Rijksoverheid

Voorkomen is beter dan genezen

Een handleiding economische veiligheid voor ondernemers

Een brochure door het Ondernemersloket Economische Veiligheid
in opdracht van het Ministerie van Economische Zaken

www.rvo.nl/olev

Inhoud

Inleiding

Voor u ligt de Handleiding Economische Veiligheid van de Rijksoverheid, samengesteld voor mkb'ers, start-ups en scale-ups die actief zijn in de internationale wereld van kennisintensieve vakgebieden en sleuteltechnologieën.[1] Let op: dit document is bedoeld om digitaal te raadplegen. Er wordt veel gebruikgemaakt van aanklikbare links naar bronnen van derden.

Wat is economische veiligheid?

Economische veiligheid gaat over het versterken en beveiligen van vitale, waardevolle en innovatieve bedrijvigheid in Nederland. Tegen oneerlijke concurrentie, cyber, diefstal, dwang, beïnvloeding door andere staten en geopolitieke schokken. Veel economische veiligheidsrisico's hebben te maken met kennisintensieve producten of diensten die op Nederlandse bodem worden ontwikkeld, zoals onderzoek of ontwikkeling van cruciale technologie. Economische veiligheid gaat ook over risico's die uw economische belangen kunnen schaden, en daarnaast impactvolle consequenties kunnen hebben voor de Nederlandse (economische) belangen of nationale veiligheid.

Economische veiligheid voor ondernemers

Economische veiligheid is dus ook belangrijk voor u, omdat uw bedrijf interessant is voor anderen – óók partijen met kwade bedoelingen. Denk bijvoorbeeld aan staten die zich dreigend opstellen tegen Nederland of zijn bondgenoten, concurrenten of criminelen. Deze kwaadwillende partijen kunnen uw onderneming op zowel een legale als een illegale manier beïnvloeden en schaden: zichtbaar én onzichtbaar. Maar in al deze gevallen zijn de gevolgen voor u vergelijkbaar. U verliest uw unieke product en loopt schade op aan uw marktpositie of reputatie. Omdat een weerbare economie van belang is voor onze veiligheid, speelt de Rijksoverheid een actieve rol bij economische veiligheid.[2] De Rijksoverheid:

- informeert bedrijven;
- biedt handelingsperspectief; en
- stelt waar nodig kaders.

Omgaan met kansen en risico's

Uw onderneming ontwikkelen, internationaal zakendoen, inkopen, aanbesteden en fuseren zijn maar een paar aspecten die horen bij internationaal ondernemen. U bent op zoek naar kansen, maar bent tegelijkertijd waakzaam voor de risico's. Deze Handleiding Economische Veiligheid behandelt de verschillende risico's op het gebied van economische veiligheid en ondernemerschap. De handleiding biedt handvatten, zodat u zo zelfstandig mogelijk de eventuele risico's kunt aanpakken. Daarnaast geeft de handleiding mee wat de Rijksoverheid voor u als ondernemer kan betekenen. Ook leest u in deze handleiding de basis van de wettelijke kaders rondom economische veiligheid, zodat u goed weet waar u rekening mee moet houden bij de doorontwikkeling van uw onderneming.

Meer weten over economische veiligheidsrisico's?

Heeft u als ondernemer vragen over economische veiligheidsrisico's? Dan kunt u altijd terecht bij het Ondernemersloket Economische Veiligheid. Stel uw vraag via veiligondernemen@rvo.nl.
Het Ondernemersloket Economische Veiligheid beantwoordt uw vraag of brengt u in contact met de juiste overheidsinstantie.

[1] Zie voor een overzicht van het Nederlandse sleuteltechnologielandschap en definities omtrent bijbehorende sleuteltechnologieën het rapport Herijking sleuteltechnologieën 2023 van TNO en NWO.

[2] Publiek gefinancierde kennisinstellingen hebben te maken met vergelijkbare uitdagingen. Zij kunnen terecht bij het Loket Kennisveiligheid. Vanuit het Loket Kennisveiligheid is er de *Nationale Leidraad Kennisveiligheid: Veilig Internationaal Samenwerken* voor kennisinstellingen. Deze leidraad bevat ook relevante informatie en handelingsperspectieven voor bedrijven.

1. Risicobeheersing

Veilig internationaal samenwerken en due diligence

Samenwerken, zowel binnen Nederland als internationaal, is essentieel voor uw bedrijf en biedt kansen. Maar het kan ook risico's met zich meebrengen. Zo verhoogt een samenwerking het aantal verbindingen dat uw bedrijf heeft met externe partijen, waarmee zij meer toegang kunnen krijgen tot uw kennis, technologie en informatiehuishouding. Ook kwaadwillende partijen kunnen de samenwerking met uw onderneming opzoeken, om zo toegang te krijgen tot uw kennis. Of om deze in te zetten voor ongewenste doeleinden. Voordat u een samenwerking aangaat is het daarom belangrijk dat u weet met wie u écht te maken heeft. U verkleint dan de kans op ongewenste kennisoverdracht en misbruik van uw kennis.

Casus
De Nederlandse hightech-onderneming A ontwikkelt gezichtsherkenningssoftware. Het idee achter de software is dat het gebruikt kan worden door sociale media-apps, om de kwaliteit van zogenaamde gezichtsfilters te verbeteren. De hightech-onderneming wordt benaderd door een bedrijf waar het nog niet eerder van gehoord heeft, afkomstig uit land B. Het bedrijf presenteert zich als een opkomend sociale media-platform en legt uit hoe het gebruik wil maken van de software van onderneming A, om ook voor hun sociale media gebruik te kunnen maken van leuke gezichtsfilters. Zij stellen voor de dienst te willen afnemen. Ook bieden zij aan om diagnostische gegevens van hun gebruikers terug te geven aan hightech-onderneming A, om de software nóg efficiënter te maken.

Hightech-onderneming A is zich ervan bewust dat de gezichtsherkenningssoftware naast het creëren van grappige filters op sociale media, potentieel óók misbruikt kan worden. Zo kunnen autoritaire regimes de hoogontwikkelde software bijvoorbeeld gebruiken om personen op te sporen op het internet.

Zoals altijd doet hightech-onderneming A een verkennend onderzoek via openbare bronnen. En zo vindt hightech-onderneming A dat het bedrijf uit land B actief wordt gesteund door de autoritaire regering van land B. Het is algemeen bekend dat deze regering zich veelvuldig schuldig maakt aan de onderdrukking van bepaalde bevolkingsgroepen in land B. Hightech-onderneming A ziet dat er een directe connectie is tussen de overheid van land B en het 'opkomende sociale media platform' uit land B. Hightech-onderneming A ziet een te groot risico op misbruik van hun software voor het schenden van mensenrechten in land B. Met als gevolg dat export van het product van hightech-onderneming A zeer onwenselijke gevolgen zou kunnen hebben. Het bedrijf slaat daarom het voorstel om met het bedrijf uit land B samen te werken af.

Veilig internationaal samenwerken en due diligence: wat kunt u doen?
Door het beheersen van het extra risico dat samenwerking met zich meebrengt, helpt u uw bedrijf veilig te groeien. Het uitvoeren van *due diligence* naar potentiële partners is een essentiële stap om de risico's van samenwerking met hen te beoordelen. Ook met behulp van publiek beschikbare informatie kunt u al veel te weten komen over andere partijen. Voordat u een samenwerking of partnerschap aangaat met een potentiële partner, is het verstandig om uzelf onder andere de onderstaande vragen te stellen.

- Is de partner verbonden aan een overheid? Denk bijvoorbeeld aan staatsgeleide bedrijven of instellingen.
- Is de partner verbonden aan het leger of de defensie-industrie?
- Wie is de 'ultimate beneficial owner' (UBO) van de organisatie? De UBO is de eigenaar, een belanghebbende, of de persoon die zeggenschap heeft.
- Heeft de organisatie een aantoonbare reputatie in de sector waar het om gaat? Als expertise ontbreekt of onduidelijk is hoe de beoogde samenwerking aansluit op de normale activiteiten van de partner, dan is dat een reden tot alertheid.
- Wat voor activiteiten ondernemen de partners nog meer? Zijn zij verbonden aan meerdere bedrijven/instellingen/organisaties?
- Welke intellectuele eigendomsrechten (IE-rechten) hebben potentiële partners geregistreerd in welke landen? Als u dit weet kunt u een indruk krijgen van de belangen van deze potentiële partner. U kunt dit onderzoeken in octrooi-, model- en merkendatabanken zoals Espacenet, DesignView en TMView. Octrooicentrum Nederland kan u hierbij ondersteunen.

- Verloopt het contact via een andere entiteit (andere naam of ander adres) dan de potentiële partnerorganisatie zelf, of verandert dit tijdens het samenwerkingsproces?
- Geeft de partner geen duidelijke antwoorden op vragen over de beoogde toepassing van de onderzoeksuitkomsten? Of maakt de partner om onduidelijke redenen bezwaar tegen bepalingen die standaard zijn in overeenkomsten, of stelt de partner excessieve geheimhoudingsbepalingen voor?

Daarnaast kunt u bij potentiële investeerders, *suppliers* of partners ook letten op de volgende mogelijke risicofactoren:

- Er is weinig tot geen informatie te vinden over de opdrachtgever of financier, bijvoorbeeld door het ontbreken van een website.
- De partner maakt gebruik van een entiteit (andere naam of ander adres) die niet gebruikelijk is voor dit soort financiering.
- De opdrachtgever of financier stelt uitzonderlijk grote bedragen beschikbaar of bijzonder gunstige financieringsvoorwaarden voor en vraagt daar bijna niets voor terug.
- De opdrachtgever of financier wil niet dat resultaten worden gepubliceerd, stelt uitzonderlijk strenge intellectuele eigendomseisen of eist geheimhouding voor eindgebruikers en specificaties.

