TNO innovation for life

HANDVATTEN CYBERSECURITY IN DE LOGISTIEKE KETEN

Robin de Veer (TNO) en Robert Wezeman (TNO)

11/12/2020

TNO · TLN · SMART PORT · ACN · CARGONAUT · REQON IT-SECURITY · Computest always on. · digital trust center. · Topsector Logistiek

INHOUD

HANDVATTEN CYBERSECURITY IN DE LOGISTIEKE KETEN

ACHTERGROND	3
OVERZICHT HANDVATTEN	7
01. BELEID	12
02. BEWUSTWORDING	20
03. KETENPARTNERS	26
04. TECHNIEK	31

TNO innovation for life

ACHTERGROND
ONDERZOEKSOPZET

- TNO, Transport en Logistiek Nederland (TLN), SmartPort, Air Cargo Netherlands (ACN), Cargonaut, REQON Security, Digital Trust Center (DTC) en Computest hebben een scan uitgevoerd om de cyber kwetsbaarheden binnen de logistieke keten in kaart brengen. Het onderzoek is mede gefinancierd uit de Topsector Logistiek en de toeslag voor Topconsortia voor Kennis en Innovatie (TKI's) van het ministerie van Economische Zaken en Klimaat.
- De doelstelling van het project is het verhogen van het bewustzijn van het belang van cybersecurity en het bieden van concrete handvatten om de beveiliging tegen cybercriminaliteit te verbeteren.
- De huidige status van cybersecurity in de logistieke keten is in kaart gebracht middels:
  - Een vragenlijst uitgezet door meerdere logistieke brancheorganisaties
  - Interviews met verschillende soorten logistieke bedrijven
  - Ethische hacks waarbij een ransomware-aanval is gesimuleerd zodat deelnemende bedrijven inzicht krijgen in de cyberveiligheid van hun IT
- De praktische handvatten in dit document komen voort uit de resultaten van de bovengenoemde onderdelen. De publicatie van de resultaten van het onderzoek naar de huidige status van cybersecurity in de logistieke sector is tegelijkertijd gepubliceerd met dit handvattendocument. Beide rapporten worden onder andere via de brancheverenigingen verspreid.

ACHTERGROND
METHODE

- De vragenlijst heeft uitgestaan van april t/m augustus 2019 en is door 242 mensen benaderd wat heeft geresulteerd in 127 (deels) ingevulde vragenlijsten. De vragenlijst was gericht aan CEO's, CISO's en (IT-)medewerkers van bedrijven in de logistieke sector die werken aan de verbetering van de cybersecurity binnen hun organisatie.
- In de periode van november 2019 tot en met mei 2020 hebben er bij acht logistieke bedrijven een interview en ethische hack plaatsgevonden. Een gevarieerde groep aan bedrijven heeft hier aan deelgenomen. Kenmerken:
  - Terminal, transportbedrijf, logistieke dienstverlener, softwarebedrijf, expediteur, intermediair, overslag
  - Vervoer via de weg, lucht en water
  - Variërend van 15 medewerkers tot 1500 medewerkers
- De handvatten in dit document kunnen van waarde zijn voor ieder bedrijf, ongeacht de grootte van het bedrijf en de mate waarin al aandacht wordt besteed aan een digitaal veilige inrichting. Zo kunnen bedrijven die al (pro)actief bezig zijn met cybersecurity de handvatten gebruiken ter bevestiging, maar ook om de volgende stappen te zetten in de digitale veiligheid van hun bedrijf. Anderzijds kunnen bedrijven die nog niet actief met het onderwerp bezig zijn de handvatten gebruiken om de eerste stappen te zetten op het gebied van cybersecurity.

ACHTERGROND

CYBERAANVAL (PETYA-VIRUS) BIJ APM TERMINALS - 2017

- In juni 2017 vond een grote cyberaanval plaats met als één van de grootste slachtoffers APM Terminals, een dochterbedrijf van Maersk. Twee grote containerterminals in de Rotterdamse haven kwamen stil te liggen en alle IT-systemen waren volledig onbruikbaar geworden.
- De impact was enorm: het duurde 10 dagen voordat APM haar eerste systemen weer actief had. Het duurde nog weken voordat de meeste systemen weer konden draaien en schepen gelost en geladen konden worden.
- De totale schade voor Maersk bedroeg $300 miljoen waarbij 2.200 applicaties, 49.000 computers en 3500 van de 6200 servers werden vernietigd.

> "We were basically average when it came to cybersecurity, like many companies. This is a wake-up call not just to become good, but to have cybersecurity as a competitive advantage."
>
> - Jim Hagemann Snabe, Raad van Bestuur Møller-Maersk

> "Company boards and audit committees need to understand that this stuff is real."
>
> - Adam Banks, Chief Technology and Information Officer Møller-Maersk

Bronnen:
https://www.infosecurity-magazine.com/interviews/infosec19-interview-banks-maersk-1/
https://info.nettitude.com/considerations-for-ship-owners-and-operators
https://www.computerweekly.com/news/252464773/NotPetya-offers-industry-wide-lessons-says-Maersks-tech-chief
https://www.computerweekly.com/news/450424559/NotPetya-attack-cost-up-to-300m-says-Maersk

