CSR Cyber Security Raad

IEDER BEDRIJF HEEFT DIGITALE ZORGPLICHTEN

EEN HANDREIKING VOOR BEDRIJVEN OP HET GEBIED VAN CYBERSECURITY

1. INLEIDING
PAGINA 4

1. INLEIDING

Informatie- en communicatietechnologie ('ICT') speelt een steeds grotere rol in onze maatschappij. Zij biedt economische mogelijkheden voor uw bedrijf, maar creëert ook nieuwe risico's. Een gebrekkige digitale veiligheid heeft grote gevolgen.

Een gebrek in uw cybersecurity – digitale veiligheid – kan ertoe leiden dat bedrijfsgeheimen en persoonsgegevens door een hack of menselijke fout op straat komen te liggen. Grote storingen kunnen zelfs tot gevolg hebben dat de business continuity van uw bedrijf in gevaar komt. Het bestuur van uw bedrijf is verantwoordelijk voor cybersecurity. Binnen het bestuur moet duidelijk zijn wie hierbij het voortouw neemt. Het is daarom noodzakelijk om cybersecurity op de agenda van het bestuur en de raad van commissarissen te plaatsen.
U kunt hierover meer informatie vinden in de door de Cyber Security Raad eerder uitgegeven 'Cyber security guide for boardroom members'. Bij kleinere bedrijven ligt de verantwoordelijkheid bij de directeur.

In 2014 leidde een datalek bij Target - een warenhuis in onder andere Canada en de Verenigde Staten - tot de diefstal van 40 miljoen debit- en creditkaartnummers. De gegevens werden gestolen door middel van op de kassasystemen geïnstalleerde malware. In de nasleep van dit incident werd de CEO ontslagen.

In 2013 bleek dat de RFID-chip (radio-frequency identification) in de sleutels van bepaalde automerken waarmee deze op afstand te openen zijn, te kunnen worden gehackt. Hierdoor konden hackers deze auto's zonder sleutel openen. In de periode daarna zijn veel auto-inbraken geweest.

Wat is cybersecurity?

‘Cybersecurity’ heeft drie aspecten:

1. **‘Beschikbaarheid’: uw ICT is beschikbaar en gebruikers hebben toegang tot het systeem.**

   - Uw ICT kan niet buiten werking worden gesteld met een Distributed Denial of Service-aanval (DDoS).
   - Regelmatige back-ups zorgen ervoor dat de business continuity niet in gevaar komt als een bedrijf slachtoffer is van ‘ransomware’ of ‘cryptoware’, waarbij hackers bedrijfsinformatie versleutelen en alleen weer ontsleutelen tegen betaling van geld.
   - De beschikbaarheid van uw ICT kan worden bedreigd door kwaadwillende software, ‘virussen’ of ‘malware’. Uw bedrijf neemt maatregelen om ‘besmetting’ door deze software te voorkomen.

2. **‘Integriteit’: de door u verwerkte gegevens zijn volledig en juist. De processen waarmee gegevens worden verwerkt, zijn juist en controleerbaar.**

   - De opgeslagen gegevens kloppen. Zij kunnen niet worden gewist of gewijzigd door een onbevoegde. Als de gegevens toch worden veranderd, kan een back-up deze gegevens vervangen.

3. **‘Vertrouwelijkheid’: alleen geautoriseerde gebruikers hebben toegang tot uw ICT en de gegevens.**

   - Onbevoegden kunnen niet, via internet of ter plaatse, toegang krijgen tot uw ICT. De beveiliging kan niet door middel van hacking of een ‘remote access tool’ worden omzeild.
   - De toegang is ten minste beveiligd door middel van een wachtwoord en bij voorkeur met een ‘tweefactorauthenticatie’. Om geld op te nemen bij een pinautomaat, zijn bijvoorbeeld een bankpas (‘iets dat de gebruiker bezit’, factor 1) en een pincode (‘iets dat de gebruiker weet’, factor 2) vereist.
   - Uw werknemers gaan niet in op ‘phishing-emails’. Zij geven geen wachtwoorden, persoonsgegevens of andere vertrouwelijke informatie aan onbevoegden die hier onder valse voorwendselen om vragen.
   - Criminelen krijgen geen toegang tot vertrouwelijke informatie door stiekem op een computerscherm mee te kijken (‘visueel hacken’).

Cybersecurity kan in gevaar komen door ‘beveiligingsincidenten’. De zorgplichten op het gebied van cybersecurity zijn erop gericht om het risico op deze incidenten te verkleinen en, als het toch mis gaat, de gevolgen van de incidenten te beperken.

Beveiligingsincidenten zijn bijvoorbeeld:

- Een werknemer verliest een laptop of usb-stick.
- Een hacker dringt het intranet van het bedrijf binnen.
- Malware zorgt ervoor dat uw ICT niet goed werkt.
- Een onbevoegd persoon verkrijgt een wachtwoord waarmee hij toegang heeft tot persoonsgegevens.
- Het elektronische slot van een auto wordt ontgrendeld zonder de sleutel.
- Een brand of stroomstoring in een datacentrum zorgt ervoor dat de gegevens tijdelijk niet beschikbaar zijn.

Verantwoordelijk voor andermans veiligheid

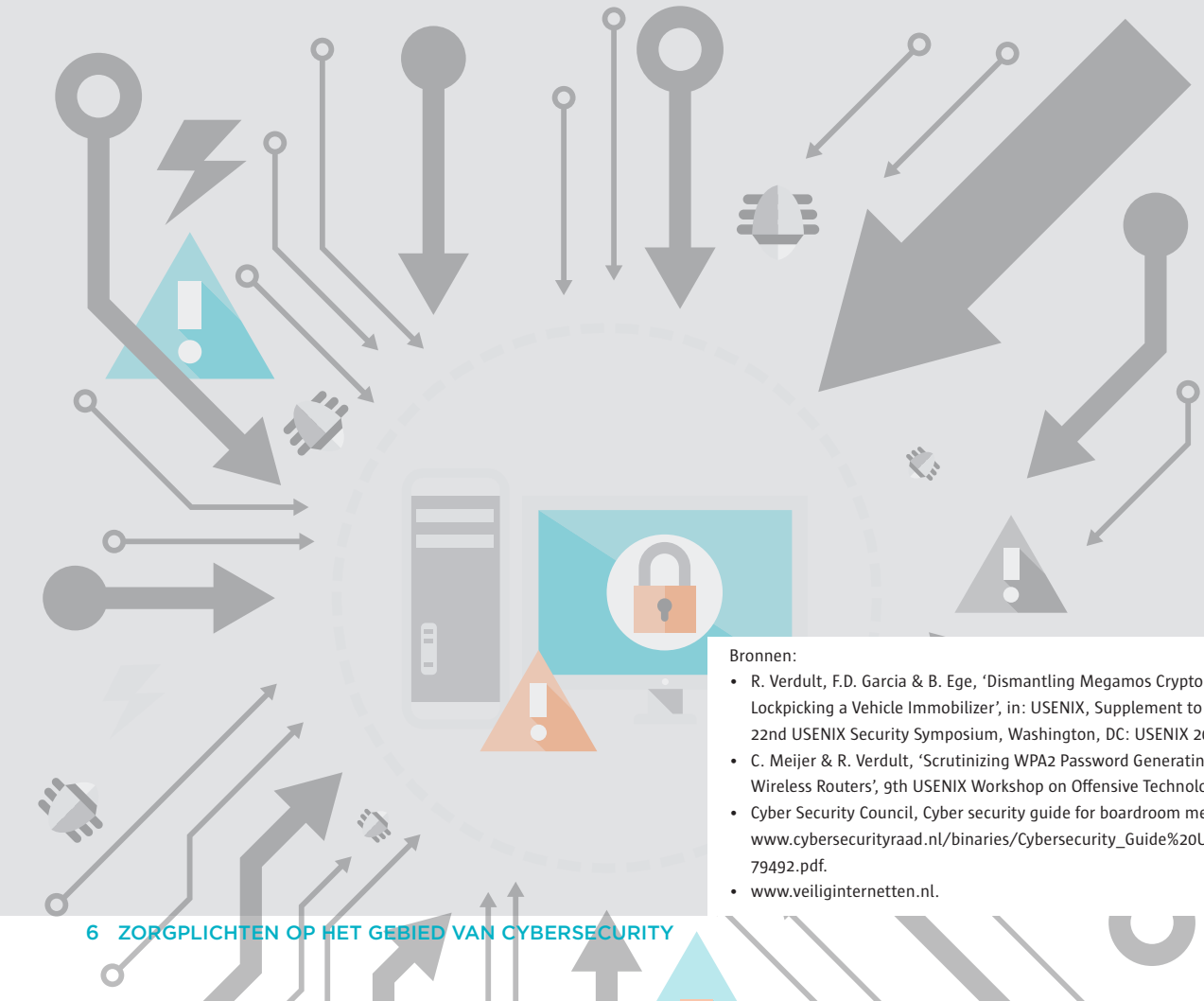
Een beveiligingsincident tast de bedrijfsvoering en de reputatie van uw bedrijf aan. Uw bedrijf maakt vaak deel uit van een keten. Uw bedrijfsvoering kan worden verstoord door een beveiligingsincident bij een van uw leveranciers, opdrachtnemers of doorverkopers. Andersom kan hun bedrijfsvoering ook afhankelijk zijn van uw cybersecurity.
Uw bedrijf heeft de plicht om – tot op bepaalde hoogte – rekening te houden met de belangen van anderen. U moet daarom onder andere zorgen voor een goede beveiliging van uw ICT en zorgen dat zij is afgestemd met de andere partijen in de keten. Een schending van deze 'zorgplichten' kan leiden tot aansprakelijkheid.

Doel van deze handreiking

Deze handreiking geeft een overzicht van de belangrijkste juridische zorgplichten op het gebied van cybersecurity en geeft de belangrijkste handvatten om deze plichten in te vullen. De handreiking is beknopt, op hoofdlijnen en niet sectorspecifiek. De handreiking behandelt bijvoorbeeld niet de specifieke zorgplichten van bedrijven die onder een bijzondere regulering vallen, zoals energiebedrijven, telecombedrijven, banken, zorginstellingen, providers vanluchtvaartdata en andere bedrijven in de 'vitale sectoren'.

U kunt de handreiking gebruiken als oriëntatie- en controlemiddel. Het is nadrukkelijk geen vervanging voor professioneel advies. In voorkomende gevallen doet u er goed aan om een gespecialiseerde jurist of beveiligingsspecialist in te schakelen en uw meldplicht te vervullen. Voor praktische tips over veilig internetgebruik kunt u terecht op www.veiliginternetten.nl.

