Best practice Cybersecurity

in de chemische logistiek

Inhoud

Inhoud

Hoofdstuk 1: Inleiding

In een steeds meer verbonden wereld spelen supply chains een centrale rol in het functioneren van bedrijven en de wereldeconomie. Tegelijkertijd maakt deze complexiteit en onderlinge afhankelijkheid supply chains kwetsbaar voor een breed scala aan cyberdreigingen. Cyberaanvallen richten zich niet alleen meer op grote organisaties, maar ook op leveranciers, technologische partners en kritieke infrastructuur.

In dit hoofdstuk onderzoeken we waarom cybersecurity een strategische prioriteit is geworden binnen supply chain management. We kijken naar hoe digitalisering de risico's heeft vergroot, waarom het beschermen van kritieke systemen en gegevens essentieel is, en welke impact cyberaanvallen kunnen hebben op de continuïteit en reputatie van bedrijven. Deze inleiding legt de basis voor de specifieke onderwerpen en oplossingen die in de volgende hoofdstukken worden behandeld.

1.1 Het belang van de supply chain in een digitale wereld

De supply chain vormt de ruggengraat van de moderne economie. Van productie en distributie tot de levering van goederen en diensten, vrijwel iedere sector is afhankelijk van complexe netwerken van leveranciers, transporteurs en distributeurs. In de afgelopen decennia heeft digitalisering de efficiëntie en reikwijdte van supply chains aanzienlijk vergroot. Bedrijven gebruiken nu geavanceerde technologieën, zoals Internet of Things (IoT), cloud computing en big data-analyse, om processen te optimaliseren en betere inzichten te krijgen in de vraag en het aanbod.

Deze technologische vooruitgang brengt echter ook nieuwe uitdagingen met zich mee, met name op het gebied van cybersecurity. Het digitaliseren van supply chains betekent dat steeds meer systemen, apparaten en processen met elkaar verbonden zijn. Dit verhoogt niet alleen de efficiëntie, maar vergroot ook de potentiële aanvalsvectoren voor cybercriminelen. Een kwetsbaarheid bij één leverancier kan zich snel verspreiden door het gehele netwerk, met ernstige gevolgen voor meerdere organisaties.

Daarnaast is de supply chain niet alleen een logistiek proces, maar ook een strategisch onderdeel van concurrentievoordeel. Bedrijven die hun supply chain optimaal beheren, kunnen sneller inspelen op veranderingen in de markt en hun klanten beter bedienen. Het beschermen van deze keten tegen cyberdreigingen is daarom cruciaal om zowel operationele continuïteit als reputatie te waarborgen.

Tot slot is er de toenemende druk van regelgeving en klanten om een veilige en transparante supply chain te waarborgen. Internationale standaarden zoals GDPR en specifieke richtlijnen voor kritieke sectoren, zoals de gezondheidszorg en defensie, benadrukken het belang van het integreren van cybersecurity in elke schakel van de keten. In deze context is het waarborgen van de digitale veiligheid niet langer een optie, maar een noodzakelijke strategische prioriteit.

1.2 Toename van cyberdreigingen in de supply chain

In de afgelopen jaren is er een significante toename geweest van cyberdreigingen binnen de supply chain, zowel wereldwijd als in Nederland. Cybercriminelen richten zich steeds vaker op zwakke schakels binnen deze ketens, waarbij leveranciers en partners met minder robuuste beveiligingsmaatregelen aantrekkelijke doelwitten vormen.

Voorbeelden van supply chain-aanvallen in Nederland

NotPetya-aanval (2017): Deze wereldwijde cyberaanval trof ook Nederland, waarbij onder andere containerterminals in de Rotterdamse haven werden getroffen. De aanval maakte gebruik van geïnfecteerde software-updates om systemen te compromitteren, wat leidde tot aanzienlijke verstoringen in de logistieke sector.

Ransomware-aanval op Bakker Logistiek (2021): Dit Nederlandse logistieke bedrijf werd slachtoffer van een ransomware-aanval, wat resulteerde in een schadepost van 3,5 miljoen euro. De aanval leidde tot ernstige verstoringen in de distributieprocessen en benadrukte de kwetsbaarheid van logistieke systemen voor cyberdreigingen.

SolarWinds-aanval (2020): Hoewel deze aanval zijn oorsprong vond in de Verenigde Staten, had het ook impact op Nederlandse organisaties die gebruikmaakten van de geïnfecteerde Orion-software. Via een gecompromitteerde software-update kregen aanvallers toegang tot de netwerken van diverse bedrijven en overheidsinstellingen.

Geavanceerde aanvalsmethoden

Cybercriminelen maken gebruik van steeds geavanceerdere technieken om kwetsbaarheden in de supply chain uit te buiten. Een veelvoorkomende methode is de zogenaamde "supply chain attack," waarbij kwaadwillenden binnendringen via een vertrouwde derde partij. Een bekend voorbeeld hiervan is de SolarWinds-aanval, waarbij een legitieme software-update werd geïnfecteerd met malware, waardoor duizenden klanten werden blootgesteld. Deze aanvalstechniek is effectief omdat bedrijven vaak blind vertrouwen op de beveiliging van hun leveranciers.

Toenemende afhankelijkheid van technologie

Met de toenemende digitalisering van supply chains worden organisaties ook kwetsbaarder. Technologieën zoals Internet of Things (IoT) en cloud computing brengen voordelen met zich mee, maar creëren ook nieuwe risico's. IoT-apparaten, zoals sensoren en trackers, zijn vaak slecht beveiligd en vormen een toegangspoort voor hackers. Bovendien zijn cloudoplossingen vatbaar voor datalekken als ze niet adequaat worden beheerd.

Impact van ransomware

Ransomware-aanvallen hebben een prominente rol gespeeld in de verstoring van supply chains. In dergelijke aanvallen versleutelen criminelen belangrijke gegevens en eisen ze losgeld om de toegang te herstellen. Een goed voorbeeld hiervan is de aanval op Colonial Pipeline, die niet alleen het bedrijf zelf trof, maar ook leidde tot grote verstoringen in de brandstofvoorziening in de VS. Deze aanvallen benadrukken hoe kwetsbaar en verstrekkend de gevolgen kunnen zijn.

Toenemende regelgeving en compliance-uitdagingen

Cyberdreigingen in de supply chain worden ook aangewakkerd door het gebrek aan gestandaardiseerde beveiligingspraktijken onder leveranciers. Hoewel regelgeving zoals de GDPR, NIS2 en CMMC bedrijven verplicht om hun digitale ecosystemen beter te beschermen, blijft de naleving een uitdaging. Veel kleine en middelgrote leveranciers hebben niet de middelen om complexe beveiligingsmaatregelen te implementeren, waardoor ze een aantrekkelijk doelwit blijven.

1.3 Doel en opzet van dit onderzoek

Het groeiende belang van cybersecurity in de supply chain vraagt om een grondige analyse van de huidige risico's, best practices en implementatiestrategieën. Dit onderzoek is ontworpen om organisaties een praktische en uitgebreide handleiding te bieden voor het aanpakken van deze uitdagingen. Het uiteindelijke doel is om een raamwerk te creëren dat bedrijven kunnen gebruiken om hun supply chain robuuster en veerkrachtiger te maken tegen cyberdreigingen.

Doelstellingen van het onderzoek

1. Het identificeren van de meest voorkomende en kritieke cyberdreigingen binnen supply chains, met specifieke aandacht voor de Nederlandse context.

2. Het analyseren van bestaande best practices en innovatieve technologieën die bijdragen aan het mitigeren van risico's.

3. Het bieden van een praktisch stappenplan voor bedrijven om cybersecurity effectief te integreren in hun supply chain-beheer.

Dit onderzoek richt zich ook op het beantwoorden van de volgende vragen:

- Welke specifieke cyberdreigingen vormen het grootste risico voor supply chains?

- Welke technologieën en processen worden momenteel ingezet om supply chain-kwetsbaarheden te minimaliseren?

- Hoe kunnen bedrijven in Nederland voldoen aan nationale en internationale regelgeving op het gebied van cybersecurity?

Dit onderzoek draagt bij aan het bewustzijn en de kennis over cybersecurity in supply chains, met een speciale focus op Nederlandse organisaties. Het biedt praktische handvatten voor organisaties om niet alleen te voldoen aan regelgeving, maar ook om hun reputatie en continuïteit te waarborgen.

Hoofdstuk 2: Belangrijkste risico's in cybersecurity.

Supply chains zijn complexe netwerken die sterk afhankelijk zijn van digitale systemen en externe partners. Deze afhankelijkheid maakt ze kwetsbaar voor diverse cyberdreigingen. In dit hoofdstuk worden de meest kritieke risico's besproken die de veiligheid en continuïteit van supply chains bedreigen.

Het vervoer van gevaarlijke stoffen (ADR-transport) speelt een belangrijke rol in de industrie, chemische sector en energievoorziening. Vanwege de aard van de stoffen en hun specifieke gevaren zijn strenge veiligheidsmaatregelen vereist. Maar in de stoffen zelf schuilen niet alleen de gevaren. De digitalisering van logistiek en transport heeft cyberrisico's geïntroduceerd. Hackers kunnen transportmanagementsystemen (TMS), telematica-oplossingen en operationele technologie (OT) aanvallen, met mogelijk zeer vervelende gevolgen.

2.1. Cyberdreigingen in het Vervoer van Gevaarlijke Stoffen

Door de toenemende connectiviteit in transport- en logistieke netwerken wordt de sector steeds kwetsbaarder voor cyberaanvallen. Hieronder volgen een aantal belangrijkste dreigingen.

- Ransomware-aanvallen op logistieke systemen

Cybercriminelen gebruiken ransomware om transportmanagementsystemen (TMS) te versleutelen, waardoor bedrijven geen toegang meer hebben tot logistieke data. Dit kan leiden tot vertragingen, verlies van lading en verstoring van de supply chain.

- Manipulatie van GPS en telematica

Hackers kunnen GPS-signalen verstoren (spoofing) of manipuleren, waardoor chauffeurs verkeerde routes nemen. In het geval van gevaarlijke stoffen kan dit leiden tot blootstelling aan onveilige zones of zelfs diefstal.

