Expertgroep

Secure E-commerce

Ketenveiligheid in digital commerce

shopping tomorrow

Takeaways

1. In tegenstelling tot andere branches, ontbreekt er in de retailbranche een orgaan om informatie over cyber-dreigingen uit te wisselen.
2. Informatie-uitwisseling moet afgestemd zijn op de cyber-volwassenheid van een organisatie, en moet tijdig en relevant zijn.
3. Het hanteren van de juiste technische standaarden voor data-uitwisseling tussen systemen, inclusief e-mail, wordt vanuit de wetgeving ondersteund.

Host

Voorzitter

Ketenveiligheid in digital commerce

Consumenten kopen steeds meer online. Door de sterk toegenomen digitalisering is er een toenemende verschuiving van fraude en (on)veiligheid van fysieke retail naar digital commerce. Als we kijken naar de keten (van inkoop tot bezorgen bij de klant), dan worden er op veel punten gegevens uitgewisseld waardoor er kwetsbaarheden ontstaan. Er zijn verschillende onderwerpen op het gebied van veiligheid binnen e-commerce. Ons onderzoek gaat in op twee thema's waarbij het begrip 'keten' centraal staat, met als doel ketenpartners te voorzien van aandachtspunten en checklists om de keten weerbaarder te maken. We richten ons hierbij op middelgrote tot grote bedrijven. In het eerste hoofdstuk gaan we in op (cyber)gegevensuitwisseling in de keten, zodat ondernemers beter en tijdig op de hoogte zijn van actuele dreigingen. Het tweede hoofdstuk beschrijft een andere vorm van gegevensuitwisseling, namelijk de technische gegevensuitwisseling tussen de systemen in de e-commerceketen.

1. Cyberinformatie-uitwisseling in de keten

In opdracht van de Cyber Security Raad heeft Herna Verhagen, CEO van PostNL, in haar rapport 'De economische en maatschappelijke noodzaak voor meer Cyber Security: Nederland Digitaal Droge Voeten'[1] gepleit voor verbetering van het delen van informatie op het gebied van cybersecurity. Aanvullend concludeert de Cyber Security Raad in zijn advies #2 van 2017[2] dat de huidige informatie-uitwisseling hoofdzakelijk gericht is op de Rijksoverheid en organisaties in de vitale infrastructuur. De bedrijven die niet zijn aangemerkt als vitale infrastructuur, ontvangen tot op heden geen informatie van de overheid over kwetsbaarheden en dreigingen, en hebben daardoor bewust of onbewust een informatietekort. Ook zijn zij veelal onvoldoende of niet aangesloten op een andere vaste structuur waarbinnen cybersecurity-gerelateerde informatie wordt gedeeld. Een landelijk dekkend stelsel van informatieknooppunten waar bedrijven terechtkunnen voor informatie ontbreekt.

Deze studie richt zich op informatiedeling tussen middelgrote en grote e-commercebedrijven met een jaaromzet hoger dan € 300.000,-. Binnen deze groep onderscheiden we drie ervaringsniveaus van informatiedeling, waarbij ieder niveau zijn specifieke vragen naar informatie en handelingsperspectief kent:

1 VERHAGEN, 2016 (NEDERLAND DIGITAAL DROGE VOETEN (WWW.CYBERSECURITYRAAD.NL/BINARIES/CYBERSECURITYADVIESHERNAVERHAGEN_TCM56-122110.PDF))

2 CYBER SECURITY RAAD – ADVIES #2 (WWW.CYBERSECURITYRAAD.NL/BINARIES/CSR_ADVIES_INFORMATIEUITWISSELING_NED_TCM107-314535.PDF)

1. **Basic:** Ik wil een community voor het delen van informatie starten. Waar te beginnen? Do's en don'ts.
2. **Advanced:** Ik ben al betrokken bij het delen van informatie. Wat kan ik leren om te verbeteren?
3. **Expert:** Ik ben al heel lang betrokken bij het delen van cybersecurity-gerelateerde informatie. Hoe kan ik de gemeenschap voor het delen van informatie aanpassen om het delen van deze informatie nog efficiënter en effectiever te maken?

