

Distributeurs

U bent verplicht te controleren of elk product dat u distribueert voldoet aan de CRA-verplichtingen. Dit houdt onder meer in dat u ervoor moet zorgen dat de SBOM's en conformiteitsregisters aanwezig zijn. Als dit niet het geval is, mag het product niet legaal binnen de EU worden verkocht.

PSIRT-verantwoordelijke

In het kader van de CRA wordt het kwetsbaarheidsbeheer een officiële verantwoordelijkheid. U moet de risico's bewaken, ernstige kwetsbaarheden binnen 24 uur melden en de toepassing van patches op alle producten coördineren

Compliance-verantwoordelijke

U moet de naleving gedurende de hele levenscyclus van de producten bewaken. Dit houdt onder meer in dat u de SBOM's bewaart, incidenten registreert en de documentatie gedurende ten minste vijf jaar bewaart. Het gebruik van een SBOM-beheertool kan u uren handmatig werk besparen en de stress in verband met audits verminderen.

Welke producten vallen onder de CRA?

Elk product met digitale componenten dat in de EU wordt verkocht, kan hieronder vallen. Dit omvat consumentenapparatuur, industriële besturingssystemen, mobiele applicaties en firmware. Voor producten die behoren tot strikt gereguleerde sectoren, zoals de automobiel- of defensie-industrie, gelden mogelijk andere regels.

Wat is de impact van de CRA op de beveiliging van de firmware van apparaten?

In het kader van de CRA wordt firmware beschouwd als software. U moet dus kwetsbaarheden bijhouden, een lijst van softwarecomponenten (SBOM) bijwerken en ervoor zorgen dat updates beschikbaar zijn gedurende de gehele ondersteuningsperiode

Hoe vergemakkelijkt de transparantie van SBOM's het kwetsbaarheidbeheer in het kader van de CRA?

SBOM's geven u inzicht in de samenstelling van uw software, inclusief componenten van derden en open source. Dus als er een nieuw CVE-kwetsbaar punt wordt gemeld, weet u onmiddellijk of u erdoor wordt getroffen. Dit verkort uw reactietijd en versterkt het incidentbeheer.

Waarom is SBOM belangrijk voor productveiligheid?

SBOM's maken softwareleveringsketens zichtbaar en beheersbaar. Ze helpen u zwakke plekken te detecteren voordat aanvallers dat doen en vereenvoudigen de rapportage over naleving. Daarom staan SBOM's centraal in de CRA-vereisten voor SBOM's en in de moderne cyberbeveiligingsstrategie

Belangrijkste vereisten van het CRA

De CRA omvat technische en organisatorische maatregelen om gebruikers en systemen te beschermen. Als u de basisvereisten begrijpt, weet u waar u moet beginnen. SBOM's zijn slechts een deel van het plaatje.

De CRA introduceert ook productclassificatieniveaus: standaard, belangrijk en kritiek. Kritieke producten, zoals firewalls of intrusiedetectiesystemen, vereisen conformiteitsbeoordelingen door derden. Als u de classificatie van uw product kent, kunt u bepalen welke verplichtingen van toepassing zijn en hoe streng uw aanpak moet zijn.

Vereisten met betrekking tot de SBOM

U moet voor elk digitaal product een SBOM opstellen, in een formaat zoals SPDX of CycloneDX. De aanbevelingen van de Europese Cyber-Resilience Act over SBOM leggen de nadruk op afhankelijkheden op het hoogste niveau, machineleesbaarheid en traceerbaarheid tussen de verschillende versies van het product. Hoewel het SBOM niet openbaar hoeft te worden gemaakt, moet het op verzoek wel beschikbaar worden gesteld aan de Europese autoriteiten.

Vereisten met betrekking tot kwetsbaarheden

U moet beschikken over een gedocumenteerd proces voor het kwetsbaarheidbeheer. Dit omvat het opvolgen van risico's met betrekking tot componenten via de SBOM, snel reageren op bekende problemen en het melden van uitgebuite kwetsbaarheden via een centraal platform. Elke vertraging of nalatigheid in dit proces kan leiden tot sancties.

Melding van incidenten en documentatie van risico's

De CRA eist bewijs dat u vanaf dag één rekening hebt gehouden met beveiliging. Dit omvat het documenteren van incidenten, risico's en SBOM-updates die aan elke versie zijn gekoppeld. Weet u niet precies wat de CRA-vereisten voor SBOM inhouden? Begin dan met het onderzoeken van de zichtbaarheid van uw afhankelijkheden en de manier waarop u de kwetsbaarheden van de componenten opvolgt.

Voorbereiding op de naleving van de CRA met behulp van SBOM's

U hoeft niet te wachten tot de deadlines om uw productontwikkeling te beginnen afstemmen op de CRA-vereisten. Door nu te handelen, zorgt u ervoor dat uw team kan profiteren van soepelere productlanceringen en onvoorziene omstandigheden kan verminderen. SBOM's vormen de basis van deze aanpak.

De CRA moedigt een proactieve, in plaats van reactieve, benadering van compliance aan. Door SBOM-tools en -processen in een vroeg stadium te integreren, kan uw team risico's opsporen voordat deze de lanceringstermijnen beïnvloeden. Dit maakt audits en documentatie achteraf ook veel minder storend.

Uitvoeren van productrisicobeoordelingen

Elk product moet worden onderworpen aan een risicobeoordeling met betrekking tot cyberbeveiliging voordat het wordt gelanceerd. U moet het gebruik van software van derden, de aanvalsoppervlakken en uw vermogen om patches toe te passen of updates uit te voeren, beoordelen. SBOM's helpen u door precies te onthullen wat er in uw code staat en waar risico's op de loer kunnen liggen.

Efficiënte implementatie van de SBOM's

Het handmatig aanmaken van SBOM's is niet schaalbaar. Gebruik in plaats daarvan tools die:

- SBOM's genereren tijdens de compilatie- of CI/CD-fasen
- Erkende formaten ondersteunen, zoals SPDX of CycloneDX
- Wijzigingen tussen versies bijhouden en waarschuwingen geven bij nieuwe risico's

CRA-vereisten integreren in ontwikkelingsprocessen

Beveiliging moet een integraal onderdeel zijn van de ontwikkeling en mag niet achteraf worden toegevoegd. U kunt controles vóór de publicatie instellen, SBOM's koppelen aan DevSecOps-tickets en analyses uitvoeren tijdens code-pushes. Door dit in uw workflow te integreren, blijft u op schema en bent u klaar voor audits.