ACHTERGROND
HANDVATTEN

- De logistiek digitaliseert snel, denk aan digitale document-uitwisseling, gebruik van online boekingsplatformen, het automatisch inschieten van orders, digitale planningen en afhandeling van transacties. Daarnaast laat de coronaperiode zien dat er steeds meer thuis gewerkt wordt. Deze manier van werken vraagt steeds meer van IT-systemen en beveiliging.
- Omdat er steeds meer gedigitaliseerd wordt en online plaatsvindt, verplaatst de criminaliteit zich ook naar de digitale wereld. Bovendien worden cybercriminelen steeds professioneler en gebruiken ze steeds geavanceerdere en verfijnde technieken.
- Doordat cyberincidenten regelmatig in het nieuws komen en mensen de dreiging ook in de privésfeer tegenkomen (denk aan phishing mails en Whatsapp-fraude), groeit het bewustzijn. Helaas vertaalt dit bewustzijn zich niet automatisch naar extra alertheid op de werkvloer, terwijl ook bedrijven een interessant doelwit zijn voor cybercriminelen.
- Het incident bij Maersk in 2017 heeft laten zien hoe groot de gevolgen van een cyberincident kunnen zijn voor de hele logistieke keten. Na het incident bij Maersk is door veel logistieke partijen geïnvesteerd in cybersecurity. Maar het momentum lijkt te verdwijnen waardoor bij veel bedrijven de alertheid weer is afgenomen.
- De handvatten in dit document zijn bedoeld om logistieke bedrijven best practices te bieden op het gebied van cybersecurity zodat bedrijven adequate maatregelen kunnen treffen en inzicht krijgen op welke vlakken de beveiliging nog verbeterd kan worden. Er worden concrete tips gegeven die bedrijven kunnen gebruiken om de cyberweerbaarheid te vergroten.

HANDVATTEN
IN VIER CATEGORIEËN

Klik op één van de onderstaande knoppen om naar de desbetreffende categorie te navigeren

BELEID

BEWUSTWORDING

KETENPARTNERS

TECHNIEK

BELEID

OVERZICHT HANDVATTEN

Hieronder staat een overzicht van alle handvatten op het gebied van beleid. Klik op één van de onderstaande blauwe knoppen om naar de desbetreffende handvat te navigeren.

	Kosten	Impact
Stel een cybersecurity verantwoordelijke aan	●●●	●●●●
Zet het onderwerp cybersecurity op de agenda van vergaderingen	●	●●●
Maak een cybercrisisplan en test het plan regelmatig	●	●●
Automatiseer het maken van back-ups	●	●●●
Zorg dat patches en updates tijdig worden uitgevoerd	●	●●●●
Leg de verantwoordelijkheden (met IT-leveranciers) rondom cybersecurity vast	●	●●●
Richt processen in rondom de in- en uitdiensttreding van personeel en automatiseer deze processen indien mogelijk	●	●

BEWUSTWORDING
OVERZICHT HANDVATTEN

Hieronder staat een overzicht van alle handvatten op het gebied van bewustwording. Klik op één van de onderstaande blauwe knoppen om naar de desbetreffende handvat te navigeren.

	Kosten	Impact
Onderken de bedrijfsrisico's	●	●●●●
Zorg dat het management handelt naar het cybersecuritybeleid	●	●●●
Maak cyberincidenten bespreekbaar en spreek verwachtingen uit	●	●●
Maak medewerkers alert en informeer regelmatig over cybersecurity en de nieuwe ontwikkelingen op dit gebied	●	●●●
Stel digitale gedragsregels op voor medewerkers	●	●●●
Leer uw medewerkers cyberaanvallen te herkennen en voer awareness tests uit	●●	●●●
Spreek elkaar aan op digitaal handelen	●	●●
Blijf op de hoogte van de laatste ontwikkelingen op het gebied van cybersecurity	●●	●●

KETENPARTNERS
OVERZICHT HANDVATTEN

Hieronder staat een overzicht van alle handvatten op het gebied van ketenpartners. Klik op één van de onderstaande blauwe knoppen om naar de desbetreffende handvat te navigeren.

	Kosten	Impact
Wees bewust van de positie van uw bedrijf in de markt en bescherm uw ‘kroonjuwelen’	● ○ ○ ○	● ● ● ○
Wees bewust van de positie van uw bedrijf in de keten en de afhankelijkheden in aan- en afvoerketens	● ○ ○ ○	● ● ○ ○
Communiceer open en transparant naar ketenpartners, zeker wanneer zich een cyberincident voordoet	● ○ ○ ○	● ● ○ ○
Neem deel aan congressen, seminars of webinars gericht op de keten om kennis over cybersecurity te vergaren, maar ook om ervaringen en ideeën over het onderwerp uit te wisselen met partners in de keten	● ● ○ ○	● ● ● ○
Sluit aan bij een cybersecurity samenwerkingsverband of CERT (in de sector)	● ● ○ ○	● ● ● ○
Maak afspraken met andere partijen over het delen van data	● ● ○ ○	● ● ● ○

TECHNIEK

OVERZICHT HANDVATTEN

Hieronder staat een overzicht van alle handvatten op het gebied van techniek. Klik op één van de onderstaande blauwe knoppen om naar de desbetreffende handvat te navigeren.

	Kosten	Impact
Maak gebruik van een sterk wachtwoordbeleid	●●○○	●●●○
Gebruik geen groepswachtwoorden	●○○○	●●●○
Maak gebruik van multi-factor authenticatie	●●●○	●●●●
Zorg dat het netwerk is onderverdeeld in verschillende segmenten	●●●●	●●●●
Maak gebruik van bekende cybersecurityprotocollen en standaarden	●●○○	●●●○
Geef gebruikers toegangsrechten op basis van de rol die de gebruiker heeft	●●●○	●●○○
Zorg dat er een overzicht bestaat van de IT-inrichting en houd deze up-to-date	●●○○	●●●○

BELEID
BOUW ROUTINES IN

BELEID

STEL EEN CYBERSECURITY VERANTWOORDELIJKE AAN

- Stel een cybersecurity verantwoordelijke aan
  - Er zijn bedrijven waarbij een fulltime Chief Information Security Officer (CISO) wordt aangesteld, maar cybersecurity kan ook als taak worden belegd bij een (IT-)medewerker. Vaak is de invulling afhankelijk van de bedrijfsgrootte en de bedrijfstak.
  - Zorg dat er uren beschikbaar zijn om de cybersecurity taken op te pakken.
  - Als IT is uitbesteed, ga er niet vanuit dat alles daarmee is geregeld. Zorg dat er duidelijke afspraken over verantwoordelijkheden worden gemaakt. Zorg daarnaast dat er ook iemand intern verantwoordelijk is.