Het op vrijwillige basis delen van informatie tussen bedrijven ontstaat, zeker als het gevoelige informatie betreft, niet vanzelf. Er moeten positieve incentives zijn om hiermee te starten. Het Europese agentschap voor netwerk- en informatiebeveiliging, ENISA, heeft hier onderzoek naar gedaan. Uit interviews komt naar voren dat een belangrijke prikkel om met informatiedeling te starten en/of deze te intensiveren onder andere kostenbesparing is.[3] De kwaliteit, waarde, tijdigheid en het gebruik van de gedeelde informatie spelen ook een cruciale rol.

De behoefte aan het soort informatie over cybersecurity is sterk afhankelijk van de *cybermaturity* van de organisatie. Bedrijven die niet of minder volwassen zijn op het gebied van cybersecurity hebben veelal behoefte aan meer generieke informatie, zoals handreikingen, best practices en stappenplannen. Bedrijven die cybermature zijn, hebben juist behoefte aan hoogwaardige informatie over dreigingen en kwetsbaarheden. Vaak hangt de cybervolwassenheid samen met de grootte van het bedrijf, maar dit is niet altijd het geval. Informatiedeling (vanuit de overheid of door bedrijven onderling) moet passen bij de doelgroep.

1.1 Welke vormen van informatiedeling zijn er?

Het delen van gevoelige informatie is geen eenvoudig onderwerp. Informatiedeling over incidenten en kwetsbaarheden raakt het strategisch, tactisch, operationeel en technisch niveau van organisaties, en omvat alle fasen van de *cyber incident response*-cyclus (preventie, preparatie, incidentrespons, herstel, nazorg/follow-up). Daarmee overstijgt het de grens van het publieke en private domein en heeft het een dilemma in zich. Het gaat immers veelal over gevoelige informatie die schadelijk kan zijn voor een organisatie enerzijds, terwijl anderzijds de informatie zeer nuttig en bruikbaar kan zijn voor anderen.[4]

Voor bedrijven binnen de vitale infrastructuur, zoals energieleveranciers en telecombedrijven, zijn ISAC's (*Information Sharing and Analysis Center*s) ingericht om cybersecurity-gerelateerde informatie te delen. Voor het overige bedrijfsleven zijn er al wel een aantal initiatieven, al dan niet in oprichting. Een niet-limitatief overzicht is opgenomen in de tabel op de volgende pagina. Deze informatieknooppunten vormen echter geen landelijk dekkend stelsel voor alle bedrijven. Voor de e-commerceketen is er bijvoorbeeld geen sectoraal informatieknooppunt.

3 LUIJF & KERNKAMPF, 2015, SHARING CYBER SECURITY INFORMATION (WWW.PUBLICATIONS.TNO.NL/PUBLICATION/34616508/OLYFG9/LUIIJF-2015-SHARING.PDF)

4 HUISTRA & KRABBENDAM-HERSMAN, 2017, TNO VERKENNING CYBERSECURITY INFORMATIEDELING BINNEN DE TOPSECTOREN, (WWW.RIJKSOVERHEID.NL/BINARIES/RIJKSOVERHEID/DOCUMENTEN/RAPPORTEN/2017/03/07/VERKENNING-CYBERSECURITY-INFORMATIE-DELING-BINNEN-DE-TOPSECTOREN/CYBERSECURITY+INFORMATIEDELING+BINNEN+DE+TOPSECTOREN.PDF)

Vitale bedrijven/ sectoren	Niet-vitale bedrijven/sectoren
ISAC's	• Niet-vitale ISAC (zoals Legal ISAC en Connect2Trust) • Digital Trust Center (verbonden aan Nationaal Cyber Security Center, maar is niet alleen gericht op kritieke infrastructuur) en diverse daaraan verbonden initiatieven voor kennisdeling en awareness, de DTC-website en (in 2019) het DTC Platform, maar ook andere websites zoals alertonline.nl en veiliginternetten.nl;
• Sectorale en regionale initiatieven zoals Brainport, Z-CERT, Cybersecurity Center Maakindustrie, FERM, CYSSEC en NIDV Cyberweerbaarheid.	