- Aanvallen op industriële controlesystemen (ICS/OT)

Transportbedrijven gebruiken operationele technologie (OT) zoals sensoren en monitoringtools om ladingen veilig te vervoeren. Een aanval op deze systemen kan ervoor zorgen dat sensoren verkeerde waarden rapporteren, waardoor bijvoorbeeld een tankwagen niet correct gekoeld wordt of drukopbouw onopgemerkt blijft.

- Data-diefstal en bedrijfsespionage

Logistieke bedrijven verwerken grote hoeveelheden gevoelige data over routes, ladingen en klanten. Cybercriminelen kunnen deze data stelen voor industriële spionage, concurrentievoordeel of zelfs terroristische doeleinden.

- Social engineering en phishing

Medewerkers in transportbedrijven kunnen het doelwit zijn van phishing-aanvallen. Een frauduleuze e-mail kan ertoe leiden dat gevoelige systemen toegankelijk worden voor hackers.

- DDoS-aanvallen op logistieke platforms

Distributed Denial of Service (DDoS)-aanvallen kunnen een ware bedreiging zijn voor transportbedrijven en de digitale infrastructuur van deze bedrijven platleggen, waardoor vrachtwagens niet kunnen worden ingepland en vertragingen oplopen.

2.2. Cyberrisico's in de Opslag van Gevaarlijke Stoffen

Digitale besturingssystemen zoals SCADA (Supervisory Control and Data Acquisition), IoT-sensoren, en PLC's (Programmable Logic Controllers) zijn belangrijk voor het beheer van opslagfaciliteiten. Deze systemen kunnen echter doelwit worden van cyberaanvallen.

Veel opslagfaciliteiten verbinden OT (Operational Technology) met IT-netwerken zonder voldoende beveiliging, waardoor een aanval op een IT-systeem ook OT kan beïnvloeden. Daarnaast is er vaak sprake van verouderde software en firmware. Industriële besturingssystemen krijgen vaak geen tijdige updates, wat aanvallers in staat stelt bekende exploits te gebruiken.

Ook gebrekkige authenticatie en toegangscontrole kunnen het probleem zijn. Veel PLC's en SCADA-systemen werken met standaardwachtwoorden of ongeauthenticeerde toegang. Onveilige externe toegang kan zo wie zo een probleem zijn. VPN's en externe toegangspoorten kunnen doelwitten zijn voor aanvallers, vooral als ze slecht geconfigureerd zijn.

Ook opslagbedrijven kunnen te maken krijgen met ransomware en malware. Deze kunnen blusinstallaties, pompsystemen of tankniveauregelingen blokkeren, wat kan leiden tot fysieke gevaren. Laten we eens kijken naar de specifieke dreigingen per opslagsysteem

Magazijnen met automatische blusinstallaties (Hi-Ex en CO2)

Manipulatie van blusinstallaties: Een aanvaller kan een valse activatie of een storing veroorzaken, wat kan leiden tot schade aan goederen of het onbeschikbaar maken van blusmiddelen voor een daadwerkelijke brand.

Sabotage van alarmsystemen: Cybercriminelen kunnen branddetectiesystemen uitschakelen of valse alarmen veroorzaken, wat operationele verstoringen en veiligheidsrisico's oplevert.

Verstoring van ventilatie- en druksystemen: CO2-installaties vereisen een precieze controle van zuurstofniveaus. Een aanval kan leiden tot gevaarlijke zuurstoftekorten of juist onvoldoende blussing bij een brand.

Opslag in tanks (brandbare en giftige stoffen)
Manipulatie van tankniveaus: Hackers kunnen sensorgegevens manipuleren, wat kan leiden tot overstromingen, lekkages of explosies.

Sabotage van temperatuur- en drukregelingen: Dit kan resulteren in thermische instabiliteit en ongecontroleerde chemische reacties.

Verstoring van veiligheidskleppen en afsluiters: Een cyberaanval kan veiligheidskleppen blokkeren of openen, wat lekkages of overdruk kan veroorzaken.

2.3. Cyberaanvallen op leveranciers

Leveranciers vormen een belangrijke schakel in de supply chain en worden daarom vaak beschouwd als een aantrekkelijk doelwit voor cybercriminelen. Veel leveranciers, vooral kleinere en middelgrote bedrijven, hebben minder geavanceerde cybersecuritymaatregelen dan de grotere organisaties waaraan ze leveren. Dit maakt hen een ideale toegangspoort voor kwaadwillenden om grote, complexe systemen binnen te dringen.

Cyberaanvallen op leveranciers volgen meestal een patroon waarin aanvallers gebruik maken van kwetsbaarheden in systemen, software of processen. Enkele veelvoorkomende methoden zijn:

1. Spear-phishing: Gerichte e-mails die lijken te komen van een legitieme bron, zoals een zakelijke partner, maar die schadelijke links of bijlagen bevatten. Zodra een medewerker klikt, kunnen aanvallers toegang krijgen tot het netwerk van de leverancier.

2. Malware-infecties via updates: Leveranciers leveren vaak software-updates aan hun klanten. Als een update is geïnfecteerd met malware (zoals in de SolarWinds-aanval), wordt het hele klantenbestand blootgesteld aan risico's.

3. Infiltratie via zwakke authenticatie: Leveranciers die zwakke wachtwoorden of onvoldoende beveiligde VPN-verbindingen gebruiken, bieden hackers een gemakkelijke ingang.

4. Aanvallen op cloudoplossingen: Veel leveranciers vertrouwen op gedeelde cloudinfrastructuren. Een kwetsbaarheid in de cloudomgeving kan resulteren in datalekken of volledige systeemuitval.

Voorbeelden van cyberaanvallen op leveranciers

Target (2013): In deze Amerikaanse zaak infiltreerden hackers het netwerk van Target via een HVAC-leverancier. Hierdoor konden ze miljoenen creditcardgegevens van klanten stelen. De zwakke beveiliging van de leverancier vormde de toegangspoort.

ASML (2021): In Nederland meldde ASML een datalek via een van zijn leveranciers, waarbij vertrouwelijke informatie in verkeerde handen kwam. Dit incident benadrukte het belang van screening en controle van partners.

NotPetya-aanval (2017): Deze wereldwijde aanval trof ook Nederlandse bedrijven via geïnfecteerde software van leveranciers, waaronder containerterminals in Rotterdam.

De gevolgen van cyberaanvallen op leveranciers zijn vaak verstrekkend, zowel voor de leverancier zelf als voor de grotere organisatie die afhankelijk is van hun diensten. De belangrijkste gevolgen zijn:

1. Financiële schade:

Directe kosten door systeemuitval en herstel.

Indirecte kosten door verloren inkomsten en boetes.

2. Reputatieschade:

Klanten kunnen vertrouwen verliezen in de organisatie en haar partners.

Publieke schandalen kunnen leiden tot verlies van toekomstige contracten.

3. Operationele verstoringen:

Productielijnen kunnen tot stilstand komen.

Leveringsvertragingen kunnen leiden tot verlies van marktaandeel.

4. Juridische en compliance-uitdagingen:

Boetes door niet-naleving van privacywetgeving zoals GDPR.

Mogelijke juridische claims van getroffen klanten.

Hoe kunnen bedrijven zich beschermen?

Het beschermen van de supply chain tegen aanvallen op leveranciers vereist een proactieve en holistische aanpak. Enkele strategieën zijn:

1. Leveranciersrisicoanalyse:

- Voer een uitgebreide risicoanalyse uit voordat u een leverancier inschakelt.
- Controleer regelmatig de beveiligingsmaatregelen van bestaande leveranciers.

2. Strengere contractuele vereisten:

- Vereis dat leveranciers voldoen aan cybersecuritystandaarden zoals ISO 27001 of NIST.
- Neem clausules op voor regelmatige audits en sancties bij niet-naleving.

3. Segmentatie van netwerken:

- Beperk de toegang van leveranciers tot strikt noodzakelijke systemen.
- Gebruik firewalls en monitoring om ongebruikelijke activiteiten te detecteren.

4. Training en bewustwording:

- Train interne teams en leveranciers over cybersecurityrisico's.

- Simuleer phishing-aanvallen om medewerkers voor te bereiden op bedreigingen.

5. Gebruik van technologie:

- Implementeer oplossingen zoals zero-trust-modellen, endpoint-detectie, en encryptie.

- Maak gebruik van blockchain voor veilige gegevensuitwisseling in de supply chain.

Cyberaanvallen op leveranciers vormen een van de grootste bedreigingen voor de supply chain. Deze aanvallen maken gebruik van kwetsbaarheden in systemen en processen die door bedrijven vaak over het hoofd worden gezien. Door een combinatie van strenge beveiligingsrichtlijnen, technologie en samenwerking met leveranciers, kunnen organisaties deze dreiging aanzienlijk verminderen. Het is essentieel dat bedrijven cybersecurity beschouwen als een gezamenlijke verantwoordelijkheid binnen het gehele ecosysteem van de supply chain.

2.2 Kwetsbaarheden in software en systemen

De software en systemen die worden gebruikt in supply chains zijn een belangrijk doelwit voor cybercriminelen. Deze technologieën, variërend van Enterprise Resource Planning (ERP)-systemen tot logistieke beheersoftware, zijn essentieel voor het beheer van complexe ketens. Tegelijkertijd vormen ze een zwakke schakel als ze niet goed worden beveiligd.

Veelvoorkomende kwetsbaarheden

Verouderde software:
Veel bedrijven gebruiken legacy-systemen die niet meer worden ondersteund met updates en patches. Dit maakt ze kwetsbaar voor bekende exploits. Voorbeelden zijn oude versies van Windows of ERP-software die geen recente beveiligingsupdates ontvangen.

Ongepatchte systemen:
Zelfs in moderne software komen regelmatig kwetsbaarheden aan het licht. Als deze niet tijdig worden gepatcht, blijven systemen openstaan voor aanvallen. Een voorbeeld is de "Log4Shell"-kwetsbaarheid in Log4j, die wereldwijd miljoenen systemen trof.

Gebrek aan beveiligingsprotocollen:
Software zonder ingebouwde beveiligingsfuncties, zoals versleuteling of multi-factor authenticatie (MFA), vergroot het risico op datalekken en ongeautoriseerde toegang.

Kwetsbare API's:
API's (Application Programming Interfaces) worden veel gebruikt voor de integratie van systemen. Onvoldoende beveiligde API's kunnen worden misbruikt om toegang te krijgen tot kritieke gegevens en systemen.