Enkele voorbeeldtaken van de cybersecurity verantwoordelijke:

- Voldoen aan algemene cybersecurity richtlijnen en standaarden, zoals ISO 27001 en 27002.
- Bewustzijn creëren bij medewerkers.
- Procedures en gedragsregels vastleggen, bijvoorbeeld hoe een medewerker dient om te gaan met een phishing mail.
- Inventariseer alle apparaten binnen het netwerk en zorg dat deze up-to-date zijn.
- Regie voeren over gebruikersrechten, back-ups en patches.

Terug naar overzicht

BELEID

ZET CYBERSECURITY OP DE AGENDA

- Zet het onderwerp cybersecurity op de agenda van vergaderingen
  - Zorg dat er tijdens vergaderingen regelmatig aandacht wordt besteed aan cybersecurity. Doe dit niet reactief, maar proactief.

> "Cybersecurity komt bij ons alleen ter sprake als er een cyberincident heeft plaatsgevonden. Dan komen er vragen, maar meer niet."

Voorbeelden van wat besproken kan worden tijdens dit agendapunt:

- Rapporteren actuele situatie en lopende acties aan directie/management
- Welke maatregelen genomen moeten worden en wie hierin welke verantwoordelijkheid en taken heeft
- Cybersecurity roadmap: waar staan we en waar willen we naartoe
- Laatste ontwikkelingen in het cyberlandschap (specifiek in de logistieke keten)
- Awareness onder medewerkers

Terug naar overzicht

BELEID

MAAK EEN CYBERCRISISPLAN

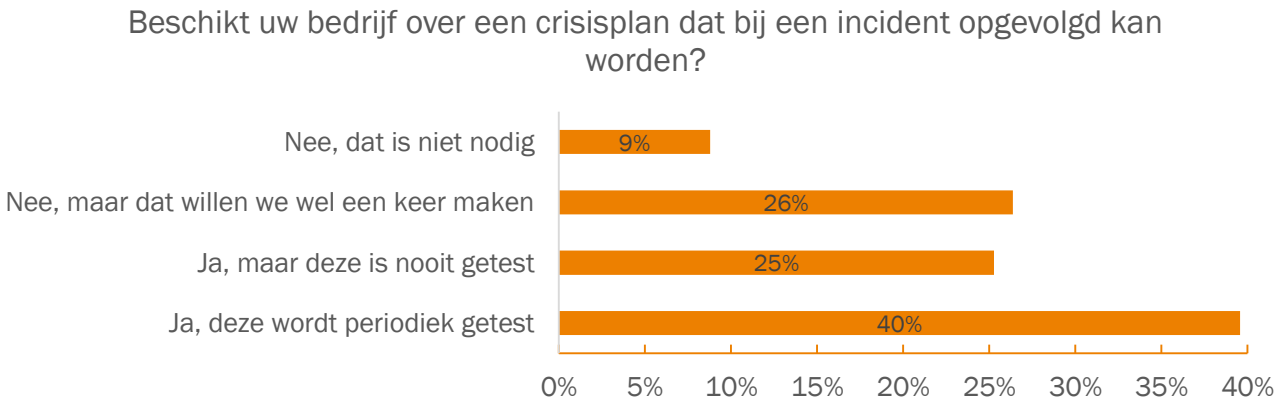
- **Maak een cybercrisisplan en test het plan regelmatig**

  Het cybercrisisplan bestaat bijvoorbeeld uit:

  - Risicoanalyse: wat is de potentiële schade als het bedrijf te maken krijgt met een cyberincident?
  - Wanneer en hoe vaak (onderdelen van) het cybercrisisplan getest moeten worden.
  - Draaiboeken wanneer er zich een cyberincident voordoet, zoals phishing, ransomware, CEO-fraude of DDoS-aanval.

Het Nationaal Crisisplan Digitaal, o.a. opgesteld door de Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV), helpt bij het opstellen van een crisisaanpak en draaiboeken voor uw eigen organisatie.

Ten tijde van de cyberaanval op de Universiteit van Maastricht eind 2019 waren cyberincidenten zoals ransomware niet opgenomen in de draaiboeken van de universiteit voor grote incidenten.



Terug naar overzicht

BELEID

MAAK BACK-UPS

- Automatiseer het maken van back-ups
  - Het maken van back-ups is van essentieel belang wanneer systemen en bestanden worden aangetast en moeten worden hersteld.
  - Door het maken van back-ups te automatiseren, kan het maken van back-ups niet worden vergeten.
  - Bepaal de retentie van de back-up, oftewel hoe ver je terug kan in de geschiedenis van de back-up, en de frequentie, hoe vaak de back-up uitgevoerd moet worden.
  - Bepaal wie er toegang mag krijgen tot de back-ups.
  - Richt de back-up in volgens de ‘3-2-1 methode’: maak minimaal 3 kopieën van de data, zet deze op 2 verschillende media waarvan 1 opgeslagen op een andere locatie. Zorg dat er ook back-ups los van het netwerk staan opgeslagen, zodat onaangetaste back-ups beschikbaar zijn mocht je bijvoorbeeld slachtoffer worden van ransomware.
  - Identificeer de hersteltijd en stel prioriteiten welke processen wanneer hersteld moeten worden.
  - Test periodiek een volledig herstel van het systeem via een back-up of draai een verificatietest.

Terug naar overzicht

BELEID

VOER PATCHES EN UPDATES TIJDIG UIT

- **Zorg dat patches en updates tijdig worden uitgevoerd**
  - Voor een goede beveiliging is het tijdig uitvoeren van software patches of updates van groot belang.
  - Zorg dat er een duidelijk overzicht is van welke IT-systemen gebruikt worden en wat de beschikbare en laatst uitgevoerde patches en updates zijn.
  - Zorg dat er een proces is voor het controleren of software up-to-date is. Het inregelen van automatische notificaties bij beschikbare updates kan hierbij helpen.
  - Installeer security updates zo snel mogelijk, of mitigeer impact wanneer er een kwetsbaarheid wordt gepubliceerd (voor het laatste is veelal specialistische kennis vereist). Zorg ervoor dat kritieke beveiligingsupdates vrijwel direct worden uitgevoerd om de continuïteit van het bedrijf te waarborgen. Houd bijvoorbeeld het NCSC in de gaten voor een overzicht van (kritieke) beveiligingsupdates.
  - Evalueer de status van het IT-landschap periodiek. Is er nieuwe IT die niet in het beleid aanwezig is (schaduw IT)? Zijn er machines die niet up-to-date zijn? Kan middels tooling of een security test technisch geverifieerd worden of er verouderde software aanwezig is?