Overzicht van organisaties en structuren voor delen van cybersecurity-informatie

De in de tabel genoemde initiatieven ontvangen (op termijn) direct van de overheid dreigingsinformatie en handelingsperspectief. Dit is geborgd in de nieuwe Wet beveiliging netwerk- en informatiesystemen (Wbni) die op 9 november 2018 van kracht is geworden. De voorwaarde om direct informatie van de overheid te verkrijgen, is dat een initiatief valt in een van de volgende drie categorieën:

- Organisaties die objectief kenbaar tot taak hebben om andere organisaties of het publiek daarover te informeren. Hieronder vallen bijvoorbeeld de ISAC's en Brainport.
- *Computer Security Incident Response Teams* (CSIRT's). Hieronder valt bijvoorbeeld de voor de zorg opgerichte Z-CERT.
- Andere computercrisisteams, zoals aangewezen bij regeling van het Ministerie van Justitie & Veiligheid of behorend tot een categorie die bij die regeling aangewezen is.

1.2 Welke kanalen zijn er voor het delen van informatie?

De kanalen voor het delen van informatie zijn vaak verbonden aan de reeds genoemde initiatieven en incentives. Deze kunnen worden samengevoegd in drie vormen van informatiedeling:

1. **Een-op-een-informatiedeling:** In deze situatie wordt informatie slechts tussen twee (of hoogstens enkele) bedrijven gedeeld. Hiervoor kunnen digitale middelen worden gebruikt, waaronder gesloten omgevingen, e-mail met encryptie en persoonlijke gesprekken, zoals tijdens of naast een ISAC.
2. **Een-op-N-informatiedeling:** In deze situatie wordt informatie van één instantie met zoveel mogelijk partijen gedeeld. Voorbeelden hiervan zijn het delen van informatie via websites (digitaltrustcenter.nl, security.nl) of via een app (CyberAlerts) waarbij de verzender (de één) zich richt op zoveel mogelijk ontvangers (de N). Een andere variant is een bedrijf dat (in plaats van een-op-een) hulp vraagt aan veel meer mensen, zoals binnen een sector. Hierbij gaat het vaak om de impact van bijvoorbeeld nieuwe wetgeving (zoals de AVG) of de implementatie van nieuwe technologie
3. **N-op-N-informatiedeling:** In deze situatie ontstaan online platformen waarin hele groepen met elkaar tot uitwisseling van informatie komen. Het Digital Trust Center lanceert hiervoor in 2019 het Digital Trust Platform, maar ook groepen via social media (WhatsApp, Facebook) en platformen van brancheorganisaties kunnen hiervoor gebruikt worden.

1.3 Conclusies en aanbevelingen voor e-commercebedrijven

Grote e-commerce-organisaties als PostNL en Jumbo – met een groot netwerk van partners en leveranciers – begrijpen hoe belangrijk het is om de organisatie tijdig te voorzien van de juiste informatie met betrekking tot cyberdreigingen en handelingsperspectieven van aanvallers. Een tijdige informatievoorziening maakt het immers onder meer mogelijk om preventieve maatregelen te nemen, waardoor de impact van een aanval wordt geminderd, óf om ten tijde van een incident correctieve maatregelen te nemen op de meest efficiënte en effectieve manier. Dit alles om de impact op de bedrijfsprocessen én de bedrijfsdoelstellingen zo minimaal mogelijk te laten zijn. Kortom, om te zorgen dat de business-as-usual kan doorgaan.

Vanwege de complexe omgeving en grote verscheidenheid aan ketenpartners onderstrepen we nogmaals het belang van het uitwisselen van informatie rondom cyberdreigingen en handelingsperspectieven. Naast de economische incentive is het maatschappelijk belang een reden dat grote e-commercebedrijven deelnemen aan verschillende initiatieven om informatie-uitwisseling mogelijk te maken of te stimuleren.