Om uzelf voor te bereiden op een eventuele samenwerking is het ook verstandig om contact te leggen met de Nederlandse ambassade in het land van de partner met wie u wilt samenwerken. De plaatselijke ambassade heeft vaak een goed kennisnetwerk in het specifieke land waar u wilt zakendoen. De belangrijkste vraag is hierbij of de ambassade bekend is met de potentiële partner. Daarnaast zijn er nog meer overheidsnetwerken die u kunnen ondersteunen als u wilt zakendoen in het buitenland. Bekijk de pagina Ondernemen in het buitenland voor meer informatie over de mogelijkheden voor ondersteuning.

Intellectueel Eigendom

Binnen uw bedrijf bouwt u waardevolle kennis op. Dit kan kennis zijn die publiek is gemaakt, maar dit kan ook kennis zijn die u binnen uw bedrijf heeft opgebouwd, en die zo waardevol is dat deze u een voordeel geeft in de markt. Hierover kunt u beslissen of u deze geheim wilt houden, of bijvoorbeeld alleen onder voorwaarden wilt delen. Daarnaast bezit u mogelijk uitvindingen of andere creatieve uitingen waarop u wijzigen in intellectuele eigendomsrechten (IE-rechten) heeft aangevraagd, of waarover u nog moet beslissen of u hier IE-rechten op wilt aanvragen zodat u dit competitieve voordeel behoudt.

Statelijke actoren of concurrenten kunnen eropuit zijn om bovenstaande te bemachtigen, om zo hun technologische capaciteiten te versterken ten koste van uw onderneming en groei. Dit kunnen zij zowel digitaal als fysiek proberen te doen.

Casus
Eindelijk was het moment daar! De CEO van tech-start-up A kon haar geluk niet op toen zij bericht ontving dat hun beoogde partner bedrijf B, gevestigd in land C, akkoord wilde gaan met een formele samenwerking in land C. In deze samenwerking zou de R&D plaatsvinden in Nederland, maar het productieproces in land C. Of de CEO van tech-start-up A volgende week naar land C wilde komen om daar formeel de samenwerking te ondertekenen? De CEO van tech-start-up A lichtte alvast haar investeerders in. Deze waren blij te horen dat hun investeringen zich nou eens zouden gaan uitbetalen, na al die jaren van geduld, tijd en moeite.

Het moment van ondertekening was dan nu eindelijk daar. Op de bovenste verdieping van een imposante wolkenkrabber in het zakendistrict van de hoofdstad van land C kwamen de ingewijden van tech-start-up A en bedrijf B samen. Het banket stond al klaar en op de centrale tafel lag een stapel documenten. De CEO van tech-start-up A nam plaats en bekeek de documenten – sommigen kwamen haar bekend voor, maar er lagen ook nieuwe documenten bij welke gingen over de uitwisseling van technologische kennis en het delen van de rechten rondom deze technologie. Ze keek met een vragende blik richting de vertegenwoordigers van bedrijf B. "Waar komt dit vandaan?" Het antwoord van bedrijf B was weinig geruststellend: "Onze excuses mevrouw, maar wij hebben ook net pas gehoord dat buitenlandse partijen verplicht zijn om in hun rechten omtrent hun technologische kennis met ons te delen als we in land C een zakelijke samenwerking aangaan."

Het zweet brak uit bij de CEO van tech-start-up A: "Wat nu? Ons IE is het bestaansrecht van onze onderneming, als we deze afstaan hebben we niks meer dat ons uniek maakt. Kan ik nog weglopen? En wat zullen onze investeerders hiervan vinden?"

Wat u kunt doen om uw intellectueel eigendom te beschermen

- Begin met het identificeren van uw meest waardevolle bezittingen, technologie, kennis, processen en data die uw bedrijf uniek en competitief maken – uw kroonjuwelen. Raadpleeg *Economisch Weerbaarder in 4 Stappen: Een Quick Guide voor Ondernemers* op www.rvo.nl/olev voor meer informatie over het identificeren van uw kroonjuwelen en de bijbehorende risico's.
- Hoewel er internationale afspraken bestaan, verschillen wet- en regelgeving rondom IE-rechten. Ook binnen de EU. Bespreek samen met de Rijksoverheid, bijvoorbeeld met Innovatie-attachées en het Octrooicentrum Nederland, hoe u hier het beste mee om kunt gaan. U kunt ook hulp zoeken bij een advocatenkantoor gespecialiseerd in het land van samenwerking. Leg ook contact met de Nederlandse ambassade in het land waar u aan de slag wilt gaan met uw product. De plaatselijke ambassade heeft vaak een goed kennisnetwerk in het specifieke land waar u wilt zakendoen. Doe hier uw voordeel mee.
- Het hebben van geregistreerde IE-rechten betekent niet dat u geen risico meer loopt. U moet voortdurend monitoren of uw IE-rechten worden geschonden. Naast uw opgebouwde kennis die u gepubliceerd heeft, beschikt u mogelijk ook over kennis die u niet of alleen onder voorwaarden wilt delen. Om deze kennis geheim te houden, zult u verschillende maatregelen moeten nemen. Denk aan de rol die uw medewerkers hierin spelen. Hen bewustmaken van de waarde van deze kennis en hen te leren hoe zij hiermee om moeten gaan is van groot belang. Ook spelen intellectueel eigendomsclausules in diverse contracten een rol bij het beschermen van uw kennis, zoals arbeidscontracten en samenwerkingsovereenkomsten.
- Zorg voor goede relaties en communicatie met uw leveranciers en distributeurs en maak eventueel gebruik van meerdere leveranciers voor verschillende onderdelen voor uw innovatie. Zowel online als offline kan kennis worden opgedaan waarvan u niet wilt dat derden deze inzien.

- In samenwerkingstrajecten worden vaak uitgebreide afspraken gemaakt over vertrouwelijke informatie. Maar deelnemers weten vaak niet hoe je daarmee moet omgaan. Dat kan leiden tot het lekken van kennis tijdens deze samenwerking. Het is daarom belangrijk om tenminste de eigen kennis te categoriseren en te labelen. Onderaan deze pagina vindt u een voorbeeld van hoe u uw eigen kennis kan categoriseren en labelen.
- Er wordt in consortia en samenwerkingstrajecten wel vaak afgesproken dat achtergrond-IE (de kennis die wordt ingebracht) eigendom blijft van de oorspronkelijke eigenaren. Maar er wordt vaak niet goed genoeg aangegeven welke IE en technische kennis alle betrokken partijen al hadden of inbrengen. Ook dit vraagt om goede voorbereiding binnen het eigen bedrijf: wat deelt u wel binnen het specifieke project en wat juist niet?
- Een ander aspect zijn de gemaakte afspraken rondom gegenereerde resultaten. Vaak wordt er afgesproken dat de resultaten eigendom zijn of worden van de partij die ze heeft gegenereerd, maar wordt er geen werkwijze afgesproken over hoe de inbreng aan innovaties wordt bijgehouden. Hierdoor kan er een gezamenlijk recht op gegenereerde resultaten ontstaan. Maak daarom vooraf duidelijke afspraken over de werkwijze waarmee de inbreng aan innovaties wordt bijgehouden.

Een algemene tip voor bovenstaande punten: plaats de afspraken over IE-toegang voor, tijdens en na het project in een overzichtelijke tabel. Voor meer informatie over het maken van samenwerkingsafspraken voor bescherming van uw intellectueel eigendom kunt u terecht bij Octrooicentrum Nederland.

Als u een uitvinding octrooieert, wordt dat gepubliceerd. Wilt u dat niet? Dan is het in sommige gevallen een optie om de uitvinding als bedrijfsgeheim te beschouwen. Een andere, interessante mogelijkheid is de combinatie van een octrooi en bedrijfsgeheim. U vraagt dan octrooi aan op het deel van de uitvinding dat te zien of te achterhalen is, maar houdt de bijbehorende kennis geheim.

Kiest u ervoor bedrijfsgeheimen te houden: maak dan onderscheid in de mate van vertrouwelijkheid. Grotere bedrijven gebruiken hiervoor categorieën van vertrouwelijkheid zoals onderstaande voorbeeld.
- **Publiek**: Generieke of algemene kennis waar andere bedrijven ook over beschikken. Deze kennis wordt vrij gedeeld.
- **Beperkt**: De eerste categorie van bedrijfsgeheimen. U bent bereid om deze kennis te delen als daar iets voor u tegenover staat. Dit kunnen bijvoorbeeld uitvindingen zijn waar octrooien op rusten en die u bereid bent te delen voor een licentievergoeding.
- **Vertrouwelijk**: De tweede categorie van bedrijfsgeheimen bevat informatie die u niet bereid bent om te delen. Deze kennis geeft u een belangrijke voorsprong op concurrentie op de lange termijn. Daarom geeft u deze kennis in principe niet prijs. Dit zijn bijvoorbeeld algoritmes, ideeën die u in de toekomst mogelijk nog wilt gaan ontwikkelen en/of octrooieren, of commerciële gegevens zoals klantenlijsten, kortingspercentages of omzetten per klant.
- **Topgeheim**: De derde categorie bedrijfsgeheimen is een zware variant: kennis die zo geheim is dat (vrijwel) geen enkele medewerker het gehele plaatje kent. De kennis is topgeheim en gefragmenteerd. Een voorbeeld hiervan is het recept van Coca-Cola.