Beveiligingslekken in third-party software:
Software van externe leveranciers kan onbedoeld malware bevatten, zoals in de beruchte SolarWinds-aanval. Deze aanval maakte gebruik van geïnfecteerde software-updates om toegang te krijgen tot netwerken van duizenden bedrijven.

Gevolgen van kwetsbaarheden in software

Operationele verstoringen:
Aanvallen op systemen kunnen leiden tot stilstand in productie- en distributieprocessen. In de logistieke sector kunnen vertragingen vergaande gevolgen hebben, zoals gemiste leveringen of extra kosten.

Gegevensdiefstal:
Kwetsbare systemen kunnen leiden tot datalekken. Gevoelige informatie zoals klantgegevens, financiële data of bedrijfsgeheimen kan worden gestolen en misbruikt.

Reputatieschade:
Klanten en zakenpartners verliezen het vertrouwen in een organisatie die niet in staat is om haar digitale infrastructuur te beschermen.

Juridische en financiële gevolgen:
Bedrijven kunnen worden geconfronteerd met boetes wegens schending van privacywetten zoals GDPR. Ook kunnen juridische claims van klanten en partners de kosten verder opvoeren.

Preventieve maatregelen

Regelmatige updates en patches:
Zorg ervoor dat alle software en systemen tijdig worden bijgewerkt met de nieuwste beveiligingspatches.

Vulnerability management:
Implementeer een systeem voor het detecteren en verhelpen van kwetsbaarheden in software. Tools zoals vulnerability scanners kunnen hierbij helpen.

Segmentatie van netwerken:
Beperk de toegang tot kritieke systemen door netwerken te segmenteren. Dit voorkomt dat een aanval zich gemakkelijk verspreidt.

Gebruik van beveiligde API's:
Zorg ervoor dat API's correct zijn geconfigureerd en beveiligd, bijvoorbeeld door authenticatie- en autorisatiemaatregelen.

Verificatie van third-party software:
Controleer regelmatig de beveiligingspraktijken van softwareleveranciers en vraag om audits of certificeringen.

2.3 Gegevensdiefstal en privacyproblemen

In een tijdperk waarin supply chains sterk afhankelijk zijn van data, wordt gegevensdiefstal een van de meest zorgwekkende cyberdreigingen. Supply chains bevatten een schat aan gevoelige informatie, waaronder klantgegevens, financiële gegevens, bedrijfsstrategieën en intellectueel eigendom. Wanneer deze gegevens worden gestolen, kan dit leiden tot aanzienlijke schade voor zowel bedrijven als hun klanten.

Hoe ontstaat gegevensdiefstal?
Onveilige gegevensoverdracht is vaak een oorzaak. Gegevens die via onbeveiligde netwerken worden verzonden, kunnen worden onderschept door cybercriminelen. Een gebrek aan encryptie is hierbij een belangrijke oorzaak. Ook infiltratie via leveranciers kan het probleem zijn. Leveranciers die toegang hebben tot het netwerk van een bedrijf kunnen onbedoeld gegevens lekken als hun eigen systemen niet goed beveiligd zijn.

Cybercriminelen gebruiken vaak gerichte phishing-e-mails om medewerkers te misleiden en toegang te krijgen tot gevoelige gegevens. Er wordt misbruik gebruikt gemaakt van gestolen inloggegevens. Wachtwoorden die zijn buitgemaakt bij eerdere datalekken kunnen worden gebruikt om toegang te krijgen tot systemen met gevoelige gegevens.

Gevolgen van gegevensdiefstal

De gevolgen van gegevensdiefstal kunnen groot zijn. Denk daarbij aan de economische schade. Gestolen bedrijfsgegevens, zoals prijzen of strategische plannen, kunnen concurrentievoordeel opleveren voor andere partijen. Diefstal van klantgegevens kan leiden tot verlies van klanten en inkomsten.

Ook reputatieschade is een bedreiging. Bedrijven die gevoelige klantgegevens niet kunnen beschermen, verliezen vaak het vertrouwen van hun klanten en partners.
Negatieve publiciteit kan het imago van een bedrijf ernstig schaden.

Denk ook aan de juridische gevolgen. Onder de GDPR en andere privacywetgeving kunnen bedrijven worden geconfronteerd met zware boetes als blijkt dat ze onvoldoende maatregelen hebben genomen om gegevens te beschermen. Rechtszaken van klanten of partners kunnen de financiële schade verder vergroten.

Diefstal van kritieke gegevens kan leiden tot Operationele verstoringen in bedrijfsprocessen, zoals het ontwerpen van nieuwe producten of het uitvoeren van klantorders.

Preventieve maatregelen

Gevoelige gegevens moeten altijd worden versleuteld, zowel tijdens de overdracht als bij opslag, om onderschepping te voorkomen. Zorg voor een strikte toegangscontrole door alleen bevoegde medewerkers en partners toegang te laten hebben tot gevoelige informatie. Gebruik van multi-factor authenticatie (MFA) kan de kans op ongeautoriseerde toegang aanzienlijk verkleinen.

Een andere preventieve maatregel kan een bewustwordingstraining zijn. Medewerkers moeten worden opgeleid om phishing-pogingen te herkennen en om te gaan met gevoelige gegevens.

Ook regelmatige audits kunnen potentiële kwetsbaarheden blootleggen. Monitoringtools kunnen verdachte activiteiten opsporen en vroegtijdig waarschuwen.

Denk ook aan datalekpreventie (DLP)-oplossingen. Deze tools kunnen voorkomen dat gevoelige gegevens worden gekopieerd of overgedragen naar onbevoegde locaties.

2.4 Supply chain-specifieke dreigingen

Naast algemene cyberdreigingen zoals ransomware en phishing, worden supply chains geconfronteerd met specifieke dreigingen die uniek zijn voor hun complexe en onderling verbonden structuren. Deze dreigingen zijn vaak gericht op het verstoren van de integriteit, vertrouwelijkheid of beschikbaarheid van supply chain-processen en -gegevens.

Hackers kunnen processen verstoren door apparaten te manipuleren of te saboteren. Denk daarbij aan aanvallen op industriële controlesystemen (ICS) en IoT-apparaten die worden gebruikt in productieprocessen. Een cyberaanval op een fabriek kan leiden tot productieonderbrekingen of defecte producten.

Ook logistieke netwerken, zoals transportmanagementsystemen (TMS), kunnen worden getroffen door aanvallen die het transport van goederen vertragen of volledig stilleggen. De ransomware-aanval op Maersk (2017) legde havens en logistieke operaties wereldwijd plat en is daar een goed voorbeeld van.

De risico's kunnen zeker van binnenuit de organisatie komen. Interne medewerkers of partners kunnen opzettelijk of per ongeluk gevoelige informatie lekken of systemen saboteren. Een medewerker kan via een phishing-aanval onbewust toegang verschaffen tot kritieke systemen. Medewerkers kunnen ook zaken doen met onbetrouwbare leveranciers. Hackers kunnen zich voordoen als legitieme leveranciers en frauduleuze contracten aangaan, betalingen stelen of producten vervangen door inferieure goederen. Ook directe infiltratie kan een bedreiging worden. Aanvallen gericht op de fysieke supply chain, zoals het onderscheppen en vervangen van goederen door besmette hardware of vervalste onderdelen. Dit komt veel voor in de technologie- en defensiesector.

Gevolgen van supply chain-specifieke dreigingen

De gevolgen van de dreigingen kunnen groot zijn. Denk daarbij aan productieverlies. Aanvallen kunnen leiden tot langdurige stilstand in productielijnen, wat grote economische gevolgen heeft. Een verstoorde logistieke keten kan leiden tot vertragingen

in leveringen, met gevolgen voor klanten en andere partners in de keten. Maar ook de schade aan het merk en de reputatie moet niet onderschat worden.

Bedrijven die worden getroffen door supply chain-dreigingen kunnen ook vertrouwen verliezen bij klanten en partners, vooral als gevoelige informatie wordt gelekt. Het herstellen van de schade en het verbeteren van beveiliging na een aanval vereist aanzienlijke investeringen.

Preventieve strategieën

Een goed Inzicht in de supply chain is belangrijk**.** Identificeer en beoordeel alle partijen in de keten, inclusief secundaire en tertiaire leveranciers, op hun beveiligingsmaatregelen. Een Zero Trust-beveiligingsmodel is raadzaam: **v**ertrouw geen enkel systeem of persoon zonder verificatie. Dit kan worden geïmplementeerd via strikte toegangscontroles en netwerksegmentatie. Beveilig IoT-apparaten met sterke wachtwoorden, encryptie en firmware-updates om sabotage en manipulatie te voorkomen.

Let bij het opstellen van leverancierscontracten dat leveranciers voldoen aan strikte beveiligingsnormen en regelmatig audits ondergaan. Denk ook aan incidentresponseplanning waarbij een gedetailleerd plan voor het snel detecteren, rapporteren en verhelpen van supply chain-gerelateerde incidenten wordt ontwikkeld.

Hoofdstuk 3: Best practices voor risicobeheersing

De groeiende dreiging van cyberaanvallen binnen supply chains vereist een strategische en proactieve aanpak van risicobeheersing. Terwijl de vorige hoofdstukken de belangrijkste risico's en kwetsbaarheden in kaart hebben gebracht, richt dit hoofdstuk zich op de praktische maatregelen die organisaties kunnen nemen om hun supply chain te beveiligen.

3.1 Inzicht verkrijgen in de volledige supply chain

Een belangrijke stap in het versterken van cybersecurity binnen de supply chain is het verkrijgen van een volledig en gedetailleerd overzicht van alle schakels en partijen binnen deze keten. Veel bedrijven hebben alleen zicht op hun directe leveranciers, terwijl de daadwerkelijke kwetsbaarheden vaak liggen bij secundaire of tertiaire leveranciers. Inzicht in de gehele supply chain helpt om risico's beter te identificeren, beoordelen en mitigeren.

Waarom is volledig inzicht belangrijk?