Uit ons onderzoek is gebleken dat er weliswaar inmiddels verschillende fora, werkgroepen en platformen zijn waarbinnen dreigingsinformatie wordt gedeeld, maar dat er geen specifiek platform is waar informatie over cyberdreigingen en handelsperspectief wordt gedeeld voor bedrijven uit de e-commerceketen. Deze bedrijven worden daardoor niet optimaal voorzien en op de hoogte gebracht van de meest actuele dreigingsinformatie rond bijvoorbeeld bestaande en nieuwe aanvalsvectoren die daadwerkelijk een bedreiging vormen voor de e-commerceketen.

Het oprichten van een e-commerce-ISAC, zoals in de Verenigde Staten al bestaat (**r-cisc.org**), kan zeker voor grote e-commerce-organisaties van grote waarde zijn. Binnen zo'n sectorale ISAC kan in een vertrouwde omgeving informatie worden gedeeld over incidenten, kwetsbaarheden en dreigingen gericht op de sector en de keten. Daarnaast is het zinvol om cross-sectoraal informatie te delen.

Tegelijkertijd blijkt uit ons onderzoek dat de belangen voor informatiedeling per bedrijf kunnen verschillen, met als resultaat een andere informatiebehoefte en handelingsperspectief dan bij grote e-commercebedrijven die hun informatie kunnen vinden in een ISAC. Zo vereist het analyseren en correleren van informatie een deskundigheidsniveau dat binnen veel bedrijven gewoonweg niet beschikbaar is. De middelgrote en kleinere e-commercebedrijven moeten op een andere manier van informatie op maat worden voorzien.

De ervaring leert dat een brancheverenigingen hierin een centrale rol kan spelen, omdat zij al haar leden kent en bij deze leden een vertrouwenspositie heeft. Wij zien dan ook een belangrijke rol voor Thuiswinkel.org als informatiehub voor alle leden, groot en klein. Wij doen daarom de aanbeveling aan Thuiswinkel.org om binnen het DTC-platform een specifieke ruimte met informatie voor de retailsector in te richten. Hierbij kan Thuiswinkel.org wellicht inspiratie opdoen bij vergelijkbare samenwerkingsverbanden die al zijn gestart, zoals Brainport, FERM en CYSSEC, maar ook bij de cyberweerbaarheidsprojecten Limburg en Noord-Nederland. Voor grote e-commercebedrijven die cybermature zijn, zien wij ook een rol binnen de sector; zij zouden bijvoorbeeld masterclasses Cyber Security kunnen aanbieden.

2. Secure interfacing in de e-commerceketen

In het vorige hoofdstuk onderzochten we de mogelijkheden van cyberinformatie-uitwisseling tussen de actoren in de e-commerceketen. In dit hoofdstuk gaan we in op de technische gegevensuitwisseling tussen de systemen in de keten en hoe dit veilig uitgevoerd kan worden.

Het is als ondernemer van belang om goede afspraken te maken op het gebied van beveiliging. Zoals met zoveel bedrijfsrisico's is voorkomen beter dan genezen. Het inrichten van het juiste niveau van beveiliging is niet alleen het hooghouden van de reputatie van je organisatie en het vermijden van schade door digitale aanvallen, maar ook het voldoen aan wet- en regelgeving. Organisaties besteden veel zaken uit die met bescherming van gegevens en beheer van netwerk- en informatiesystemen te maken hebben. De onderneming blijft echter zelf nog steeds aansprakelijk voor de correcte verwerking, waardoor het weglekken of misbruik van gegevens en systemen een bedrijfsrisico blijft. Afspraken maken met – en toezicht houden op – leveranciers van specialistische diensten zorgt ervoor dat de afhandeling van betalingen, de gegevensopslag en het beschermen van eventuele bedrijfsgeheimen betrouwbaar en volledig gebeurt.