Zes van de acht partijen die de ethische hack hebben ondergaan bleken nog kwetsbaar voor de zeer ernstige EternalBlue-exploit, waarvan al sinds april 2017 bekend is dat het gebruikt wordt voor cyberaanvallen.

Terug naar overzicht

BELEID

LEG VERANTWOORDELIJKHEDEN VAST

- **Leg de verantwoordelijkheden (met IT-leveranciers) rondom cybersecurity vast**
  - Het is belangrijk dat verschillende verantwoordelijkheden rondom IT-systemen worden gedefinieerd en vastgelegd. Deze afspraken zijn van belang als je als bedrijf een externe IT-leverancier hebt, maar ook wanneer IT binnenshuis geregeld is, is het van belang om vast te leggen wie waar verantwoordelijk voor is.
  - Waar continuïteit van de bedrijfssystemen al onderdeel is van bestaande afspraken met een externe IT-leverancier, is het ook aan te raden om expliciete afspraken en verantwoordelijkheden vast te leggen omtrent beveiliging en cybersecurity.

Bekijk ook de checklist van het Digital Trust Center voor het maken van afspraken met een IT-leverancier.

Terug naar overzicht

BELEID

RICHT PROCESSEN RONDOM IN- EN UITDIENSTTREDING IN

- **Richt processen in rondom de in- en uitdiensttreding van personeel en automatiseer deze processen indien mogelijk**
  - Neem cyberveilig handelen op als onderdeel van de indiensttreding. De indiensttreding is tevens het geschikte moment om een nieuwe medewerker bekend te maken met de digitale manier van werken, zoals de omgang met bedrijfsdata, het handelen bij digitale dreigingen, wachtwoordenbeleid en werken op afstand.
  - Door de processen rondom in- en uitdiensttreding in te richten en te automatiseren kunnen de risico's worden ingeperkt, bijvoorbeeld door accounts van vertrekkende medewerkers direct te deactiveren en rechten tot het bedrijfsnetwerk en bedrijfsdata te ontnemen.

Belangrijke handelingen bij de in- en uitdiensttreding zijn:

- Het toekennen, maar ook verwijderen van accounts en gebruikersrechten.
- Afgeven en terugnemen van hardware zoals laptop, mobiel en token.
- Afgeven en terugnemen van software zoals licenties op programma's.

Het Digital Trust Center heeft een template ontwikkeld dat kan worden gebruikt bij het opstellen van een in- en uitdiensttredingsbeleid.

Terug naar overzicht

BEWUSTWORDING
CREËER BEWUSTZIJN

BEWUSTWORDING
ONDERKEN DE BEDRIJFSRISICO'S

Onderken de bedrijfsrisico's

Een aantal redenen waarom cybersecurity serieus moet worden genomen:

- Meer dan 20% van de bedrijven gaf aan dat tijdelijk hun bedrijfsproces niet gefunctioneerd heeft vanwege een cyberincident. Daarnaast gaven veel bedrijven aan dat er regelmatig pogingen tot cyberfraude zijn. Dit inzicht onderstreept het belang van cyberweerbaarheid.
- De digitale risico's zijn onverminderd groot en de digitale dreiging is permanent. Cybercrime wordt steeds professioneler en geavanceerder. Doordat bedrijven het geëiste losgeld blijven betalen, blijft deze vorm van criminaliteit actueel.[1]
- Vergroting van digitale weerbaarheid blijft het belangrijkste instrument om digitale risico's in voldoende mate te kunnen beheersen. Zowel de kans dat cyberincidenten zich voordoen, als de impact ervan, kunnen zo worden verkleind.[1]

Terug naar overzicht

1) Cybersecuritybeeld Nederland 2020, Nationaal Coördinator Terrorismebestrijding en Veiligheid (NCTV)

BEWUSTWORDING

HET MANAGEMENT MOET HET VOORTOUW NEMEN

- **Zorg dat het management handelt naar het cybersecuritybeleid**
  - Het is van belang dat bestuurders de noodzaak van cybersecurity inzien en aandacht besteden aan het onderwerp door hier actief beleid voor in te richten. Het inrichten van een dergelijk beleid zal ook de awareness bij de rest van de organisatie en medewerkers beïnvloeden.
  - Kijk bij het cybersecuritybeleid niet alleen naar de dagelijkse praktijk en de korte termijn, maar ook naar de (middel)lange termijn, bijvoorbeeld door een roadmap op te stellen waarin de toekomstplannen m.b.t. gebruikte technologieën of software beschreven staat.
  - Bestuurders hebben een voorbeeldfunctie. Het cybersecure handelen van bestuurders zal het gedrag van de andere medewerkers beïnvloeden. Zorg dat het management zich aan de cybersecurityregels houdt.

- **Maak cyberincidenten bespreekbaar en spreek verwachtingen uit**
  - Zorg dat medewerkers bij iemand terecht kunnen indien er zich een cyberincident voordoet of heeft voorgedaan. Denk hierbij aan een intern meldpunt.
  - Zet cybersecurity op de agenda bij teamoverleggen.
  - Spreek de verwachtingen die u van medewerkers heeft ten aanzien van cybersecurity uit.

