Rijksoverheid

Economisch weerbaarder
in 4 stappen

Een quick guide voor ondernemers

www.rvo.nl/olev

Inleiding

Voor u ligt *Economisch Weerbaarder In 4 Stappen: Een Quick Guide voor Ondernemers.* Hierin richten we ons op de bescherming van uw meest waardevolle bezittingen: de technologie, kennis, processen en data die uw bedrijf uniek en competitief maken – 'uw kroonjuwelen'.
Deze Quick Guide focust op:

- de prioritering van uw kroonjuwelen;
- de risico-inschatting rondom deze kroonjuwelen;
- het opzetten van een goed en gemakkelijk te onderhouden veiligheidsinfrastructuur.

Zo stelt u deze essentiële elementen, het bestaansrecht van uw bedrijf én uw concurrentiepositie veilig tegen bijvoorbeeld kwaadwillende statelijke actoren, concurrenten en (cyber)criminelen.

Het is onmogelijk om elk element van uw onderneming 100% waterdicht te maken. Daarom ligt de focus van deze Quick Guide op het identificeren van wat voor uw bedrijf van levensbelang is. Zo kunt u stapsgewijs aan de slag met het beveiligen van uw bedrijf en bedrijfsprocessen, van *need to have* naar *nice to have*. Versterk vandaag nog uw weerbaarheid in 4 stappen: het stappenplan is voor iedereen uitvoerbaar. Al kan het handig zijn om extern hulp in te roepen van (veiligheids)consultants of juridisch adviseurs.

STAP 1. Wijs een veiligheids-verantwoordelijke aan

Het is belangrijk om een veiligheidsverantwoordelijke in het bestuur van uw organisatie te hebben, omdat dit ervoor zorgt dat de veiligheid van uw bedrijf altijd prioriteit heeft binnen uw bestuur. Idealiter heeft deze persoon sectorspecifieke kennis of ervaring in het vakgebied in kwestie. De veiligheidsverantwoordelijke is de eindverantwoordelijke voor alle veiligheidsgerelateerde elementen van uw onderneming. Deze persoon is ook het contactpunt voor andere partijen en belanghebbenden tijdens incidenten.

Naast een veiligheidsverantwoordelijke is het ook aan te raden om een Intellectueel Eigendom (IE)-verantwoordelijke aan te wijzen. De IE-verantwoordelijke zorgt dat uw waardevolle kennis, kunde en informatie goed beschermd blijft en schakelt met de veiligheidsverantwoordelijke als er sprake is van risico's. Zo zorgt u ervoor dat u belangrijke IE-kwesties snel op managementniveau kan bespreken.

Ook voor kleine ondernemingen is het zinvol om tenminste één persoon aan te wijzen als eindverantwoordelijke voor veiligheidsgerelateerde zaken. Zo is het voor iedereen duidelijk wie bepaalde risico's en incidenten monitort en aankaart in de organisatie.

STAP 2. Bepaal wat u wilt beschermen

Om uw risico's te identificeren begint u met het in kaart brengen van uw kroonjuwelen. Uw kroonjuwelen zijn de technologie, kennis, processen en data die uw bedrijf uniek en competitief maken (uw bezittingen); het bestaansrecht van uw bedrijf. Hierbij horen bijvoorbeeld ook de gegevens van klanten en werknemers en de reputatie van uw bedrijf.

Categoriseer uw bezittingen van hogere naar lagere waarde. En bedenk wat het voor uw bedrijf betekent als u (een van) deze bezittingen verliest, of deze in de verkeerde handen vallen. Sta ook stil bij de ondersteunende systemen die aan de basis liggen van uw kroonjuwelen. Om een voorbeeld te geven: uw klantinformatie is zeer belangrijk voor uw bedrijf. Als u deze informatie in een online database heeft opgeslagen, is deze database dus ook zeer belangrijk.