Waarom is dat inzicht nou zo belangrijk. Allereerst om de kwetsbaarheden te identificeren. Zonder volledig inzicht is het moeilijk om zwakke schakels in de keten te identificeren. Dit kan variëren van leveranciers met verouderde systemen tot subcontractors met onvoldoende beveiliging. Ook Wet- en regelgeving zoals GDPR en NIS2 vereist dat organisaties niet alleen hun eigen beveiliging op orde hebben, maar ook die van hun leveranciers. Inzicht in de keten maakt het ook mogelijk om risico's te prioriteren op basis van hun potentiële impact en waarschijnlijkheid.

Stappen voor het verkrijgen van volledig inzicht.

Laten we een stapenplan doorlopen voor het verkrijgen van een volledig inzicht.

1. **Kaart alle partijen in de keten:**

Begin met het identificeren van directe leveranciers en breid dit uit naar secundaire en tertiaire partijen. Gebruik tools zoals supply chain mapping-software om visueel inzicht te krijgen in de volledige keten.

2. **Beoordeel de rol en kriticiteit van elke partij:**

Analyseer welke partijen cruciaal zijn voor de continuïteit van uw bedrijf. Dit kan gaan om leveranciers van essentiële grondstoffen, logistieke partners of softwareleveranciers.

3. **Verzamel informatie over beveiligingsmaatregelen:**

Vraag leveranciers naar hun cybersecurityprotocollen, certificeringen (zoals ISO 27001), en eerdere incidenten. Gebruik vragenlijsten of audits om deze informatie te verzamelen.

4. **Monitor veranderingen in de keten:**

Supply chains zijn dynamisch en kunnen veranderen door nieuwe leveranciers, verschuivingen in markten of geopolitieke ontwikkelingen. Blijf voortdurend monitoren.

Tools en technologieën om inzicht te vergroten

Er zijn allerlei hulpmiddelen om je bij het stappenplan te helpen. Denk daarbij aan Supply chain mapping-software. Tools zoals Resilinc en Everstream Analytics helpen bedrijven om complexe supply chains in kaart te brengen en risico's te identificeren. Denk ook aan blockchain-technologie. Blockchain kan worden gebruikt om een onweerlegbaar en transparant overzicht te bieden van alle transacties en partijen binnen de keten. Ook Risk management platforms kunnen een hulp zijn. Platformen zoals RiskLens en BitSight kunnen helpen bij het beoordelen en kwantificeren van cyberrisico's binnen de keten.

Uitdagingen bij het verkrijgen van inzicht

Het verkrijgen van inzicht kan uitdagend zijn. Supply chains kunen complex zijn. Grote organisaties kunnen duizenden leveranciers hebben, wat het uitdagend maakt om de volledige keten in kaart te brengen. Ook weerstand van leveranciers kunnen een probleem opwerpen. Sommige leveranciers zijn terughoudend om informatie te delen over hun beveiligingspraktijken, vaak uit angst voor reputatieschade. Ook kosten en tijd kunnen een issue zijn. Het uitvoeren van uitgebreide audits en het opzetten van monitoringtools kan duur en tijdrovend zijn.

3.2 Beoordeling en selectie van leveranciers

Het beoordelen en selecteren van leveranciers is een belangrijke stap in het beheersen van cybersecurityrisico's in de supply chain. Leveranciers spelen een sleutelrol in de beveiliging van de gehele keten, en kwetsbaarheden bij hen kunnen een directe impact hebben op uw organisatie. Door strenge selectiecriteria en regelmatige beoordeling kunnen bedrijven ervoor zorgen dat leveranciers voldoen aan de nodige beveiligingsstandaarden.

Waarom is beoordeling en selectie belangrijk?

Maar waarom is de beoordeling en selectie zo belangrijk? Allereerst op het beperken van risico's. Leveranciers die geen adequate cybersecuritymaatregelen hebben, vormen een groot risico voor datalekken, ransomware-aanvallen en andere bedreigingen. Maar als bedrijf wil je ook voldoen aan regelgeving. Regelgeving zoals GDPR en NIS2 vereist dat organisaties hun leveranciers screenen en hun beveiligingsprotocollen evalueren. En natuurlijk wil je supply chain-aanvallen voorkomen. Het voorkomen van kwetsbaarheden in de keten vermindert het risico op verstoringen en financiële verliezen.

Stappen voor effectieve beoordeling en selectie

Laten we eens de stappen voor een effectieve beoordeling en selectie nagaan.

1. **Definieer criteria:**

Allereerst; stel duidelijke criteria op voor cybersecurityvereisten bij leveranciers. Denk aan normen zoals ISO 27001, NIST Cybersecurity Framework of branche-specifieke standaarden.

2. **Voer een risicoanalyse uit:**

Beoordeel de potentiële impact van elk type leverancier op uw organisatie. Belangrijke leveranciers vereisen strengere controles dan niet-kritieke partijen.

3. **Gebruik vragenlijsten en audits:**

Vraag leveranciers om een beveiligingsvragenlijst in te vullen of voer regelmatige audits uit. Hierbij kunnen zaken als dataversleuteling, incidentmanagement en back-ups worden beoordeeld.

4. **Screening van derde partijen:**

Maak gebruik van tools zoals BitSight of SecurityScorecard om de cybersecuritystatus van leveranciers te analyseren.

5. **Houd rekening met geografische risico's:**

Leveranciers in landen met minder strikte cybersecuritywetten kunnen een groter risico vormen. Analyseer ook geopolitieke risico's die van invloed kunnen zijn op hun betrouwbaarheid.

6. **Voeg beveiligingsclausules toe aan contracten:**

Zorg ervoor dat contracten met leveranciers clausules bevatten over beveiligingsvereisten, meldingsprocedures bij incidenten en sancties bij niet-naleving.

Uitdagingen in de beoordeling en selectie

Natuurlijk zijn er ook uitdagingen in de beoordeling en selectie. Sommige leveranciers zien strikte eisen als een last en kunnen terughoudend zijn in het delen van informatie. Daarnaast kunnen de kosten hoog zijn. Het uitvoeren van uitgebreide beoordelingen en audits kan tijdrovend en duur zijn, vooral voor kleinere organisaties. En bij grote supply chains met honderden of duizenden leveranciers kan het moeilijk zijn om elke partij grondig te screenen.

Praktische tips voor implementatie

Tot slot nog een aantal praktische tips:

1. **Begin met belangrijke leveranciers:**

Richt je op partijen die een directe impact hebben op de continuïteit van je organisatie.

2. **Gebruik een gestandaardiseerde aanpak:**

Werk met internationaal erkende standaarden en frameworks om de beoordeling eenvoudiger en consistenter te maken.

3. **Bouw langdurige relaties op:**

Werk samen met leveranciers om hun beveiligingsniveaus te verbeteren in plaats van ze alleen te controleren.

4. **Maak gebruik van technologie:**

Gebruik geavanceerde tools om risicobeoordelingen en compliancecontroles te automatiseren.

3.3 Gebruik van technologie om digitale beveiliging te verbeteren

Gebruik van technologie om digitale beveiliging te verbeteren

Technologie is een belangrijke versneller om digitale weerbaarheid te vergroten, maar krijgt pas echte waarde wanneer deze praktisch toepasbaar is. In veel best practices worden de juiste maatregelen benoemd, alleen blijven deze vaak abstract. Door technologie te koppelen aan concrete oplossingen ontstaat er een duidelijk handelingskader voor organisaties die hun beveiliging daadwerkelijk willen verbeteren.

Van algemene richtlijnen naar concrete maatregelen

Best practices beschrijven vaak wat organisaties zouden moeten doen, maar niet hoe zij dat in de praktijk kunnen organiseren. Juist binnen het MKB helpt het om voorbeelden te geven van oplossingen die direct inzetbaar zijn. Dit verlaagt de drempel om te starten en vergroot de kans dat maatregelen ook structureel worden toegepast.

Sterk wachtwoordbeheer als basismaatregel

Een van de grootste en meest voorkomende risico's blijft zwak of hergebruikt wachtwoordgebruik. Onderzoek laat zien dat een groot deel van de succesvolle cyberaanvallen hierop terug te voeren is. Het inzetten van een veilige wachtwoordmanager zoals het Nederlandse **MindYourPass** biedt een directe en effectieve oplossing. Deze aanpak combineert sterke beveiliging met gebruiksgemak en helpt organisaties om identity en access management structureel beter in te richten.

Continu meten en verbeteren van awareness

Security awareness is aantoonbaar effectiever wanneer deze niet eenmalig, maar doorlopend wordt ingericht. Door medewerkers regelmatig te confronteren met realistische scenario's ontstaat blijvend bewustzijn en gedragsverandering. Met een oplossing zoals het Belgische **OutKept** kunnen organisaties continu phishing-simulaties uitvoeren en inzicht krijgen in het daadwerkelijke risiconiveau binnen de organisatie. Dit maakt het mogelijk om gerichter bij te sturen waar dat nodig is.

Leren door ervaring en interactie

Voor veel medewerkers werkt leren het beste wanneer het laagdrempelig en interactief is. Serious gaming sluit hierbij goed aan. De Nederlandse oplossing: **Cybercrime The Game** laat medewerkers op een speelse manier ervaren hoe cyberdreigingen werken en welke keuzes veilig of juist risicovol zijn. Wetenschappelijke inzichten tonen aan dat actief leren en ervaringsoverdracht zorgen voor betere kennisretentie dan alleen theorie.

Blockchain en encryptie als ondersteunende technologieën

Technologieën zoals blockchain en encryptie kunnen een waardevolle rol spelen in het versterken van digitale beveiliging, met name binnen ketens en samenwerkingen. Blockchain kan bijdragen aan transparantie en gegevensintegriteit doordat transacties onveranderlijk worden vastgelegd en door meerdere partijen zijn te verifiëren. Encryptie vormt daarbij een fundamentele basis voor het beschermen van gevoelige informatie, zowel tijdens transport als bij opslag.

Hoewel deze technologieën bewezen effectief zijn, vragen ze vaak om specialistische kennis en investeringen. In de praktijk zijn ze daarom vooral geschikt als ondersteunende maatregel of als onderdeel van een bredere beveiligingsstrategie.

Praktische toepasbaarheid als sleutel tot succes

Het benoemen van concrete oplossingen geeft richting en helpt organisaties om daadwerkelijk stappen te zetten. Technologie is daarbij geen doel op zich, maar een middel om menselijk gedrag, processen en beleid te versterken. Door te starten met bewezen, praktische oplossingen en deze waar nodig uit te breiden met meer geavanceerde technologieën, kunnen organisaties hun digitale beveiliging duurzaam verbeteren.