De CSR nodigt brancheorganisatie uit om deze handreiking specifiek uit te werken voor hun leden.



Bronnen:

- R. Verdult, F.D. Garcia & B. Ege, 'Dismantling Megamos Crypto: Wirelessly Lockpicking a Vehicle Immobilizer', in: USENIX, Supplement to the Proceedings of the 22nd USENIX Security Symposium, Washington, DC: USENIX 2013.
- C. Meijer & R. Verdult, 'Scrutinizing WPA2 Password Generating Algorithms in Wireless Routers', 9th USENIX Workshop on Offensive Technologies 2015.
- Cyber Security Council, Cyber security guide for boardroom members, 2015. www.cybersecurityraad.nl/binaries/Cybersecurity_Guide%20UK_vdef_tcm56-79492.pdf.
- www.veiliginternetten.nl.

2. HEEFT MIJN BEDRIJF ZORGPLICHTEN OP HET GEBIED VAN CYBERSECURITY?

Ieder bedrijf dat gebruik maakt van ICT, heeft zorgplichten op het gebied van cybersecurity. Dit geldt dus ook als ICT slechts een ondersteunende rol speelt in uw bedrijf.

Ook als u 'niets bijzonders doet' met computers en deze 'alleen maar' gebruikt voor uw bedrijfsvoering, heeft u toch een zorgplicht om uw systemen te beveiligen. Het volgende voorbeeld maakt dat duidelijk.

Zorgplichten in de praktijk

Een distributiecentrum is gespecialiseerd in de opslag, verpakking en distributie van tijdschriften. Het krijgt deze tijdschriften van de uitgever en levert ze af bij detaillisten of bezorgers. De directeur is van mening dat hij zich geen zorgen hoeft te maken over cybersecurity, aangezien het bedrijf niets bijzonders met computers doet. De directeur zit ernaast. Het bedrijf heeft verschillende medewerkers in dienst, en verwerkt de 'persoonsgegevens' van deze medewerkers. Bovendien heeft het, om de tijdschriften te verpakken, een lijst van de namen en adressen van de abonnees (Hoofdstuk 3). Het bedrijf maakt daarnaast gebruik van computers om overzicht te houden over de inkomende, uitgaande en opgeslagen tijdschriften. Een hack zou ertoe kunnen leiden dat het bedrijf het overzicht kwijt raakt, en hierdoor te laat is met het afleveren van de tijdschriften waardoor aansprakelijkheden ontstaan (Hoofdstuk 4). Een hack kan er bovendien toe leiden dat persoonsgegevens worden ontvreemd, wat aanleiding kan zijn voor een melding bij de Autoriteit Persoonsgegevens.

De zorgplichten kunnen op verschillende manieren ontstaan:
1. Uw bedrijf verwerkt persoonsgegevens met behulp van ICT (Hoofdstuk 3).
2. Uw bedrijf maakt gebruik van ICT in de bedrijfsvoering (Hoofdstuk 4).
3. Uw bedrijf ontwikkelt, produceert of levert producten of diensten waarvan een ICT-component deel uitmaakt (Hoofdstuk 5).

Strenge zorgplichten voor de consument

Uw bedrijf heeft zowel zorgplichten ten opzichte van andere bedrijven, maar ook ten opzichte van ‘consumenten’. Deze zorgplichten zijn in grote lijnen dezelfde. Wel zijn de plichten ten opzichte van consumenten over het algemeen strenger. Bovendien heeft uw bedrijf in dat geval minder vrijheid om in een contract af te spreken waar het op het gebied van cybersecurity wel en niet toe verplicht is en om aansprakelijkheden uit te sluiten. Deze mogelijkheden zijn ruimer als u zaken doet met een ander bedrijf.

De producent van zelfrijdende auto’s weet dat er een risico bestaat dat de sensors van de auto in bepaalde gevallen niet werken. Het is daarom noodzakelijk dat de bestuurder blijft opletten. De producent contracteert met de taxicentrales dat zij hun chauffeurs goed moeten instrueren. Het opnemen van een vergelijkbare contractuele bepaling in de overeenkomsten met consumenten is onvoldoende. De producent weet dat de consumenten deze voorwaarden niet goed lezen. Hij moet extra maatregelen nemen om ervoor te zorgen dat consumenten goed zijn gewaarschuwd.

3. ZORGPLICHTEN OP GROND VAN DE VERWERKING VAN PERSOONSGEGEVENS

De verwerking van persoonsgegevens leidt tot zorgplichten op het gebied van cybersecurity. Persoonsgegevens zijn gegevens die betrekking hebben op een persoon, de 'betrokkene'. Voldoende is dat de betrokkene identificeerbaar is aan de hand van de gegevens in uw bedrijf.

Gegevens waarmee een betrokkene, bijvoorbeeld uw klant, direct kan worden geïdentificeerd, zijn bijvoorbeeld naam, adres en woonplaats (NAW-gegevens). Het kan echter ook gaan om indirect identificerende gegevens, bijvoorbeeld als een gegeven wordt gebruikt waarmee uiteindelijk ook de burgerlijke identiteit kan worden gevonden, zoals (in veel gevallen bij) een IP-adres of een paspoortnummer. Voldoende is verder dat iemand kan worden 'herkend' in een groep (kan worden onderscheiden van anderen), ook als geen link is te leggen naar de unieke identiteit van een persoon. Een voorbeeld hier is een cookie, waarbij de website-eigenaar de bezoeker wel kan herkennen, maar deze persoon niet kan relateren aan NAW- of andere identificerende gegevens.

Gegevensbescherming

Persoonsgegevens worden in de regel verwerkt met behulp van ICT. Zij worden bijna altijd (ook) in digitale vorm opgeslagen. Indien uw bedrijf persoonsgegevens verwerkt, heeft het zorgplichten op grond van de Wet Bescherming Persoonsgegevens ('WBP'). De Algemene Verordening Gegevensbescherming ('AVG') breidt deze plichten verder uit. Zij is van toepassing vanaf 25 mei 2018. Op dat moment vervalt de WBP. De regels verplichten uw bedrijf in het bijzonder om passende technische en organisatorische beveiligingsmaatregelen te nemen, waaronder begrepen een adequate cybersecurity.

Voorbeelden van persoonsgegevens zijn informatie over geslacht, seksuele voorkeur, religie, leeftijd, naam, huwelijkse staat, familie, gezondheidstoestand of beroep, (e-mail)adressen, telefoonnummers, vingerafdrukken, ip-adressen, cookies, de waarde van een huis en gedragsgegevens die worden uitgelezen bij het gebruik van ICT diensten en producten.

De invoering van de AVG leidt niet tot een grote verandering met betrekking tot de zorgplichten op het gebied van cybersecurity. Onder de AVG is een aantal verplichtingen dat eerder alleen voor de verantwoordelijke gold, waaronder de beveiligingsverplichtingen, ook rechtstreeks van toepassing op bewerkers. Bewerkers verwerken persoonsgegevens uitsluitend ten behoeve van een verantwoordelijke, zoals bijvoorbeeld cloud providers. Verder codificeert de AVG verschillende zorgplichten, zoals de verplichting om een verwerking 'privacy-by-design' (en 'security-by-design') in te richten. Dit betekent bijvoorbeeld dat gegevens waar mogelijk moeten worden gepseudonimiseerd, om schade bij verlies of diefstal te voorkomen.

Verplichte schadevergoeding

De begrippen 'persoonsgegevens' en 'verwerking' worden ruim geïnterpreteerd. Bijna alle bedrijven verwerken hierdoor persoonsgegevens. Het is niet nodig dat uw bedrijf de gegevens op een bijzondere manier gebruikt in de bedrijfsvoering. Ook als uw bedrijf een lijst met gegevens over uw klanten of werknemers bijhoudt, verwerkt het persoonsgegevens. Alle handelingen met betrekking tot persoonsgegevens zijn verwerkingen. Ook het verzamelen of het bewaren van gegevens geldt als een verwerking. Andere voorbeelden zijn het vastleggen, ordenen, bijwerken, wijzigen, raadplegen, verspreiden, uitwissen of weggooien van de gegevens.

Een schending van de beveiligingsplichten heeft grote gevolgen. De Autoriteit Persoonsgegevens is de Nederlandse toezichthouder op het gebied van de bescherming van persoonsgegevens. Zij kan een boete opleggen van maximaal € 820.000 per overtreding of 10 % van de jaaromzet. Zodra de AVG van toepassing is, zal de maximale boete € 10.000.000 of 2 % van de wereldwijde omzet van het bedrijf zijn. Uw bedrijf kan bovendien worden aangesproken tot het vergoeden van de door de schending veroorzaakte schade.

Invulling zorgplichten

De Autoriteit Persoonsgegevens heeft verschillende beleidsregels gepubliceerd waarin de zorgplichten worden uitgewerkt. Deze beleidsregels bieden algemene aanwijzingen over de invulling van de zorgplichten, maar ook bijzondere plichten voor specifieke situaties. De bijzondere zorgplichten op het gebied van de bescherming van persoonsgegevens worden in deze handreiking niet uitgewerkt. Hieronder volgt een aantal belangrijke aanwijzingen.

- Uw bedrijf houdt rekening met cybersecurity voordat er wordt begonnen met de verwerking van de persoonsgegevens ('privacy-by-design', waaronder begrepen 'security-by-design').
- Uw bedrijf voert een risicoanalyse uit voordat er wordt begonnen met de verwerking van de persoonsgegevens. Als er grote risico's voor de betrokkenen bestaan, voert uw bedrijf een 'privacy impact assessment' uit.
- Uw bedrijf verzamelt en bewaart alleen noodzakelijke gegevens ('dataminimalisatie').
- Uw bedrijf beperkt de verspreiding van en de toegang tot de persoonsgegevens tot een minimum.
- Indien uw bedrijf persoonsgegevens door een andere partij laat verwerken, sluit het een overeenkomst. In deze overeenkomst wordt de andere partij onder andere verplicht om te zorgen voor cybersecurity.
- Uw bedrijf neemt passende technische en organisatorische beveiligingsmaatregelen.
- Uw bedrijf controleert regelmatig of de genomen maatregelen nog steeds voldoende zijn.
- Uw bedrijf heeft een adequate procedure voor het melden, oplossen en opvolgen van beveiligingsincidenten.
- Uw bedrijf meldt inbreuken in verband met persoonsgegevens ('datalekken') binnen 72 uur aan de Autoriteit Persoonsgegevens. Als er een hoog risico bestaat dat de inbreuk in verband met persoonsgegevens ongunstige gevolgen heeft voor de betrokkenen, meldt uw bedrijf de inbreuk ook aan de betrokkenen.