Toepassing van de wet en impact op de bedrijven

De CRA voorziet in een duidelijke planning voor de toepassing en concrete gevolgen bij niet-naleving. Maar er zijn ook voordelen: proactieve teams kunnen van compliance een betrouwbaar bedrijfsmiddel maken. Hoe eerder u handelt, hoe soepeler de overgang zal verlopen.

De CRA overbrugt de kloof tussen softwarebeveiliging en productaansprakelijkheid. Zodra de wet is geïmplementeerd, zullen de nationale autoriteiten controles uitvoeren en bewijs van naleving eisen. Als u deze naleving duidelijk kunt aantonen, levert dat u een operationeel en reputatievoordeel op.

Timing en sancties

Hieronder zetten we alles nog eens op een rijtje...

- De CRA is op 10 december 2024 in werking getreden
- De aangifte van kwetsbaarheden wordt verplicht vanaf 11 september 2026
- Volledige naleving van de SBOM is vereist vanaf 11 december 2027
- Maximale sanctie: 15 miljoen euro of 2,5% van de jaaromzet

U heeft nog tijd, maar sommige verplichtingen zijn al van kracht; wachten tot 2027 is een riskante beslissing.

Commerciële en financiële risico's

Bij niet-naleving staat er veel meer op het spel dan alleen juridische aansprakelijkheid. U kunt te maken krijgen met:

- Vertraagde lanceringen of geblokkeerde toegang tot de EU-markt
- Verlies van vertrouwen bij klanten of partners
- Hogere kosten door overhaaste correcties of wijzigingen op het laatste moment

Door u vroeg voor te bereiden, vermijd u deze valkuilen en beschermt u uw financiële resultaten

Naleving als concurrentievoordeel

Naleving van de CRA-normen toont aan dat u veiligheid serieus neemt. Dankzij begeleiding gedurende de hele levenscyclus en volledige zichtbaarheid op uw CRA SBOM-processen in de EU versterkt u het vertrouwen van zowel toezichthouders als klanten

BEOORDELING VAN DE DREIGINGSCONTEXT

In een supply chain-relatie tussen Infrabel en zijn leveranciers is de dreigingscontext tweerichtingsverkeer.

Enerzijds moet Infrabel anticiperen op risico's die bij leveranciers kunnen ontstaan, met name het gecompromitteerd raken van essentiële componenten of diensten die de beveiliging van zijn kritieke infrastructuur kunnen beïnvloeden.

Anderzijds worden onze leveranciers zelf blootgesteld aan dreigingen vanuit de bedrijfsomgeving van Infrabel, zoals de verspreiding van cyberaanvallen, regelgevende druk of de openbaarmaking van kwetsbaarheden die hun reputatie en activiteiten kunnen aantasten

Deze wederzijdse band betekent dat elke partij niet alleen haar eigen belangen moet beschermen, maar ook nauw moet samenwerken om gedeelde risico's te identificeren en te verminderen. Transparantie, coördinatie op het vlak van kwetsbaarheidsbeheer en de toepassing van gemeenschappelijke normen zoals IEC 62443 versterken de algehele weerbaarheid van de bevoorradingsketen, terwijl ze tegelijkertijd de duurzaamheid en conformiteit van de activiteiten voor Infrabel en zijn leveranciers waarborgen.

Georganiseerde misdaad

Risicobron

De actoren van de georganiseerde misdaad omvatten gestructureerde cybercriminele organisaties zoals maffia's, bendes of gespecialiseerde groeperingen. Deze entiteiten opereren met winstoogmerk en maken deel uit van een georganiseerd, gestructureerd en voortdurend evoluerend crimineel ecosysteem

Dit ecosysteem is gebaseerd op een specialisatie van rollen, waaronder :

- Ontwikkelaars van malware
- Aanvalsoperatoren
- Initial Access Brokers
- Tussenpersonen die gespecialiseerd zijn in de doorverkoop van gegevens of toegang

Dit model, dat vaak wordt aangeduid als "Cybercrime-as-a-Service" (CaaS) of "Ransomware-as-a-Service" (RaaS), maakt het mogelijk om aanvalcapaciteiten te bundelen en aanvallen te industrialiseren.

Georganiseerde criminelen kunnen ook samenwerken met andere samenwerken met andere partijen, met name gespecialiseerde bureaus, om hun technische capaciteiten te versterken of bepaalde fasen van de aanval uit te besteden.

Beoogde doelstellingen

De actoren van de georganiseerde misdaad streven voornamelijk doelstellingen na die vallen onder de categorie 'winstbejag', zoals gedefinieerd in de EBIOS Risk Manager-methode.

Deze doelstellingen komen concreet neer op :

- Het nastreven van direct financieel gewin, met name via ransomware-campagnes die erop gericht zijn systemen te blokkeren en losgeld te eisen

- Financiële fraude, waaronder mechanismen zoals CEO-identiteitsfraude en online oplichting
- Indirecte winstgeneratie door de doorverkoop van gevoelige gegevens of toegang tot gehackte systemen
- Exploitatie van IT-middelen (botnets, cryptomining)

Daarnaast vallen bepaalde operaties ook onder de categorie 'belemmering van de werking', met name wanneer cybercriminelen systemen onbeschikbaar maken om de druk op het slachtoffer te verhogen (bijv. versleuteling van gegevens, stopzetting van kritieke diensten).

Hoewel het uiteindelijke doel financieel is, kunnen de operationele gevolgen dus een grote impact hebben op de bedrijfscontinuïteit.

Motivatie

Zeer hoog - motieven zijn uitsluitend financieel Cybercriminelen streven ernaar hun winst te maximaliseren door kritieke of kwetsbare organisaties als doelwit te kiezen en door operationele druk uit te oefenen om snelle betalingen te verkrijgen.

Middelen

Hoog tot zeer hoog - deze actoren beschikken over aanzienlijke financiële middelen, toegang tot geavanceerde tools en een gestructureerde organisatie. Sommige groepen zijn in staat om 0-day-kwetsbaarheden te verwerven of te ontwikkelen en te investeren in complexe aanvalsinfrastructuren.