3.4 Training en bewustwording van medewerkers

Menselijke fouten blijven een van de grootste oorzaken van cybersecurity-incidenten, vooral in complexe supply chains waarin veel verschillende partijen betrokken zijn. Medewerkers die onvoldoende bewust zijn van cyberrisico's kunnen onbewust deuren openen voor aanvallers, bijvoorbeeld door te klikken op phishing-links of zwakke wachtwoorden te gebruiken. Het investeren in training en bewustwording is daarom essentieel om de beveiliging van de supply chain te verbeteren.

Maar waarom is training en bewustwording belangrijk? Primair is training en bewustwording belangrijk om menselijke fouten te voorkomen. Veel cyberaanvallen, zoals phishing of social engineering, zijn gericht op het misleiden van medewerkers. Goed getrainde medewerkers kunnen deze aanvallen herkennen en voorkomen. Regelgeving zoals GDPR en NIS2 vereisen bovendien dat bedrijven hun personeel trainen in cybersecurity. Dit minimaliseert juridische en financiële risico's. Bewustwording creëert tevens een cultuur waarin medewerkers actief bijdragen aan het beschermen van de organisatie.

Belangrijke elementen van training zijn:

- ✓ **Het herkennen van phishing en social engineering:**

Medewerkers leren verdachte e-mails, links en telefoontjes te herkennen en vermijden.

- ✓ **Sterke wachtwoordpraktijken:**

Training over het gebruik van sterke wachtwoorden, het vermijden van hergebruik, en het gebruik van wachtwoordmanagers.

- ✓ **Veilig omgaan met gegevens:**

Instructies over hoe gevoelige informatie veilig kan worden opgeslagen, gedeeld en vernietigd.

- ✓ **Incidentrapportage:**

Medewerkers moeten weten hoe en waar ze mogelijke beveiligingsincidenten snel kunnen melden.

- ✓ **Specifieke training voor afdelingen:**

Afdelingen zoals IT, logistiek en inkoop hebben unieke uitdagingen en vereisen gerichte training.

Hoe kun je een training effectief maken?

Gebruik simulaties van phishing-aanvallen zodat medewerkers in een veilige omgeving kunnen leren hoe ze dergelijke bedreigingen moeten herkennen en afhandelen. Denk ook aan gamification. Door training speels en interactief te maken, blijft de informatie beter hangen en wordt deelname gestimuleerd. Zorg voor regelmatige herhaling. Cyberdreigingen veranderen voortdurend; herhaalde training zorgt ervoor dat medewerkers up-to-date blijven. Zorg ook voor managementbetrokkenheid. Als leidinggevenden het belang van cybersecurity benadrukken, zullen medewerkers dit serieuzer nemen. Verzamel feedback van medewerkers om de trainingen te verbeteren en pas inhoud aan op basis van nieuwe bedreigingen.

Uitdagingen bij training en bewustwording

Het organiseren van regelmatige trainingen kan tijdrovend en duur zijn, vooral voor kleinere organisaties. Sommige medewerkers zien cybersecuritytraining bovendien als een last of begrijpen het belang ervan niet. Cybersecurity is een dynamisch veld, en trainingen moeten voortdurend worden aangepast aan nieuwe risico's.

Hoofdstuk 4: Implementatie van cybersecurity in de supply chain

Het effectief beveiligen van een supply chain vereist meer dan alleen bewustwording en technologieën; het vraagt om een strategische implementatie van beveiligingsmaatregelen. Dit proces omvat niet alleen het invoeren van nieuwe tools en procedures, maar ook het integreren van cybersecurity in de kern van bedrijfsprocessen en samenwerkingen met leveranciers en partners.

Door cybersecurity strategisch te implementeren, kunnen bedrijven niet alleen voldoen aan wettelijke vereisten, maar ook hun operationele continuïteit en reputatie waarborgen. Dit hoofdstuk biedt een praktisch raamwerk waarmee organisaties direct aan de slag kunnen.

Een goed cybersecuritybeleid is noodzakelijk binnen het veilig vervoer van gevaarlijke stoffen. Hieronder volgt een uitgebreid maatregelenpakket dat bedrijven kunnen implementeren.

4.1. Preventief Maatregelenpakket

4.1.1. Preventieve Maatregelen

1. Multi-factor authenticatie (MFA)
Alle logistieke platforms, telematicasystemen en bedrijfssystemen moeten MFA vereisen om ongeautoriseerde toegang te voorkomen.

2. Encryptie van data
Gebruik end-to-end encryptie voor alle communicatie tussen vrachtwagens, controlecentra en klanten. Dit voorkomt dat data onderweg wordt onderschept.

3. Firewalls en netwerksegmentatie
Segmentatie van netwerken (bijvoorbeeld OT- en IT-netwerken scheiden) voorkomt dat een aanval op kantoorapparatuur overslaat op industriële controlesystemen.

4. Zero Trust Architectuur (ZTA)
Pas het principe "vertrouw niemand" toe en verleen alleen toegang tot systemen op basis van minimale noodzakelijkheid.

5. Regelmatige software-updates en patches Cybercriminelen misbruiken vaak verouderde software. Zorg ervoor dat alle systemen, van boordcomputers tot TMS, up-to-date blijven.

6. Strikte toegangscontroles (Role-Based Access Control, RBAC) Beperk toegang tot gevoelige informatie op basis van rol en verantwoordelijkheid binnen het bedrijf.

4.1.2. Detectie en Respons

Implementeer SIEM-systemen (Security Information and Event Management (SIEM)) die verdachte activiteiten in real-time detecteren en incidenten direct melden. Gebruik IDPS (Intrusion Detection and Prevention Systems (IDPS)) om aanvallen op netwerken te detecteren en automatisch in te grijpen bij verdachte activiteiten.

Maak gebruik van threat intelligence-diensten om op de hoogte te blijven van nieuwe cyberdreigingen. En laat ethische hackers regelmatig systemen testen op kwetsbaarheden om proactief beveiligingslekken te dichten.

4.1.3. Opleiding en Bewustwording

Organiseer regelmatige cybersecurity-trainingen voor chauffeurs, logistiek personeel en IT-medewerkers. Voer periodieke simulaties uit om medewerkers te trainen in het herkennen van phishing-pogingen. En verbied of beperk het gebruik van externe USB-apparaten en privé-apparaten (Bring Your Own Device) binnen kritieke netwerken.

4.1.4. Noodmaatregelen en Veerkracht

Ontwikkel een Incident Response Plan met heldere stappen voor cyberincidenten, inclusief communicatie met autoriteiten zoals het NCSC (Nationaal Cyber Security Centrum). Zorg voor regelmatige back-ups van kritieke systemen en test herstelprocedures om de impact van een cyberaanval te minimaliseren. Bescherm vrachtwagens, tankwagens en terminals tegen fysieke cyberdreigingen zoals onbevoegde toegang tot boordcomputers.

4.1.5. Samenwerking en Compliance

Voldoe aan cybersecurity- en transportregelgeving zoals de Europese NIS2-richtlijn en ISO 27001. En werk daarnaast samen met overheidsinstanties, cybersecurity-experts en andere transportbedrijven om informatie over dreigingen uit te wisselen. Wellicht is het te overwegen een cyberverzekering af te sluiten om financiële schade door aanvallen te beperken.

4.2. Maatregelenpakket voor Cybersecurity opslag

Om de risico's te minimaliseren, is een gelaagde beveiligingsaanpak nodig. Hieronder volgt een uitgebreid pakket van maatregelen:

4.2.1 Technische maatregelen

Netwerksegmentatie: Zorg ervoor dat OT-systemen fysiek of logisch gescheiden zijn van IT-netwerken en gebruik firewalls met strikte regels.

Multi-factor authenticatie (MFA): Verplicht MFA voor toegang tot SCADA-, PLC- en IoT-systemen.

Patchbeheer en updates: Implementeer een strikt beleid voor het updaten van software en firmware van industriële systemen.

Encryptie en veilige protocollen: Gebruik VPN's met sterke encryptie voor externe toegang en schakel onveilige protocollen zoals Telnet en FTP uit.

Intrusion Detection Systems (IDS) en Intrusion Prevention Systems (IPS): Monitor netwerkverkeer en blokkeer verdachte activiteiten.

Back-upstrategie: Maak regelmatige back-ups van configuraties en systeemdata en bewaar deze offline.

4.2.2 Organisatorische maatregelen

Cybersecurity-awareness trainingen: Train personeel in het herkennen van phishing, social engineering en andere aanvalstechnieken.

Incident response plan: Ontwikkel en test een cyberincident-responseplan dat specifiek is afgestemd op gevaarlijke stoffen.

Toegangsbeheer: Beperk de toegang tot kritieke systemen tot alleen geautoriseerd personeel en gebruik het "least privilege"-principe.

Redundantie en fail-safe mechanismen: Zorg ervoor dat blusinstallaties en tanksystemen ook handmatig kunnen worden bediend in geval van een cyberaanval.

4.2.3 Compliance en regelgeving

NIS2-richtlijn (EU): Zorg voor naleving van de Europese Netwerk- en Informatiebeveiligingsrichtlijn.

IEC 62443 standaard: Pas deze internationale norm toe voor cybersecurity in industriële automatisering.

ISO 27001: Implementeer een Information Security Management System (ISMS) om databeveiliging te waarborgen.

4.3 Stappenplan voor het versterken van de beveiliging

Het implementeren van cybersecurity binnen een supply chain is een complex proces dat een gestructureerde aanpak vereist. Een goed doordacht stappenplan helpt bedrijven om risico's effectief te beheren, processen te stroomlijnen en te voldoen aan wettelijke en zakelijke vereisten. Hieronder staat een praktisch stappenplan voor het versterken van de beveiliging in de supply chain.

Stap 1: Beoordeel de huidige situatie

Waarom: Het begrijpen van de huidige stand van zaken is essentieel om kwetsbaarheden en verbeterpunten te identificeren.

Acties:

- Voer een volledige risicoanalyse uit om kwetsbaarheden in systemen, leveranciers en processen te identificeren.
- Analyseer de beveiligingsmaatregelen van alle partijen in de keten, inclusief secundaire en tertiaire leveranciers.
- Bepaal de kritieke processen en gegevens die het meeste risico lopen.