STAP 3. Identificeer en maak een inschatting van de risico's

Maak vervolgens een overzicht van uw kroonjuwelen, samen met de risico's die u aan deze kroonjuwelen kunt koppelen. Bedenk ook alvast vanuit welke hoek een risico kan komen. Dit kunnen statelijke actoren of concurrenten, maar ook (cyber)criminelen zijn. Zijn er specifieke buitenlandse overheden actief of geïnteresseerd in uw kroonjuwelen? Denk daarbij aan overheden van landen die in het Dreigingsbeeld Statelijke Actoren 2 (DBSA 2) worden genoemd. Neem bijvoorbeeld uw klantengegevens (een voorbeeld van een kroonjuweel): deze zijn zeer waardevol en moeten altijd beschermd worden. Wat als een werknemer deze klantgegevens per ongeluk deelt met een partij die deze niet mag inzien? Of wat als u deze gegevens (tijdelijk) kwijtraakt omdat cybercriminelen in dienst van een buitenlandse overheid uw systeem zijn binnengedrongen en uw systeem hebben gegijzeld?

Vervolgens maakt u een inschatting van de waarschijnlijkheid dat het risico zich voordoet en de grootte van de impact die dit zou hebben op uw bedrijf. Dit kunt u zowel kwantitatief als kwalitatief benaderen:

Kwantitatief risico's inschatten

Bij een kwantitatieve inschatting van de kansen en kosten kunt u risico's cijfermatig beschouwen. Bijvoorbeeld: als u uit ervaring weet dat uw bedrijf 4 tot 5 keer per jaar last heeft van een stroomstoring dan kunt u een inschatting van het kwantitatieve risico maken:

- kans stroomstoring: 5 keer per jaar;
- kosten stroomstoring: gederfde inkomsten door gemiste productietijd + arbeidskosten van werknemers die niet kunnen werken + elektromonteur + eventueel andere bijkomende kosten.

Kwalitatief risico's inschatten

Kunt u de kans en mogelijke gevolgen lastig in cijfers en geld uitdrukken? Dan kunt u de risico's kwalitatief inschatten. Zo kunt u misschien moeilijk uitrekenen hoe groot de kans is dat uw klantgegevens opzettelijk worden gedeeld door een *insider* die samenwerkt met een kwaadwillende partij. U weet ook niet wat de kosten van eventuele reputatieschade zouden kunnen zijn. Bij gebrek aan ervaring met bepaalde incidenten kunt u bijvoorbeeld wel kijken naar de incidentenhistorie van andere, soortgelijke ondernemingen. Bij een kwalitatieve risicoschatting schat u de kansen en kosten in op een schaal van 'laag', 'gemiddeld' tot 'hoog'. De praktijk leert dat bedrijven vaak kwalitatieve en kwantitatieve inschattingen met elkaar combineren.

Van alle stappen kan stap 3 het lastigst zijn. Zeker in een vroeg stadium van de onderneming. Het is zeer waarschijnlijk dat u de meeste risico's nog nooit heeft meegemaakt. U kunt er daarom voor kiezen om extern hulp in te schakelen bij het inschatten van de risico's, kansen en kosten. Denk hierbij aan de hulp van consultants, juridisch adviseurs of specialisten die penetratietesten uitvoeren (pentesters).

STAP 4. Onderneem actie en krijg grip op de risico's

Op dit punt heeft u een (grof) idee van:
- wat uw kroonjuwelen zijn;
- welke risico's op deze kroonjuwelen van toepassing zijn;
- hoe groot de waarschijnlijkheid is dat deze risico's zich voordoen;
- wat de negatieve gevolgen hiervan zouden zijn.

Het is nu tijd om risicoverminderende maatregelen te nemen. Hieronder ziet u een simpele uitvoering van een risicomatrix. Deze kunt u zelf uitbreiden als u wilt. Aan de hand van deze risicomatrix kunt u een inschatting maken van de soort acties die u kunt ondernemen.