Terug naar overzicht

BEWUSTWORDING

CREËER AWARENESS BIJ MEDEWERKERS (1/2)

- **Maak medewerkers alert en informeer regelmatig over cybersecurity en nieuwe ontwikkelingen op dit gebied**
  - Houd uw medewerkers alert. Hierdoor blijft het onderwerp op de radar bij medewerkers en zal men bewuster aandacht besteden aan het veilig uitvoeren van digitale handelingen.
  - Het onder de aandacht brengen van het onderwerp kan middels een nieuwsbrief, nieuwsbericht, periodieke training of voorlichting, gerichte campagne, awareness test, of agendapunt bij een vergadering. Herhaling van dezelfde boodschap kan hierbij zeker geen kwaad.
- **Stel digitale gedragsregels op voor medewerkers**

  Waar veel bedrijven al gedragsregels opstellen voor werkplekken, is het ook verstandig om regels op te stellen die medewerkers moeten hanteren wanneer men digitaal werkt. Deze digitale gedragsregels bestaan vaak uit een aantal basisregels waarvan verwacht wordt dat medewerkers zich hieraan houden. Voorbeelden van regels zijn:
  - Gebruik sterke wachtwoorden (zie NIST-richtlijnen op pagina 32).
  - Deel nooit je inloggegevens en wachtwoorden, ook niet met je collega's.
  - Wees alert op verdachte e-mails en telefoontjes.
  - Gebruik niet zomaar openbare WiFi-netwerken.
  - Hanteer een clean desk/screen beleid en vergrendel apparaten wanneer de werkplek wordt verlaten.

Terug naar overzicht

BEWUSTWORDING

CREËER AWARENESS BIJ MEDEWERKERS (2/2)

- Leer uw medewerkers cyberaanvallen te herkennen en voer awareness tests uit
  - Een goede manier om inzicht te krijgen in het digitale gedrag van medewerkers en om medewerkers bewust te maken van hun handelen, is het uitvoeren van een test. Denk hierbij aan het verspreiden van een opgezette phishing mail binnen de organisatie om te testen hoe vaak er op een link wordt geklikt, of er wachtwoorden worden afgegeven of een schadelijke bijlage wordt geopend. De uitkomsten van de test kunnen gebruikt worden om medewerkers aan te spreken en om de beveiliging verder op orde te brengen. Bovendien kunnen de uitkomsten naderhand worden gecommuniceerd zodat de hele organisatie ervan kan leren.

- Spreek elkaar aan op digitaal handelen
  - Een open en transparante sfeer op de werkvloer zorgt ervoor dat medewerkers elkaar eerder durven aan te spreken op het digitaal veilig handelen.

Terug naar overzicht

BEWUSTWORDING

BLIJF OP DE HOOGTE VAN DE LAATSTE ONTWIKKELINGEN

- **Blijf op de hoogte van de laatste ontwikkelingen op het gebied van cybersecurity.** Belangrijke informatiebronnen:
  - Het Digital Trust Center (DTC) helpt met veilig digitaal ondernemen en verschaft informatie en advies om Nederlandse bedrijven weerbaarder te maken tegen cyberdriegingen. Daarnaast ontwikkelt het tools zoals de Basisscan Cyberweerbaarheid, stimuleert het samenwerking tussen bedrijven, en biedt het binnenkort een online gesloten omgeving, de Digital Trust Community, waarbinnen actuele en relevante informatie kan worden uitgewisseld. Ook heeft het DTC een wegwijzer ontwikkeld die bedrijven helpt een passend initiatief te vinden waar men met hun specifieke cybersecurity-hulpvraag terecht kan.
  - Het Nationaal Cyber Security Centrum (NCSC) is het expertisecentrum voor cybersecurity in Nederland en verstrekt informatie om de digitale weerbaarheid van de Nederlandse samenleving te vergroten.
  - Alert Online stimuleert meer bewustwording van cybersecurity. Alert Online organiseert bijeenkomsten en publiceert jaarlijks het Cybersecurity Bewustzijnsonderzoek.
  - FERM is onderdeel van het Port Cyber Security Programma van de Rotterdamse haven. Dit programma heeft als doel om de samenwerking tussen bedrijven in de Rotterdamse haven te stimuleren en bewustzijn met betrekking tot cyberrisico's te verhogen. Wat FERM is voor de Rotterdamse haven, is CYSSEC (Cyber Synergie Schiphol Ecosysteem) voor het gehele Schiphol ecosysteem. Beide organisaties bieden nieuws, informatie, bijeenkomsten, scans en tests.
  - Brancheverenigingen en samenwerkingsverbanden in de logistiek, zoals Transport en Logistiek Nederland (TLN), SmartPort en ACN, bieden ook informatie over cybersecurity.

Terug naar overzicht

KETENPARTNERS
BETREK DE KETEN EN DOE HET SAMEN

KETENPARTNERS

POSITIE VAN HET BEDRIJF IN DE MARKT EN KETEN

- **Wees bewust van de positie van uw bedrijf in de markt en bescherm uw ‘kroonjuwelen’**
  - Eén van de drijfveren van cybercriminelen voor het uitvoeren van een cyberaanval of hack is economisch gewin. Maar een bedrijf kan ook een interessant doelwit zijn vanwege de producten of diensten die het levert. Een overslagterminal of een transportbedrijf kan bijvoorbeeld een interessant doelwit zijn wanneer criminelen invloed willen uitoefenen op het verdere vervoer van specifieke illegale ladingen. Deze producten en/of diensten die de waarde van het bedrijf kenmerken zijn de zogenoemde kroonjuwelen.
  - Om in te schatten welke risico’s uw bedrijf loopt vanwege de producten en/of diensten die het aanbiedt, kunt u in kaart brengen welke kroonjuwelen uw bedrijf interessant maken voor cybercriminelen. Het kan hierbij gaan over digitale, maar ook fysieke kroonjuwelen. Zijn deze kroonjuwelen momenteel beveiligd? Is de huidige beveiliging voldoende of moet de beveiliging verbeterd worden?
  - Het Digital Trust Center heeft een stappenplan ontwikkeld om de kroonjuwelen van een bedrijf in kaart te brengen.
- **Wees bewust van de positie van uw bedrijf in de keten en de afhankelijkheden in aan- en afvoerketens**
  - Een cyberincident op uw bedrijf kan ook gevolgen hebben voor bedrijven waarmee u in verbinding staat. Om uw bedrijf goed te wapenen tegen cyberincidenten is het van belang dat uw bedrijf zich realiseert waar in de keten het zich bevindt. Bovendien is het van belang om te weten welke partijen afhankelijk zijn van uw bedrijf, maar ook van welke bedrijven uw bedrijf zelf afhankelijk is. Deze analyse kan inzichten opleveren waarmee de cyberveiligheid verbeterd kan worden. Bijvoorbeeld, is uw bedrijf niet te afhankelijk van een toeleverancier? Is het niet verstandiger om meerdere toeleveranciers te hebben om zo het risico voor uw bedrijf bij uitval van één van deze toeleveranciers te beperken?