- Na een inbreuk in verband met persoonsgegevens neemt uw bedrijf maatregelen om de gevolgen te beperken en dergelijke inbreuken in de toekomst te voorkomen.
- Uw bedrijf houdt bij welke beveiligingsmaatregelen het neemt.
- Uw bedrijf houdt de verwerkingen van persoonsgegevens bij.
- Indien uw bedrijf bij de verwerking van de persoonsgegevens samenwerkt met andere partijen, zorgt u ervoor dat ook deze partijen de zorgplichten op het gebied van cybersecurity vervullen. Uw bedrijf sluit hiervoor een overeenkomst met de andere partijen.

Bronnen:

- Artikel 4, 5, 24, 25, 32, 33, 34, 82 en 83 AVG.
- Artikel 1, 34a, 49 en 66 WBP.
- Artikel 23 Wetboek van Strafrecht.
- College Bescherming Persoonsgegevens, CBP Richtsnoeren. Beveiliging van persoonsgegevens, 2013.
- College Bescherming Persoonsgegevens, De meldplicht datalekken in de Wet bescherming persoonsgegevens (Wbp), Beleidsregels voor toepassing van artikel 34a van de Wbp, 2015.
- Autoriteit Persoonsgegevens, Boetebeleidsregels, 2016.
- https://autoriteitpersoonsgegevens.nl/.

4. ZORGPLICHTEN OP GROND VAN HET GEBRUIK VAN ICT

Uw bedrijf is verantwoordelijk voor de door u gebruikte ICT. Dit wordt niet anders als uw ICT slechts een ondersteunende rol speelt of als u de ICT niet zelf heeft ontwikkeld. Dit kan u in een moeilijke positie brengen: aan de ene kant mist uw bedrijf de expertise om te garanderen dat de ICT veilig is, aan de andere kant kan een beveiligingsincident uw bedrijfsvoering grondig verstoren.

U kunt in een overeenkomst afspreken dat uw bedrijf niet verantwoordelijk is voor gebreken in de cybersecurity van de door u gebruikte ICT. Uw bedrijf kan bijvoorbeeld bedingen dat het geen of slechts een beperkte schadevergoeding hoeft te betalen als het door een probleem met de ICT te laat is met het vervullen van zijn contractuele verplichtingen. De meeste zakelijke wederpartijen zullen hier alleen mee akkoord gaan indien u op uw beurt een garantie geeft dat u uw ICT-systemen goed heeft beveiligd.

Duidelijke afspraken

Het is aan te bevelen om de afspraken over cybersecurity duidelijk te formuleren. Bij vage termen bestaat er een reëel risico dat de rechter de bepalingen, in het geval van een conflict, uitlegt in het nadeel van uw bedrijf. Stel dat uw bedrijf in de overeenkomst vastlegt dat het niet aansprakelijk is als een ‘cyberaanval’ ertoe leidt dat het te laat is met het vervullen van zijn verplichtingen. Zonder nadere omschrijving van deze term, kan er een conflict ontstaan over de vraag of een bepaalde vorm van malware als een cyberaanval moet worden gekwalificeerd.

De mogelijkheden tot het maken van afspraken zijn in het bijzonder beperkt als de wederpartij een ‘consument’ is. Een beding in de algemene voorwaarden van een overeenkomst heeft geen rechtsgevolgen (‘is vernietigbaar’) als het zeer nadelig (‘onredelijk bezwarend’) is voor de consument. Een clausule die bepaalt dat uw bedrijf geen of beperkte plichten op het gebied van cybersecurity heeft, is waarschijnlijk onredelijk bezwarend.

Gemaakte afspraken gelden bovendien alleen ten opzichte van de partij met wie u de overeenkomst hebt gesloten.

Verouderde software

Uw bedrijf kan niet iedere verplichting uitsluiten. Het blijft aansprakelijk als het bijvoorbeeld, met medeweten van de bedrijfsleiding, bewust ('opzettelijk of bewust roekeloos') gebruik maakt van ICT waarvan de cybersecurity sterk tekortschiet. Een bedrijf dat bewust gebruik maakt van sterk verouderde software en geen maatregelen neemt om zijn computers en netwerken te beveiligen, kan zich waarschijnlijk niet beroepen op een clausule die aansprakelijkheid uitsluit als het gebrek aan beveiliging tot schade leidt.

Bronnen: zie pagina 16

Digitale veiligheid bij handelspartners

Uw bedrijf is mede afhankelijk van de cybersecurity van andere bedrijven in de keten. Bij ketenafhankelijkheid kunt u uw afnemers niet tevreden stellen als een beveiligingsincident ertoe leidt dat uw toeleverancier zijn verplichtingen aan u niet nakomt. Dit speelt in het bijzonder als uw handelspartners de beschikking hebben over uw bedrijfsinformatie of persoonsgegevens die u nodig heeft voor uw bedrijfsvoering. Het is daarom van belang om met uw handelspartners afspraken te maken over cybersecurity. Een keten is zo sterk als haar zwakste schakel.

- Uw bedrijf maakt afspraken over cybersecurity met andere bedrijven in de keten.

Ken uw risico's

Het is van belang om de risico's te kennen die zijn verbonden aan de door uw bedrijf gebruikte ICT. Welke beveiligingsincidenten kunnen er optreden als uw digitale veiligheid – cybersecurity – onvoldoende is? Hoe groot is de kans op deze incidenten? In hoeverre tasten zij de reputatie en bedrijfsvoering van uw bedrijf aan? Hoe groot zijn de gevolgen als de ICT tijdelijk niet beschikbaar is of als er vertrouwelijke informatie lekt? Leiden de incidenten ook tot schade voor andere bedrijven of consumenten? Is uw bedrijf hier verantwoordelijk voor? In hoeverre is het praktisch en economisch mogelijk om risico's te verkleinen? Op basis van de antwoorden op deze vragen stelt uw bedrijf vast welke eisen er aan de cybersecurity van de gebruikte ICT moeten worden gesteld.

Investeren in cybersecurity kost geld, maar leidt eveneens tot economische voordelen. Een vergroting van de beschikbaarheid, integriteit en vertrouwelijkheid van de ICT verhoogt de efficiëntie van uw bedrijfsvoering en voorkomt het ontstaan van aansprakelijkheid en reputatieschade. Het is vanuit praktisch en economisch oogpunt echter niet mogelijk om 100 % veiligheid te bewerkstelligen. De vaststelling van de eisen aan cybersecurity vereist daarom een afweging van de kosten en baten.

- Uw bedrijf kent de risico's van het gebruik van de ICT.
- Uw bedrijf heeft op basis van een kosten-batenanalyse vastgesteld welke risico's acceptabel zijn.
- Uw bedrijf stelt een budget voor cybersecurity beschikbaar. Bij het vaststellen van dit budget houdt u rekening met de vastgestelde risico's.

Vooraf nadenken over zorgplichten

Uw bedrijf dient al voordat het nieuwe ICT producten of diensten inkoopt of gaat gebruiken, vast te stellen of de ICT voldoet aan de voor uw bedrijf noodzakelijke cybersecurity. Het is daarnaast van belang om duidelijke afspraken te maken met de bedrijven waarvan u het product of de dienst afneemt. Welke service krijgt uw bedrijf als er een storing ontstaat? Wat zijn uw rechten als de ICT, ondanks deze service, gedurende een bepaalde tijd niet beschikbaar is? Hoe lang heeft u recht op security patches? De meeste leveranciers van ICT zullen aansprakelijkheid voor een gebrek in de cybersecurity uitsluiten in het contract dat u met ze aangaat. Stelt u dit vooral ter discussie tijdens de onderhandelingen.

De toegang tot het ICT-netwerk van een bedrijf is beveiligd door middel van een tweefactorenauthenticatie. Een gebruiker kan alleen inloggen als hij de beschikking heeft over een fysieke 'token' en een wachtwoord. Nadat de ontwikkelaar is gehackt, worden alle tokens vervangen. Het bedrijf kan het systeem hierdoor tijdelijk niet gebruiken. Het lijdt een schade van ruim een miljoen euro. De ontwikkelaar verschaft nieuwe tokens, maar weigert schadevergoeding te betalen. De overeenkomst bevat ingewikkelde, gedetailleerde garanties. Zij bevat echter ook een clausule waarin het recht op schadevergoeding wordt uitgesloten.

- Voordat uw bedrijf gebruik gaat maken van nieuwe ICT, stelt het vast of de cybersecurity van deze ICT aan uw eisen voldoet.
- Uw bedrijf maakt duidelijke afspraken met de leveranciers van de door u gebruikte ICT.

Beveiliging van uw ICT

Bij ingebruikneming van ICT is het noodzakelijk om technische en organisatorische maatregelen te nemen ter verzekering van de cybersecurity. Deze maatregelen dienen te beveiligen tegen zowel beveiligingsincidenten op afstand ('via het internet') als tegen fysieke inbreuken. Uw bedrijf dient bijvoorbeeld eveneens maatregelen te nemen om ervoor te zorgen dat de ICT op een veilige manier wordt gebruikt.

Na een 'zero-day-attack' brengt de softwareontwikkelaar direct een security patch uit. Het bedrijf installeert deze patch echter pas een maand later, en blijft hierdoor kwetsbaar.

Het is van belang om de toegang tot de ICT te beperken. Een 'tweefactorauthenticatie' verdient hierbij de voorkeur. Een combinatie van een gebruikersnaam en een wachtwoord is niet altijd voldoende.

Bij een tweefactorauthenticatie verkrijgt de gebruiker slechts toegang tot de ICT als hij aan verschillende voorwaarden voldoet. De toegang is bijvoorbeeld beveiligd door een fysieke factor ('iets dat de gebruiker bezit', bijvoorbeeld een bankpas) in combinatie met een mentale factor ('iets dat de gebruiker weet', een wachtwoord of pincode).

Als er wachtwoorden worden gebruikt, moeten zij voldoende ingewikkeld zijn. Een geboortedatum, '123456789' en de naam van de gebruiker zijn onacceptabel en mogen niet mogelijk zijn. Het wachtwoord dat een werknemer gebruikt voor toegang tot belangrijke bedrijfsgeheimen of ICT, dient daarnaast niet hetzelfde te zijn als het wachtwoord dat hij ook privé gebruikt. De werknemers mogen het wachtwoord bovendien niet laten rondslingeren, bijvoorbeeld door het op een briefje te schrijven en op de computer te plakken.

Zie voor meer informatie over het veilig gebruik van wachtwoorden ook Nationaal Cyber Security Centrum, Factsheet Gebruik tweefactorauthenticatie, 2015.