Melding doen van (vermoedens van) spionage of ongewenste beïnvloeding?

Neem dan contact op met de AIVD. Beveiligingsincidenten met (mogelijke) aantasting van zogenaamde 'Te Beschermen Belangen van Defensie' moeten door ABDO-bedrijven gemeld worden aan het Bureau Industrieveiligheid van de MIVD.

Meer weten over octrooien?
- Voor meer informatie over de verschillende manieren om uw uitgewerkte ideeën, concepten en uitvindingen te beschermen bekijkt u de brochure over de basis van intellectueel eigendom van Octrooicentrum Nederland.
- Informatie over geheimhouding vindt u op de website van Rijksdienst voor Ondernemend Nederland (RVO).
- Andere vragen of een afspraak maken met een octrooiadviseur? Neem dan tijdens kantooruren contact op met Octrooicentrum Nederland op telefoonnummer 088 042 40 02 of stuur een e-mail naar octrooicentrum@rvo.nl.

Buitenlandse dienstreizen

Bij het reizen naar het buitenland kunnen uw bedrijf en vertegenwoordigers van uw bedrijf risico's lopen. Zo kunnen zij bespioneerd worden door kwaadwillende statelijke actoren of concurrenten. Ook kunnen apparaten en datadragers met daarop gevoelige informatie gestolen worden. Hierdoor kunt u bijvoorbeeld uw IE kwijtraken, kunt u gechanteerd worden, kan er een datalek ontstaan of kan uw bedrijf imagoschade oplopen.

Casus
De vertegenwoordiger van bedrijf A, een tech-start-up, reist af naar land B. In land B zal de vertegenwoordiger een internationale conferentie bijwonen en ook werk van zijn bedrijf presenteren. Bedrijf A hoopt zo potentiële investeerders voor hun start-up te werven, dat is hard nodig als ze willen groeien.

Eenmaal geland in land B, staat de vertegenwoordiger in de rij voor de paspoortcontrole. Het paspoort is in orde. Dan wordt hem door de douane gevraagd zijn laptop en datadragers af te geven voor controle. De vertegenwoordiger is hier niet over te spreken. Er staat namelijk zeer gevoelige informatie op de laptop en datadragers over het unieke idee waarmee bedrijf A groot wil worden. De douane geeft aan geen reden te hoeven opgeven voor een doorzoeking en dat dit routine is, maar dat de gefrustreerde reactie van de vertegenwoordiger wel erg verdacht is. Ze nemen de laptop en datadragers tijdelijk in beslag voor onderzoek. Ze geven aan contact met de vertegenwoordiger op te nemen als het onderzoek is afgerond.

Een week later wordt de vertegenwoordiger gebeld door de douane: het onderzoek is afgerond en er is niks verdachts gevonden. De vertegenwoordiger mag zijn spullen weer komen ophalen, maar houdt een knagend gevoel over aan het voorval. Wat als de douane alles heeft kunnen lezen en misschien zelfs gekopieerd heeft? En wie heeft het nog meer kunnen inzien?

Wat u kunt doen tegen de risico's bij buitenlandse dienstreizen
Onderneem de onderstaande acties voordat u op reis gaat:

- Leg contact met de Nederlandse ambassade in het land van bestemming. Stel hen op de hoogte van uw plannen en vraag om praktische steun en advies.
- Als u vermoedt dat er reële risico s verbonden zijn aan het aankomende buitenlandbezoek, ga dan binnen uw organisatie na of u een tijdelijke laptop en telefoon kunt meenemen op reis. U verkleint hiermee het risico dat uw standaard-werkapparatuur, inclusief de gegevens hierop, terechtkomen bij hackers of buitenlandse inlichtingendiensten.
- Als u uw eigen apparaten meeneemt, zorg er dan voor dat hier zo min mogelijk gevoelige gegevens op staan.
- Hoognodige bestanden kunt u ook in de cloud opslaan. Zo voorkomt u dat u deze gegevens op een apparaat mee moet nemen.
- Zorg ervoor dat al uw apparaten privacyschermen hebben. Dit is speciale folie waardoor mensen niet kunnen meekijken met wat er op uw scherm gebeurt.
- Zorg ervoor dat op al uw apparaten antivirussoftware is geïnstalleerd en dat deze periodiek scans uitvoert. Pas de standaardinstellingen van uw apparatuur aan door de volgende maatregelen:
  - zet het automatisch zoeken naar netwerken en daarmee verbinden uit;
  - zorg dat andere verbindingsdiensten zoals bluetooth en GPS (lokalisatiediensten) zoveel mogelijk uitgeschakeld zijn;
  - zet de automatische beeldschermvergrendeling bij inactiviteit van uw apparaat aan en zorg dat u alleen toegang tot uw apparaten krijgt met een inlogcode;
  - installeer de meest recente softwareversies op al uw apparaten. Denk hierbij zowel aan de besturingssystemen als de geïnstalleerde software.
- Zorg dat u thuis of op kantoor beschikt over een back-up van de belangrijke gegevens die u meeneemt op reis. Dan bent u die in het geval van diefstal niet kwijt.
- Gebruik geen losse datadragers, zoals een USB-stick, omdat het makkelijk is om deze te verliezen of te stelen. Kiest u er toch voor om losse datadragers te gebruiken, zorg dan dat u:
  - hier zo min mogelijk gevoelig materiaal op plaatst;
  - een versleutelde gegevensdrager gebruikt met een pincode voor toegangsbeveiliging.

Tijdens uw reis

- Vervoer de apparaten die u meeneemt altijd in uw handbagage en niet in de koffer die u incheckt.
- Maak geen gebruik van openbare laadstations. Aanvallers zijn in staat om USB-oplaadpunten zo aan te passen dat kwaadaardige software wordt geïnstalleerd. Of dat gevoelige gegevens van het aangesloten apparaat automatisch worden gekopieerd, ook wel *juice jacking* genoemd. Gebruik altijd een wandstopcontact of een eigen powerbank.
- Maak geen gebruik van openbare internetverbindingen, zoals vaak beschikbaar bij restaurants, hotels, beurzen en congressen.
  - Maakt u toch gebruik van openbare internetverbindingen? Gebruik dan een Virtual Private Network (VPN). Zorg dat u deze voorafgaand aan uw reis nog in Nederland heeft aangeschaft en geïnstalleerd, aangezien in sommige landen websites van bepaalde VPN-dienstenaanbieders worden geblokkeerd.
- Wees u ervan bewust dat uw telefoon gebruikt kan worden om u af te luisteren. Zet daarom uw telefoon uit en haal de batterij er zo mogelijk uit als u fysiek een vertrouwelijk gesprek voert.
- Laat op reis nooit uw apparaten onbeheerd achter, zelfs niet in de kluis van het hotel. Draag als het mogelijk is uw apparaten altijd bij u.
- Pas op met geschenken en goodie bags die u ontvangt van contacten, zeker als deze gadgets bevatten zoals USB-sticks. Hier kan kwaadaardige software op staan. Gebruik dergelijke apparatuur nooit.
- Deel niet teveel informatie over uw verblijf op sociale media wanneer u op zakenreis bent. Criminelen thuis kunnen hiervan eventueel gebruikmaken om bij u thuis in te breken. Kwaadwillende partijen in het land van uw reis kunnen deze informatie gebruiken om u te schaduwen.

Meer weten over veiligheidsrisico's bij reizen naar het buitenland?

Bekijk voordat u op reis gaat:

- het Dreigingsbeeld Statelijke Actoren (DBSA 2). Het DBSA 2 bevat een analyse van de AIVD, MIVD en NCTV over dreigingen die uitgaan van specifieke staten. Ook bevat het informatie over hoe deze dreigingen tot uiting kunnen komen.
- de kleurcode per land van het ministerie van Buitenlandse Zaken.
- de AIVD-brochure over reizen naar het buitenland.
- de pagina Onderweg en op Reis van het Digital Trust Center met informatie over maatregelen die u kunt nemen als u veilig op reis wilt gaan.

Inkoop van buitenlandse producten en diensten

Bij een vrijemarkteconomie hoort ook het inkopen van buitenlandse producten en diensten. Hier kunnen ook veiligheidsrisico's aan verbonden zijn. Dit hangt af van het type product of dienst dat wordt geleverd, de opdrachtgever en het bedrijf dat de opdracht wordt gegund. Afhankelijk hiervan kan er een risico bestaan dat:

- hoogwaardige of gevoelige kennis of informatie weglekt;
- vitale bedrijfsprocessen worden verstoord; of
- strategische afhankelijkheden ontstaan.

Denk bijvoorbeeld aan het inkopen van nieuwe digitale infrastructuur, clouddiensten en software, of de vervanging van systemen waar veel persoonsgegevens op staan. Daarnaast is voor sommige opdrachten fysieke toegang tot gevoelige locaties nodig. Het is dus goed om na te denken over maatregelen om risico's te beheersen. Bedrijven kunnen namelijk bewust of onbewust gecontroleerd worden door een statelijke actor. Deze actor kan via het bedrijf proberen om de geopolitieke, strategische en economische macht van een land te vergroten door het verkrijgen van bijvoorbeeld informatie, geld, middelen of grondstoffen. In sommige landen is ook wetgeving van kracht die private partijen verplicht om samen te werken en data te delen met de overheid uit het land van herkomst.