Terug naar overzicht

KETENPARTNERS

BESPREEK CYBERVEILIGHEID MET KETENPARTNERS (1/2)

- **Communiceer open en transparant naar ketenpartners, zeker wanneer zich een cyberincident voordoet**
  - Onderhoud contact met naastgelegen bedrijven in de keten over cybersecurity gerelateerde onderwerpen.
  - Indien er een cyberincident bij uw bedrijf plaatsvindt, kunnen ook uw klanten en ketenpartners hier hinder van ondervinden. Het is daarom van belang dat u hier snel, open en transparant met hen over communiceert zodat andere bedrijven op de hoogte zijn en eventueel hulp kunnen bieden om het incident te verhelpen. Het is voor beide partijen van belang dat het incident snel en zonder schade wordt verholpen.

- **Neem deel aan congressen, seminars of webinars gericht op de keten om kennis over cybersecurity te vergaren, maar ook om ervaringen en ideeën over het onderwerp uit te wisselen met partners in de keten**

  Voorbeelden van events:
  - Port Cyber Café van FERM voor bedrijven uit de Rotterdamse haven
  - CYSSEC bijeenkomsten voor bedrijven uit het Schiphol ecosysteem
  - Ga voor andere actuele cybersecurity initiatieven naar de wegwijzer gepubliceerd door het Digital Trust Center

Terug naar overzicht

KETENPARTNERS

BESPREEK CYBERVEILIGHEID MET KETENPARTNERS (2/2)

- Sluit aan bij een cybersecurity samenwerkingsverband of CERT (in de sector)
  - Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals dat snel kan handelen bij digitale beveiligingsincidenten. Een CERT geeft preventieadvies, maar kan ook ondersteunen bij het oplossen van beveiligingsincidenten om de schade te beperken en een snel herstel van de bedrijfsvoering te realiseren. Bedrijven kunnen ook bij een CERT terecht voor informatie of beantwoording van cybersecuritygerelateerde vragen.
  - Een voorbeeld is het FERM programma van de Rotterdamse haven. Dit programma heeft als doel om de samenwerking tussen bedrijven in de Rotterdamse haven te stimuleren en bewustzijn met betrekking tot cyberrisico's te verhogen. Ook is er sinds 2018 een Haven Cybermeldpunt waar bedrijven in de Rotterdamse haven melding kunnen maken van grootschalige IT-verstoringen.
  - Wat FERM is voor de Rotterdamse haven, is CYSSEC (Cyber Synergie Schiphol Ecosysteem) voor het gehele Schiphol ecosysteem. Hier kunnen o.a. afhandelaren, luchtvrachtexpediteurs, -verladers en -carriers zich bij aansluiten.
  - Het Digital Trust Center houdt een actueel overzicht bij van alle sectorale en regionale samenwerkingsverbanden op het gebied van cybersecurity.

Terug naar overzicht

KETENPARTNERS
DELEN VAN DATA

- **Maak afspraken met andere partijen over het delen van data**
  - Maak afspraken met de partijen waarmee data wordt gedeeld en leg deze afspraken vast. In deze afspraken wordt vastgelegd welke data gedeeld wordt, wie de data kan gebruiken, waar de data voor gebruikt wordt, wat de bewaartermijn van de data is, etc.
  - Deel alleen data wanneer dit noodzakelijk is en deel niet meer data dan nodig.
  - Zorg dat de techniek voor het uitwisselen van de data goed beveiligd is.
  - Een van de gegevens die wordt uitgewisseld zijn de pincodes voor het ophalen van een vracht. Tijdens de interviews is gebleken dat er vaak onzorgvuldig met de pincodes wordt omgesprongen en het gebruik hiervan fraudegevoelig is. Ga na welke voorwaarden er gelden voor het delen van deze pincodes en zorg dat de pincode op een veilige manier in handen komt van de juiste persoon/partij.

SUTC helpt logistieke bedrijven om veilig, efficiënt en papierloos digitaal data te delen. De logistieke sector gebruikt bijvoorbeeld iShare voor het delen van logistieke data. iShare is een afsprakenstelsel of een set van afspraken waarmee partijen elkaar toegang verstrekken tot hun data en drempelloos data delen. iShare regelt de identificatie, autorisatie en authenticatie. Ook (air)port community systemen als Cargonaut en Portbase faciliteren een veilige manier van data-uitwisseling tussen bedrijven onderling en met overheidsinstanties.

Terug naar overzicht

TECHNIEK
ZORG VOOR EEN VEILIGE INFRASTRUCTUUR

TECHNIEK
STERK WACHTWOORDBELEID

- **Maak gebruik van een sterk wachtwoordbeleid**
  - Een sterk wachtwoord voldoet aan de NIST 800-63 (National Institute of Standards and Technology) wachtwoordrichtlijnen: *"Easy to remember but hard to guess".* Wachtwoorden opgesteld volgens de NIST-richtlijnen zijn moeilijk te kraken, zelfs met moderne brute force methoden. Enkele van de NIST aanbevelingen:
    - Het gekozen wachtwoord bestaat uit minimaal 8 karakters.
    - Het gekozen wachtwoord komt niet voor in de lijst met zwakke wachtwoorden (blacklist). Deze lijst bevat eerder gecompromitteerde wachtwoorden, veel voorkomende wachtwoorden zoals 'Password1', contextspecifieke woorden zoals de naam van de gebruiker, en repeterende of opvolgende karakters zoals 'aaaaaaa' en 'qwerty1234'.
  - Gebruik geen wachtwoorden, maar 'wachtzinnen'. Zinnen zijn lang, makkelijk te onthouden, maar lastiger te kraken.
  - Stel als bedrijf wachtwoordmanagers beschikbaar aan werknemers. Dit stimuleert het gebruik van moeilijke en verschillende wachtwoorden, terwijl de werknemers zelf maar één belangrijk wachtwoord hoeven te onthouden.