Activiteit

Zeer hoog - cybercriminelen voeren voortdurende, vaak geautomatiseerde campagnes uit, waarbij ze het volgende combineren:

- Grootschalige opportunistische aanvallen
- Semigerichte aanvallen
- Gerichte operaties tegen organisaties met een hoge waarde.

Werkwijze

De actoren van de georganiseerde misdaad gebruiken gestructureerde en geïndustrialiseerde aanvalsketens, waarin verschillende technieken worden gecombineerd:

- Phishing-campagnes voor initiële toegang
- Uitbuiting van kwetsbaarheden op blootgestelde systemen (VPN's, servers, toepassingen)
- Verhoging van privileges en zijwaartse bewegingen
- Inzet van ransomware met dubbele afpersing (versleuteling + lekken van gegevens)
- Gebruik van botnets voor grootschalige aanvallen
- Gerichte fraude (bijv. CEO-identiteitsfraude)

Deze aanvallen kunnen opportunistisch of gericht zijn, afhankelijk van de waargenomen waarde van het doelwit. De beschikbaarheid van online toegankelijke aanvalskits stelt ook minder ervaren actoren in staat om efficiënte aanvallen uit te voeren.

Gerichte activiteitensectoren

Cybercriminelen richten zich in de eerste plaats op :

- Kritieke infrastructuur (transport, energie) ;
- Grote bedrijven ;
- Organisaties die afhankelijk zijn van hun informatiesystemen;
- Entiteiten met een lage maturiteit op het gebied van cyberbeveiliging.

In het geval van Infrabel is de spoorwegsector een bijzonder aantrekkelijk doelwit omwille van :

- De kriticiteit van de diensten
- Afhankelijkheid van IT/OT-systemen
- Operationele druk die het betalen van losgeld in de hand werkt

Het arsenaal aan aanvalsmiddelen

Cybercriminelen beschikken over een gevarieerd en voortdurend evoluerend arsenaal aan aanvalsmiddelen:

- ransomware
- Online beschikbare aanvalkits
- Command-and-control-infrastructuren (C2)
- botnets
- Tools om kwetsbaarheden te misbruiken
- Eerste toegang gekocht op clandestiene markten
- Tools voor het exfiltreren en versleutelen van gegevens

Wapenfeiten

- aanval op Colonial Pipeline
- WannaCry-aanval

Deze incidenten illustreren het vermogen van cybercriminelen om kritieke infrastructuren te verstoren, grote economische gevolgen te veroorzaken en kwetsbaarheden op grote schaal uit te buiten.

Staatsaanvallen

Risicobron

Staatsaanvallers omvatten staten, hun inlichtingendiensten en cybermilitaire eenheden. Deze entiteiten beschikken over een gestructureerde organisatie en geavanceerde, aanzienlijke, zelfs vrijwel onbeperkte middelen, waardoor ze gedurende lange tijd cyberaanvallen kunnen uitvoeren.

Deze actoren onderscheiden zich door hun vermogen om complexe, geplande en gecoördineerde operaties uit te voeren, gesteund door stabiele middelen en vastgelegde procedures. Ze zijn in staat om hun tools en methoden aan te passen aan de topologie van het doelwit en een hoge mate van discretie te behouden.

Ze kunnen ook indirecte vectoren gebruiken, in het bijzonder door leveranciers of partners te compromitteren, en sommigen hebben de mogelijkheid om onbekende (0-day) kwetsbaarheden te verwerven of te ontdekken.

Beoogde doelstellingen

Staatsaanvallers streven meerdere doelstellingen na, die voornamelijk vallen onder de volgende categorieën die zijn gedefinieerd in de EBIOS Risk Manager-methode

- Spionage
  - strategische informatie verzamelen (industrieel, politiek, militair) ;
  - langdurige bewaking van informatiesystemen ;
  - verwerven van Intellectueel eigendomsrecht
- strategische voorpositionering
  - infiltratie van systemen met het oog op toekomstige actie
  - het behouden van langdurige toegang
  - voorbereiding van sabotage- of destabilisatieoperaties.
- Beïnvloeding
  - verspreiding van informatie of verkeerde informatie
  - schade aan het imago van een organisatie of staat
  - manipulatie van de publieke opinie
- Belemmering van de werking (in bepaalde gevallen)
  - sabotage van kritieke systemen
  - verstoring van essentiële diensten
  - opzettelijke aantasting van operationele capaciteiten

Deze doelstellingen maken deel uit van een logica van macht, soevereiniteit en strategisch voordeel, en kunnen veranderen afhankelijk van de geopolitieke context.

Motivatie

Zeer hoog - strategische, politieke, economische of militaire motivaties. Deze actoren handelen vanuit een langetermijnvisie en in het nationaal belang.

Middelen

Zeer hoog - vrijwel onbeperkte menselijke, technische en financiële middelen. Het vermogen om geavanceerde tools te ontwikkelen of aan te schaffen, inclusief 0-day kwetsbaarheden.

Activiteit

Matig tot hoog: operaties vinden minder vaak plaats dan bij de georganiseerde misdaad, maar zijn doelgericht, discreet en worden op de lange termijn uitgevoerd.

Werkwijze

Staatsaanvallers voeren geavanceerde APT-campagnes (Advanced Persistent Threat) uit, die in verschillende fasen zijn gestructureerd:

- initiële gerichte compromittering (phishing, supply chain, uitbuiten van kwetsbaarheden)
- implementatie van persistentiemechanismen
- uitbreiding van rechten en onopvallende laterale bewegingen
- verzamelen van informatie op lange termijn

- behoud van duurzame toegang
- eventueel uitvoeren van impactvolle acties (sabotage)

Deze aanvallen worden gekenmerkt door hun discretie, hun aanpassingsvermogen en hun duur.

Doelsectoren

Staatsaanvallers richten zich in de eerste plaats op:

- kritieke infrastructuren (vervoer, energie, gezondheid)
- strategische industrieën
- overheidsinstellingen
- hightechbedrijven

In het geval van Infrabel is de spoorwegsector een strategisch doelwit vanwege zijn rol in de nationale continuïteit en logistiek.