Mogelijke risico's die kunnen ontstaan:

- Verstoring van de continuïteit van de vitale infrastructuur. Dit zorgt voor ernstige verstoring van de Nederlandse samenleving, bijvoorbeeld wanneer het betalingsverkeer of de telecommunicatie wegvalt.
- Het weglekken van hoogwaardige kennis of vertrouwelijke informatie.
- Sterke afhankelijkheid van partijen en landen met andere geopolitieke belangen. Exportbeperkende maatregelen of politieke druk, dreiging en manipulatie zijn niet ondenkbaar.

U wilt natuurlijk liever voorkomen dat uw bedrijf terechtkomt in een dergelijke, onveilige situatie. Maar hoe voorkomt u dit?

Casus

Bedrijf A, een B2B-groothandel in randapparatuur voor computers, ontvangt voor het nieuwe jaar een nieuwe prijsopgave van hun cloud-storage-provider. De prijzen gaan weer omhoog. Na een kort belletje weet bedrijf A ook waarom: de energieprijzen gaan omhoog, dus ook de prijzen voor het gebruik van data-centra. Bedrijf A laat het hier niet bij zitten en gaat op zoek naar een nieuwe cloud-storage-provider die goedkoper is. Bedrijf A heeft namelijk een groot klantenbestand, dat veilig moet worden opgeslagen. Maar het liefst wel zo goedkoop mogelijk. Na een zoektocht komen ze uit bij een cloud-storage-provider in het buitenland, in land B. De cloud-storage-provider is de helft goedkoper in vergelijking tot de provider in Nederland. Bij een interne bespreking binnen bedrijf A over de mogelijke overstap, ontstaat vervolgens grote commotie. De jurist in dienst van bedrijf A die zich bezighoudt met de privacy, wijst het bedrijf erop dat volgens de lokale wetgeving in land B de inlichtingendiensten daar toegang hebben tot alle gegevens opgeslagen in datacentra in land B. Dus ook de gegevens van bedrijf A als dat ervoor kiest de gegevens in de datacentra in land B op te slaan. De inlichtingendienstendiensten uit land B krijgen zo mogelijk inzicht in welke Nederlandse organisaties gebruikmaken van welke randapparatuur. Dat zou zeer onwenselijk zijn. Uiteindelijk wordt binnen bedrijf A afgezien van het overstappen naar een nieuwe provider en besluit het bij de originele duurdere, maar beter betrouwbare cloud-storage-provider te blijven.

Hoe kunt u de risico's rondom inkoop en aanbestedingen herkennen en verminderen?

Wij raden u aan om gebruik te maken van de Toolbox veilig inkopen, opgesteld in 2024 door de Rijksoverheid. Met deze toolbox maakt u gebruik van 3 instrumenten:

- QuickScan: hierin staan vragen die u helpen met het bepalen of er een gevaar is voor de nationale veiligheid bij een inkoopopdracht of aanbesteding.
- Risicoanalyse: als er risico's uit de QuickScan komen, doe dan een risicoanalyse om vast te stellen welke risico's dit precies zijn en hoe u ze kunt wegnemen of verminderen.
- Quickguide: geeft u een overzicht van het aanbestedingsrechtelijk handelingsperspectief om risico´s te beheersen.

Stel ook kritische vragen zoals:

- Weet de opdrachtnemer wat hij of zij moet doen bij beveiligingsincidenten en voldoen zijn of haar eventuele onderaannemers aan de beveiligingseisen?
- Kan er een strategische afhankelijkheid ontstaan?
- Kan er gevoelige informatie (zoals persoonsgegevens) weglekken?
- Kan de continuïteit van de levering in gevaar komen en wat zou dit voor gevolgen hebben?
- Komt het personeel in aanraking met gevoelige informatie?
- Wat gebeurt er met de informatie na beëindiging van het contract?

Het voor uzelf beantwoorden van onder andere de bovenstaande vragen kan u helpen u beter voor te bereiden op de mogelijke veiligheidsrisico's bij het inkopen in het buitenland.

Vestigingen in het buitenland

Om verschillende redenen kan het interessant zijn voor uw onderneming om zich (ook) te vestigen in het buitenland. Maar dit kan ook risico's met zich meebrengen. Zo kunt u minder zicht krijgen op het doen en laten van medewerkers die mogelijk wel een groot inzicht in uw (geheime) bedrijfsprocessen hebben. Ook kan het de uitwisseling van informatie en goederen tussen uw onderneming, leveranciers en afnemers bemoeilijken. Hierdoor kunnen er zwaktes in de keten ontstaan. Maar ook kunnen buitenlandse overheden, concurrenten of investeerders in het betreffende land via bijvoorbeeld *lawfare* (juridische oorlogsvoering) invloed proberen uit te oefenen over uw bedrijf en bedrijfsprocessen. Zo kunt u verwikkeld raken in een dure en oneerlijke juridische strijd. Verliest u deze juridische strijd? Dan loopt u het risico (delen van) uw onderneming of intellectueel eigendom kwijt te raken. Kortom, een vestiging openen in het buitenland kan een goed idee zijn. Wél is er een goede voorbereiding voor nodig. Hoe pakt u dit aan?

Casus
Bedrijf A is gespecialiseerd in de ontwikkeling en productie van draagbare, zeer krachtige warmtebeeldcamera's in Nederland. Deze zijn bedoeld voor gebruik in de bouwsector. De camera's van bedrijf A onderscheiden zich dan ook in hun waterdichtheid en valbestendigheid. Maar bedrijf A produceert alleen in Nederland en het productieproces is erg kleinschalig. Bedrijf A wil graag uitbreiden naar het buitenland.

Op een dag ontvangt bedrijf A bericht van een andere partij (partij B). Partij B houdt zich bezig met het produceren van camera's op grote schaal in land C. Partij B is zeer geïnteresseerd in bedrijf A, en zou graag willen investeren in het bedrijf. Uiteindelijk zou partij B bedrijf A ook willen helpen met het uitbreiden van de productie in Land C. Bedrijf A wil graag opschalen en vind het een aanlokkelijk aanbod, maar besluit niet op een dergelijke toenadering in te gaan. Land C heeft onder andere meerdere keren laten zien het niet zo nauw te nemen met IE-rechten. Als bedrijf A in zee zou gaan met partij B, kan het wel eens zo zijn dat de productieprocessen die aan de basis liggen van hun technologisch hoogwaardige camera's weglekt naar de verkeerde partijen. Dat zou meer problemen kunnen opleveren dan voordelen.

Hoe kunt u de risico's omtrent vestigingen in het buitenland indammen?
Bekijk voordat u een vestiging opent in het buitenland:
- De pagina internationaal ondernemen van de RVO voor advies.
- De pagina over het starten van een bedrijf in het buitenland van het Ondernemersplein.
- De plaatselijke wetgeving en verdiep u in het ondernemingsklimaat van het land waar u naar wil uitbreiden:
- Wat voor gevolgen heeft het bijvoorbeeld voor uw intellectueel eigendom als u een deel van uw productieketen verplaatst naar het betreffende land?
- Welke regels gelden er voor dataopslag?
- Heeft het land een positieve of negatieve reputatie als het gaat om het huisvesten van buitenlandse ondernemingen met hoogtechnologische producten?
- Leg ook contact met de Nederlandse ambassade in het land waar u aan de slag wilt gaan met uw product. De plaatselijke ambassade heeft vaak een goed kennisnetwerk in het specifieke land waar u wilt zakendoen.
- Het Dreigingsbeeld Statelijke Actoren (DBSA 2) om een beter beeld te krijgen van het betreffende land.
- De kleurcode per land van het ministerie van Buitenlandse Zaken.

Sta daarnaast stil bij de volgende punten:
- Exportcontrolewetten verschillen per land. Controleer of uw technologie te maken heeft met lokale exportcontroles bij het betreden van nieuwe markten of het samenwerken met internationale partners.
- Aangezien u het zicht kan verliezen over een verhoogd aantal werknemers dat exclusief in het buitenland werkt, is het verstandig om extra aandacht te besteden aan veiligheid en integriteit bij het aannemen van nieuw personeel, en de digitale en fysieke beveiliging van uw data en bedrijfsprocessen. Geef uw werknemers alléén toegang tot de processen in de keten waar zij toegang tot moeten hebben. Integreer fysieke en digitale compartimentalisering in uw bedrijfsprocessen.

Personeelsbeleid

Uw bedrijf groeit en u wilt graag meer personeel aannemen. Aandacht voor een zorgvuldig personeelsbeleid is belangrijk voor het welbevinden van uw werknemers en het succes van uw bedrijf.

Zo kunnen werknemers, in opdracht van kwaadwillende statelijk actoren, concurrenten of criminelen, eropuit zijn uw gevoelige kennis en bedrijfstechnologie te stelen. Ook kan een werknemer om verschillende redenen radicaal of riskant gedrag gaan vertonen, bijvoorbeeld door psychologische problemen, geldproblemen of een gevoel van algemene onvrede. Zo kan een werknemer nonchalant omgaan met de regels rondom vertrouwelijke informatie, of in ruil voor geld vertrouwelijke informatie aan derden verkopen. Zogenaamde *insider threats* kunnen verwoestende gevolgen hebben voor uw bedrijf, omgeving en mogelijk de Nederlandse samenleving.