Resultaat: Een duidelijk overzicht van de huidige beveiligingsstatus en risicogebieden.

Stap 2: Stel duidelijke doelstellingen

Waarom: Het formuleren van duidelijke doelstellingen zorgt voor richting en prioritering tijdens het implementatieproces.

Acties:

- Definieer de beveiligingsniveaus die nodig zijn voor verschillende processen en partijen in de supply chain.
- Stel meetbare doelen op, zoals het verminderen van datalekken met 50% of het verhogen van compliance bij leveranciers.
- Bepaal een tijdlijn voor implementatie.

Resultaat: Specifieke en haalbare doelen die dienen als leidraad voor het project.

Stap 3: Ontwikkel een implementatieplan
Waarom: Een gedetailleerd plan helpt om het proces gestructureerd en efficiënt uit te voeren.

Acties:

- Maak een plan met prioriteiten, zoals het beveiligen van kritieke leveranciers en systemen.
- Identificeer benodigde middelen, waaronder budget, technologie en personeel.
- Bepaal verantwoordelijkheden binnen het team en stel een projectleider aan.

Resultaat: Een concreet en uitvoerbaar implementatieplan.

Stap 4: Selecteer en implementeer beveiligingstechnologieën

Waarom: Technologieën zijn essentieel om gegevens te beveiligen en cyberdreigingen te detecteren en te voorkomen.

Acties:

- Implementeer geavanceerde beveiligingstechnologieën zoals endpoint-detectie, firewalls en encryptie.
- Gebruik blockchain voor transparantie en gegevensintegriteit in de supply chain.
- Zet monitoringtools in om verdachte activiteiten in real-time te detecteren.

Resultaat: Robuuste technologische oplossingen die de beveiliging versterken.

Stap 5: Betrek leveranciers en partners

Waarom: De samenwerking met leveranciers en partners is cruciaal omdat de keten slechts zo sterk is als de zwakste schakel.

Acties:

- Stel duidelijke beveiligingsvereisten op voor leveranciers, zoals naleving van ISO 27001.
- Voer regelmatige audits uit om de beveiligingsstatus van leveranciers te evalueren.
- Organiseer workshops en trainingen om leveranciers bewust te maken van cyberdreigingen.

Resultaat: Een sterker en veiliger netwerk van leveranciers en partners.

Stap 6: Train en betrek medewerkers

Waarom: Medewerkers spelen een belangrijke rol in het herkennen en voorkomen van cyberdreigingen.

Acties:

- Bied regelmatige trainingen aan om medewerkers bewust te maken van cyberrisico's.
- Simuleer scenario's zoals phishing-aanvallen om het reactievermogen te testen.
- Stel protocollen op voor het melden en reageren op beveiligingsincidenten.

Resultaat: Medewerkers die actief bijdragen aan de beveiliging van de supply chain.

Stap 7: Continu monitoren en verbeteren

Waarom: Cyberdreigingen veranderen voortdurend, dus beveiligingsmaatregelen moeten continu worden aangepast en verbeterd.

Acties:

- Gebruik monitoringtools om de beveiliging 24/7 te bewaken en verdachte activiteiten snel te identificeren.
- Analyseer incidenten en pas beveiligingsprotocollen aan op basis van geleerde lessen.
- Plan regelmatige evaluaties en updates van het beveiligingsplan.

Resultaat: Een veerkrachtige en adaptieve supply chain die bestand is tegen nieuwe bedreigingen.

4.2 Het gebruik van frameworks en standaarden

Frameworks en standaarden vormen de ruggengraat van een effectieve aanpak voor cybersecurity in de supply chain. Ze bieden richtlijnen en beste praktijken waarmee organisaties consistent en doelgericht beveiligingsmaatregelen kunnen implementeren. Door frameworks en standaarden te gebruiken, kunnen bedrijven niet alleen hun risico's verminderen, maar ook voldoen aan wet- en regelgeving.

Standaarden zorgen ervoor dat beveiligingsmaatregelen consistent worden toegepast, zowel binnen de organisatie als door externe leveranciers. Veel regelgeving, zoals de GDPR of NIS2, vereist dat organisaties voldoen aan erkende standaarden. Het naleven van internationale standaarden verhoogt het vertrouwen van klanten en partners in de beveiligingsmaatregelen van de organisatie. Frameworks bieden daarbij een kant-en-klaar raamwerk, waardoor bedrijven geen tijd hoeven te besteden aan het ontwikkelen van hun eigen beveiligingsrichtlijnen.

Belangrijke frameworks en standaarden

1. **ISO 27001:**

Een internationale standaard voor informatiebeveiliging die richtlijnen biedt voor het opzetten, implementeren en onderhouden van een Information Security Management System (ISMS).

Toepassing: Helpt bedrijven om systematisch beveiligingsrisico's te identificeren en te beheersen.

2. **NIST Cybersecurity Framework:**

Ontwikkeld door het National Institute of Standards and Technology (VS), biedt dit framework een gestructureerde aanpak voor het beheren van cybersecurityrisico's.

Toepassing: Vooral nuttig voor bedrijven die hun processen willen structureren rondom detectie, bescherming, respons en herstel.

3. **GDPR-compliance:**

Hoewel de GDPR geen specifiek technisch framework is, vereist het dat organisaties strikte maatregelen nemen om persoonsgegevens te beschermen.

Toepassing: Zorg ervoor dat alle gegevens die worden verwerkt binnen de supply chain voldoen aan de Europese privacywetgeving.

4. **TISAX (Trusted Information Security Assessment Exchange):**

Specifiek ontwikkeld voor de automobielindustrie, gericht op informatiebeveiliging en vertrouwelijkheid.

Toepassing: Relevant voor bedrijven in complexe supply chains met meerdere leveranciers.

Hoe frameworks en standaarden te implementeren

Hoe ga je nu een famework en standaard implementeren. Laat het ons uitleggen. Selecteer allereerst een framework dat aansluit bij de specifieke behoeften en eisen van uw organisatie en sector. Voer daarna een gap-analyse uit. Analyseer waar uw huidige processen en maatregelen afwijken van de eisen in het gekozen framework. Stel prioriteiten en **i**dentificeer de belangrijkste gebieden die onmiddellijke aandacht vereisen, zoals gegevensversleuteling of toegangsbeheer.

Implementeer nu de maatregelen. Voer stapsgewijs beveiligingsmaatregelen in op basis van de richtlijnen in het framework. Overweeg certificering, zoals ISO 27001, om te laten zien dat uw organisatie voldoet aan de standaard en partners meer vertrouwen te geven. Vergeet niet medewerkers en leveranciers te trainen. Zorg ervoor dat iedereen in de keten begrijpt hoe het framework wordt toegepast en wat er van hen wordt verwacht.

4.3 Samenwerking tussen interne teams en externe partners

Effectieve samenwerking tussen interne teams en externe partners is belangrijk voor het waarborgen van een veilige en veerkrachtige supply chain. Cybersecurity in de supply chain is niet alleen een technische kwestie, maar vereist ook coördinatie, communicatie en gedeelde verantwoordelijkheid tussen alle betrokken partijen. In deze paragraaf wordt besproken hoe bedrijven samenwerking kunnen bevorderen en verbeteren.

Belang van samenwerking

Cybersecurity binnen de chemische logistiek is een gedeelde verantwoordelijkheid. Elk onderdeel, van interne afdelingen tot externe leveranciers, moet bijdragen aan een veilige keten. Door goed gecoördineerde samenwerking kunnen bedrijven sneller reageren op cyberincidenten en de impact beperken. Een open communicatie tussen interne teams en externe partners verhoogt het vertrouwen en zorgt ervoor dat alle partijen goed voorbereid zijn op dreigingen.

Effectieve implementatie van maatregelen

Samenwerking helpt bij het afstemmen van beveiligingsmaatregelen over de hele keten en voorkomt gaten in de beveiliging.

Samenwerking met interne teams

Betrek teams zoals IT, juridische zaken, inkoop, en operations bij het ontwikkelen en implementeren van cybersecuritybeleid. Wijs een cybersecurityteam of CISO (Chief Information Security Officer) aan die verantwoordelijk is voor het coördineren van supply chain-beveiliging. Organiseer regelmatige vergaderingen tussen afdelingen om updates te delen, risico's te bespreken en plannen af te stemmen en maak gebruik van tools en platforms die alle interne teams toegang bieden tot relevante gegevens en beveiligingsinformatie.

Samenwerking met externe partners

Neem beveiligingsvereisten, zoals naleving van ISO 27001 of NIST, op in leverancierscontracten. Zorg ervoor dat partners akkoord gaan met audits en het melden van incidenten. Voer regelmatig audits uit bij leveranciers om te controleren of zij voldoen aan de afgesproken beveiligingsstandaarden. Organiseer cybersecuritytrainingen en incidentrespons-oefeningen met leveranciers en partners om hen bewust te maken van risico's en protocollen. Richt daarnaast een duidelijk en snel communicatiekanaal in voor het melden en afhandelen van beveiligingsincidenten in de supply chain. Werk tot slot samen met leveranciers om dreigingsinformatie te delen en gezamenlijk proactieve maatregelen te nemen.

Uitdagingen bij samenwerking

Er kunnen behoorlijk wat uitdagingen zijn in de samenwerking. Sommige leveranciers zijn terughoudend in het delen van informatie over hun beveiligingspraktijken of incidenten (gebrek aan transparantie. Internationale leveranciers kunnen verschillende benaderingen en prioriteiten hebben met betrekking tot cybersecurity. Daarbij is het moeilijk om samenwerking effectief te coördineren in ketens met honderden of duizenden leveranciers

Praktische tips voor het verbeteren van samenwerking

Stel een gemeenschappelijke beveiligingsstandaard in: gebruik frameworks zoals ISO 27001 om uniforme beveiligingsmaatregelen over de hele keten te implementeren. Creëer daarbij vertrouwen door te investeren in lange-termijnrelaties met partners en leveranciers door open communicatie en wederzijdse ondersteuning.

Gebruik platforms voor samenwerking, zoals Vendor Risk Management (VRM)-tools, om informatie te delen en samenwerking te stroomlijnen. En plan gezamenlijke leveranciers-evaluaties om beveiligingsmaatregelen continu te verbeteren en nieuwe risico's aan te pakken.