Bij het nemen van beveiligingsmaatregelen hoeft uw bedrijf het wiel niet opnieuw uit te vinden. U kunt gebruik maken van beveiligingsstandaarden, gedragscodes of certificeringsmechanismen die op uw situatie van toepassing zijn.

Er worden regelmatig nieuwe beveiligingsstandaarden, gedragscodes en certificerings-mechanismen ingevoerd. De bestaande regels worden bovendien vaak bijgewerkt.
Uw bedrijf dient daarom te monitoren of er op zijn gebied nieuwe regels worden gepubliceerd.

Een 'algemene' beveiligingsstandaard is bijvoorbeeld de door de 'International Organization for Standardization' opgestelde NEN-ISO/IEC 27002:2013+C2:2015 nl. Deze standaard geeft een grote hoeveelheid relevante aanknopingspunten, maar geeft door zijn algemene en technologie-neutrale formulering slechts in beperkte mate handreikingen voor concrete maatregelen. Specifieke beveiligingsstandaarden schrijven dikwijls concretere maatregelen voor.

De 'Payment Card Industry Data Security Standard' formuleert verschillende vereisten bij de verwerking van betalingen door middel van credit cards.

De richtlijn 'Beveiligingsrichtlijnen voor mobiele apparaten' formuleert verschillende aanwijzingen voor een veilig gebruik van mobiele apparaten. De richtlijn adviseert bijvoorbeeld om volgsoftware te gebruiken en regelmatig back-ups te maken.

- Uw bedrijf implementeert technische en organisatorische beveiligingsmaatregelen.
- Uw bedrijf neemt maatregelen om de ICT te beschermen tegen virussen en malware.
- Uw bedrijf heeft een systeem om ervoor te zorgen dat security patches snel en regelmatig worden uitgevoerd.
- Binnen uw bedrijf bestaan regels die zien op een veilig gebruik van ICT.
- Uw bedrijf beveiligt fysieke ICT en gegevensdragers tegen diefstal.
- Uw bedrijf beveiligt de toegang tot de ICT minimaal door middel van een wachtwoord en bij voorkeur met een tweefactorauthenticatie.
- Uw bedrijf voldoet aan relevante beveiligingsstandaarden, gedragscodes of certificeringsmechanismen.
- Uw bedrijf legt vast op welke manier de ICT is beveiligd.

Bronnen: zie pagina 16

Controle van de beveiliging

ICT verandert voortdurend en kwaadwillende hackers verzinnen steeds nieuwe manieren om bij u binnen (proberen) te komen. Cybersecurity vereist dan ook doorlopend aandacht. Het is mogelijk dat de door uw bedrijf gebruikte ICT niet langer voldoende beveiligd is. U dient bovendien te controleren of de beveiligingsmaatregelen consequent worden toegepast. Het is raadzaam om uw beveiliging regelmatig door een externe partij te laten valideren en om u daarover te laten adviseren.

Meer praktijkvoorbeelden

U heeft een bouwbedrijf en werkt samen met een aantal onderaannemers. De belangrijkste onderaannemer heeft de projectdocumentatie in de cloud opgeslagen van een cloud provider. De cloud provider heeft een beveiligingsincident. De onderaannemer kan hierdoor niet bij de documentatie, waardoor vertraging in de uitvoering van de projecten optreedt.

*Een fabrikant van onderdelen voor fietsen wordt getroffen door **ransomware**. Hij heeft tijdelijk geen toegang tot de ontwerpen van een onderdeel voor een nieuwe fiets. De fiets kan hierdoor niet in productie worden genomen. De fabrikant kan zich waarschijnlijk niet ten opzichte van zijn afnemers beroepen op de aanval door ransomware. Dit levert in beginsel geen geval van 'overmacht' op.*

*Een webwinkel gebruikt door een ander bedrijf ontwikkelde drones om zijn producten af te leveren. Voordat de koper in de webwinkel een product bestelt, moet hij toezeggen om de webwinkel niet aansprakelijk te stellen als een drone bij de aflevering schade veroorzaakt. Door een **gebrek in de beveiliging** valt de drone op een auto. De eigenaar van de auto spreekt de webwinkel aan. De webwinkel kan zich niet beroepen op de afspraak met de koper. Hij kan zich bovendien niet verweren met het argument dat niet de winkel, maar de ontwikkelaar van de drones verantwoordelijk is voor het ongeluk.*

*Een grote bank begeleidt regelmatig fusies van beursgenoteerde bedrijven. Zij maakt hiervoor gebruik van de diensten van een internationaal advocatenkantoor. Door een beveiligingsincident bij het advocatenkantoor zijn **hackers** in staat om op de beurs te handelen met voorkennis. De bank is hierdoor verplicht om de fusieonderhandelingen vroegtijdig bekend te maken.*

*Een bedrijf wil gebruik gaan maken van op afstand bestuurbare fabrieksdeuren. Voordat het de deuren en de daarbij behorende software aanschaft, stelt het vast dat de **cybersecurity onvoldoende** is. Het bedrijf spreekt daarom met de ontwikkelaar af dat de beveiliging wordt verbeterd. Het gaat de fabrieksdeuren niet afnemen en betalen als de ontwikkelaar hier niet in slaagt.*

*Een **hacker** slaagt er niet in om via het internet controle over op afstand bestuurbare sluizen te krijgen. Hij kan de gebruikte **tweefactorauthenticatie** niet omzeilen zonder fysieke 'token'. De hacker gaat daarom naar het gebouw van waaruit de sluizen worden bestuurd. Hij loopt naar binnen en steelt een 'token' van een ervaren medewerker. Deze medewerker had de 'token', in strijd met de binnen het bedrijf geldende afspraken, op een flexplek laten liggen.*

*Een bedrijf dat belangrijke en vertrouwelijke informatie via e-mail verstuurt, kiest voor een e-mailprogramma dat sterke **end-to-end versleuteling** ondersteunt. Om gebruik te maken van deze sterke vorm van versleuteling is het noodzakelijk om digitale certificaten uit te wisselen. In de praktijk doen de gebruikers dit echter niet. De versleuteling wordt daarom niet gebruikt.*

*Een dief breekt in bij de woning van een officier van justitie. Hij steelt de werktelefoon en een **USB-stick**. De werktelefoon is goed beveiligd. Het is niet mogelijk om toegang te verkrijgen zonder de code en de vingerafdruk van de officier. De USB-stick is echter niet goed beveiligd: de informatie over een drugszaak is onversleuteld opgeslagen.*

*Door '**Heartbleed**', een programmeerfout in 'OpenSSL', is een grote hoeveelheid websites kwetsbaar. Nadat de fout bekend is geworden, controleert een kledingzaak of zijn webwinkel ook kwetsbaar is. Het neemt daarom contact op met de ontwikkelaar van zijn website.*

*Nadat een hacker erin is geslaagd om de voor de **tweefactorauthenticatie** benodigde 'token' tijdens kantooruren te stelen, neemt het bedrijf verschillende maatregelen. Een tijdlang is iedereen alert. Na een paar maanden blijkt echter dat medewerkers hun **'tokens'** weer gewoon op hun bureaus laten liggen.*

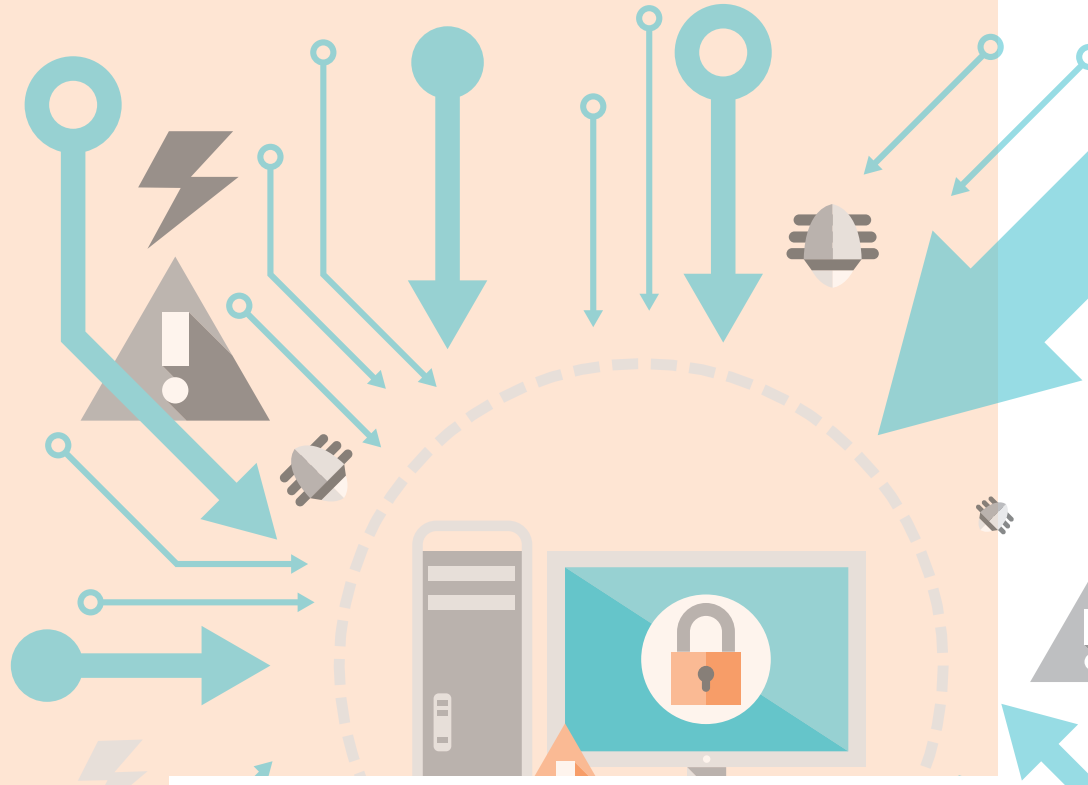
- Uw bedrijf controleert of laat controleren of de cybersecurity nog steeds voldoende is.
- Uw bedrijf onderzoekt of laat onderzoeken of er beveiligingsincidenten hebben plaatsgevonden.
- Uw bedrijf controleert of laat controleren of de genomen maatregelen consequent zijn geïmplementeerd en worden nageleefd.

Bronnen: zie onder

Maatregelen bij beveiligingsincidenten

Er bestaat altijd een risico dat er ondanks de maatregelen toch een beveiligingsincident plaatsvindt. In dat geval dient uw bedrijf maatregelen te nemen om de gevolgen van het incident te beperken en verdere incidenten te voorkomen.