Raakt u technologie, geheimen of gevoelige informatie kwijt door het handelen van een medewerker? Dan kan alle tijd en geld die u geïnvesteerd heeft in de ontwikkeling van uw bedrijf voor niets zijn geweest, terwijl uw concurrent of een andere staat er met de winst vandoor gaat. Wees u er ook van bewust dat werknemers niet altijd uit eigen beweging gevoelige informatie doorspelen aan kwaadwillende derde partijen. In sommige landen kunnen overheden hun (voormalig) burgers dwingen tot medewerking. Uw personeelsbeleid is er daarom niet alleen om uw bedrijf te beschermen, maar ook om uw medewerkers te beschermen.

Goed personeelsbeleid is gericht op het gehele samenwerkingstraject met de medewerker; van sollicitatie tot werk, en zelfs tot na het uitdiensttreden. Maar hoe ziet een goed personeelsbeleid eruit? En hoe kunt u het zo veilig mogelijk maken voor alle betrokken partijen?

Casus
De frustratie had zich geleidelijk opgebouwd, maar afgelopen donderdag was voor werknemer A toch écht de druppel die de emmer deed overlopen. Deze donderdag had hij een functioneringsgesprek met zijn manager. Eigenlijk had werknemer A gehoopt dat hij promotie zou krijgen tot teamleider. Dit zou meer dan verdiend zijn geweest na 15 jaar zwoegen aan verschillende nieuwe voertuigmodellen, zo vond werknemer A zelf. In plaats daarvan kreeg hij tegenvallend nieuws te horen: de positie was naar collega B gegaan. Werknemer A had collega B nota bene zelf nog ingewerkt. Voor werknemer A was de maat nu vol. Sinds deze tegenvaller is werknemer A alleen maar bezig geweest met wraak. Hij heeft zich voorgenomen om – onopvallend, maar geleidelijk – de blauwdrukken van een revolutionair, nieuw voertuigdesign van zijn werkgever te kopiëren en te verkopen aan de hoogste bieder. Voor werknemer A maakt het niet meer uit wie deze hoogste bieder is.

Wat u kunt doen met betrekking tot personeelsbeleid
In personeelsbeleid is er onderscheid te maken tussen verschillende fasen:
- werving;
- in dienst;
- uit dienst.

Tijdens deze fasen zijn er verschillende elementen waar u als werkgever op kunt – en soms moet – letten. Bij alle fasen is een belangrijke rol weggelegd voor uw veiligheidscoördinator en HR-functionaris. Daarnaast is het belangrijk u bewust te zijn van uw kroonjuwelen en de bijbehorende risico-inschatting: de context is dus belangrijk. Sommige functies zijn gevoeliger dan anderen en vereisen dus meer aandacht. Het is altijd belangrijk dat u een open veiligheidscultuur stimuleert in uw bedrijf. Zorg er tijdens alle fasen voor dat ongewenst of verdacht gedrag en veiligheidsrisico's besproken kunnen worden.

In de wervingsfase is het verstandig om te letten op de volgende zaken:
- Aard van de functie: het invullen van een kritieke functie vereist natuurlijk gepaste aandacht voor de integriteit van de kandidaat.
- Identiteit van de sollicitant: is de persoon wel wie hij of zij zegt te zijn? Let op: u moet zich houden aan de privacywetgeving. Lees meer over wat u wel én niet mag vragen als het gaat over de persoonsgegevens van een sollicitant tijdens het sollicitatieproces op de pagina Persoonsgegevens van sollicitanten van de Autoriteit Persoonsgegevens.
- Cv en netwerk van de sollicitant: heeft iemand in een land met een verhoogd risicoprofiel gewerkt?

Controleer hiervoor de DBSA 2. Zitten er opvallende gaten in iemands cv? Heeft of had de kandidaat interessante of gevoelige nevenfuncties?

- Referenties: deze kunt u bij de sollicitant opvragen. Wel heeft u nadrukkelijk toestemming nodig van de sollicitant om contact op te nemen met de opgegeven referenten. Daarnaast mag u de referenten alleen vragen stellen over zaken die direct verband houden met de functie in kwestie.
- Gevoelige technologie of informatie: wordt hiermee gewerkt in de nieuwe rol? Dan kunt u van de kandidaat in kwestie bij selectie een Verklaring Omtrent Gedrag (VOG) eisen. Een VOG is functie-specifiek, en kijkt enkel een bepaalde termijn terug in Nederlandse databases voor bepaalde strafbare feiten. Komt de kandidaat van buiten Nederland of de EU? Dan biedt een met de VOG vergelijkbare buitenlandse verklaring misschien een uitkomst. Let op dat als u een VOG eist voor een bepaalde functie, u dit al aangeeft in de vacaturetekst, zodat de sollicitant hierop voorbereid is.
- Mogelijkheid tot toebrengen schade aan de nationale veiligheid: zou iemand in deze functie de nationale veiligheid kunnen schaden? Zo ja, dan moet deze functie als vertrouwensfunctie worden bestempeld. Het aanwijzen van een vertrouwensfunctie en het instellen van een veiligheidsonderzoek kan alleen nadat alle in redelijkheid te nemen fysieke en organisatorische maatregelen zijn genomen, maar desondanks restrisico's overblijven waarbij schade aan de nationale veiligheid mogelijk is. Lees hier meer over op de website van de AIVD. Voor het vervullen van een vertrouwensfunctie bij ABDO-bedrijven of private bedrijven in de vitale infrastructuur, is een verklaring van geen bezwaar (vgb) noodzakelijk. Een vgb wordt na een veiligheidsonderzoek afgegeven door de AIVD of MIVD.
- Integriteit: neem daarvoor een integriteitstest af.
- Aangeboden arbeidsovereenkomst: neem geheimhoudingsbepalingen op in de arbeidsovereenkomst die ook geldig blijven tijdens de uit-dienstfase.

Let tijdens de in-dienstfase op dat:

- Nieuw personeel bij indiensttreding door middel van leermodules kennismaakt met de bedrijfsnormen en -waarden. Let ook op dat het personeel leert hoe het verantwoord en veilig omgaat met gevoelige kennis, technologie en informatie. Creëer een cultuur waarin veiligheid centraal staat.
- Uw personeel regelmatig zulke leermodules blijft volgen, zeker na grote veranderingen binnen het bedrijf of de sector (bijvoorbeeld bij aanpassingen in privacywetgeving).
- Op uw intranet leermodules en handboeken te vinden zijn over de normen, waarden en regels binnen uw bedrijf.
- Uw personeel zich vrij voelt om persoonlijke en professionele problemen te bespreken met u, anderen of vertrouwenspersonen. Personen met problemen moeten geholpen worden en zich gesteund voelen, anders loopt u het risico dat de problemen tot uiting komen op de werkvloer.
- Uw personeel geen onnodige toegang heeft tot die processen en of informatie die zij niet nodig hebben voor het uitvoeren van hun werkzaamheden. Dit vergroot alleen maar het risico van verlies en diefstal van waardevolle en gevoelige zaken. Werk op basis van de principes van *need to know* en *least privilige:*
  - *Need to know* houdt in dat men alleen werkt met die data en processen die men nodig heeft voor het goed uitvoeren van zijn of haar werk;
  - *Least privilege* houdt in dat er per gebruiker en of functiesoort vastgelegd wordt welke toegangs-rechten van toepassing zijn op het uit te voeren werk. In de praktijk kan dit bijvoorbeeld inhouden dat een medewerker op een bepaalde netwerkschijf alleen het recht heeft om documenten te lezen, terwijl dezelfde medewerker op een andere netwerkschijf het recht heeft om documenten te lezen en te schrijven. Hou de toegangsrechten van uw werknemers bij in een zogenaamde rechtenmatrix.

Let tijdens de uit-dienstfase op dat:

- u nazorg geeft aan personeel dat met gevoelige dossiers heeft gewerkt. Houd contact met hen.

Wat de Rijksoverheid voor u kan betekenen

- Zie de website van het Ondernemersplein voor vragen over het aannemen of detacheren van personeel uit Nederland, de Europese Economische Ruimte (EER) en Zwitserland, of kennismigranten van buiten de EU/EER.
- Lees meer over *insider threats* en hoe u hiermee omgaat in de de folder Omgaan met Insider Threats: Good Practices van Nederlandse Organisaties van het Nationaal Cyber Security Centrum.
- Wilt u een melding doen over (vermoedens van) spionage of ongewenste beïnvloeding? Neem contact op met de AIVD. Bedrijven met een ABDO-autorisatie kunnen ook contact opnemen met het Bureau Industrieveiligheid van de MIVD.

Cyberdreigingen

Er zijn verschillende manieren waarop kwaadwillende actoren uw onderneming kunnen aangrijpen, zowel fysiek als digitaal. In dat laatste geval spreken we over een cyberaanval. Zowel statelijke actoren als concurrenten en criminelen (of een samenwerkingsverband daarvan) kunnen cyberaanvallen uitvoeren. U kunt ook gewoon het slachtoffer worden van een cyberincident waar geen kwade opzet achter zit, maar die veroorzaakt wordt door bijvoorbeeld een stroomstoring of defecte apparatuur. We zullen in dit hoofdstuk vooral ingaan op cyberaanvallen. Veelvoorkomende vormen van cyberaanvallen zijn:

- *Ransomware* (gijzelsoftware): uw digitale bedrijfssystemen worden gegijzeld. Om de controle over uw systemen en of informatie terug te krijgen moet u losgeld betalen.
- *Phishing*: een kwaadwillende actor doet zich voor als een ander en ontvreemd zo gevoelige informatie bij u of een ander.
- *Denial of Service en Distributed Denial of Service ((D)DoS)*: aanvallers zenden opzettelijk enorme hoeveelheden data naar (een van) uw server(s) om deze omgeving(en) te overbelasten en onbereikbaar te maken.
- Insidergerelateerde dreigingen: cyberrisico's of dreigingen die vanuit de eigen organisatie en of contactenkring komen. Insiders met slechte intenties kunnen veel schade aanrichten met:
  - diefstal;
  - fraude;
  - spionage; en/of
  - het lekken van IE of bedrijfskritische of vertrouwelijke gegevens.