Het arsenaal aan aanvalsmiddelen

- geavanceerde malware (APT)
- 0-dagen exploits
- persistentie en stealth tools
- command-and-control-infrastructuren (C2)
- spionage- en exfiltratiehulpmiddelen
- supply chain-technieken

Wapenfeiten

- SolarWinds-aanval
- Stuxnet-aanval

Deze operaties illustreren het vermogen van staatsactoren om complexe, onopvallende aanvallen uit te voeren met een grote strategische impact.

Terrorist

Risicobron

Terroristische actoren omvatten cyberterroristen, cybermilities en gewelddadige ideologische groeperingen die cyberspace gebruiken als een als een aanvullend actiemiddel naast hun traditionele operaties.

Deze actoren beschikken doorgaans over beperkte technische middelen in vergelijking met staatsaanvallers of de georganiseerde misdaad, maar compenseren deze zwakte met een sterke vastberadenheid en door zich te richten op kritieke infrastructuren. Hun acties zijn vaak gericht op een onmiddellijke en zichtbare impact.

Hun slagkracht kan worden versterkt door het gebruik van online beschikbare tools of door opportunistische samenwerkingen met andere actoren (gespecialiseerde bureaus, cybercriminelen).

Beoogde doelstellingen

Terroristische actoren streven voornamelijk doelstellingen na die vallen onder de categorie 'belemmering van de werking', zoals gedefinieerd in de EBIOS Risk Manager-methode. Deze doelstellingen komen neer op.

- Belemmering van de werking
  - essentiële diensten onbeschikbaar maken (bijv. nooddiensten, kritieke systemen)
  - stilstand van industriële of energiesystemen veroorzaken
  - de normale werking van een organisatie of infrastructuur verstoren
  - informatiesystemen verzadigen (bijv. DDoS-aanvallen)
- Beïnvloeding
  - media-aandacht voor acties
  - verspreiding van ideologische boodschappen
  - creëren van een klimaat van angst of onveiligheid

Deze doelstellingen zijn vooral bedoeld om een sterke maatschappelijke impact te hebben door zichtbare en onmiddellijke destabilisatie te veroorzaken.

Motivatie

Zeer hoog: sterke ideologische drijfveren, vaak gekoppeld aan een streven naar destabilisatie, vernietiging of media-aandacht

Middelen

Laag tot gemiddeld: beperkte technische middelen, maar gecompenseerd door het gebruik van toegankelijke hulpmiddelen en een sterke vastberadenheid

Activiteit

Laag tot matig: minder frequente aanvallen, maar met potentieel grote impact, vaak uitgelokt in specifieke contexten (spanningen, eisen).

Werkwijze

Terroristen gebruiken relatief eenvoudige maar doeltreffende werkwijzen, gericht op onmiddellijke impact:

- dDoS-aanvallen (Denial of Service)
- kwetsbaarheden in websites uitbuiten
- bekladding van sites (defacement)
- verstoring van industriële of kritieke systemen
- een combinatie van cyber- en media-acties

Deze aanvallen zijn over het algemeen ongenuanceerd, maar doelgericht en vastberaden, met een onmiddellijk effect.

Doelsectoren

Terroristische actoren richten zich voornamelijk op :

- kritieke infrastructuren (transport, energie, gezondheid)
- overheidsdiensten
- organisaties met een grote zichtbaarheid

In het geval van Infrabel is de spoorwegsector een strategisch doelwit omwille van :

- zijn rol bij het waarborgen van de continuïteit van overheidsdiensten
- Zijn directe impact op de samenleving
- zijn zichtbaarheid in de media

Het arsenaal aan aanvalsmiddelen

- dDoS-tools
- scripts voor het uitbuiten van kwetsbaarheden
- defacement tools
- online beschikbare aanvalskits

Wapenfeiten

- dDoS-aanvallen tegen overheids- en ziekenhuisdiensten ;
- campagnes om websites van de overheid te bekladden;
- pogingen om industriële systemen te verstoren.

Deze incidenten illustreren het vermogen van terroristische actoren om een impact te genereren die niet in verhouding staat tot hun technische middelen.

Ideologische activist

Risicobron

Ideologische activisten zijn hacktivisten, militante collectieven of gemeenschappen die zich inzetten voor een politieke, maatschappelijke of milieukwestie. Deze actoren gebruiken cyberspace als een middel om zich uit te drukken en actie te ondernemen, om hun eisen te kracht bij te zetten of organisaties aan de kaak te stellen.

In tegenstelling tot terroristische actoren is hun doel meestal niet vernietiging maar zichtbaarheid en invloed. Ze kunnen spontaan of gecoördineerd handelen, vaak via online gemeenschappen of sociale netwerken.

Hun slagkracht is gebaseerd op collectieve mobilisatie, de virale verspreiding van campagnes en het gebruik van toegankelijke tools.

Beoogde doelstellingen

Ideologische activisten streven voornamelijk doelstellingen na die vallen onder de categorie invloed, zoals gedefinieerd in de EBIOS Risk Manager-methode. Deze doelstellingen komen tot uiting in:

- Beïnvloeding
  - verspreiding van informatie of militante boodschappen
  - schade aan de reputatie van een organisatie

    - openbaar maken van gevoelige gegevens om praktijken aan de kaak te stellen
    - de publieke opinie mobiliseren via sociale netwerken
- Belemmering van de werking
    - eenmalige verstoring van diensten (bijv. DDoS)
    - tijdelijke aantasting van het imago of de activiteiten
    - symbolische blokkering van platforms of diensten

Deze acties zijn vooral bedoeld om media-aandacht te genereren en de publieke perceptie te beïnvloeden, in plaats van blijvende schade aan te richten.

Motivatie

Hoog: sterke ideologische drijfveren, gekoppeld aan een doel (politiek, milieu, maatschappij) Streven naar zichtbaarheid en media-aandacht.

Middelen

Laag tot matig: beperkte technische middelen, maar vermogen om een groot aantal actoren te mobiliseren en toegankelijke tools te gebruiken.

Activiteit

Matig tot hoog: activiteit afhankelijk van de actualiteit en de verdedigde doelen, met campagnes die grootschalig maar eenmalig kunnen zijn.

Werkwijze

Ideologische activisten ondernemen actie om zichtbaarheid te krijgen:

- dDoS-aanvallen gericht op het onbeschikbaar maken van diensten
- verminken van websites (defacement)
- openbaar maken van gegevens (datalekken)
- beïnvloedingscampagnes op sociale media
- online gemeenschappen mobiliseren

Deze acties worden vaak bevestigd en gaan gepaard met een communicatiestrategie om hun impact te versterken.