- Na een incident onderzoekt uw bedrijf het incident, hoe het heeft kunnen ontstaan en hoe ernstig de gevolgen zijn.
- Uw bedrijf legt beveiligingsincidenten vast.
- Uw bedrijf neemt zo snel mogelijk stappen om het incident op te lossen en (verdere) negatieve gevolgen te voorkomen of te beperken.
- Uw bedrijf onderzoekt of u het beveiligingsincident moet melden, bijvoorbeeld omdat dit is afgesproken in een overeenkomst of omdat er persoonsgegevens (Hoofdstuk 3) zijn gelekt.
- Na een incident neemt uw bedrijf maatregelen om vergelijkbare incidenten in de toekomst te voorkomen.



Bronnen ***Verouderde software***:
- Artikel 6:75, 173, 233 en 248 Burgerlijk Wetboek.

Bronnen ***Beveiliging van uw ICT***:
- Nationaal Cyber Security Centrum, Beveiligingsrichtlijnen voor mobiele apparaten, 2012.
- NEN-ISO/IEC, Information technology— Security techniques — Code of practice for information security controls (ISO/IEC 27002), 2013.
- Nationaal Cyber Security Centrum, Factsheet Gebruik tweefactorauthenticatie, 2015.
- PCI Security Standards Council, Payment Card Industry Data Security Standard, 2016.
- www.forumstandaardisatie.nl/open-standaarden/lijsten-met-open-standaarden/.

Bronnen ***Controle van de beveiliging***:
- Centraal Planbureau (m.m.v. Nationaal Cyber Security Centrum), Risicorapportage Cyberveiligheid Economie, 2016, p. 17.

5. ZORGPLICHTEN IN VERBAND MET PRODUCTEN OF DIENSTEN MET EEN ICT-TOEPASSING

Als uw bedrijf een product of dienst met een ICT-toepassing ontwikkelt, produceert of levert, moet het instaan voor de cybersecurity van de ICT. Deze plicht is gebaseerd op verschillende grondslagen en bestaat onafhankelijk van uw plaats in de keten.

Onder producten of diensten met een ICT-toepassing vallen onder andere websites, software, operating systems, firmware, applicaties, cloud diensten en tastbare producten met een ICT-component. Tastbare producten met een ICT-component zijn bijvoorbeeld laptops en mobiele telefoons, maar ook apparaten die zijn aangesloten op het 'internet der dingen': alledaagse gebruiksvoorwerpen met een ICT-component. Een voorbeeld hiervan is een tandenborstel die bijhoudt of je goed poetst.

Verplichtingen van de verkoper

Indien uw bedrijf producten of diensten met een ICT-toepassing verkoopt, is het ten opzichte van de koper verplicht om een product te leveren dat aan de overeenkomst beantwoordt ('conformiteit'). Hiervoor is onder andere vereist dat de ICT de eigenschappen bezit die de koper mag verwachten en die voor een normaal gebruik nodig zijn. Cybersecurity kan als zo'n eigenschap worden beschouwd. Een koper mag bijvoorbeeld verwachten dat een mobiele telefoon en een sleutel waarmee op afstand een auto kan worden ontsloten, een basisbeveiliging hebben tegen hacken. U hoeft dus niet te garanderen dat het product onder alle omstandigheden 100 % veilig is. Het moet 'veilig genoeg' zijn om normaal te worden gebruikt. Als het product deze veiligheid niet bezit, heeft de koper recht op herstel of vervanging. Een 'consument' heeft bovendien recht op prijsvermindering, schadevergoeding en ongedaanmaking van de koop ('ontbinding').

Ten tijde van de verkoop mogen er geen bekende beveiligingslekken bestaan. Het is niet nodig om te garanderen dat er ook op een later moment geen kwetsbaarheden aan het licht komen. Of de koper in dat geval mag verwachten dat de beveiliging binnen een redelijke tijd wordt bijgewerkt, bijvoorbeeld door een security patch, hangt af van de omstandigheden van het geval, waaronder de beoogde levensduur van het product.

In Europees verband is een Richtlijn in voorbereiding betreffende de levering van digitale inhoud, die expliciet maakt dat veiligheid, toegankelijkheid en continuïteit onder de plicht tot conformiteit vallen. Het voorstel bepaalt bovendien dat ook updates (waaronder security patches) onder conformiteit vallen.

- Het product is 'veilig genoeg' om normaal te worden gebruikt.

Bronnen: zie pagina 24

Informatieplichten
Het is voor uw bedrijf van belang om geen onrealistische verwachtingen bij de koper in het leven te roepen. U dient niet te stellen of te impliceren dat de cybersecurity van het product of de dienst sterker is dan deze in werkelijkheid is. Dit geldt bij de marketing van het product, ten tijde van de onderhandelingen en in de koopovereenkomst. In sommige gevallen dient u de koper zelfs actief te waarschuwen dat de cybersecurity minder sterk is dan hij mag verwachten of dat de beveiliging van een bepaald product binnenkort niet langer meer zal worden onderhouden. Dit geldt in het bijzonder als u het product of de dienst aan een consument verkoopt. U mag geen belangrijke informatie over cybersecurity achterhouden of op onduidelijke, onbegrijpelijke of dubbelzinnige wijze verstrekken.

Voordat een consument een mobiele telefoon koopt, wordt hij geïnformeerd over de periode waarin de producent de beveiliging zal blijven bijwerken. Hij weet bovendien in welke gevallen hij recht heeft op een security patch.

- De koopovereenkomst, de onderhandelingen en de marketing scheppen realistische verwachtingen. Zij stellen of suggereren niet dat de cybersecurity sterker is dan zij in werkelijkheid is of dat een product langer zal worden onderhouden dan in werkelijkheid het geval is.
- Het bedrijf waarschuwt indien de cybersecurity minder sterk is dan de koper mag verwachten of indien een bepaald product op korte termijn niet meer zal worden onderhouden.

Bronnen: zie pagina 24

Contractuele afspraken
Uw bedrijf kan afspraken maken over de cybersecurity van de geleverde producten of diensten met een ICT-toepassing. U kunt echter niet iedere verplichting uitsluiten.
Zie voor de grenzen van de mogelijkheden van contractuele afspraken hoofdstuk 4.

- Koopovereenkomsten met andere bedrijven bevatten bepalingen die de rechten en plichten op het gebied van cybersecurity nader bepalen.

Cybersecurity in de keten
De (mogelijke) omstandigheid dat uw bedrijf de producten niet zelf ontwikkelt, ontslaat u niet van de verantwoordelijkheid ten opzichte van uw afnemers. Het is aan te bevelen om in dit geval duidelijke afspraken te maken met uw leveranciers. Op welke manier werkt u samen als de eindgebruiker een beroep doet op een gebrek in de cybersecurity? Wie is er uiteindelijk verantwoordelijk? U kunt in de koopovereenkomst afspreken dat uw bedrijf niet verantwoordelijk of aansprakelijk is voor (een gebrek in) de cybersecurity van het verkochte product. Deze afspraak is echter alleen bindend als u het product verkoopt aan een ander bedrijf. U kunt de verplichting tot conformiteit niet beperken als het product, direct of via een doorverkoper, aan een consument wordt verkocht.

- Uw bedrijf maakt afspraken met zijn leveranciers en tussenpersonen. Hierin zijn de verplichtingen op het gebied van cybersecurity opgenomen en wordt de verantwoordelijkheid verdeeld in het geval van een gebrek in de beveiliging.

Andere overeenkomsten
De plicht tot conformiteit bestaat alleen bij koopovereenkomsten. Ook andere overeenkomsten verplichten uw bedrijf echter om rekening te houden met de belangen van de wederpartij. Zij kunnen zorgplichten op het gebied van cybersecurity laten ontstaan. Deze plichten zijn in grote lijnen dezelfde als de plichten die voortvloeien uit een koopovereenkomst. Uw bedrijf heeft de hiervoor besproken zorgplichten dus ook als uw bedrijf de ICT op grond van een andere overeenkomst dan een koopovereenkomst levert.

Bronnen: zie pagina 24

Een overeenkomst tot het ontwikkelen van 'maatwerk', of 'Software-as-a-Service', wordt meestal als overeenkomst van 'opdracht' gekwalificeerd. De ontwikkelaar is in dat geval verplicht om zich als een 'goed opdrachtnemer' te gedragen. Alle overeenkomsten verplichten bovendien tot hetgeen voortvloeit uit de 'redelijkheid en billijkheid'.

Verantwoordelijkheid voor derden
De cybersecurity van de door u geleverde producten en diensten is van grote betekenis voor uw afnemers. Zij zijn echter niet de enigen die hier belang bij hebben. In sommige gevallen kunnen ook anderen, met wie uw bedrijf geen overeenkomst heeft, belang hebben bij de cybersecurity. De zorgplichten gelden in dat geval ook ten opzichte van deze personen.

Het is daarom van belang om uit te zoeken wie er belang heeft bij de cybersecurity van uw product of dienst. Zijn dit alleen de partijen met wie u zaken doet? Of wordt het product of de dienst ook doorverkocht? Zijn de beschikbaarheid, integriteit en vertrouwelijkheid alleen van belang voor de gebruiker? Of kan een gebrekkige cybersecurity ook tot schade bij anderen leiden?

U dient daarnaast de omvang van de risico's te kennen die zijn verbonden aan de door uw bedrijf geleverde producten of diensten. De omvang van de risico's wordt in de eerste plaats bepaald door de kans op een beveiligingsincident en verder door de impact van een beveiligingsincident. Ook als de kans op een incident beperkt is, kunnen de risico's groot zijn. Dit geldt in het bijzonder als de gevolgen substantieel kunnen zijn, bijvoorbeeld omdat er een risico bestaat op 'fysieke' schade of lichamelijk letsel. Het is daarnaast van belang om te onderzoeken of en in hoeverre het praktisch en economisch mogelijk is om de risico's te verkleinen. Op basis van deze analyse stelt uw bedrijf vast welke eisen er aan de cybersecurity van de producten of diensten moeten worden gesteld. Hoe groter de risico's, hoe strenger de eisen aan cybersecurity.

U kunt niet met de benadeelde afspreken dat uw bedrijf niet verantwoordelijk is. Uw bedrijf heeft immers geen overeenkomst met deze partij gesloten. Het is wel mogelijk om met een andere partij, bijvoorbeeld de afnemer of gebruiker van uw product of dienst, afspraken te maken. Dit ontslaat uw bedrijf echter niet van zijn plichten ten opzichte van de benadeelde.

Zie voor de grenzen van de mogelijkheden van contractuele afspraken hoofdstuk 4.