Insidergerelateerde dreigingen kunnen zich zowel binnen als buiten het cyberdomein voordoen. Lees meer over insider threats en hoe u hier mee om kunt gaan in de folder Omgaan met Insider Threats: Good Practices van Nederlandse Organisaties van het Nationaal Cyber Security Centrum.

Bovenstaande voorbeelden zijn maar een paar vormen van cyberaanvallen. Helaas zijn er nog veel meer scenario's mogelijk. Het cyberdomein ontwikkelt zich voortdurend. Dit betekent ook dat aanvallers steeds nieuwe manieren zullen vinden om slachtoffers te maken. Zorg daarom dat u periodiek kijkt naar uw eerder genomen maatregelen, en of dezen nog functioneren zoals bedoeld. Hoe kunt u in het licht van bovenstaande uitdagingen toch een gedegen verdediging opwerpen?

Casus

Advocatenkantoor A is gevestigd in Nederland en beheert de dossiers van enkele tientallen cliënten. Daarnaast communiceert het kantoor met rechtbanken over gevoelige zaken. Ook is het kantoor onderdeel van het financieel verkeer tussen verschillende partijen.

Op een zekere maandagochtend klikt een medewerker van advocatenkantoor A, in een moment van onoplettendheid, in een e-mail die afkomstig lijkt te zijn van een partner, op een link. De link blijkt kwaadaardig. Het e-mailadres van de afzender lijkt op dat van een partner, maar na nog eens goed gekeken te hebben blijkt er ergens in het adres een punt te zijn ingevoegd. Het kwaad is nu echter al geschied. Het computersysteem en de database van het kantoor gaan op slot. Er verschijnt een bericht op het scherm met een aftellende klok en het bericht "Uw computersysteem en database zijn versleuteld, betaal 1.000 Bitcoins binnen 24 uur om de versleuteling op te heffen". Daarnaast opent zich een chatbox om berichten uit te wisselen met de gijzelnemer.

Maar advocatenkantoor A had al verwacht ooit in een dergelijke situatie terecht te komen en is gelukkig voorbereid. Zo maakte het kantoor regelmatig back-ups van het computersysteem en de database en bewaarde deze back-ups fysiek in een afgesloten omgeving. Er wordt besloten géén losgeld te betalen aangezien advocatenkantoor A de criminelen niet wil belonen, maar ook omdat het geen garantie geeft dat de gijzeling daarmee over is. Wel wordt er aangifte gedaan bij de politie en een melding gemaakt van een potentieel datalek bij de Autoriteit Persoonsgegevens. Het kantoor neemt contact op met de beheerder van hun systemen, die het geheel reset en de back-ups activeert. Advocatenkantoor A leidt schade, maar zonder de getroffen maatregelen had dit veel erger kunnen zijn.

Wat u kunt doen om uw cybersecurity te verbeteren

Er zijn gelukkig veel dingen die u kunt doen om uw cybersecurity te verbeteren, zowel op individueel als organisatorisch niveau. Hier is het uitgangspunt: 100% veilig is onmogelijk, maar daarom gaat u voor de maximale beveiliging van uw meest belangrijke bezittingen.

Individueel niveau

Op individueel niveau is het belangrijk dat alle werknemers in uw onderneming er een gezonde digitale hygiëne op nahouden. Dit geldt ook voor uw ketenpartners en hun werknemers. Digitale hygiëne houdt in dat werknemers en partners:

- zich bewust zijn van cyberdreigingen en hiernaar handelen;
- niet zomaar klikken op dubieuze links;
- geen gebruikmaken van zogenaamde *shadow-IT*. Dit zijn applicaties die een werknemer gebruikt voor werk, maar die niet zijn beoordeeld of goedgekeurd door de cybersecurity-eindverantwoordelijke.

Zorg dat nieuwe werknemers bij indiensttreding een introductie op maat krijgen in de digitale hygiëne. Zorg ook dat werknemers die al langer in dienst zijn periodiek een opfriscursus volgen.

Organisatieniveau

Op organisatieniveau is het belangrijk dat u vanaf het begin een alomvattende cyberverdediging opzet en u tenminste de basis op orde heeft. Begin daarom bij voorkeur met het inzetten van de volgende 7 basismaatregelen als u dat nog niet gedaan heeft. Hiermee kunt u namelijk op een relatief gemakkelijke manier een grote positieve impact maken op de staat van uw cyberveiligheid:

1. Maak een back-up van uw belangrijkste bestanden

Een reservekopie (back-up) kan een laatste redmiddel zijn als uw bedrijf is aangevallen. Zorg daarom voor één of meerdere goede back-ups van de bestanden die u nodig heeft voor uw bedrijfsvoering. Denk hierbij bijvoorbeeld aan uw klantdata en dossiers. Kopieer de belangrijkste bestanden naar een externe harde schijf, koppel deze vervolgens los en berg deze op een veilige plaats op. En bewaar minimaal één back-up op een andere locatie. Werkt u in de *cloud*? Let dan op: dit betekent niet dat er automatisch een back-up van uw gegevens wordt gemaakt. Lees meer over hoe u een goede back-up maakt op de website van het Digital Trust Center.

2. Stel inloggen in meerdere stappen in

Met multifactorauthenticatie (MFA) voegt u aan het inloggen met een wachtwoord een extra inlogvereiste toe. Dit heet ook wel 'inloggen in 2 stappen' of 'tweefactorauthenticatie (2FA)'. Hiermee voorkomt u misbruik van uw account. Een voorbeeld van een extra stap is dat een sms naar uw smartphone wordt gestuurd met een toegangscode. Of u ontgrendelt uw account met een code van een authenticatie-app of via uw vingerafdruk. Stel MFA op zoveel mogelijk plekken in, in ieder geval bij uw zakelijke e-mailaccount en uw belangrijke bedrijfsapplicaties of bedrijfssystemen. Bekijk hoe dit werkt bij een paar veelgebruikte accounts. Kunt u dit niet zelf? Vraag uw IT-dienstverlener om dit voor u te doen. Lees meer over MFA en 2FA op de website van het Digital Trust Center.

3. Zet automatische updates aan

Software-updates bevatten vaak verbeteringen voor de gebruiker. Ook bevatten ze vaak beveiligingsupdates. Voert u een update niet of later uit? Dan kan uw beveiliging kwetsbaar worden. Zo kan er een beveiligingslek ontstaan. Kwaadwillenden zoeken actief naar manieren om binnen te dringen via zo'n een lek. Wacht daarom niet met het updaten van apparaten die met het internet verbonden zijn. Zet bij voorkeur 'automatisch updaten' aan. Denk hierbij niet alleen aan uw computer of smartphone, maar ook aan uw printer, slimme deurbel, website, server, router, etc.. Lees meer over automatisch updaten op de website van het Digital Trust Center.

4. Gebruik antivirussoftware

Een antivirusprogramma of antivirussoftware dat u beschermt tegen internetvirussen en malware is op veel apparaten inmiddels standaard aanwezig. Soms kunt u ook zelf een antivirusproduct kiezen. Installeer een antivirusprogramma en zorg dat deze software up-to-date blijft. Doe dit op alle computers, telefoons en servers binnen uw bedrijf. Zo loopt u minder risico op schade door virussen en andere malware. Lees meer over antivirussoftware op de website van het Digital Trust Center.

5. Controleer de beveiligingsstandaarden van uw e-mail
Via internet.nl kunt u de beveiliging van uw e-mailadres en domeinen controleren. De website vertelt u of uw e-mailadres en/of domeinnaam voldoet aan de moderne beveiligingsstandaarden. Zo krijgt u een beeld van hoe uw website en e-maildomeinen ervoor staan qua veiligheid. Uw domeinnaam is het gedeelte achter de '@' bij uw e-mailadres. Lees meer over e-mail beveiligingsstandaarden op de website van het Digital Trust Center.

6. Leer phishing herkennen
Maak uzelf en uw medewerkers alert en zorg ervoor dat jullie phishing kunnen herkennen. Oefenen kan hierbij helpen. Doe de phishingquiz of speel de phishingbingo van het Digital Trust Center. Ook de tool 'eerst checken dan klikken' kan helpen phishing te leren herkennen. U kunt ook een phishingtest starten in samenwerking met een IT-dienstverlener. Controleer altijd het e-mailadres, de afzender en de inhoud van een bericht. Let daarbij op de volgende punten:

- controleer of de domeinnaam en het e-mailadres van de afzender hetzelfde zijn;
- controleer of de domeinnaam overeenkomt met het website-adres;
- let op details: ziet u het verschil tussen info@31008mailers.nl en info@31oo8mailers.nl?;
- Klik niet op een link als u deze niet vertrouwt, maar beweeg met de aanwijzer van uw muis over de link. Zo ontdekt u waar de link écht naar toe gaat.

Lees meer over phishing op de website van het Digital Trust Center.

