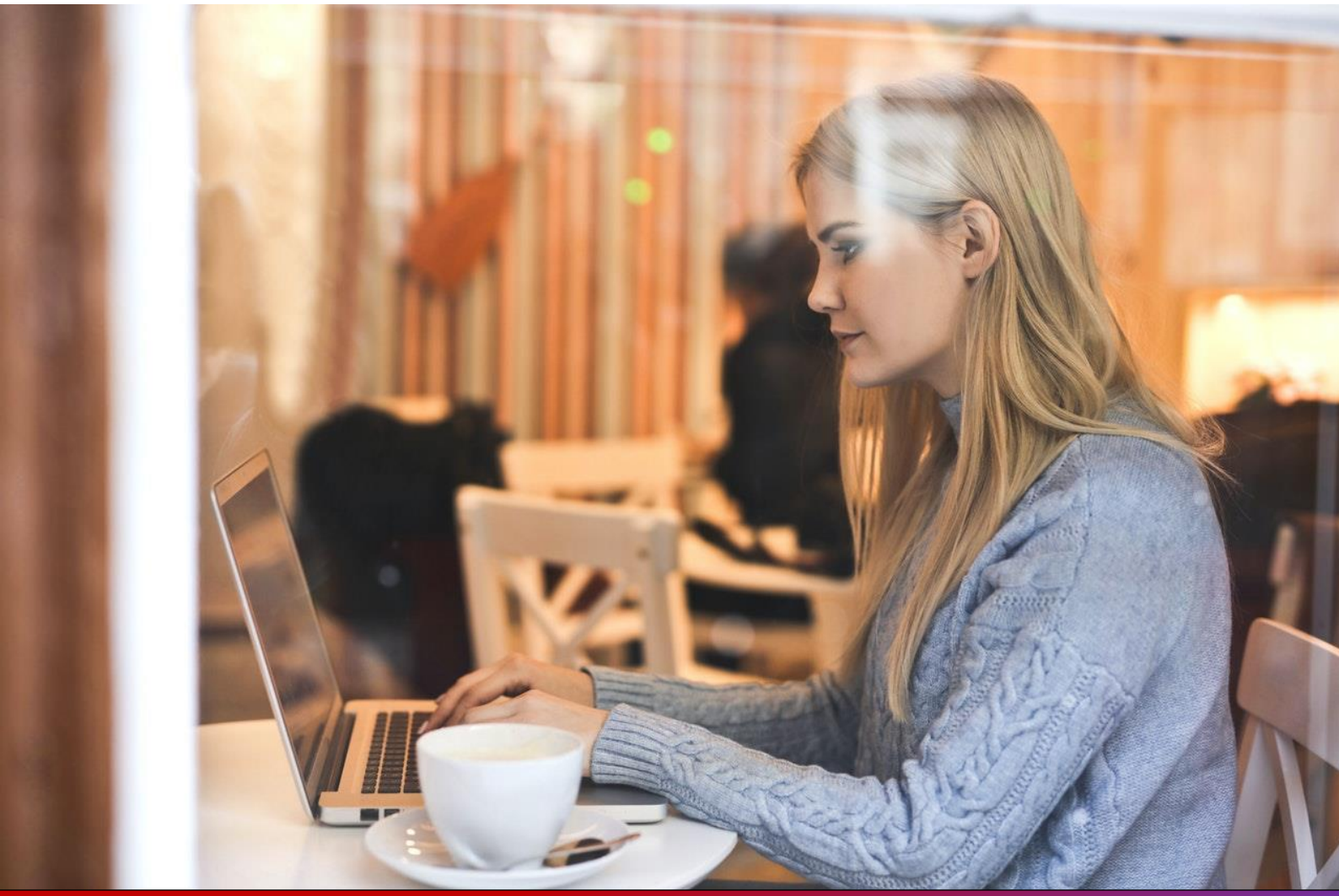

White paper

Organiseren Coordinated Vulnerability Disclosure (CVD)