- Uw bedrijf stelt vast wie er belang heeft bij de cybersecurity van de door hem ontwikkelde en geleverde producten en diensten met een ICT-toepassing.
- Uw bedrijf kent de risico's van een gebrek in de cybersecurity van zijn product of dienst.
- Uw bedrijf stelt op basis van een kosten-batenanalyse vast welke risico's bij zijn product of dienst acceptabel zijn.
- Uw bedrijf maakt afspraken met de partijen van wie de cybersecurity mede afhankelijk is. Hierin zijn de verplichtingen op het gebied van cybersecurity opgenomen en wordt de verantwoordelijkheid verdeeld in het geval van een gebrek in de beveiliging.

Bronnen: zie pagina 24

De beveiliging van producten of diensten met een ICT-toepassing

Uw bedrijf dient de door u ontwikkelde producten of diensten te voorzien van adequate cybersecurity. Een effectieve vervulling van deze zorgplicht is slechts mogelijk als cybersecurity al in een vroeg stadium op de agenda staat. Hoewel het niet nodig is om de cybersecurity in iedere fase van het project op orde te hebben, behoort het product uiteindelijk goed beveiligd te zijn. U kunt dit mede bewerkstelligen door een klimaat te creëren dat de ontwikkeling van een goed beveiligd product stimuleert, ook als dit de ontwikkeling kan vertragen of voor extra kosten zorgt.

Bij 'agile' ontwikkeling wordt de software regelmatig aangepast aan veranderende behoeften. Het is hierbij vaak niet mogelijk om vooraf te bepalen welke eisen uiteindelijk aan de beveiliging worden gesteld. De ontwikkelaar kan er in dit geval echter wel rekening mee houden dat het mogelijk moet zijn om de cybersecurity in een later stadium aan te passen.

Uw bedrijf kan de cybersecurity van het product of de dienst versterken door beveiligingsmechanismen te implementeren. Welke maatregelen nodig zijn, verschilt per ICT-toepassing.

Een website herkent DDoS aanvallen en 'filtert' ze eruit. De website blijft hierdoor online.

Uw bedrijf kan bij het implementeren van beveiligingsmechanismen gebruik maken van beveiligingsstandaarden, gedragscodes of certificeringsmechanismen die op uw product of dienst van toepassing zijn.

De cybersecurity van een product of dienst kan bovendien worden versterkt door het moeilijk te maken om de ICT aan te passen of de beveiliging uit te schakelen. Als de ICT toch wordt aangepast, wordt dit automatisch in een logboek bijgehouden. Het kan ook nodig zijn om het product of het productieproces te beschermen tegen 'fysieke' inbreuken.

De toegang tot een fabriek voor zelfrijdende auto's wordt beveiligd door een alarm en een bewaker. Werknemers hebben een pasje nodig om binnen te komen. De software is bovendien zo geprogrammeerd dat kleine aanpassingen van de sensoren ertoe leiden dat het niet meer mogelijk is om de zelfrijdende modus te gebruiken.

Meer praktijkvoorbeelden

Door een beveiligingslek in een computerprogramma is een hacker op eenvoudige wijze in staat om de computer van de gebruiker over te nemen. De kennis van dit gebrek is wijdverbreid. De verkoper die dit product verkoopt ondanks kennis van de onveiligheid, kan zich niet beroepen op een clausule die aansprakelijkheid uitsluit. Dit geldt in het bijzonder als het beveiligingslek niet is bekend gemaakt aan de afnemer waardoor de afnemer geen schadebeperkende maatregelen heeft kunnen treffen.

Een grote webwinkel verkoopt mobiele telefoons aan consumenten. Hij produceert de telefoons echter niet zelf, en heeft daarom geen invloed op de cybersecurity. Toch kunnen de consumenten de webwinkel aanspreken als blijkt dat de telefoons niet veilig zijn. De webwinkel spreekt met de producent af dat de producent de cybersecurity in dat geval verbetert en de kosten voor zijn rekening neemt. Als de producent weigert om dergelijke afspraken te maken, kiest de winkel ervoor om de telefoons niet langer aan te bieden.

Een bedrijf ontwikkelt 'slimme' thermostaten. Het verkoopt deze thermostaten aan energiemaatschappijen, die ze aan haar klanten geeft. Het bedrijf heeft geen overeenkomsten met de klanten. Toch is het ten opzichte van de klanten van de energiemaatschappij verplicht om te zorgen voor een deugdelijke cybersecurity.

Een bedrijf ontwikkelt en verkoopt software waarmee de gebruiker online persoonsgegevens kan verzamelen en beheren. Als een hacker door een gebrek in de beveiliging toegang krijgt tot de verzamelde gegevens, is dit niet alleen nadelig voor de gebruiker van de software, maar ook voor de 'betrokkenen' van wie de persoonsgegevens op straat liggen. Het bedrijf kan met de gebruikers van de software afspreken dat zij de kosten van een datalek voor hun rekening nemen. Dit ontslaat het bedrijf echter niet van zijn zorgplichten ten opzichte van de betrokkenen.

Het bedrijf spreekt met de gebruikers van de software af dat de gebruikers hacks altijd melden. Deze informatie stelt het bedrijf in staat om de gebreken in de cybersecurity te verhelpen. Het contract verplicht de gebruikers bovendien om beveiligingsupdates van de software altijd uit te voeren. Dit voorkomt verdere datalekken.

Een bedrijf ontwikkelt een 'slimme' elektriciteitsmeter. Het apparaat meet het energieverbruik van verschillende huishoudelijke apparaten en verstuurt de resultaten naar een centrale server. Het bedrijf kan hierdoor voorspellen waar en wanneer er extra energiecapaciteit nodig is. Om de privacy van zijn klanten te beschermen, heeft het bedrijf er al bij de ontwikkeling rekening mee gehouden dat de meter voldoende capaciteit moet hebben om de informatie versleuteld te versturen. Iemand die de signalen van de energiemeter onderschept, kan daarom niet zien hoeveel elektriciteit de klant gebruikt. Toch heeft het bedrijf de cybersecurity van de elektriciteitsmeter niet goed uitgedacht. Als iemand niet thuis is, zullen aanzienlijk minder keer gegevens worden doorgestuurd. Deze informatie kan interessant zijn voor inbrekers. Toen een werknemer dit gevaar tijdens de ontwikkeling ter sprake wilde brengen, werd hij door de leidinggevende overruled.

De ontwikkelaar van een mobiele telefoon verplicht de gebruikers om een toegangscode in te stellen. Het toestel wordt geblokkeerd als iemand te vaak achter elkaar een onjuiste code invoert.

De ontwikkelaar en hosting provider van websites zorgen ervoor dat de website van een klant na een DDoS-aanval snel weer online komt. Nader onderzoek wijst uit dat de website niet goed beveiligd was, en daardoor kwetsbaar was voor de aanval. De ontwikkelaar is in beginsel aansprakelijk. Omdat de website snel weer online is gebracht, valt de door de aanval veroorzaakte schade echter mee.

Een computerprogramma blijkt kwetsbaar te zijn voor een nieuw virus. Het risico is echter gemakkelijk te vermijden door een bepaalde functie niet te gebruiken. De ontwikkelaar stelt de gebruikers op de hoogte en blokkeert de functie tijdelijk. Hij werkt ondertussen aan een security patch.

De producent van zelfrijdende auto's weet dat de sensoren onder bepaalde weersomstandigheden niet goed werken. Hij vreest echter voor reputatieschade, en maakt dit gebrek niet wereldkundig. De producent verwacht het gebrek binnen een week te kunnen verbeteren. Binnen deze week gebeurt er echter een dodelijk ongeluk. De producent is aansprakelijk voor de schade.

Een besturingssysteem van een PC heeft een ingebouwde 'firewall'. Als de firewall wordt uitgezet, staat er een duidelijk zichtbaar icoon op de taakbalk. De gebruiker wordt bovendien regelmatig gewaarschuwd dat zijn PC niet goed is beveiligd.

De aanpassing van een website vereist een tweefactorauthenticatie. Er wordt bovendien een logboek bijgehouden van alle wijzigingen van de website. Dit logboek kan niet door één persoon worden gewijzigd.

- Uw bedrijf houdt al bij de ontwikkeling rekening met cybersecurity (security-by-design).
- Binnen uw bedrijf wordt de ontwikkeling van goed beveiligde producten of diensten door middel van organisatorische maatregelen gestimuleerd.
- Uw product of dienst heeft een ingebouwde technische beveiliging.
- Uw product of dienst voldoet aan relevante beveiligingsstandaarden, gedragscodes of certificeringsmechanismen.
- Uw bedrijf neemt maatregelen om de onbevoegde aanpassing van de ICT of de uitschakeling van de beveiliging tegen te gaan.
- Uw bedrijf houdt aanpassingen van het product of de dienst in een logboek bij.
- Uw bedrijf houdt bij op welke manieren het product of de dienst beveiligd is.

Bronnen: zie pagina 24

Het updaten van de beveiliging

Zelfs als uw bedrijf adequate maatregelen heeft genomen ter beveiliging van uw product of dienst, kan het voorkomen dat de ICT-toepassing op een later moment niet langer veilig is. Dit kan worden veroorzaakt door voortschrijdend inzicht of de ontwikkeling van de techniek. Uw bedrijf dient daarom regelmatig te controleren of de cybersecurity nog steeds in orde is.

De telefoons van een smartphonefabrikant maken gebruik van het Android besturingssysteem. In dit systeem wordt een fout ontdekt, de 'Stagefright-bug'. Ook de mobiele telefoons van de fabrikant blijken daardoor niet meer veilig te zijn.

Versleuteling door middel van 'hashing' kan worden gekraakt met brute computerkracht. Een toename van de beschikbare computerkracht kan ertoe leiden dat de aanvankelijk adequate versleuteling op een later moment te makkelijk is te kraken.

Als blijkt dat de cybersecurity niet langer in orde is, dient uw bedrijf de beveiliging bij te werken. Dit stelt u in staat om veilige ICT aan nieuwe klanten te leveren. U kunt bovendien de bestaande gebruikers ondersteuning bieden door een security patch uit te brengen. In sommige gevallen is het nodig om de gebruikers te waarschuwen dat de cybersecurity (tijdelijk) niet op orde is. De gebruikers kunnen in dat geval maatregelen nemen om het risico op een beveiligingsincident te verkleinen, terwijl u aan een security patch werkt. Bij serieuze incidenten dient u gebruikers bovendien op gepaste wijze bij te staan om schade die uit het incident voortvloeit te beperken.

De beveiliging kan sneller worden bijgewerkt als uw bedrijf de gebruikers stimuleert om beveiligingsincidenten in verband met uw product of dienst te melden. U kunt aan de hand van deze incidenten beoordelen of, en op welke manier, de cybersecurity moet worden bijgewerkt.