2.1 Checklist voor partners, afnemers en leveranciers

Steeds meer essentiële delen van de bedrijfsvoering worden buiten de fysieke omgeving van de organisatie geleverd. Hierbij kun je denken aan webapplicaties en dataopslag via cloudleveranciers. Om jou en je onderneming een handvat te bieden, hebben we in samenwerking met experts op het gebied van e-commerce en beveiliging een checklist ontwikkeld. Het doel van deze checklist is om inzage te verkrijgen in de beveiliging van je bedrijfsgegevens en -processen wanneer je deze via interfacing deelt met derden. Laat de checklist invullen door je partners, afnemers en leveranciers en bepaal vervolgens welke punten voor jou van belang zijn.

In de paragrafen 2.2 t/m 2.4 worden eerst de achtergronden van de checklist toegelicht en de checklist zelf is in paragraaf 2.5 opgenomen.

2.2 Gegevensopslag

E-commercebedrijven slaan vaak veel klant-, bestel- en betaalinformatie op. Maar ook de informatie van samenwerkingen, medewerkers en leveranciers wordt vastgelegd, zoals inkoop- en salarisinformatie. Het is niet de bedoeling dat deze gevoelige informatie inzichtelijk is voor derden. Een aantal goede beveiligingsmaatregelen zijn bijvoorbeeld:

- Informatie enkel toegankelijk maken voor een beperkte groep gebruikers.
- Een register bijhouden van wie wanneer welke informatie heeft ingezien.
- Informatie versleuteld opslaan in een bestand of database.
- Bepaalde gevoelige informatie, zoals betaalinformatie of medische gegevens, bewust niet opslaan of automatisch verwijderen nadat de dienst geleverd is.

Wanneer je gegevens van je onderneming of klanten verstuurt aan leveranciers of derde partijen, dan kun je vragen naar de beveiligingsmaatregelen die deze partij heeft genomen.

2.3 Veranderende wet- en regelgeving

Het beschermen van informatiesystemen is niet vrijblijvend. Net als er in een kantoorpand brandvoorschriften gelden, zijn er voor gegevensverwerking vereisten om te voldoen aan een beveiligingsniveau opgelegd vanuit wet- en regelgeving. We benadrukken dat de aansprakelijkheid bij de eigenaar van de gegevens ligt, en niet bij de partij die in het beheer of de verwerking voorziet.

Daardoor kunnen ook overtredingen van derden een ongewenst effect hebben in de vorm van boetes of reputatieschade.

Hierbij spelen ondernemerschap en het inschatten van risico's een rol. De globale strekking van de wetgeving[5] ten aanzien van persoonsgegevens is als volgt: *De verantwoordelijke legt, rekening houdend met de stand der techniek, uitvoeringskosten, en omvang van risico's, passende technische en organisatorische maatregelen ten uitvoer om (persoons)gegevens te beveiligen.* Er zijn dus geen vaste eisen als "Iedereen moet een antivirusproduct op alle systemen hebben." Voor beveiligingskaders is de insteek dat de organisatie zelf prioriteiten kan bepalen via het 'pas toe of leg uit'-principe, waarmee op basis van een doordachte risicoanalyse een maatregel wel of niet wordt uitgevoerd.

Een gecalculeerd risico kan bijvoorbeeld zijn dat iedereen bedrijfscomputers, laptops en mobiele apparatuur voor privédoeleinden mag gebruiken om het nieuwe werken te faciliteren. Dit onder de voorwaarde dat medewerkers een handtekening zetten onder een 'acceptabel gebruik'-richtlijn, waarin staat welke acties wel en niet zijn toegestaan. Bewustwording en training worden soms als overbodig beschouwd, maar ze helpen medewerkers in te zien hoe makkelijk informatie te achterhalen is en wat de gevolgen daarvan zijn. Periodieke sessies, misschien zelfs verplicht, en het delen van best practices helpen bij het ontwikkelen van een betere securitycultuur.