Wil je testen hoe sterk jouw wachtwoord is? Probeer het uit met de wachtwoordkraaktest van Veiliginternetten.

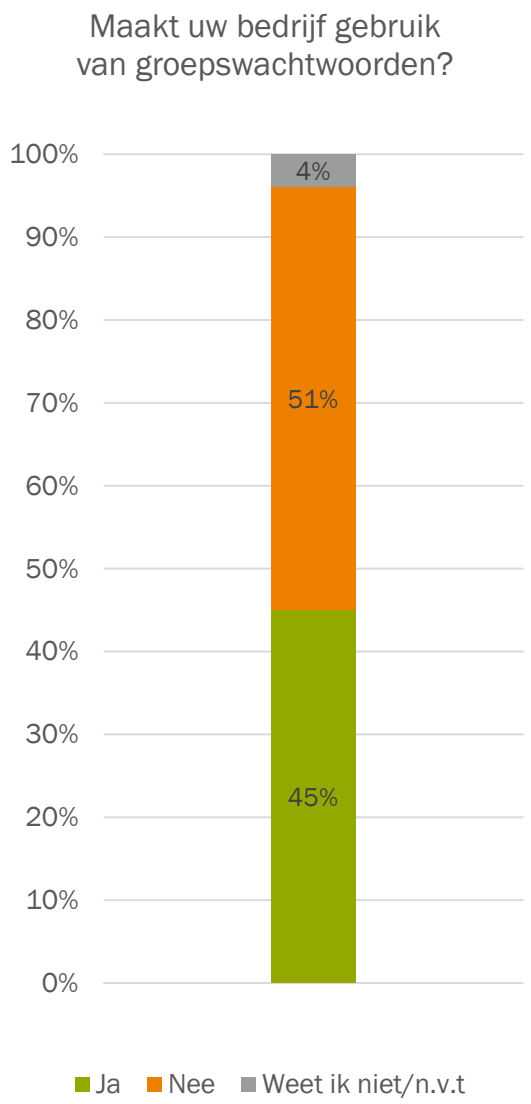
Terug naar overzicht

TECHNIEK

VOORKOM GROEPSWACHTWOORDEN

- Gebruik geen groepswachtwoorden
  - Zorg dat elke gebruiker zijn eigen sterke wachtwoord heeft om toegang te krijgen tot de systemen.
  - Zorg ervoor dat individuele wachtwoorden niet gedeeld worden met andere medewerkers en groepswachtwoorden worden.
  - Richt het systeem zo in dat bij afwezigheid van een medewerker de inkomende mail doorgezet kan worden naar de mailbox van een collega. Op deze manier kunnen lopende zaken afgehandeld worden zonder het delen van wachtwoorden.

Bij een groot aantal van de geïnterviewde partijen worden wachtwoorden regelmatig gedeeld onder medewerkers om zo toegang te krijgen tot bijvoorbeeld mail bij afwezigheid van een collega. Dit zorgt ervoor dat makkelijkere wachtwoorden worden gekozen en dat individuele wachtwoorden als groepswachtwoorden worden gebruikt.



Terug naar overzicht

TECHNIEK

MAAK GEBRUIK VAN MULTI-FACTOR AUTHENTICATIE

- Maak gebruik van multi-factor authenticatie
  - Bij multi-factor authenticatie krijgt de gebruiker pas toegang tot een applicatie of systeem na het succesvol doorlopen van minimaal twee stappen. Bij iedere stap wordt bewijs aangeleverd, zoals:
    1. Kennis: iets wat alleen de gebruiker weet, bijvoorbeeld een pincode.
    2. Bezit: iets wat alleen de gebruiker bezit, bijvoorbeeld een bankpas.
    3. Inherentie: iets wat alleen de gebruiker is, bijvoorbeeld een vingerafdruk.
  - Bij tweestapsverificatie (two-factor authenticatie) vindt de authenticatie plaats middels twee stappen. Het kan bijvoorbeeld gebruikt worden door een wachtwoord te combineren met een token of een one-time-password die gegenereerd wordt met de telefoon. Ook het gebruik van een zogenoemde Authenticator-app op de telefoon is in opkomst.
  - Het is wenselijk om minimaal de essentiële systemen en het werken op afstand te beveiligen met multi-factor authenticatie.
  - NIST heeft ook richtlijnen opgesteld voor het veilig inrichten van multi-factor authenticatie.

Terug naar overzicht

TECHNIEK

MAAK GEBRUIK VAN NETWERKSEGMENTATIE

- **Zorg dat het netwerk is onderverdeeld in verschillende segmenten**
  - Netwerksegmentatie is het onderverdelen van het netwerk in verschillende segmenten om te voorkomen dat een virus, bijvoorbeeld ransomware, zich vrij kan rond bewegen binnen het gehele netwerk.

> Bij 5 van de 8 bedrijven betrokken bij de ethische hack was er geen adequate netwerksegmentatie. Een aanvaller die het interne netwerk binnen weet te komen, kan dan gelijk het volledige netwerk aanvallen.

  - Kantoorautomatisering (KA), oftewel de software en hardware in en rond het kantoor, moet gescheiden zijn en op een ander netwerk zitten dan alle andere IT, OT en IoT. Dit omdat hackers vaak binnendringen via je KA-omgeving.
  - Een belangrijk onderdeel is de segmentatie tussen het interne netwerk en het internet. Idealiter worden er zo min mogelijk diensten ontsloten naar het internet.
  - Sla back-ups ook gesegmenteerd op. Gebruik hiervoor de ‘3-2-1 methode’: maak minimaal 3 kopieën van de data, zet deze op 2 verschillende media waarvan 1 opgeslagen op een andere locatie.