Gemakkelijk en betaalbaar een krachtige beheersmaatregel toepassen

Versie, juni 2022

Aanleiding

Cyberdreigingen ontstaan door kwetsbaarheden in de ICT-infrastructuur, toepassingen en of in de organisatie van bedrijfsactiviteiten. Zij kunnen het effectief beschermen van bedrijfsactiviteiten en van bedrijfs- en persoonsgegevens ondermijnen.[1] Uiteindelijk kunnen deze kwetsbaarheden de continuïteit van de bedrijfsvoering bedreigen en een bedrijf zelfs stil leggen. De oorzaken van de kwetsbaarheden kunnen liggen in bijvoorbeeld de complexiteit van de digitale systemen, het ontbreken van "*security by design*", het onjuist implementeren en of het onvoldoende testen. De oorzaken kunnen ook liggen bij ketenpartners die producten, toepassingen en diensten aan het bedrijf leveren.

Een kwetsbaarheid kan door een onbekende onderzoeker worden opgemerkt. Als deze onderzoeker te goeder trouw is, wil hij graag de onderzoeksresultaten delen met het bedrijf. Het is belangrijk om op een juiste manier met de onderzoeker/ melder en de melding om te gaan om te voorkomen dat de informatie in ongewenste handen valt alvorens het bedrijf de kwetsbaarheid kan verhelpen.

Met een Coordinated Vulnerability Disclosure (CVD)-beleid kan een bedrijf inregelen dat kwetsbaarheden die buiten het bedrijf zijn gesignaleerd op een gecontroleerde wijze (onder uw regie) worden afgehandeld. In het beleid worden kaders aangegeven voor het documenteren en analyseren van deze kwetsbaarheden en het snel verhelpen ervan door het treffen van passende maatregelen. Hierdoor blijven de gevolgen voor de bedrijfsvoering beperkt.

De bedrijfsleiding en het management sturen hun beveiligingsorganisatie aan. In de praktijk blijkt dat het aansturen van de eigen beveiligingsorganisaties en die van de leveranciers van IT-diensten een uitdaging is. De oorzaak is vaak het onvoldoende op orde hebben van de basishygiëne. Veelal is er geen of onvoldoende overzicht en inzicht in systemen en de datastromen waardoor het systematisch zoeken naar en vinden van kwetsbaarheden wordt bemoeilijkt. Ook is het bewustzijn en het kennisniveau bij het management en medewerkers te laag en blijken contractuele afspraken over het wegnemen van kwetsbaarheden niet sluitend te zijn. CVD gaat ervan uit dat bedrijven de basishygiëne op orde hebben.

De onbekende onderzoekers die kwetsbaarheden in de infrastructuur en of de toepassingen ontdekken hebben veelal geen relatie met de organisatie. Om een escalatie van een kwetsbaarheid te voorkomen heeft de bedrijfsleiding er echter wel belang bij snel een relatie met de onbekende onderzoeker op te bouwen. Beide partijen zullen aan het opbouwen van een vertrouwensrelatie voorwaarden willen stellen.

De EU onderkent de belangen van bedrijven en onbekende onderzoekers bij het uitwisselen van ontdekte kwetsbaarheden in de infrastructuur en de toepassingen. Het agentschap ENISA van de EU heeft in samenwerking met de lidstaten een Coordinated Vulnerability Disclosure (CVD) model ontwikkeld en draagt dat ook uit, zie ENISA, Coordinated Vulnerability Disclosure policies in the EU.

In de Europese Netwerk- en InformatieBeveiligingsrichtlijn 2, NIB2, blijft een plicht om cyberincidenten binnen 24 uur te melden. Een nieuwe preventieve maatregel is het verplicht implementeren van procedures voor het melden van kwetsbaarheden in IT-producten en -diensten alsmede de implementatie daarvan. Het melden van kwetsbaarheden door een specifieke groep van bedrijven noemen wij ook wel Coordinated Vulnerability Disclosure (CVD). Zie blog van mr. dr. A.W. Duthler van First Lawyers over noodzaak implementeren CVD.