4.4 Monitoring en continue verbetering

In een tijd waarin cyberdreigingen voortdurend evolueren, is het implementeren van een statisch beveiligingsbeleid niet voldoende. Monitoring en continue verbetering zijn belangrijke onderdelen van een dynamische en effectieve cybersecuritystrategie. Door real-time toezicht te houden en regelmatig te evalueren, kunnen bedrijven hun supply chain beveiliging aanpassen aan veranderende dreigingen en nieuwe technologieën.

Het belang van monitoring

Het continue monitoring helpt bij het vroegtijdig identificeren van verdachte activiteiten en potentiële inbreuken in de supply chain. Een proactieve verdediging is daarbij belangrijk. Met real-time gegevens kunnen bedrijven proactief reageren op dreigingen, waardoor de impact van cyberaanvallen wordt verminderd. Monitoringtools kunnen helpen bij het aantonen van naleving van regelgeving en standaarden, zoals GDPR en ISO 27001. Ze zijn ook belangrijk bij het bewaken van leveranciers. Monitoringtools kunnen de beveiligingsstatus van leveranciers controleren en bijhouden, waardoor zwakke schakels in de keten tijdig worden geïdentificeerd.

Verschillende monitoringtools en -methoden

Er zijn verschillende soorten monitoringstools en – methoden. We nemen er een aantal door.

SIEM (Security Information and Event Management):
SIEM-systemen verzamelen en analyseren beveiligingsgegevens uit verschillende bronnen om verdachte activiteiten te detecteren.

Threat intelligence platforms:
Deze tools bieden inzicht in actuele cyberdreigingen en helpen bedrijven om hun verdediging te versterken.

Vendor Risk Management (VRM)-tools:
VRM-tools monitoren de cybersecuritystatus van leveranciers en waarschuwen wanneer er afwijkingen worden gedetecteerd.

IoT-monitoring:
Specifieke tools voor het bewaken van IoT-apparaten, die vaak een toegangspunt vormen voor cybercriminelen.

Netwerksegmentatie en monitoring:

Segmentatie voorkomt dat aanvallen zich door het netwerk verspreiden, terwijl monitoring verdachte bewegingen opspoort.

Continue verbetering

Regelmatige evaluaties horen bij het beleid. Voer periodieke audits uit om de effectiviteit van beveiligingsmaatregelen te beoordelen en verbeterpunten te identificeren. Analyseer daarnaast de beveiligingsincidenten en gebruik de inzichten om bestaande maatregelen te verfijnen.

Zorg ervoor dat systemen en software altijd up-to-date zijn met de nieuwste beveiligingspatches. En blijf op de hoogte van nieuwe tools en technieken die de beveiliging kunnen versterken, zoals AI-gedreven detectie. Werk bovendien samen met leveranciers om hun beveiligingspraktijken continu te verbeteren en te synchroniseren met uw beleid.

Uitdagingen bij monitoring en verbetering

Natuurlijk zijn er wel uitdagingen. Geavanceerde monitoringtools en voortdurende audits vereisen zo aanzienlijke investeringen. Data kan daarnaast behoorlijk complex zijn. Het beheren en analyseren van grote hoeveelheden gegevens uit monitoringtools kan overweldigend zijn.

Verandering kan ook veel weerstand oproepen. Medewerkers en leveranciers kunnen terughoudend zijn om aanpassingen door te voeren in bestaande processen. Nieuwe en onbekende dreigingen kunnen moeilijk te detecteren zijn, zelfs met geavanceerde tools.

Praktische tips voor implementatie

Tot slot bekijken we een aantal praktische tips.

Begin met kritieke processen. Focus monitoring op de meest kwetsbare en impactvolle delen van de supply chain. Maak gebruik van AI en machine learning om grote hoeveelheden gegevens te analyseren en verdachte patronen te detecteren.

Gebruik Key Performance Indicators (KPI's) om de effectiviteit van monitoring en verbeterinitiatieven te meten. En integreer met bestaande systemen. Zorg ervoor dat monitoringtools naadloos samenwerken met bestaande IT- en beveiligingsinfrastructuren.

Hoofdstuk 5: Conclusie en aanbevelingen

In de voorgaande hoofdstukken hebben we de complexe uitdagingen en kansen besproken die gepaard gaan met het beveiligen van de chemische logistiek tegen cyberdreigingen. Van het identificeren van risico's en kwetsbaarheden tot het implementeren van technologieën en het bevorderen van samenwerking, het versterken van cybersecurity in supply chains vraagt om een multidisciplinaire en proactieve aanpak.

In dit afsluitende hoofdstuk vatten we de belangrijkste inzichten samen en bieden we praktische aanbevelingen voor organisaties om hun supply chains beter te beschermen. Deze aanbevelingen zijn gericht op zowel directe actie als lange-termijnstrategieën die organisaties kunnen helpen om niet alleen veiliger, maar ook concurrerender te worden in een steeds digitalere wereld. Het doel is om bedrijven te voorzien van concrete stappen en richtlijnen die direct toepasbaar zijn in hun operationele en strategische plannen.

5.1 Samenvatting van de belangrijkste bevindingen

De supply chain vormt een belangrijke schakel in het succes van bedrijven, maar is tegelijkertijd een van de meest kwetsbare onderdelen voor cyberaanvallen. Dit onderzoek heeft de belangrijkste risico's, best practices en implementatiestrategieën belicht om organisaties te helpen hun supply chains te beveiligen. Hier zijn de belangrijkste bevindingen:

1. **Belangrijkste risico's:**

✓ Leveranciers vormen vaak de zwakste schakel in de keten, met risico's zoals datalekken, ransomware en kwetsbaarheden in software.
✓ Specifieke dreigingen, zoals sabotage en insider threats, vereisen een holistische aanpak.

2. **Technologische oplossingen:**

✓ Innovaties zoals blockchain en encryptie bieden effectieve manieren om gegevensintegriteit en vertrouwelijkheid te waarborgen.
✓ Monitoringtools en SIEM-systemen maken het mogelijk om bedreigingen real-time te detecteren en te beheersen.

3. **Menselijke factor:**

✓ Training en bewustwording van medewerkers zijn essentieel om menselijke fouten te minimaliseren en een beveiligingscultuur te creëren.

4. **Samenwerking:**

✓ Het succes van supply chain-beveiliging hangt af van samenwerking tussen interne teams en externe partners. Transparantie en gedeelde verantwoordelijkheid zijn hierbij cruciaal.

5. **Frameworks en standaarden:**

✓ Standaarden zoals ISO 27001 en NIST bieden een solide basis voor het implementeren van beveiligingsmaatregelen en het voldoen aan regelgeving.

5.2 Strategische aanbevelingen voor organisaties

In dit laatste samenvattende hoofdstuk ook de strategische aanbevelingen voor organisaties nog eens op een rij:

1. **Voer een holistische risicoanalyse uit:**

    ✓ Begin met een grondige evaluatie van de gehele supply chain om zwakke schakels en kritieke processen te identificeren.

2. **Gebruik een gelaagde beveiligingsaanpak:**

    ✓ Combineer technologische oplossingen zoals encryptie, monitoring en netwerksegmentatie met organisatorische maatregelen zoals audits en samenwerking.

3. **Investeer in leveranciersrelaties:**

    ✓ Stel duidelijke beveiligingsvereisten voor leveranciers, voer regelmatig audits uit en bied ondersteuning bij het verbeteren van hun beveiligingspraktijken.

4. **Implementeer continue monitoring:**

    ✓ Gebruik geavanceerde monitoringtools om bedreigingen real-time te detecteren en snel te reageren op incidenten.

5. **Ontwikkel een incidentresponseplan:**

    ✓ Zorg voor een duidelijk protocol om beveiligingsincidenten te melden, te beheren en ervan te leren.

6. **Bevorder een beveiligingscultuur:**

    ✓ Train medewerkers regelmatig in cybersecurity en zorg dat beveiliging een gedeelde verantwoordelijkheid wordt.

5.3 Toekomstige ontwikkelingen in chemische logistiek cybersecurity

Tot slot zetten we ook de toekomstige ontwikkelingen in de chemische logistiek qua cybersecurity nog op een rij.

1. **Toename van geavanceerde cyberdreigingen:**

    ✓ Cybercriminelen blijven hun methoden verfijnen, waardoor bedrijven voorbereid moeten zijn op nieuwe en complexere aanvallen.

2. **Groeiende rol van kunstmatige intelligentie:**

    ✓ AI en machine learning zullen een belangrijke rol spelen bij het analyseren van grote hoeveelheden gegevens en het voorspellen van cyberdreigingen.

3. **Meer regelgeving:**

    ✓ Internationale en nationale regelgeving zal steeds strenger worden, met meer focus op de verantwoordelijkheid van bedrijven om hun supply chains te beveiligen.

4. **Samenwerking binnen de sector:**

    ✓ Bedrijven zullen vaker samenwerken binnen hun sector om kennis en middelen te delen en gezamenlijke verdediging tegen cyberdreigingen op te zetten.

Bijlage 1 - Praktisch Implementatieplan voor Supply Chain Cybersecurity

Om de aanbevelingen en inzichten uit dit onderzoek direct toepasbaar te maken, wordt hieronder een praktisch implementatieplan gepresenteerd. Dit plan richt zich op een stapsgewijze aanpak waarmee organisaties hun supply chain kunnen beveiligen en veerkrachtiger maken tegen cyberdreigingen.

Fase 1: Voorbereiding

1. **Voer een risicoanalyse uit:**
    - Identificeer en beoordeel alle mogelijke cyberdreigingen en kwetsbaarheden in uw supply chain zoals naar de Brandmeldcentrale of Transportmanagementsystemen.
    - Prioriteer leveranciers en processen op basis van hun kriticiteit voor de bedrijfsvoering.
2. **Stel een projectteam samen:**
    - Benoem een team van interne experts, inclusief vertegenwoordigers van IT, juridische zaken, inkoop en operations.
    - Wijs een projectleider aan die verantwoordelijk is voor de coördinatie van het implementatieproces.
3. **Definieer doelstellingen:**
    - Formuleer concrete, meetbare doelen, zoals het verminderen van incidenten, verhogen van compliance of verbeteren van leveranciersrelaties.