Als de software na een crash opnieuw wordt opgestart, krijgt de gebruiker een pop-up waarin hij wordt gevraagd om een rapport van de crash naar de ontwikkelaar te sturen.

- Uw bedrijf controleert de cybersecurity van het product of de dienst regelmatig.
- Uw bedrijf werkt gedurende een bepaalde periode de cybersecurity bij als zij niet langer in orde is.
- Uw bedrijf gebruikt een systeem om security patches door te voeren naar de gebruikers.
- Uw bedrijf stimuleert de gebruikers om beveiligingsincidenten door te geven. Deze incidenten worden onderzocht. U neemt maatregelen om vergelijkbare incidenten in de toekomst te voorkomen.
- Uw bedrijf biedt de gebruikers ondersteuning bij beveiligingsincidenten.
- De gebruikers (kunnen) worden gewaarschuwd als de cybersecurity niet op orde is.

Bronnen: zie onder

Bronnen ***Verplichtingen van de verkoper***:
- Artikel 7:5, 17, 21, 22, 25 en 47 Burgerlijk Wetboek.
- Artikel 2 lid 1, 3 en 6 Voorstel Richtlijn betreffende de levering van digitale inhoud, COM(2015) 634 final.
- HR 27 april 2012, Nederlandse Jurisprudentie 2012, 293 (Beeldbrigade/Hulskamp).
- Rechtbank Amsterdam (voorzieningenrechter) 8 maart 2016, ECLI:NL:RBAMS:2016:1175.

Bronnen ***Informatieplichten***:
- Artikel 6:193a-193j en 228 Burgerlijk Wetboek.
- Rechtbank Amsterdam (voorzieningenrechter) 8 maart 2016, ECLI:NL:RBAMS:2016:1175.

Bronnen ***Andere overeenkomsten***:
- Artikel 6:248 en 7:401 Burgerlijk Wetboek.
- Rechtbank Arnhem 7 december 2011, ECLI:NL:RBARN:2011:BU9785.
- W.F.R. Rinzema, 'Kwaliteit en software: een goede zaak', Computerrecht 2012, p. 104.

Bronnen ***Verantwoordelijkheid voor derden***:
- Artikel 6:162 en 185-193 Burgerlijk Wetboek.
- Richtlijn 85/374/EEG (productaansprakelijkheid).
- Hoge Raad 5 november 1965, Nederlandse Jurisprudentie 1966, 136 (Kelderluik).

Bronnen ***De beveiliging van de producten of diensten met een ICT-toepassing***:
- Artikel 6 Richtlijn betreffende de levering van digitale inhoud, COM(2015) 634.
- Nationaal Cyber Security Centrum, ICT-Beveiligingsrichtlijnen voor Webapplicaties, 2015.
- Nationaal Cyber Security Centrum, Beveiligingsrichtlijnen voor mobiele apparaten, 2012.
- PCI Security Standards Council, Payment Card Industry Data Security Standard, 2016.
- www.forumstandaardisatie.nl/open-standaarden/lijsten-met-open-standaarden/.

Bronnen ***Het updaten van de beveiliging***:
- Centraal Planbureau (m.m.v. Nationaal Cyber Security Centrum), Risicorapportage Cyberveiligheid Economie, 2016, p. 17.
- Article 29 Data Protection Working Party, Opinion 05/2014 on Anonymisation Techniques, 0829/14/EN WP216, 2014, p. 20.
- Rechtbank 's-Gravenhage 11 juli 2001, Computerrecht 2001, p. 268.
- Rechtbank Amsterdam (voorzieningenrechter) 8 maart 2016, ECLI:NL:RBAMS:2016:1175.

6. WIE IS ER BINNEN MIJN BEDRIJF VERANTWOORDELIJK VOOR CYBERSECURITY?

Cybersecurity is de verantwoordelijkheid van het bestuur. Bij kleinere bedrijven is de directeur verantwoordelijk.

Het bestuur of de directie moet ervoor zorgen dat de gebruikte ICT bijdraagt aan een efficiënte bedrijfsvoering. Het is bovendien verantwoordelijk voor de beheersing van de uit het gebruik van ICT voortvloeiende risico's en de naleving van de zorgplichten op het gebied van cybersecurity. De bestuurder met een bijzondere verantwoordelijkheid voor ICT, de Chief Information Officer ('CIO'), neemt het voortouw. Het bestuur en de CIO laten zich bij de uitvoering van deze taken bijstaan door een interne ICT-auditor.

De raad van commissarissen houdt toezicht op het bestuur. Als het bestuur onvoldoende aandacht besteedt aan cybersecurity, dient de raad van commissarissen het bestuur op deze omissie te wijzen. Bij de controle is een belangrijke rol weggelegd voor de auditcommissie. Deze commissie is verantwoordelijk voor het toezicht op het gebied van de beheersing van risico's en de naleving van de relevante regels. Zij dient ook te letten op risico's en regels in verband met cybersecurity.

Het is mogelijk dat uw bedrijf geen CIO, interne ICT-auditor of raad van commissarissen heeft. Dit verandert niets aan de verdeling van de verantwoordelijkheid: het bestuur is uiteindelijk verantwoordelijk voor cybersecurity. Als het bestuur expertise op het gebied van cybersecurity mist, verdient het aanbeveling om de hulp van een ICT-adviseur in te schakelen.

Bronnen: zie pagina 26

Binnen een bedrijf wordt regelmatig gewerkt met digitale persoonsgegevens en andere vertrouwelijke informatie. Om de vertrouwelijkheid van deze informatie te garanderen, worden de werknemers verplicht om hun computer te vergrendelen als zij hun werkplek verlaten. Deze regels worden duidelijk gecommuniceerd naar iedere nieuwe werknemer. Als een werknemer zijn computer ontgrendeld achterlaat, wordt hij daarop aangesproken.

De rol van werknemers

Een hoog niveau van cybersecurity kan slechts worden bereikt als het belang ervan is doorgedrongen tot de hele organisatie. U neemt daartoe organisatorische maatregelen.

- Uw bedrijf stelt beleidsregels of protocollen op het gebied van cybersecurity op. U verspreidt deze beleidsregels onder de werknemers en werkt ze, indien nodig, bij. U houdt toezicht op de naleving van deze regels.
- Uw bedrijf informeert en traint de werknemers die te maken hebben met ICT. De mate en wijze van de training zijn afgestemd op de functie en verantwoordelijkheden van de werknemer.
- Binnen uw bedrijf is het duidelijk wie er verantwoordelijk is voor de beveiliging en wie contactpersoon is voor vragen en meldingen omtrent de beveiliging.
- De werknemers weten bij wie zij beveiligingsincidenten kunnen en moeten melden. Zij worden gestimuleerd om dit consequent te doen, onder andere door het creëren van een cultuur van alertheid, door cybersecurity bespreekbaar te maken en door werknemers te 'belonen' voor het melden van beveiligingsincidenten (die zij niet zelf moedwillig hebben veroorzaakt). Er bestaat een procedure voor het melden van incidenten.
- De informatie over deze beveiligingsincidenten en de manier waarop en tijdspanne waarin zij zijn opgelost, wordt doorgegeven aan het management.

Bronnen: zie onder

Bronnen:

- Principe II.1, III.1, III.5 en V.III Monitoring Commissie Corporate Governance Code. De Nederlandse corporate governance code. Beginselen van deugdelijk ondernemingsbestuur en best practice bepalingen, 2009.
- Principe 1.2, 1.3, 1.4 en 1.5 Monitoring Commissie Corporate Governance Code. De Nederlandse corporate governance code. Voorstel voor herziening, 2016.
- Cyber Security Council, Cyber security guide for boardroom members, 2015. www.cybersecurityraad.nl/binaries/Cybersecurity_Guide%20UK_vdef_tcm56-79492.pdf.
- NEN-ISO/IEC, Information technology — Security techniques — Information security Management systems — Requirements (ISO/IEC 27001), 2013.

Bronnen ***De rol van werknemers***:

- NEN-ISO/IEC, Information technology — Security techniques — Information security Management systems — Requirements (ISO/IEC 27001), 2013.
- NEN-ISO/IEC, Information technology — Security techniques — Code of practice for information security controls (ISO/IEC 27002), 2013, onder andere paragraaf 7, 11.2 en 16.1.

SAMENVATTING

Ieder bedrijf dat gebruik maakt van ICT, heeft zorgplichten op het gebied van cybersecurity. Dit geldt ook als ICT slechts een ondersteunende rol speelt. Een gebrek in de cybersecurity kan uw bedrijfsvoering in de war gooien en reputatieschade veroorzaken. Een schending van de zorgplichten kan daarnaast tot aansprakelijkheid leiden. De vervulling van deze plichten is daarom zowel vanuit een economisch als een juridisch oogpunt van groot belang. Zij is uiteindelijk de verantwoordelijkheid van het bestuur of (bij kleinere bedrijven) de directeur.

Deze handreiking geeft de belangrijkste handvatten om de zorgplichten op het gebied van cybersecurity in te vullen. Zij is beknopt en dient slechts als een oriëntatie- en controlemiddel. De handreiking is nadrukkelijk geen vervanging voor professioneel advies. Indien uw bedrijf wordt geconfronteerd met de in deze handreiking opgenomen verplichtingen, doet u er goed aan om een gespecialiseerde jurist of beveiligingsspecialist in te schakelen.

Deze samenvatting geeft een overzicht van de belangrijkste zorgplichten op het gebied van cybersecurity. De plichten worden nader uitgewerkt in de handreiking.

CHECKLIST CYBERSECURITY

Persoonsgegevens zijn gegevens die betrekking hebben op een persoon. Een bedrijf dat deze gegevens verzamelt of op een andere manier verwerkt, heeft verschillende zorgplichten.