Doelsectoren

Ideologische activisten richten zich vooral op :

- overheids- of regeringsorganisaties
- bedrijven die betrokken zijn bij sociale kwesties (energie, transport, milieu)
- organisaties met veel media-aandacht

In het geval van Infrabel kan de spoorsector het doelwit zijn in verband met :

- milieukwesties
- politieke of sociale beslissingen
- zichtbare belemmering van de dienst

Het arsenaal aan aanvalsmiddelen

- dDoS-tools
- verminkingsscripts
- verspreidingsplatforms (sociale media)
- gegevensverspreidingstools
- toegankelijke aanvalskits

Wapenfeiten

- Anonymous - openbaarmakingscampagnes en DDoS
- Killnet - gecoördineerde DDoS-aanvallen

Deze acties illustreren het vermogen van activisten om gemeenschappen te mobiliseren en aanzienlijke media-aandacht te genereren.

Gespecialiseerd bureau

Risicobron

De gespecialiseerde bureaus brengen geavanceerde technische spelers samen, soms "cyberhuurlingen" genoemd, met een hoog niveau van expertise in offensieve cyberbeveiliging. In tegenstelling tot traditionele cybercriminelen richten deze spelers zich niet noodzakelijkerwijs rechtstreeks op hun eindslachtoffers, maar fungeren ze als dienstverleners of leveranciers van offensieve capaciteiten.

Ze ontwerpen, ontwikkelen en stellen aanvalsinstrumenten, diensten of infrastructuren ter beschikking die door andere actoren, zoals cybercriminelen of staatsactoren, worden gebruikt. Hun activiteiten maken deel uit van een gestructureerd businessmodel en dragen bij aan de industrialisering van cyberaanvallen.

Deze spelers zitten vaak achter de ontwikkeling van aanvalskits, malware of diensten die op clandestiene markten verkocht worden, waardoor het voor minder ervaren profielen makkelijker wordt om toegang te krijgen tot aanvallende middelen.

Beoogde doelstellingen

Gespecialiseerde bureaus streven voornamelijk doelstellingen na die vallen onder de categorie 'winstbejag', zoals gedefinieerd in de EBIOS Risk Manager-methode.

Deze doelstellingen komen neer op:

- Winstbejag
  - ontwikkeling en verkoop van aanvalstools (malware, exploits, aanvalskits)
  - leveren van hackingdiensten op aanvraag
  - te gelde maken van technische capaciteit (infrastructuur, toegang, tools)
  - verkoop van kwetsbaarheden, inclusief potentieel onbekende (0-day) kwetsbaarheden
- strategische voorpositionering
  - derden blijvende toegang bieden tot gecompromitteerde systemen

- indirecte deelname aan langetermijnoperaties die door andere actoren worden uitgevoerd

Deze doelstellingen weerspiegelen een logica van technische dienstverlening en het te gelde maken van offensieve competenties, in plaats van een directe focus op de uiteindelijke slachtoffers

Motivatie

Hoog: voornamelijk financiële motivatie, gebaseerd op het te gelde maken van geavanceerde technische competenties en gespecialiseerde diensten

Middelen

Hoog: sterke technische expertise, vermogen om geavanceerde tools te ontwikkelen, toegang tot geavanceerde technische middelen.

Activiteit

Matig tot hoog: activiteit afhankelijk van de vraag, met een indirecte maar structurerende rol in talrijke cyberoperaties.

Werkwijze

De gespecialiseerde bureaus interveniëren voornamelijk in de ondersteuning of in de aanloop naar aanvallen, door middel van

- ontwikkeling van malware en exploitatietools
- maken en verspreiden van aanvalskits
- verkoop van initiële toegang tot gecompromitteerde systemen
- terbeschikkingstelling van technische infrastructuur (servers, C2, botnets)
- piraterijdiensten op aanvraag

Zij spelen een centrale rol in de industrialisering van cyberaanvallen door de toegang tot offensieve capaciteit voor andere actoren te vergemakkelijken.

Doelsectoren

Gespecialiseerde bureaus richten zich niet rechtstreeks op specifieke sectoren, maar hun tools kunnen worden ingezet tegen :

- Kritieke infrastructuur
- grote bedrijven
- overheidsinstellingen

In de context van Infrabel vormen deze actoren een indirecte dreiging, omdat ze de mate van verfijning van de aanvallen verhogen.

Het arsenaal aan aanvalsmiddelen

- Op maat gemaakte malware
- exploits (inclusief 0-days)

- aanvalskits
- command-and-control-infrastructuren (C2)
- persistentie en ontwijkingstools
- platforms voor cybercriminele diensten

Wapenfeiten

Aangezien gespecialiseerde bureaus ondersteunende spelers zijn, zijn hun acties zelden direct zichtbaar. Hun bijdrage kan echter worden gezien in :

- de verspreiding van veelgebruikte aanvalskits
- het beschikbaar stellen van tools die worden gebruikt in grote ransomwarecampagnes
- ontwikkeling van exploits die door verschillende groepen aanvallers worden hergebruikt

Deze elementen illustreren hun sleutelrol in de structurering van het cybercriminele ecosysteem.

Amateur-aanvaller

Risicobron

Amateur-aanvallers zijn personen met beperkte tot gemiddelde computervaardigheden, vaak "scriptkiddies" genoemd. Deze spelers ontwikkelen over het algemeen geen eigen tools, maar gebruiken oplossingen die online beschikbaar zijn, vaak kant-en-klaar.

Hun activiteiten vinden plaats tegen een achtergrond waarin offensieve tools steeds toegankelijker worden, wat wordt vergemakkelijkt door de verspreiding van aanvalskits, tutorials en gespecialiseerde platforms. Deze toegankelijkheid verlaagt de technische drempels en stelt een groot aantal individuen in staat om aanvallen uit te voeren, zelfs zonder diepgaande expertise.

Deze actoren kunnen alleen opereren of binnen kleine informele gemeenschappen, zonder sterke organisatorische structuur.

Beoogde doelstellingen

Amateur-aanvallers streven voornamelijk doelen na die vallen onder de categorie uitdaging/plezier, zoals gedefinieerd in de EBIOS Risk Manager-methode.