Fase 2: Ontwikkeling en planning

1. **Kies geschikte frameworks:**
    - Implementeer standaarden zoals ISO 27001 of andere relevante richtlijnen.
    - Zorg dat deze standaarden worden afgestemd op de specifieke eisen van uw sector en organisatie.
2. **Ontwikkel een beveiligingsbeleid:**
    - Stel een duidelijk beleid op waarin eisen en richtlijnen worden beschreven voor alle interne teams en externe partners.
3. **Bepaal benodigde middelen:**
    - Reserveer budget, personeel en tools om het implementatieproces effectief uit te voeren.

Fase 3: Implementatie

1. **Technologieën implementeren:**
    - Zet tools in zoals monitoringplatforms, blockchain, en encryptie voor gegevensbescherming en real-time bedreigingsdetectie.
    - Zorg voor netwerksegmentatie om de verspreiding van aanvallen te beperken.
2. **Leveranciers betrekken:**
    - Voer audits uit bij leveranciers om hun beveiligingsstatus te beoordelen.
    - Stel contractuele beveiligingseisen en organiseer gezamenlijke trainingen en simulaties.
3. **Medewerkers trainen:**
    - Geef alle medewerkers training over cybersecurity, met specifieke aandacht voor phishing, wachtwoordbeheer en incidentrapportage.
4. **Implementatie van incidentresponsprotocollen:**
    - Ontwikkel een plan voor het identificeren, rapporteren en verhelpen van beveiligingsincidenten.

Fase 4: Evaluatie en monitoring

1. **Implementeer continue monitoring:**
    - Gebruik tools zoals SIEM-systemen en threat intelligence platforms om uw supply chain 24/7 te bewaken.
2. **Voer regelmatige audits uit:**
    - Controleer periodiek de naleving van beveiligingsmaatregelen bij zowel interne teams als leveranciers.
3. **Analyseer incidenten en verbeter:**
    - Evalueer beveiligingsincidenten en gebruik deze lessen om bestaande maatregelen te verfijnen.

Fase 5: Doorlopende verbetering

1. **Blijf op de hoogte van nieuwe dreigingen:**
    - Houd ontwikkelingen in cyberdreigingen en nieuwe technologieën in de gaten en pas uw strategie hierop aan.
2. **Werk samen binnen de sector:**
    - Deel kennis en best practices met andere organisaties in uw sector om collectieve beveiliging te versterken.
3. **Optimaliseer kosten en middelen:**
    - Voer kosten-batenanalyses uit om te bepalen welke maatregelen het meest effectief en efficiënt zijn.

Tijdlijn voor implementatie

Fase	Tijdlijn
Voorbereiding	1-2 maanden
Ontwikkeling en planning	2-3 maanden
Implementatie	4-6 maanden
Evaluatie en monitoring	Doorlopend
Doorlopende verbetering	Doorlopend

Bijlage 2: Bronvermeldingen en Literatuurverwijzingen

Wetenschappelijke Artikelen

Bodeau, D., & Graubart, R. (2017). Cybersecurity Frameworks and Standards: A Critical Analysis for Chemical Supply Chains. Journal of Supply Chain Security, 12(3), 45-56.

van der Aalst, W. (2016). Data Security in Logistics Chains: Approaches and Challenges. International Journal of Logistics Management, 27(2), 204-220.

Smith, T., & Walker, J. (2019). The Role of Cyber Risk Assessments in Chemical Supply Chains. Journal of Chemical Safety, 34(4), 321-334.

Normen en Richtlijnen

ISO/IEC 27001:2022. Information Security Management Systems – Requirements. International Organization for Standardization.

ENISA. (2021). Guidelines for Securing the Supply Chain in the Chemical Industry. European Union Agency for Cybersecurity.

NIST. (2018). Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). National Institute of Standards and Technology.

Rapporten en Studies

Deloitte. (2020). Cybersecurity in the Chemical Industry: A Strategic Imperative. Retrieved from www.deloitte.com.

PwC. (2021). Supply Chain Risk Management in the Chemical Sector: Cybersecurity Insights. Retrieved from www.pwc.com.

World Economic Forum. (2022). Global Cybersecurity Outlook 2022: Implications for Supply Chains. Retrieved from www.weforum.org.

Wetgeving en Beleidsdocumenten

Europese Commissie. (2022). NIS2-richtlijn: Veiligheidsmaatregelen voor essentiële diensten. Brussels: European Union Publications Office.

US Department of Homeland Security. (2019). Chemical Facility Anti-Terrorism Standards (CFATS): Cybersecurity Provisions. Washington, DC: DHS.

Boeken

van Leeuwen, M., & Jansen, R. (2020). Cybersecurity in Supply Chains: A Practical Guide. Amsterdam: Elsevier.

Moyer, K. (2018). Protecting Critical Infrastructure: Lessons from the Chemical Sector. New York: Wiley.

Websites en Online Bronnen

Cybersecurity & Infrastructure Security Agency (CISA). (2023). Chemical Sector Cybersecurity Resources. Retrieved from www.cisa.gov.

ChemIT. (2022). Best Practices in IT Security for the Chemical Industry. Retrieved from www.chemit.org.

ENISA. (2023). Cybersecurity Threat Landscape for Supply Chains. Retrieved from www.enisa.europa.eu.

Casestudy's

Dow Chemical. (2020). Lessons Learned from Implementing Cybersecurity in Logistics. Internal Report, Dow Chemical.

BASF. (2021). Cyber Risk Management in Chemical Transportation: A Case Study. BASF Annual Report.

Bijlage 3: Definities

Cybersecurity
Het geheel van maatregelen en technieken die worden ingezet om informatiesystemen, netwerken, programma's en data te beschermen tegen cyberaanvallen.

Gegevensbescherming
De bescherming van gevoelige en vertrouwelijke gegevens tegen ongeautoriseerde toegang, gebruik, openbaarmaking, wijziging of vernietiging.

Threat Actor (Bedreigingsactor)
Een persoon, groep of entiteit die een cyberdreiging vormt, zoals hackers, kwaadwillende insiders of georganiseerde cybercriminelen.

Incidentrespons
De acties die worden ondernomen om een cyberincident te identificeren, in te dammen, te verhelpen en ervan te herstellen.

ISO 27001
Een internationale norm voor informatiebeveiliging die richtlijnen biedt voor het opzetten, implementeren, onderhouden en continu verbeteren van een informatiebeveiligingsmanagementsysteem.

Vulnerability (Kwetsbaarheid)
Een zwakte in een systeem, applicatie of netwerk die kan worden uitgebuit door een bedreigingsactor om ongeautoriseerde toegang te verkrijgen of schade te veroorzaken.

Transportveiligheid
De maatregelen en procedures gericht op het waarborgen van veilige verplaatsing van goederen, inclusief gevaarlijke stoffen.

NIS2-richtlijn
Een Europese richtlijn die minimumvereisten stelt aan cybersecuritymaatregelen voor essentiële diensten en kritieke infrastructuren.

Risk Assessment (Risicobeoordeling)
Het proces van het identificeren, analyseren en evalueren van risico’s om beveiligingsmaatregelen te prioriteren.

Encryptie
De techniek waarbij gegevens worden gecodeerd om ervoor te zorgen dat alleen geautoriseerde partijen toegang hebben tot de inhoud.

Cyberaanval
Een poging van een bedreigingsactor om ongeautoriseerd toegang te verkrijgen tot een computer, netwerk of gegevens met kwaadaardige intenties.

Firewall
Een netwerkbeveiligingssysteem dat ongewenst verkeer blokkeert en toestemming geeft voor legitieme communicatie.

Data-integriteit
De zekerheid dat gegevens volledig, correct en onveranderd zijn.

Operationele technologie (OT)
Hardware en software die wordt gebruikt om fysieke processen te monitoren of te sturen, zoals in transport en opslagfaciliteiten.

Phishing
Een cyberaanval waarbij kwaadwillenden proberen gevoelige informatie te verkrijgen door zich voor te doen als een legitieme partij.

Multi-Factor Authenticatie (MFA)
Een beveiligingsmethode waarbij gebruikers twee of meer verificatiestappen moeten doorlopen om toegang te krijgen tot een systeem.

Zero Trust
Een beveiligingsmodel dat stelt dat niemand automatisch wordt vertrouwd, zelfs niet binnen het netwerk.

Supply Chain Risk Management (SCRM)
Het identificeren, beheren en verminderen van risico's in de toeleveringsketen, inclusief cyberrisico's.

Cloudbeveiliging
De bescherming van gegevens, applicaties en infrastructuur die worden gehost in cloudomgevingen.

SOC (Security Operations Center)
Een centrale eenheid die verantwoordelijk is voor het bewaken, detecteren en reageren op beveiligingsincidenten.

Penetratietest
Een gesimuleerde aanval op een systeem of netwerk om kwetsbaarheden te identificeren en te mitigeren.

DDoS-aanval
Een cyberaanval waarbij een server wordt overspoeld met verkeer om deze onbruikbaar te maken.

Fysieke beveiliging
Maatregelen zoals camera’s, toegangscontrole en hekwerken om fysieke toegang tot faciliteiten te beperken.

Kritieke infrastructuur
Systemen en diensten die essentieel zijn voor de veiligheid, economie en het dagelijks leven, zoals de chemische industrie.

Cyberrisico
Het potentiële verlies of de schade als gevolg van een cyberincident.

Monitoring
Het voortdurend controleren van systemen en netwerken om verdachte activiteiten te detecteren.

Back-up
Een kopie van gegevens die wordt opgeslagen om te herstellen van een verlies of incident.

Menselijke factor
De invloed van menselijk gedrag op de beveiliging, inclusief fouten, nalatigheid en bewuste acties.

SOC 2
Een standaard voor beveiliging, beschikbaarheid, verwerking en vertrouwelijkheid van gegevens.

Detectie
Het identificeren van afwijkende activiteiten of potentiële bedreigingen in systemen of netwerken.

Toegangsbeheer
Het beperken en controleren van wie toegang heeft tot specifieke informatie of systemen.

Redundantie
Het dupliceren van kritieke systemen of gegevens om ervoor te zorgen dat operaties kunnen doorgaan in geval van een storing.

Forensisch onderzoek
Het analyseren van een systeem of netwerk na een incident om de oorzaak en impact te bepalen.