Grote gevolgen	**Afdekken:** u dekt het risico af door bijvoorbeeld een verzekering af te sluiten. Het probleem is hiermee echter nog niet wezenlijk opgelost, anders dan dat u misschien (gedeeltelijk) vergoed zou kunnen worden voor eventuele geleden schade.	**Stoppen:** hieronder vallen de risico's met een grote kans én grote gevolgen. Als u dit constateert, is het goed om na te denken over tot in hoeverre de activiteit het grote risico waard is.
Kleine gevolgen	**Accepteren:** u weet dat u een risico loopt, maar u accepteert het risico.	**Mitigeren:** u neemt maatregelen waardoor u het risico zoveel mogelijk beperkt en mogelijk zelfs kunt uitsluiten.
	Kleine kans	**Grote kans**

De combinatie van kansen en gevolgen van het risico bepalen welk soort actie u moet ondernemen. Bekijk ook de *Handleiding Economische Veiligheid voor Ondernemers*. Deze gaat dieper in op de verschillende risico's waar u als ondernemer mee te maken kunt krijgen en biedt handelingsperspectief.

Voorbeeld

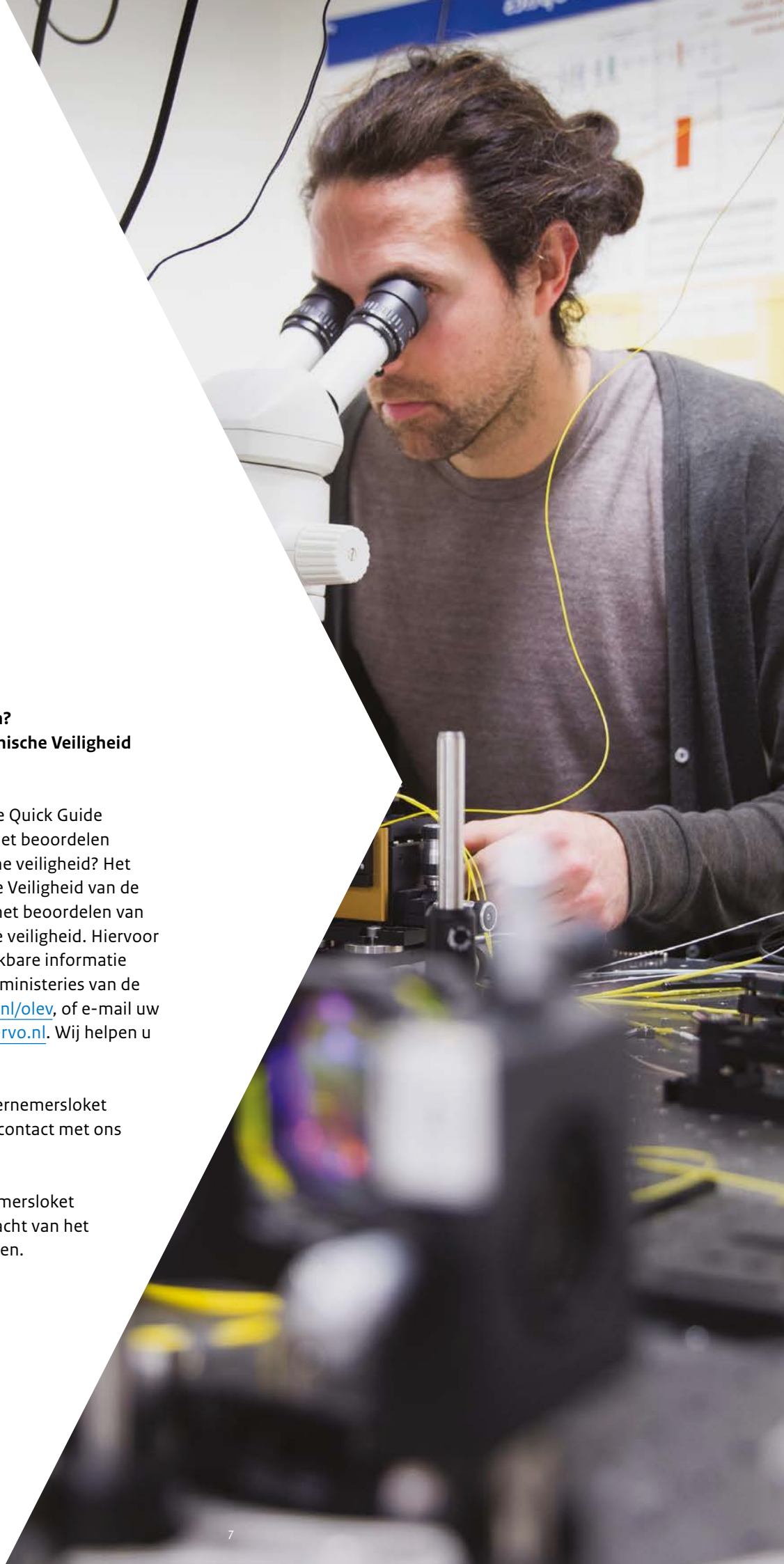
Uw klantgegevens (een zeer waardevol, gevoelig bezit) liggen opgeslagen in database A. De servers ervan staan in land B. U merkt op dat in land B de regering een wetsvoorstel wil doen, waardoor de plaatselijke politie en inlichtingendiensten volledige toegang krijgen tot de informatie die is opgeslagen in de servers in land B. Zij krijgen daarmee ook toegang tot informatie van buitenlandse partijen die daar opgeslagen ligt. Stel dat uw bedrijf werkzaam is in een zeer gevoelig domein, en u hebt klanten die bewust zakendoen met u maar niet met partijen uit land B, juist vanuit privacyoverwegingen, dan loopt u een risico. De kans is nu erg aannemelijk dat in de nabije toekomst de overheid van land B inzicht krijgt in uw klantgegevens (kans: groot). De gevolgen hiervan zouden zeer serieus kunnen zijn. Een mogelijk gevolg is dat uw klanten er misschien voor zullen kiezen om de samenwerking met u te beëindigen als u geen passende maatregelen neemt (gevolgen: zeer groot).