Deze doelstellingen komen neer op:

- Uitdaging/plezier (hoofddoel)
  - hun technische vaardigheden testen
  - een uitdaging aangaan of beveiligingsmechanismen omzeilen
  - erkenning krijgen binnen een gemeenschap
  - experimenteren met aanvalstools en -technieken
- Winstbejag (secundair, opportunistisch doel)
  - Opportunistische uitbuiting van kwetsbaarheden voor eenmalige winst
  - indirecte deelname aan frauduleuze activiteiten

Deze drijfveren zijn doorgaans weinig gestructureerd en kunnen snel veranderen naargelang de kansen of individuele belangen.

Motivatie

Laag tot gemiddeld: motivaties die voornamelijk verband houden met nieuwsgierigheid, uitdaging of erkenning, met soms opportunistische uitwassen.

Middelen

Beperkt: sterke afhankelijkheid van online beschikbare tools, weinig ontwikkelings- of aanpassingsvermogen.

Activiteit

Hoog: groot aantal actoren die veelvuldig aanvallen uitvoeren, vaak geautomatiseerd en opportunistisch.

Werkwijze

Amateuraanvallers voeren eenvoudige, meestal opportunistische aanvallen uit:

- geautomatiseerde scans van blootgestelde systemen
- Uitbuiting van gekende kwetsbaarheden
- gebruik van scripts of kant-en-klare aanvalspakketten
- pogingen om ongeautoriseerde toegang te krijgen tot blootgestelde diensten

Deze aanvallen zijn niet erg geavanceerd, maar kunnen efficiënt zijn in het geval van een configuratiefout of ongepatchte kwetsbaarheden.

Doelsectoren

Amateur-aanvallers richten zich op een opportunistische manier op:

- systemen die op het internet staan
- kleine en middelgrote ondernemingen
- organisaties met gekende kwetsbaarheden

In de context van Infrabel kunnen deze actoren zich richten op blootgestelde of slecht geconfigureerde systemen, ongeacht de sector.

Het arsenaal aan aanvalsmiddelen

- online beschikbaar exploit-scripts
- geautomatiseerde kwetsbaarheidsscanners
- brute-force-tools
- openbaar toegankelijke aanvalskits

Wapenfeiten

Amateur-aanvallers worden zelden in verband gebracht met grote aanvallen. Hun impact is vooral te zien in :

- een groot aantal pogingen tot aanvallen;
- opportunistische inbreuken in slecht beveiligde systemen;
- een indirecte bijdrage aan de totale druk op blootgestelde systemen.

Wraakzuchtige aanvaller

Risicobron

Wraakzuchtige aanvallers zijn individuen die gedreven worden door een gevoel van onrechtvaardigheid of frustratie, meestal gekoppeld aan een directe relatie met de organisatie die het doelwit is. Het kunnen werknemers of voormalige werknemers, dienstverleners of partners zijn die een wrok hebben ontwikkeld tegen de entiteit.

Deze spelers onderscheiden zich door hun interne kennis van informatiesystemen, procedures en business processen. Deze kennis is een groot voordeel, waardoor ze specifieke kwetsbaarheden kunnen identificeren en bepaalde beveiligingsmechanismen kunnen omzeilen.

In tegenstelling tot andere profielen is hun motivatie persoonlijk en emotioneel, wat hun vastberadenheid en hun vermogen om gerichte actie te ondernemen kan versterken.

Beoogde doelstellingen

Wraakzuchtige aanvallers streven voornamelijk doelen na die vallen onder de categorie 'belemmering van de werking', zoals gedefinieerd in de EBIOS Risk Manager-methode

Deze doelstellingen komen neer op:

- Belemmering van de werking
  - verstoring van de activiteiten van de organisatie
  - sabotage van interne systemen of processen
  - wijziging of verwijdering van gegevens
  - blokkering of verslechtering van diensten
- Beïnvloeding
  - schade aan het imago van de organisatie
  - openbaarmaking van interne informatie
  - Slechte werking aan het licht willen brengen of de reputatie willen schaden.

Deze doelen houden rechtstreeks verband met een gerichte wens om schade aan te richten, die vaak evenredig is aan de wrok van de aanvaller.

Motivatie

Hoog: sterke persoonlijke motivatie, vaak gekoppeld aan een conflict of een gevoel van onrechtvaardigheid. Kan leiden tot vastberaden en volhardend gedrag.

Middelen

Laag tot matig: wisselend technisch niveau, maar gecompenseerd door een grondige interne kennis van systemen en processen.

Activiteit

Laag tot matig: over het algemeen eenmalige maar gerichte acties die een aanzienlijke impact kunnen hebben.

Werkwijze

Wraakzuchtige aanvallers ondernemen gerichte actie, vaak op basis van hun voorkennis:

- misbruik van rechten of privileges
- verwijdering of wijziging van gegevens
- sabotage van systemen of procedures
- omzeilen van beveiligingscontroles
- openbaarmaking van interne informatie

Deze acties zijn over het algemeen nauwkeurig en gericht op een directe impact.

Doelwitten

Wraakzuchtige aanvallers richten zich voornamelijk op hun eigen organisatie of een entiteit waarmee ze een directe relatie hebben gehad.

In het geval van Infrabel hebben de risico's betrekking op :

- interne systemen
- operationele procedures
- gevoelige gegevens met betrekking tot de spoorwegexploitatie.

Het arsenaal aan aanvalsmiddelen

- legitieme of misbruikte interne toegang
- interne tools
- eenvoudige scripts
- kennis van systemen en procedures

Wapenfeiten

Wraakzuchtige aanvallers worden zelden in verband gebracht met aanvallen die de media halen, maar hun impact kan aanzienlijk zijn

- Interne sabotage van systemen
- verwijdering van kritieke gegevens
- openbaarmaking van gevoelige informatie

Deze incidenten illustreren het hoge risico dat gepaard gaat met dreigingen van binnenuit.

Pathologische kwaadwilligheid

Risicobron

Pathologische kwaadwilligen zijn personen die handelen uit opportunisme, irrationele motieven of soms uit winstbejag. Tot dit profiel behoren met name oneerlijke concurrenten, malafide klanten, fraudeurs of geïsoleerde individuen die zonder gestructureerde logica te werk gaan.