MYOBI heeft dit model CVD voor bedrijven – groot en klein – geoperationaliseerd. In deze white paper bespreken wij een implementatie- en beheerstrategie.

[1] Zie het persbericht "Datalekken door cyberaanvallen bijna verdubbeld", naar aanleiding van het jaarverslag Autoriteit Persoonsgegevens.

Strategie

Bewustwording

De bedrijfsleiding onderkent het belang van het effectief organiseren van Coordinated Vulnerability Disclosure (CVD) voor het borgen van de continuïteit van haar bedrijfsvoering. Met behulp van een bewustwordings- en trainingsprogramma CVD bespreekt de bedrijfsleiding met het management en de medewerkers het belang van CVD voor de bedrijfsvoering. Een toegankelijke businesscase CVD vanuit het perspectief van het bedrijf, het management en de medewerkers vormt een onderdeel van het bewustwordingsprogramma.

Als er voldoende draagvlak is in het bedrijf voor het organiseren van informatieveiligheid, in het bijzonder CVD, dan voert de bedrijfsleiding een projectplan, gericht op implementatie en beheer CVD, uit. Wij schetsen hieronder de contouren van het projectplan.

Voorbereiden

Een bedrijf registreert zich als gebruiker van het MYOBI Vertrouwensnetwerk en krijgt van Duthler Academy de beschikking over een bedrijfsspecifieke leeromgeving. Duthler Associates geeft, via haar leeromgeving (tenant), aan gebruikers/ bedrijven op het vertrouwensnetwerk toegang tot bewustwordings- en trainingsprogramma's.

De Contract Board, waarvan Duthler Associates lid is, onderhoudt een portfolio met draaiboeken en contracttypen CVD. De juristen van Duthler Associates kunnen deze portfolio desgewenst bedrijfsspecifiek maken. Met de draaiboeken en contracttypen is een bedrijf in staat om de bedrijfsprocessen van een CVD effectief te organiseren.

Het bedrijf kan uiteraard ook professionele ondersteuning inroepen voor een bedrijfsspecifieke implementatie en onderhoud van de CVD, zie hiervoor de volgende link.

De voorbereiding bestaat uit:

- Opstellen van een CVD-Beleid;
- Het toewijzen van taken, bevoegdheden en verantwoordelijkheden;
- Het operationaliseren van het beleid in interne processen en verantwoording hierover;
- Het communiceren van het beleid en de uitwerking hiervan in een effectief kennis- en verandermanagement voor medewerkers;
- Het trainen van betrokken medewerkers. Er is specifieke aandacht voor de CVD-coördinator;
- Opstellen van de CVD-verklaring. Deze verklaring sluit aan op de TTP-policy van MYOBI en wordt bedrijfsspecifiek gemaakt en onderhouden. De verklaring wordt gepubliceerd op de website van het bedrijf en geeft de voorwaarden en afspraken weer waaronder een onderzoeker een kwetsbaarheid kan melden aan het bedrijf. Zie als voorbeeld de CVD beleid van MYOBI;
- De CVD-overeenkomsten en draaiboeken, die het bedrijf met partners (bijvoorbeeld klanten, interne en externe medewerkers en leveranciers van IT-diensten) en externe onderzoekers afspreekt, worden bedrijfsspecifiek gemaakt en onderhouden;
- De draaiboeken CVD sluiten aan op de interne bedrijfsprocessen van het bedrijf;
- Het bedrijf kan op afroep ondersteuning door professionals van Duthler Associates afspreken;

- Het bedrijf ontwikkelt een strategie en maakt desgewenst afspraken voor het inschakelen van technische, organisatorische en juridische specialisten; en
- MYOBI zorgt ervoor dat alle afspraken, documenten en whatsapp-verkeer in beveiligde processen gewaarmerkt en gedeponeerd worden.