2.4 Veilige communicatie tussen leverancier en je bedrijf

Wanneer gegevens worden uitgewisseld met een leverancier, dan zijn hiervoor diverse typen van koppelingen mogelijk. Sommige leveranciers bieden een standaardportaal of API-achtige oplossing, andere leveranciers werken via e-mailberichten.

Het is belangrijk dat de communicatie tussen de leverancier en je bedrijf veilig verloopt. Dit wil zeggen, een kwaadwillende die in staat is om de communicatie onderweg te onderscheppen, mag niet in staat zijn om de gecommuniceerde gegevens in te zien. In de volgende paragrafen worden een aantal van de meest voorkomende interfacemogelijkheden besproken en geven we per mogelijkheid aan wat de aandachtspunten zijn.

API of webservice

Via een API of webservice van de leverancier kunnen gegevens worden verstuurd. De meeste API's zijn gebaseerd op SOAP (dat XML-berichten gebruikt) of REST (dat vaak XML- of JSON-berichten gebruikt). Doorgaans wordt door de leverancier een gebruikersaccount verstrekt waarmee je je bij de webdienst kunt authentiseren.

Om te voorkomen dat aanvallers mee kunnen kijken in je communicatiestromen, is het noodzakelijk een veilige (SSL/TLS-)verbinding te gebruiken. Voor web-based API's kun je een veilige verbinding herkennen aan het gebruik van https:// in de URL (in plaats van http://).

FTP-, SMB- of andere bestandsuitwisselingsdiensten

Door in te loggen op een bestandsuitwisselingdienst van je leverancier is het mogelijk om direct bestanden te uploaden en downloaden. Over het algemeen is er een gebruikersaccount vereist om een verbinding op te zetten.

5 WWW.PRIVACY-REGULATION.EU/NL/ARTIKEL-32-BEVEILIGING-VAN-DE-VERWERKING-EU-AVG.HTM

Een aantal van deze bestandsuitwisselingsdiensten maken standaard geen gebruik van een veilige verbinding. Bestandsuitwisselingsdiensten als SFTP, FTPS of SSH maken wel gebruik van een veilige, versleutelde verbinding.

Als dit bijvoorbeeld een website is die je kunt bezoeken met je browser of een mobiele app, let dan op 'https' in de URL en op het slotje in de adresbalk.

Het is vaak niet noodzakelijk om een bestandsuitwisselingsdienst toegankelijk te maken voor het gehele internet. Het is technisch heel goed mogelijk om toegang tot de dienst te beperken tot bijvoorbeeld een aantal specifieke IP-adressen. Dit verkleint de kans dat een aanvaller het systeem kan aanvallen.

E-mail
Communiceer je gegevens met een leverancier via e-mail? Wees je er dan van bewust dat e-mail per definitie een onveilig medium is. Zo wordt er standaard geen gebruikgemaakt van een veilige verbinding om e-mailberichten te versturen en ontvangen. Ook is het vrij eenvoudig om e-mailberichten te versturen uit naam van een andere persoon of een ander domein.

Om e-mail toch veilig te kunnen gebruiken, kun je een aantal technische en organisatorische maatregelen doorvoeren. Op organisatieniveau kun je bijvoorbeeld medewerkers trainen om nep-e-mailberichten te herkennen. Dit verkleint de kans dat medewerkers onbedoeld kwaadaardige software binnenhalen of gegevens met kwaadwillenden delen (phishing).

Tevens kunnen een aantal technische maatregelen worden doorgevoerd om het versturen en ontvangen van e-mailberichten veiliger te maken. Controleer of je e-mailsysteem de juiste e-mailstandaarden gebruikt, zoals DMARC, DKIM, SPF en (start)TLS. Je kunt dit controleren op diverse sites, waaronder **www.internet.nl.** Ga met de testresultaten naar je beheerder en vraag de juiste standaarden te implementeren.

2.5 Checklist

Met de achtergrondinformatie uit de vorige paragrafen kun je via onderstaande checklist je partners, afnemers en leveranciers uitvragen, bewustmaken en indien nodig aanspreken.