7. Print een bellijst voor noodsituaties
Heeft u door een cyberaanval geen toegang meer tot uw informatiesystemen? Dan is er sprake van een noodgeval. Zorg daarom dat u beschikt over een geprint document met de contactgegevens van uw IT-dienstverlener, softwareleverancier of securitybedrijf. Bekijk een voorbeeld van een effectieve bellijst. Heeft u belangrijke klanten en (keten)partners? Zorg dan dat uw IT-dienstverlener ook bij hen geregistreerd staat als contactpersoon bij cyberaanvallen. Lees meer over het opstellen van een effectieve bellijst op de website van het Digital Trust Center.

U heeft de 7 basismaatregelen geïmplementeerd, wat nu?
Goed dat u de eerste maatregelen genomen hebt. Maar er zijn nog meer maatregelen die u kunt nemen om de basis van cybersecurity op orde te hebben. Haal uw volgende actiepunten op met de CyberVeilig Check voor ZZP en MKB van het Digital Trust Center. Download uw eigen actielijst en ga met praktische instructies en tips aan de slag.

Wat is verder relevant voor u als het gaat om cybersecurity?

- Elke vorm van cybercriminaliteit is strafbaar. Denk aan het verspreiden van virussen en andere malware, phishing, identiteitsfraude, factuurfraude, CEO-fraude en ransomware. Als u te maken krijgt met deze vormen van cybercriminaliteit, doe dan altijd aangifte bij de politie.
- Heeft u sterke vermoedens dat er een datalek heeft plaatsgevonden binnen uw bedrijf? Dan bent u verplicht dit binnen 72 uur van kennisname te melden bij de Autoriteit Persoonsgegevens via het Meldformulier datalekken.
- Bekijk alle informatie over cyberdreigingen en cybersecurity op de websites van het Nationaal Cyber Security Centrum (NCSC) en het Digital Trust Center.

Een veilige toeleveringsketen

De frequentie en omvang van zowel vraag- als aanbodschokken voor de industrie is wereldwijd vergroot door factoren als de pandemie, samen met veranderingen in de wereldeconomie, de geopolitieke situatie en het klimaat. Blootstelling aan al deze factoren leveren kwetsbaarheden en potentiële risico's op voor toeleveringsketens. Het is van groot belang dat industrieën en sectoren dat begrijpen. De beste manier om deze factoren te weerstaan en proactief aan te pakken, is als u een diversiteit aan wereldwijde partners en bronnen blijft waarborgen.

Casus
Bedrijf A is een toonaangevend bedrijf gespecialiseerd in kleine, krachtige zonnepanelen. Bedrijf A is voor de productie afhankelijk van bepaalde grondstoffen van partner B uit land C. De samenwerking tussen bedrijf A en partner B is doorgaans goed. Bedrijf A heeft het volste vertrouwen in hun ketenpartner. Maar vertrouwen blijkt niet genoeg.

Een werknemer van partner B is op werkbezoek bij bedrijf A, om meer te leren over de bedrijfsprocessen van bedrijf A. De werknemer van partner B moet voor overleg bellen met collega's in land C. Maar de werknemer van partner B belt via de onbeveiligde wifi-verbinding van het hotel. Cybercriminelen zijn al een tijd geleden dit netwerk binnengedrongen en kijken mee met iedereen die gebruikmaakt van deze verbinding. Twee maanden na terugkomst in land C krijgt de werknemer van partner B een bericht van het hotel waar hij tijdens zijn bezoek verbleef. De inbraak in het netwerk is opgemerkt en alle gasten die er de afgelopen periode verbleven wordt aangeraden hun apparaten te scannen voor virussen. Onbekend is of er gevoelige informatie is meegenomen door de netwerkinbrekers, maar bedrijf A is allerminst te spreken als zij dit nieuws van Partner B vernemen. Partner B bleek de zwakste schakel.

Wat u kunt doen om de veiligheid van uw toeleveringsketen te verbeteren
Het onderhouden van een veilige toeleveringsketen kan voor ondernemers een uitdaging zijn. Het gaat namelijk niet alleen over uw bedrijf, maar juist ook om de organisaties en bedrijven waarmee u samenwerkt. Gelukkig kunt u op verschillende manieren wel een positieve invloed uitoefenen, en een veilige, gebalanceerde keten nastreven. Dit kunt u doen met de volgende 4 stappen:

1. Breng toeleveringsketens in kaart
Ten eerste is het belangrijk dat u een goed beeld krijgt van uw toeleveringsketens. Waar komen uw producten vandaan, en hoe essentieel zijn deze producten voor het succes van uw onderneming? Zijn ze *nice to have* of *need to have*? Kijk bij het indexeren van uw toeleveringsketens naar de geografische lengte van uw toeleveringsketens en de hoeveelheid schakelpunten, zoals grensposten en douanes, in deze keten. Hoe groter de lengte van, en het aantal schakelpunten binnen, uw toeleveringsketen, hoe gevoeliger de toeleveringsketen. Dit risico is verwaarloosbaar als het gaat om een niet-kritiek product voor uw bedrijf, maar als het gaat om een essentieel element moet u nagaan of u het risico kunt spreiden.

De producten die u krijgt via deze toeleveringsketens kunt u indelen in 4 verschillende categorieën:
- **Niet-kritieke producten**: uw verdienmodel komt niet in gevaar als deze producten wegvallen en doorgaans zijn deze producten makkelijk te verkrijgen.
- **Knelpuntproducten**: deze producten zijn niet essentieel voor uw verdienmodel, maar de beschikbaarheid van deze producten is soms onzeker.
- **Hefboomproducten**: producten in deze categorie zijn essentieel voor uw verdienmodel, maar ze zijn over het algemeen breed verkrijgbaar. Zelfs als er een verkooppunt wegvalt.
- **Strategische producten**: deze producten zijn essentieel voor het draaiende houden van uw onderneming. Tegelijkertijd is de aanvoer van deze producten onderhevig aan risico's en verstoring. De aanvoer is dus niet altijd zeker. Vooral aan deze categorie moet u aandacht besteden.

2. Kwetsbaarheden en risicoschatting
Nu u een beter beeld heeft van wat de strategische producten zijn die u via uw toeleveringsketens geleverd krijgt, moet u per strategisch product kijken waar de potentiële gevoeligheden zitten. Dit kunt u doen door kritische vragen te stellen over de volgende verschillende momenten in de toeleveringsketen:

- **Levering**: welke leveranciers leveren dit strategische product? Is het mogelijk om elders meer leveranciers te vinden? Merkt u problemen bij bepaalde leveranciers, bijvoorbeeld met tijdige levering?
- **Ontvangst**: hoe komen de producten uw kant op: door havens of vliegvelden? En zijn deze plekken vaak druk of rustig? Hoeveel grenzen moeten deze producten over en komen hier extra kosten bij kijken? Wat zijn uw huidige voorraden van dit product en voor welke periode kunt u een verstoring van de toelevering volhouden?
- **Productie**: als de bovenstaande elementen vragen opleveren, stelt u vervolgvragen. Kunt u vervangende producenten vinden voor het strategische product dichter bij huis? Verwacht u een tekort aan essentiële grondstoffen of vakmanschap die nodig zijn voor dit strategische product?
- **Opslag**: kunt u het strategische product op grote schaal bewaren – zowel als geheel als in onderdelen? Wat is ervoor nodig om het product op grote schaal op te slaan en een buffervoorraad aan te leggen?
- **Bezorging**: hoe makkelijk of moeilijk is het om het product te vervoeren naar een afnemer, zijn er speciale handelingen voor vereist?
- **Recycling**: kunt u het product hergebruiken? Wat is daarvoor nodig met betrekking tot afvalverwerking rondom het product?

Verwacht u problemen met een of meer van de hierboven genoemde momenten uit de toeleveringsketen, mogelijk veroorzaakt door zowel interne als externe factoren? Dan kunt u spreken van een gevoelige toeleveringsketen.

Op dit punt is het voor uzelf duidelijk hoe uw toeleveringsketen functioneert en welke mogelijke zwaktes het bevat op welke specifieke momenten. U kunt nu beoordelen hoe reëel de risico's zijn rondom deze geïdentificeerde zwaktes. Dit kunt u doen door het opstellen van een risicomatrix. Met deze risicomatrix kijkt u per geïdentificeerde gevoeligheid hoe gróót de mogelijkheid is dat een risico zich hier voordoet. Ook bekijkt u hoe groot de impact daarvan zou kunnen zijn op uw bedrijf. Is er een grote mogelijkheid dat een risico zich voordoet? En heeft het een grote negatieve impact op uw bedrijf? Dan is het verstandig om risicoverminderende maatregelen te nemen.

3. Verminder de impact
Om de impact van mogelijke risico's binnen de toeleveringsketen te verminderen, kunt u de hieronder genoemde mogelijk risicoverminderende maatregelen gebruiken. U kunt deze maatregelen ook combineren:

- **Diversificatie**: bent u afhankelijk van één leverancier? Verken de mogelijkheden om uw afhankelijkheden te spreiden over verschillende leveranciers, zodat u niet in de problemen raakt als er één wegvalt.
- **Partnerschappen**: verken of er andere organisaties zijn die dezelfde uitdagingen hebben – misschien kunt u samen de krachten bundelen.
- **Aanleggen van voorraden**: als u ziet dat het aanbod nogal eens kan wijzigen, kunt u overwegen om strategische voorraden aan te leggen. Zo heeft u genoeg producten als het aanbod (tijdelijk) stilvalt.
- **Binnenlandse productie organiseren**: is het aanbod buiten het eigen land instabiel? Verken de mogelijkheden om productiemogelijkheden in het eigen land op te zetten of uit te breiden.
- **Onderzoek alternatieven**: zijn er andere producten die het strategische product misschien kunnen vervangen? Misschien kunt u (delen van) het strategische product recyclen om ze zo efficiënter te gebruiken.