Deze actoren worden gekenmerkt door onvoorspelbaar gedrag en het ontbreken van een duidelijke strategie. Hun technische niveau varieert: sommigen beschikken over voldoende vaardigheden om zelf aanvallen uit te voeren, terwijl anderen gebruikmaken van online beschikbare tools of hun acties uitbesteden aan gespecialiseerde bureaus.

Deze combinatie van opportunisme, variabiliteit van middelen en onvoorspelbaarheid is een bijzondere risicofactor, die detectie en anticipatie complex maakt.

Beoogde doelstellingen

Pathologische kwaadwilligen streven uiteenlopende doelstellingen na, die voornamelijk vallen onder de categorieën winstbejag en, in sommige gevallen, belemmering van de werking, zoals gedefinieerd in de EBIOS Risk Manager-methode.

Deze doelstellingen komen neer op:

- Winstbejag
  - fraude of oplichting
  - opportunistisch misbruik van kwetsbaarheden
  - op zoek naar eenmalig financieel gewin
  - gebruik van externe diensten om aanvallen uit te voeren
- Belemmering van de werking
  - opportunistische verstoring van systemen of diensten
  - schadelijke acties zonder duidelijk strategisch doel
  - kwetsbaarheden misbruiken om storingen te veroorzaken

In tegenstelling tot andere profielen maken deze doelstellingen geen deel uit van een gestructureerde logica, maar vloeien ze voort uit individuele mogelijkheden of motivaties.

Motivatie

Variabel: opportunistische, irrationele of financiële drijfveren, zonder strategische samenhang. Kan impulsief gedrag inhouden.

Middelen

Laag tot matig: hangt sterk af van het individu, met de mogelijkheid om gebruik te maken van toegankelijke tools of externe dienstverleners.

Activiteit

Laag tot matig: opportunistische, niet-systematische acties, maar moeilijk te voorspellen

Werkwijze

Pathologische kwaadwilligen voeren opportunistische en heterogene acties uit

- Misbruiken van gekende kwetsbaarheden

- gebruik van online beschikbare aanvalskits
- gebruik van gespecialiseerde bureaus
- digitale fraude of oplichting
- opportunistische pogingen tot compromittering

Deze aanvallen volgen niet noodzakelijkerwijs een gestructureerd patroon en zijn sterk afhankelijk van kansen.

Doelwitten

Pathologische kwaadwilligen richten zich op opportunistische wijze op:

- toegankelijke of kwetsbare organisaties
- blootgestelde diensten
- systemen met exploiteerbare kwetsbaarheden

In het geval van Infrabel hebben de risico's voornamelijk betrekking op blootgestelde of onvoldoende beveiligde systemen.

Het arsenaal aan aanvalsmiddelen

- online beschikbare tools
- aanvalskits
- eenvoudige scripts
- uitbestede hackingdiensten

Wapenfeiten

De acties van pathologische kwaadwilligen halen zelden de media, maar omvatten:

- opportunistische fraude
- misbruik van niet-gepatchte kwetsbaarheden
- geïsoleerde, ongecoördineerde aanvallen

Deze incidenten illustreren een diffuse dreiging die moeilijk te voorzien is.

RISICOCATALOGI

De belangrijkste rapporten van de nationale overheden, de Europese agentschappen en de Threat Intelligence-stakeholders tonen een evolutie van de dreigingen, die waarschijnlijk een directe impact zullen hebben op de continuïteit van de essentiële diensten van Infrabel, zijn operationele cyberweerbaarheid en het vertrouwen van zijn stakeholders.

In deze context voert Infrabel regelmatig risicoanalyses uit op basis van de EBIOS Risk Manager-methodologie. Deze risico's worden geïdentificeerd door de trends uit referentierapporten te consolideren en vervolgens te vertalen naar bedrijfsuitdagingen om een gestructureerd, hiërarchisch en relevant beeld te bieden voor de besluitvorming

De bij Infrabel geïdentificeerde risico's hangen ook nauw samen met de relatie die het onderhoudt met zijn leveranciers binnen de toeleveringsketen. Elke kwetsbaarheid of elk incident bij een leverancier kan een rechtstreekse impact hebben op de veiligheid en de continuïteit van de kritieke diensten van Infrabel. Een storing of cyberaanval bij een kritieke partner kan bijvoorbeeld grote verstoringen veroorzaken of zelfs de operationele weerbaarheid van het bedrijf in gevaar brengen.

Omgekeerd hebben de beveiligingseisen en -praktijken van Infrabel ook invloed op de leveranciers, die aan strenge normen moeten voldoen om de betrouwbaarheid en de naleving van de regelgeving in de hele supply chain te waarborgen.

Deze onderlinge afhankelijkheid onderstreept het belang van proactief risicobeheer, gebaseerd op nauwe samenwerking en voortdurende beoordeling van dreigingen en zwakke punten binnen het partnernetwerk.

Risico	Definitie
Grote onderbreking van essentiële dienstverlening	Het onvermogen om de continuïteit van een of meer kritieke diensten van de missie van Infrabel te waarborgen, vormt een groot risico voor de organisatie. Dit risico vertaalt zich in een onderbreking van essentiële functies, die de stabiliteit en de operationele weerbaarheid van de onderneming in het gedrang brengen.
Kritieke storing in de Supply Chain	Een incident bij een leverancier kan een directe impact hebben op de activiteiten, wat leidt tot aanzienlijke verstoringen in de toeleveringsketen en de operationele organisatie.
Ernstige niet-naleving van regelgeving	Het niet kunnen voldoen aan de wettelijke vereisten vormt een groot risico voor de organisatie. Deze niet-naleving kan ernstige gevolgen hebben en de legitimiteit en continuïteit van de bedrijfsactiviteiten aantasten. Het is dan ook van essentieel belang om ervoor te zorgen dat aan de wettelijke verplichtingen wordt voldaan, teneinde de naleving te handhaven en de missie ook in de toekomst te kunnen blijven verzekeren.