Terug naar overzicht

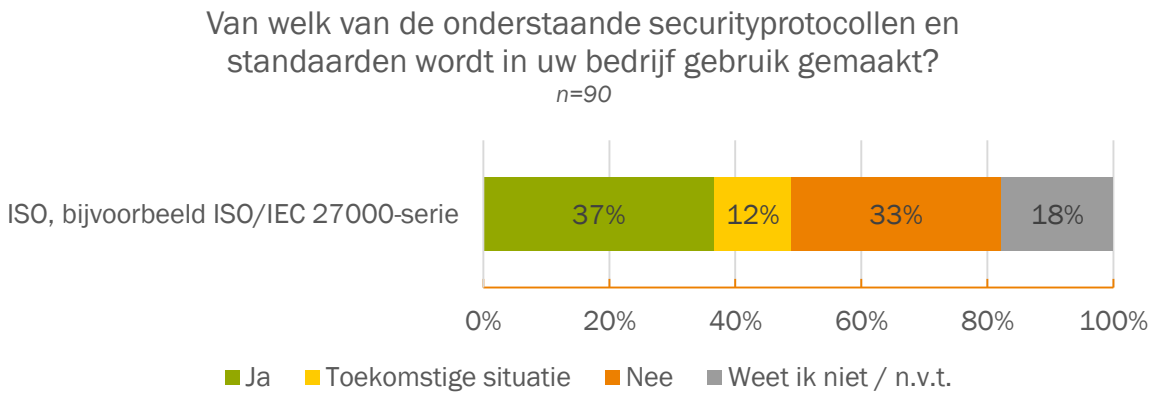
TECHNIEK

MAAK GEBRUIK VAN BEKENDE SECURITYPROTOCOLLEN EN STANDAARDEN

- **Maak gebruik van bekende cybersecurityprotocollen en standaarden**
  - Door gebruik te maken van protocollen en standaarden voor cybersecurity en informatiebeveiliging kan je als bedrijf via een gestructureerde aanpak snel tot een minimaal beveiligingsniveau komen.
  - Juist omdat cybersecurity niet de kern is van uw logistieke bedrijfsvoering is het van belang aandacht te besteden aan deze protocollen en ze toe te passen.
  - Naast protocollen gericht op de IT, zijn er ook specifieke protocollen gericht op de Operationele Technologie (OT). Standaarden zoals IEC 62443 en NIST SP 800-82 laten zien welke maatregelen er specifiek voor de OT genomen kunnen worden in vergelijking tot de IT.

Enkele cybersecurityprotocollen en standaarden:

- ISO 27001/27002
- Algemene Verordening Gegevensbescherming (AVG)
- NIST Cybersecurity Framework (NIST CSF)



Terug naar overzicht

TECHNIEK

KEN TOEGANGSRECHTEN TOE O.B.V. ROLLEN

- **Geef gebruikers toegangsrechten op basis van de rol die de gebruiker heeft**
  - In plaats van aan elke gebruiker individueel zijn rechten toe te wijzen is het efficiënter om te werken met rechten op basis van verschillende rollen, zoals netwerkbeheerder, planning, HR, administratie, etc.
  - De rol(len) die een gebruiker krijgt toegewezen gaat gepaard met specifieke toegangsrechten, zoals de toegang tot een bepaald netwerk, (gevoelige) data, of software. Hierbij geldt het principe van minimale bevoegdheid. Bij elke rol hoort slechts de toegang tot het deel van het netwerk wat nodig is om het werk wat bij de rol hoort efficiënt uit te kunnen voeren.
  - Door deze aanpak, genaamd role-based access control (RBAC), goed uit te voeren kan de impact van ransomware beter worden geanalyseerd en beperkt, omdat van een iedere gebruiker bekend is welke rechten het wel en niet heeft. Ook helpt RBAC om beter zicht te houden op tijdelijke uitzonderingen die gelden voor gebruikers en om deze weer terug te draaien zodra de uitzondering niet meer nodig is.
  - Het is belangrijk om de toegekende rollen actueel te houden en minimaal eens per jaar te toetsen. Dit voorkomt dat werknemers onterecht rechten behouden en dat er meer rollen dan medewerkers ontstaan, omdat er tijdelijke rollen worden aangemaakt en niet worden teruggezet.
  - Het Digital Trust Center biedt met een rechtenmatrix een praktisch handvat waarmee bepaald kan worden waartoe iemand binnen de organisatie toegang heeft.

Terug naar overzicht

TECHNIEK

HOUD EEN INVENTARIS BIJ VAN DE TOTALE IT-INRICHTING

- Zorg dat er een overzicht bestaat van de IT-inrichting en houd deze up-to-date
  - Inventariseer alle apparaten binnen het netwerk. Controleer regelmatig op updates en installeer deze zo spoedig mogelijk. Wanneer een apparaat niet geüpdatet kan worden om functionele redenen, is het aan te raden om deze af te zonderen zodat de impact van een incident via dit apparaat geen impact heeft op de rest van het netwerk.
  - Wanneer er nieuwe apparatuur wordt aangeschaft, dient deze opgenomen te worden in de inventaris. Vervolgens dient het standaard wachtwoord te worden gewijzigd in een sterk en uniek wachtwoord.
  - Evalueer de permissies van de interne fileshares periodiek. Dit om te voorkomen dat uitzonderingen die gemaakt zijn niet meer worden teruggedraaid.

Bij het ransomware-incident bij de Universiteit van Maastricht eind 2019 was er geen goed overzicht van de IT-infrastructuur. Dit heeft er voor gezorgd dat de impact en diepgeworteldheid van het virus moeilijk in kaart te brengen was.
Na het incident heeft de Universiteit van Maastricht de gehele centrale en decentrale IT-infrastructuur in kaart gebracht.

Terug naar overzicht