De beste oplossing is de actie die met het minste geregel het grootste effect heeft.

4. Evalueer de interventie
Het is belangrijk dat u periodiek evalueert of de risicoverminderende maatregelen die u heeft genomen, een positieve impact hebben op de toeleveringsketen. Doorloop daarom op vaste momenten het stappenplan. Doe dit ook na impactvolle gebeurtenissen, zoals bijvoorbeeld natuurrampen of oorlogen.

2. Wettelijke kaders

Hieronder vindt u een overzicht van een aantal belangrijke juridische kaders waar u rekening mee moet houden, en die te maken hebben met economische veiligheid. Let wel: deze lijst is niet uitputtend.

Het (wettelijk) stelsel van investeringstoetsing - Wet Vifo

Op 1 juni 2023 trad de Wet Veiligheidstoets investeringen, fusies en overnames (Wet Vifo) in werking. De Wet Vifo introduceert een veiligheidstoets voor investeringen, fusies en overnames die mogelijk een risico vormen voor de nationale veiligheid. De veiligheidstoets geldt voor specifieke vitale aanbieders, beheerders van bedrijfscampussen en ondernemingen die beschikken over (zeer) sensitieve technologie. Vitale aanbieders zijn partijen die een dienst aanbieden waarvan de continuïteit van vitaal belang is voor de Nederlandse samenleving. Vitale aanbieders in de telecom-, gas- en elektriciteitssector hebben te maken met hun eigen sectorale investeringstoetsing die specifiek is afgestemd op de kenmerken van de sector. Onder de Wet Vifo vallen vitale aanbieders uit allerlei sectoren waarover private bedrijven zeggenschap kunnen krijgen, zoals vitale aanbieders in het bankwezen en het havengebied. De Wet Vifo heeft ook betrekking op vitale bedrijven die geprivatiseerd kunnen worden. Een vitale aanbieder kan namelijk onderdeel zijn van een vennootschap waarvan overheden de enige eigenaren zijn.

Een fusie, overname of investering is mogelijk risicovol als het tot de volgende zaken kan leiden:

- Het verstoren van de continuïteit van de vitale infrastructuur. Processen zoals energievoorziening en telecom zijn zo essentieel voor onze samenleving, dat uitval of verstoring zorgt voor ernstige maatschappelijke ontwrichting.
- Het weglekken van hoogwaardige kennis of technologie. Kennis en technologie kan via fusies, overnames of investeringen in handen komen van een kwaadwillende partij.
- Risicovolle strategische afhankelijkheden, bijvoorbeeld situaties waarin Nederland door een ander land (politiek) onder druk kan worden gezet.

Een melding maken in het kader van de Wet Vifo?

U heeft een wettelijke meldplicht bij het Bureau Toetsing Investeringen (BTI) als de voorgenomen verwervingsactiviteit binnen de reikwijdte van de Wet Vifo valt. Zowel de investeerders als de ondernemingen zelf moeten dan een wijziging van zeggenschap of invloed melden bij het BTI.
De Wet Vifo stelt dat er melding moet worden gedaan als er sprake is van:

- wijzigingen van zeggenschap vanaf 50% bij vitale aanbieders en sensitieve technologie; en
- wijzigingen van zeggenschap vanaf 10% bij zeer sensitieve technologie.

U kunt een melding maken op de website van het BTI.

Vragen over de Wet Vifo?

Kijkt u voor meer informatie over de Wet Vifo op de website van het BTI.

Exportcontrole van strategische goederen

Produceert uw bedrijf strategische goederen? Dan gelden er mogelijk regels bij het exporteren van uw goederen, technologie of diensten. Deze strategische goederen kunnen namelijk worden ingezet voor ongewenst eindgebruik. Daarom is in sommige gevallen een exportvergunning van de Nederlandse overheid nodig, specifiek geldt dat voor:

1. Militaire goederen
Militaire goederen zijn producten die zijn opgenomen op de Gemeenschappelijke EU lijst van militaire goederen. Voorbeelden zijn pantservoertuigen, oorlogsschepen en specialistische militaire apparatuur.

2. Goederen voor tweeërlei gebruik (dual-use-goederen)
Goederen die voor tweeërlei gebruik geschikt zijn, kennen zowel een civiele als een militaire toepassing. Bijvoorbeeld: bepaalde brandvertragers worden in de bouw gebruikt maar ook als grondstof voor gifgas. Onder goederen worden ook test- en productieapparatuur, materialen, software, en technologie verstaan. Wanneer u dual-use-goederen wil uitvoeren uit Nederland is vaak ook een exportvergunning vereist. Welke dual-use-goederen een exportvergunning vereisen staat in de bijlage I van de EU Dual-Use Verordening (2021/821).

3. Strategische diensten
Strategische diensten zijn diensten die verband houden met strategische goederen. Het gaat om:
- niet-fysieke overdracht van programmatuur en technologie, bijvoorbeeld via telefoon of per mail;
- het verlenen van technische bijstand;
- het verrichten van tussenhandeldiensten.

Onder strategische diensten vallen bijvoorbeeld reparaties en onderhoud van militaire of dual-use-goederen, instructies in het gebruik ervan en bepaalde softwareleveranties.

4. Foltergoederen en diensten
Guillotines, duimschroeven, stroomschokapparaten, pepperspray en verdovende middelen zijn voorbeelden van foltergoederen. Afhankelijk van het goed is de uitvoer (incl. technische bijstand en tussenhandeldiensten) gereguleerd dan wel verboden op basis van de EU anti-folterverordening.

5. Sanctiegoederen
Sommige sancties behelzen maatregelen die de export van bepaalde goederen naar het gesanctioneerde land verbieden, of onderwerpen aan een vergunningplicht.

Hoe weet u of u met exportregels rondom strategische goederen heeft te maken?
- Welke dual-use-goederen een exportvergunning vereisen staat in de bijlage I van de EU Dual-Use Verordening (2021/821).
- Militaire goederen zijn producten die zijn opgenomen in de gemeenschappelijke EU-lijst van militaire goederen.
- Voor de export van foltergoederen kunnen eveneens beperkingen gelden. Welke dat zijn staat vermeld in Verordening EU 2019/125, ook wel de EU-anti-folterverordening genoemd. Meer informatie vindt u op de website van de Douane onder Folterwerktuigen.
- U bent zelf verantwoordelijk om na te gaan of u een exportvergunning nodig heeft. Meer informatie vindt u op de website van de Rijksoverheid. Neem bij twijfel contact op met de Centrale Dienst voor In- en Uitvoer (CDIU) van de Douane.
- Wordt u geconfronteerd met verdachte aanvragen of bestellingen? Neem dan contact op met de Unit Contraproliferatie van de AIVD en de MIVD. Bedrijven met een ABDO-autorisatie nemen contact op met het Bureau Industrieveiligheid van de MIVD.

Algemene Verordening Gegevensbescherming (AVG)

De Algemene Verordening Gegevensbescherming (AVG) geldt voor alle ondernemers. Heeft u een klantenbestand of een personeelsadministratie? Dan verwerkt u persoonsgegevens. Het is belangrijk voor ondernemers om zich aan de AVG te houden. Maar de AVG kan voor sommigen ook ingewikkeld zijn – zeker in een context van internationale handel en samenwerking.

Weet u niet zeker waar u moet beginnen? Gebruik dan de AVG-Regelhulp van de Autoriteit Persoonsgegevens. Deze Regelhulp helpt u te verduidelijken wat u moet ondernemen om te voldoen aan de eisen van de AVG. Mocht uw onderneming toch te maken krijgen met een datalek? Dan bent u onder de AVG verplicht dit datalek binnen 72 uur na kennisname te melden bij de Autoriteit Persoonsgegevens.

Meer weten over economische veiligheid of relevante wet- en regelgeving?

Heeft u na het doornemen van deze brochure nog verdere vragen over economische veiligheid of de relevante wet- en regelgeving waarmee u in aanraking kunt komen? Of wilt u meer weten? Dan kunt u altijd terecht bij het Ondernemersloket Economische Veiligheid. Stel uw vraag via veiligondernemen@rvo.nl. Het Ondernemersloket Economische Veiligheid beantwoordt uw vraag of brengt u in contact met de juiste overheidsinstantie.

WEGWIJZER VOOR VEILIG ZAKENDOEN IN EEN COMPLEXE WERELD

Dit is een publicatie van:

Rijksdienst voor Ondernemend Nederland
Prinses Beatrixlaan 2 | 2595 AL Den Haag
Postbus 93144 | 2509 AC Den Haag
Contact
www.rvo.nl

Deze publicatie is tot stand gekomen in opdracht van het ministerie van Economische Zaken.

Publicatienummer: RVO-196-2024/HL-INNO

De Rijksdienst voor Ondernemend Nederland (RVO) stimuleert duurzaam, agrarisch, innovatief en internationaal ondernemen. Met subsidies, het vinden van zakenpartners, kennis en het voldoen aan wet- en regelgeving. RVO werkt in opdracht van ministeries en de Europese Unie.

RVO is een onderdeel van het ministerie van Economische Zaken.

www.rvo.nl/olev