Checklist zorgplichten op grond van de verwerking van persoonsgegevens (Hoofdstuk 3):

- [ ] Uw bedrijf houdt rekening met cybersecurity voordat er wordt begonnen met de verwerking van de persoonsgegevens ('privacy-by-design', waaronder begrepen 'security-by-design').
- [ ] Uw bedrijf voert een risicoanalyse uit voordat er wordt begonnen met de verwerking van de persoonsgegevens. Als er grote risico's voor de betrokkenen bestaan, voert uw bedrijf een 'privacy impact assessment' uit.
- [ ] Uw bedrijf verzamelt en bewaart alleen noodzakelijke gegevens ('dataminimalisatie').
- [ ] Uw bedrijf beperkt de verspreiding van en de toegang tot de persoonsgegevens tot een minimum.
- [ ] Indien uw bedrijf persoonsgegevens door een andere partij laat verwerken, sluit het een overeenkomst. In deze overeenkomst wordt de andere partij onder andere verplicht om te zorgen voor cybersecurity.
- [ ] Uw bedrijf neemt passende technische en organisatorische beveiligingsmaatregelen.
- [ ] Uw bedrijf controleert regelmatig of de genomen maatregelen nog steeds voldoende zijn.
- [ ] Uw bedrijf heeft een adequate procedure voor het melden, oplossen en opvolgen van beveiligingsincidenten.
- [ ] Uw bedrijf meldt inbreuken in verband met persoonsgegevens ('datalekken') binnen 72 uur aan de Autoriteit Persoonsgegevens. Als er een hoog risico bestaat dat de inbreuk in verband met persoonsgegevens ongunstige gevolgen heeft voor de betrokkenen, meldt uw bedrijf de inbreuk ook aan de betrokkenen.
- [ ] Na een inbreuk in verband met persoonsgegevens neemt uw bedrijf maatregelen om de gevolgen te beperken en dergelijke inbreuken in de toekomst te voorkomen.
- [ ] Uw bedrijf houdt bij welke beveiligingsmaatregelen het neemt.
- [ ] Uw bedrijf houdt de verwerkingen van persoonsgegevens bij.
- [ ] Indien uw bedrijf bij de verwerking van de persoonsgegevens samenwerkt met andere partijen, zorgt u ervoor dat ook deze partijen de zorgplichten op het gebied van cybersecurity vervullen. Uw bedrijf sluit hiervoor een overeenkomst met de andere partijen.

Uw bedrijf is verantwoordelijk voor de door u gebruikte ICT. Dit wordt niet anders als de ICT slechts een ondersteunende rol speelt.

Checklist zorgplichten op grond van het gebruik van ICT (Hoofdstuk 4):

- [ ] Uw bedrijf maakt afspraken over cybersecurity met andere bedrijven in de keten.
- [ ] Uw bedrijf kent de risico's van het gebruik van de ICT.
- [ ] Uw bedrijf heeft op basis van een kosten-batenanalyse vastgesteld welke risico's acceptabel zijn.
- [ ] Uw bedrijf stelt een budget voor cybersecurity beschikbaar. Bij het vaststellen van dit budget houdt u rekening met de vastgestelde risico's.
- [ ] Voordat uw bedrijf gebruik gaat maken van nieuwe ICT, stelt het vast of de cybersecurity van deze ICT aan uw eisen voldoet.
- [ ] Uw bedrijf maakt duidelijke afspraken met de leveranciers van de door u gebruikte ICT.
- [ ] Uw bedrijf implementeert technische en organisatorische beveiligingsmaatregelen.
- [ ] Uw bedrijf neemt maatregelen om de ICT te beschermen tegen virussen en malware.
- [ ] Uw bedrijf heeft een systeem om ervoor te zorgen dat security patches snel en regelmatig worden uitgevoerd.
- [ ] Binnen uw bedrijf bestaan regels die zien op een veilig gebruik van ICT.
- [ ] Uw bedrijf beveiligt fysieke ICT en gegevensdragers tegen diefstal.
- [ ] Uw bedrijf beveiligt de toegang tot de ICT minimaal door middel van een wachtwoord en bij voorkeur met een tweefactorauthenticatie.
- [ ] Uw bedrijf voldoet aan relevante beveiligingsstandaarden, gedragscodes of certificeringsmechanismen.
- [ ] Uw bedrijf legt vast op welke manier de ICT is beveiligd.
- [ ] Uw bedrijf controleert of laat controleren of de cybersecurity nog steeds voldoende is.
- [ ] Uw bedrijf onderzoekt of laat onderzoeken of er beveiligingsincidenten hebben plaatsgevonden.
- [ ] Uw bedrijf controleert of laat controleren of de genomen maatregelen consequent zijn geïmplementeerd en worden nageleefd.
- [ ] Na een incident onderzoekt uw bedrijf het incident, hoe het heeft kunnen ontstaan en hoe ernstig de gevolgen zijn.
- [ ] Uw bedrijf legt beveiligingsincidenten vast.
- [ ] Uw bedrijf neemt zo snel mogelijk stappen om het incident op te lossen en (verdere) negatieve gevolgen te voorkomen of te beperken.
- [ ] Uw bedrijf onderzoekt of u het beveiligingsincident moet melden, bijvoorbeeld omdat dit is afgesproken in een overeenkomst of omdat er persoonsgegevens (Hoofdstuk 3) zijn gelekt.
- [ ] Na een incident neemt uw bedrijf maatregelen om vergelijkbare incidenten in de toekomst te voorkomen.

Als uw bedrijf producten of diensten met een ICT-toepassing aanbiedt, dient het ervoor te zorgen dat de cybersecurity in orde is.

Checklist zorgplichten in verband met producten of diensten met een ICT-toepassing (Hoofdst. 5):

- [ ] Het product is 'veilig genoeg' om normaal te worden gebruikt.
- [ ] De koopovereenkomst, de onderhandelingen en de marketing scheppen realistische verwachtingen. Zij stellen of suggereren niet dat de cybersecurity sterker is dan zij in werkelijkheid is of dat een product langer zal worden onderhouden dan in werkelijkheid het geval is.
- [ ] Het bedrijf waarschuwt indien de cybersecurity minder sterk is dan de koper mag verwachten of indien een bepaald product op korte termijn niet meer zal worden onderhouden.
- [ ] Koopovereenkomsten met andere bedrijven bevatten bepalingen die de rechten en plichten op het gebied van cybersecurity nader bepalen.
- [ ] Uw bedrijf maakt afspraken met zijn leveranciers en tussenpersonen. Hierin zijn de verplichtingen op het gebied van cybersecurity opgenomen en wordt de verantwoordelijkheid verdeeld in het geval van een gebrek in de beveiliging.
- [ ] Uw bedrijf stelt vast wie er belang heeft bij de cybersecurity van de door hem ontwikkelde en geleverde producten en diensten met een ICT-toepassing.
- [ ] Uw bedrijf kent de risico's van een gebrek in de cybersecurity van zijn product of dienst.
- [ ] Uw bedrijf stelt op basis van een kosten-batenanalyse vast welke risico's bij zijn product of dienst acceptabel zijn.
- [ ] Uw bedrijf maakt afspraken met de partijen van wie de cybersecurity mede afhankelijk is. Hierin zijn de verplichtingen op het gebied van cybersecurity opgenomen en wordt de verantwoordelijkheid verdeeld in het geval van een gebrek in de beveiliging.
- [ ] Uw bedrijf houdt al bij de ontwikkeling rekening met cybersecurity (security-by-design).
- [ ] Binnen uw bedrijf wordt de ontwikkeling van goed beveiligde producten of diensten door middel van organisatorische maatregelen gestimuleerd.
- [ ] Uw product of dienst heeft een ingebouwde technische beveiliging.
- [ ] Uw product of dienst voldoet aan relevante beveiligingsstandaarden, gedragscodes of certificeringsmechanismen.
- [ ] Uw bedrijf neemt maatregelen om de onbevoegde aanpassing van de ICT of de uitschakeling van de beveiliging tegen te gaan.
- [ ] Uw bedrijf houdt aanpassingen van het product of de dienst in een logboek bij.
- [ ] Uw bedrijf houdt bij op welke manieren het product of de dienst beveiligd is.
- [ ] Uw bedrijf controleert de cybersecurity van het product of de dienst regelmatig.
- [ ] Uw bedrijf werkt gedurende een bepaalde periode de cybersecurity bij als zij niet langer in orde is.
- [ ] Uw bedrijf gebruikt een systeem om security patches door te voeren naar de gebruikers.
- [ ] Uw bedrijf stimuleert de gebruikers om beveiligingsincidenten door te geven. Deze incidenten worden onderzocht. U neemt maatregelen om vergelijkbare incidenten in de toekomst te voorkomen.
- [ ] Uw bedrijf biedt de gebruikers ondersteuning bij beveiligingsincidenten.
- [ ] De gebruikers (kunnen) worden gewaarschuwd als de cybersecurity niet op orde is.

Voor alle bedrijven geldt dat zij cybersecurity binnen hun bedrijf moeten stimuleren.

Checklist zorgplichten in verband met de organisatie van uw bedrijf (Hoofdstuk 6):

- [ ] Uw bedrijf stelt beleidsregels of protocollen op het gebied van cybersecurity op. U verspreidt deze beleidsregels onder de werknemers en werkt ze, indien nodig, bij. U houdt toezicht op de naleving van deze regels.
- [ ] Uw bedrijf informeert en traint de werknemers die te maken hebben met ICT. De mate en wijze van de training zijn afgestemd op de functie en verantwoordelijkheden van de werknemer.
- [ ] Binnen uw bedrijf is het duidelijk wie er verantwoordelijk is voor de beveiliging en wie contactpersoon is voor vragen en meldingen omtrent de beveiliging.
- [ ] De werknemers weten bij wie zij beveiligingsincidenten kunnen en moeten melden. Zij worden gestimuleerd om dit consequent te doen, onder andere door het creëren van een cultuur van alertheid, door cybersecurity bespreekbaar te maken en door werknemers te 'belonen' voor het melden van beveiligingsincidenten (die zij niet zelf moedwillig hebben veroorzaakt). Er bestaat een procedure voor het melden van incidenten.
- [ ] De informatie over deze beveiligingsincidenten en de manier waarop en tijdspanne waarin zij zijn opgelost, wordt doorgegeven aan het management.

CSR Cyber Security Raad

Colofon

Deze handreiking is in opdracht van de Cyber Security Raad geschreven door dr. Pieter Wolters en Prof. dr. Corjo Jansen van de Radboud Universiteit, Onderzoekcentrum Onderneming & Recht.

De auteurs bedanken de CSR begeleidingscommissie voor hun waardevolle commentaar: Voorzitter prof. dr. Lokke Moerel (Tilburg University, Morrison & Foerster LLP, Cyber Security Raad). Leden: Liesbeth Holterman (Nederland ICT), Danny ter Laak (Parket-Generaal, Openbaar Ministerie), Reinout Rinzema (Ventoux Advocaten), Peter van Schelven (BIJ PETER – Wet & Recht), Ronald Verbeek (CIO Platform Nederland) en Maurice Wessling (Consumentenbond). Daarnaast bedanken zij Elly van den Heuvel (Cyber Security Raad), Eline Attema (Cyber Security Raad), Martin Bobeldijk (Cyber Security Raad), Myrthe Bronsdijk, Mireille Hildebrandt en Paul Verbruggen voor hun onmisbare ondersteuning.

Opmaak: BKB, Drukwerk: Xerox/OBT, Concept en advies: Turnaround Communicatie

Nijmegen, februari 2017

www.cybersecurityraad.nl

CSR Cyber Security Raad