Gegevensopslag, wet- en regelgeving
Je deelt gegevens van je onderneming en/of klanten met een andere partij:

- Worden gegevens van mijn onderneming en/of mijn klanten gescheiden opgeslagen van gegevens van andere klanten?
- Wordt er gebruikgemaakt van versleuteling bij de opslag van gegevens van mijn onderneming en/of mijn klanten?
- Hoelang worden gegevens van mijn onderneming en/of mijn klanten bewaard?
- Hoe worden gegevens van mijn onderneming en/of mijn klanten door de leverancier gebruikt?
- Voldoet de partij aan de AVG-richtlijnen bij het opslaan van persoonsgegevens?
- Voldoet de partij nog aan andere privacy- en security-gerelateerde richtlijnen?
- Worden systemen van de partij regelmatig bijgewerkt met de nieuwste softwarepatches en -updates?

Je hebt zelf systemen waarbij je gegevens verwerkt:

- Worden er periodiek kwetsbaarhedenscans uitgevoerd op systemen die direct toegankelijk zijn via internet?
- Wordt het bewustzijn van medewerkers gestimuleerd door bijvoorbeeld awareness-trainingen?
- Wordt er gebruikgemaakt van monitoringoplossingen die bijvoorbeeld toegangslogs op een centrale plek bewaren en deze doorzoekbaar maken?

Veilige communicatie tussen leverancier en bedrijf

Je gebruikt een API of webservicekoppeling met een andere partij:

- Is een gebruikersaccount of API-key vereist voor het gebruik van de API? Zo ja, is dit account voorzien van een wachtwoord of key van minimaal twaalf tekens?
- Wordt er voor alle communicatiestromen gebruikgemaakt van een veilige verbinding (SSL/TLS)?

Je gebruikt een bestandsuitwisselingsdienst van een andere partij, zoals FTP, SMB- of SSH:

- Is een gebruikersaccount vereist voor het gebruik van de bestandsuitwisselingsdienst? Zo ja, is dit account voorzien van een wachtwoord van minimaal twaalf tekens?
- Wordt er gebruikgemaakt van een veilige verbinding (SSL/TLS)? SFTP-, FTPS- en SSH-diensten maken hier standaard gebruik van. Het is dus aan te raden om een van deze diensten te gebruiken.
- Is de bestandsuitwisselingsdienst beperkt toegankelijk gemaakt?

Je gebruikt een klant-, leveranciers- of cloudportaal van een andere partij:

- Is een gebruikersaccount vereist voor het gebruik van de bestandsuitwisselingsdienst? Zo ja, is dit account voorzien van een wachtwoord van minimaal twaalf tekens?
- Wordt er gebruikgemaakt van een veilige verbinding (SSL/TLS)?

Je gebruikt voornamelijk e-mail als medium om gegevens naar een andere partij te sturen:

- Wordt er gebruikgemaakt van een veilige verbinding (SSL/TLS) voor het ophalen en versturen van e-mailberichten?
- Bieden je e-mailsystemen voldoende bescherming tegen phishing?

HOSTS

Gerrie de Jonge
CIO Parcels & Logistics
PostNL Pakketten Benelux BV

Gunther Cleijn
Cyber Security Officer
PostNL Pakketten Benelux BV

VOORZITTER

Roland van Kortenhof
Manager Operations
Thuiswinkel.org

Leden expertgroep

Dennis Pieterse
Senior security advisor
T-Systems Nederland B.V.

Diederik Perk
Threat Intelligence Advisor
Fox-IT

Hans Minten
Master Security Analist
wehkamp

Michel Teuwen
Senior Information Security Consultant
Jumbo Groep Holding B.V.

Nick Pinto
Teamleider Fraude
wehkamp

Nicole Mallens
Senior beleidssecretaris
VNO-NCW & MKB-Nederland

Thomas Stols
Cybersecurity specialist
Computest

Raymond van den Hoek
IT Security Manager
bol.com

Aan deze bluepaper werkte ook mee:

Raymond Bierens
PhD Researcher
T.U. Delft