Domino-effect tussen infrastructuren	Wanneer zich een incident voordoet in een kritieke infrastructuur, kan de impact snel overslaan naar andere essentiële sectoren. Dit verspreidingsfenomeen, dat vaak het domino-effect wordt genoemd, benadrukt de sterke onderlinge afhankelijkheid tussen verschillende infrastructuren. Zo kan een aanvankelijke verstoring in een sector grote gevolgen hebben voor aanverwante domeinen, waardoor de ernst van de situatie toeneemt en de noodzaak van aangepaste crisisbeheersingsmechanismen nog groter wordt
Verlies van controle over operationele/industriële processen	De verstoring of kwaadwillige beïnvloeding van fysieke activiteiten vormt een aanzienlijk risico voor operationele of industriële processen. Deze dreiging kan leiden tot een verlies van controle over de activiteiten, waardoor de veiligheid en integriteit van de betrokken systemen in gevaar komen. . Het is daarom van cruciaal belang om ongeoorloofde manipulatie te voorkomen om de goede werking en betrouwbaarheid van de activiteiten te waarborgen
Compromittering van gevoelige of strategische gegevens	De blootstelling of diefstal van kritieke gegevens vormt een grote bedreiging voor essentiële infrastructuren. Het compromitteren van deze gevoelige informatie kan grote gevolgen hebben voor de veiligheid, vertrouwelijkheid en integriteit van de betrokken sectoren. Dit soort incidenten benadrukt de noodzaak om robuuste maatregelen te nemen om strategische gegevens te beschermen en de impact te beperken in het geval van een lek of ongeautoriseerde toegang.
Aantasting van de integriteit van kritieke gegevens	Het heimelijk manipuleren van kritieke gegevens vormt een aanzienlijke bedreiging voor organisaties. Als er met deze informatie wordt geknoeid, kan dit beslissingen beïnvloeden die binnen operationele of industriële processen worden genomen. Dit risico vloeit voort uit het feit dat vervalste of gewijzigde gegevens onopgemerkt blijven, wat leidt tot keuzes die men neemt of richtingen die met uitgaat en die niet langer op betrouwbare informatie zijn gebaseerd. Het bewaren van de integriteit van de gegevens is daarom essentieel om de relevantie en veiligheid van strategische beslissingen te garanderen.
Grootschalige afpersing	Aanvallen met afpersing op grote schaal leiden tot het blokkeren van IT-systemen, waardoor organisaties geen toegang meer hebben tot hun essentiële bedrijfsmiddelen. Deze incidenten gaan meestal gepaard met grote financiële en reputatiedruk, waardoor slachtoffers gedwongen worden snel in te gaan op de eisen van de aanvallers om de gevolgen voor hun activiteiten en hun publieke imago te beperken

Verlies van publiek/institutioneel vertrouwen	Het verlies van publiek of institutioneel vertrouwen uit zich voornamelijk in een aantasting van de geloofwaardigheid van de betrokken entiteit. Wanneer zich een beveiligingsincident voordoet, of het nu gaat om een datalek of kwaadwillige manipulatie, kan de perceptie van betrouwbaarheid van een organisatie snel worden aangetast. Het vertrouwen van partners, klanten en het grote publiek neemt af, met blijvende schade aan het imago en de reputatie van de instelling. Dit fenomeen is een van de belangrijkste gevolgen van cyberdreigingen, omdat het niet alleen de externe relaties ondermijnt, maar ook de interne stabiliteit van de entiteit.
In gevaar brengen van mensenlevens	Cyberincidenten kunnen directe fysieke gevolgen hebben en mensenlevens in gevaar brengen. Wanneer een kritiek systeem wordt gecompromitteerd, kan dit leiden tot storingen of onderbrekingen die de veiligheid van de betrokken personen in gevaar kunnen brengen.
Kritieke afhankelijkheid van systemen waarover men geen volledige controle heeft	De weerbaarheid van een organisatie kan worden ondermijnd door haar afhankelijkheid van technologische systemen waarover ze geen volledige controle heeft. Deze situatie stelt de entiteit bloot aan extra risico's, aangezien elke storing of kwetsbaarheid in deze systemen grote gevolgen kan hebben voor de activiteiten en het vermogen om incidenten het hoofd te bieden.
Instrumentalisatie in een geopolitieke context	De entiteit kan worden uitgebuit in een geopolitieke context, waar zij als strategisch hefboom fungeert. Dit houdt in dat de entiteit wordt gebruikt door actoren die politieke, economische of militaire doelstellingen willen beïnvloeden of bereiken, door gebruik te maken van haar positie of specifieke capaciteiten.
Laattijdige detectie van een groot incident	De langdurige aanwezigheid van een aanvaller in het informatiesysteem is een situatie waarin de inbraak niet snel wordt ontdekt. Dit betekent dat een kwaadwillende persoon gedurende een langere periode in de IT-omgeving van de organisatie kan blijven, waardoor de risico's en mogelijke gevolgen voor de gegevensbeveiliging en het algehele functioneren van de entiteit toenemen.
Onvermogen om een grote cybercrisis te beheersen	Het vermogen om een grote cybercrisis te beheersen is afhankelijk van een solide organisatie en de juiste processen. Een falend organisatorisch crisismanagement kan grote gevolgen hebben, zoals een inefficiënte reactie op een aanval en een verergering van de impact op de kritieke activiteiten van de entiteit. Het is daarom essentieel dat crisisstructuren en -

	procedures duidelijk worden gedefinieerd en regelmatig worden getest om hun doeltreffendheid in het geval van een incident te garanderen.
Verlies van kritieke competenties	Het verlies van kritieke competenties kan zich voordoen wanneer de organisatie sterk vertrouwt op bepaalde personeelsleden met specifieke kennis of expertise. Deze afhankelijkheid van sleutelfiguren stelt de entiteit bloot aan verhoogde risico's als deze mensen tijdelijk of permanent niet beschikbaar zijn. Een dergelijke situatie kan het vermogen van de organisatie om haar activiteiten voort te zetten, efficiënt te reageren op incidenten of de continuïteit van haar activiteiten te waarborgen, ondermijnen

Deze risico's zijn niet alleen generiek van aard, maar vormen ook een essentiële basis voor het opstellen van gedetailleerde strategische scenario's en de vertaalomslag ervan naar operationele scenario's. Ze maken het ook mogelijk om prioriteiten te stellen op het gebied van risicobeheer, weerbaarheid en veiligheidsbeheer.

Tot slot moet deze analyse in een voortdurend veranderende omgeving regelmatig opnieuw worden herzien om rekening te houden met nieuwe dreigingstrends en veranderingen in het informatiesysteem en de afhankelijkheden van de entiteit.