Als u de risicomatrix gebruikt, ziet u dat u met deze combinatie van kans en gevolgen in het rode vak 'Stoppen' uitkomt. Het is dan verstandig om de activiteit (samenwerking met de partij achter database A) stop te zetten en uw gegevenshuishouding te migreren naar een andere databasehouder.

Blijf risico's identificeren en leer van incidenten

Het is belangrijk om met enige regelmaat te bekijken of uw risico-matrix nog actueel is. Uw bedrijf, de omgeving waarin het actief is en de technologie staan niet stil. Dit kan maken dat u eerder geïdentificeerde risico's in de nieuwe werkelijkheid anders beoordeelt in de risico-matrix. Het kan ook betekenen dat er zich niet eerder geïdentificeerde risico's voordoen. Bespreek de risico's daarom periodiek met uw veiligheidsverantwoordelijke of adviseurs.

Het is belangrijk om te leren van incidenten: u leert meer over de waarschijnlijkheid van het risico en de kosten die het met zich meebrengt. Neem deze ervaring mee en doe er uw voordeel mee voor in de toekomst. Beschouw de stappen 2, 3 en 4 als een cyclus die u minstens één keer per jaar doorloopt.



Ondersteuning nodig of vragen?
Het Ondernemersloket Economische Veiligheid is er om u te helpen

Heeft u naar aanleiding van deze Quick Guide nog vragen? Of zoekt u hulp in het beoordelen van risico's omtrent economische veiligheid? Het Ondernemersloket Economische Veiligheid van de Rijksoverheid ondersteunt u in het beoordelen van de risico's omtrent economische veiligheid. Hiervoor maken zij gebruik van de beschikbare informatie en expertise van verscheidende ministeries van de Rijksoverheid. Bezoek www.rvo.nl/olev, of e-mail uw vraag. naar veiligondernemen@rvo.nl. Wij helpen u graag verder.

Heeft u een vraag voor het Ondernemersloket Economische Veiligheid? Neem contact met ons op via: www.rvo.nl/olev.

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

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-197-2024/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