Het bedrijf heeft in haar bedrijfsspecifieke leeromgeving de beschikking over generieke bewustwordings- en trainingsprogramma's. De bedrijfsleiding kan besluiten gebruik te maken van aanvullende programma's en of de programma's bedrijfsspecifiek te maken.

Security researchers and vulnerability disclosure

Security researchers are generally motivated to participate in vulnerability disclosure:

For profit

For prestige or to advance their career

For the challenge, to learn and have fun

For ethical or ideological reasons.

Researchers are motivated by both financial and non-financial incentives, so while financial consideration may play a part, it is not the only motivating factor. Most researchers are also motivated by more than one or a combination of factors and motivations can shift depending on the task at hand.

There are also a number of barriers to researcher participation in vulnerability disclosure:

Fear of hostility or punishment

Legal barriers or uncertainty

Lack of appropriate vulnerability disclosure avenues

Insufficient or slow vendor or coordinator communication.

Clear, transparent and accessible vulnerability disclosure policies that provide legal safeguards for researchers, as well as efficient and respectful communication channels, are critical enablers for successful vulnerability disclosure.

Source: ENISA study on the Economics of Vulnerability Disclosure

Implementeren en beheren

Voor een succesvolle implementatie is het nodig dat de processen duidelijk zijn en de medewerkers bereid zijn het CVD-beleid effectief toe te passen (en dus de toegevoegde waarde van het organiseren van CVD inzien).

Processen

Iedereen – elk persoon in elk land - kan de beveiliging van een infrastructuur testen en kwetsbaarheden ontdekken. Er zijn veel bronnen, trainingen en tools op het internet beschikbaar voor zulke onderzoeken, zie bijvoorbeeld SANS overzicht van open source tools, of zie SANS penetration testing blueprint.

De centrale vraag is: "*Wat doet een onbekende onderzoeker met de informatie over kwetsbaarheden van uw netwerk of applicaties*?" Het antwoord is ontnuchterend: "*Zo snel als mogelijk moet het bedrijf de kwetsbaarheid kennen, inschatten wat de risico's zijn voor de continuïteit van de bedrijfsvoering en de kwetsbaarheid verhelpen*".

Bij het afwerken van dergelijke processen is het belangrijk dat:

- De onbekende onderzoeker zich serieus behandeld voelt;
- De onbekende onderzoeker de garantie heeft niet in een strafrechtelijke of civielrechtelijke procedure te worden getrokken;
- De informatie over kwetsbaarheden van het netwerk of applicaties onmiddellijk wordt onderzocht en op hun risico's voor discontinuïteit wordt ingeschat;
- Het bedrijf met betrokken partijen afspraken maakt hoe de kwetsbaarheid wordt weggenomen; en
- Het bedrijf met de onderzoeker afspraken maakt over de wijze van erkenning van de onderzoeker.

Uit een studie van ENISA zijn de motivaties en op te lossen vraagstukken van een onbekende onderzoeker (security researcher) op een rij gezet. Zie de figuur hierboven.

Onbekende onderzoeker meldt zich bij MYOBI

De CVD-verklaring op de website van een bedrijf, die ook gebruiker is van het vertrouwensnetwerk, verwijst een onbekende onderzoeker die een melding van een kwetsbaarheid wil doen naar MYOBI. MYOBI vangt de onbekende onderzoeker op en authentiseert de identiteit van de onderzoeker. De onderzoeker krijgt van MYOBI een eigen omgeving met de rol van Bedrijfsproces-coördinator en toegang tot het bewustwordings- en trainingsprogramma CVD. De onbekende onderzoeker kan – als hij dat wil - met behulp van een pseudoniem de kwetsbaarheid melden bij het bedrijf.[2]

Voor elke melding van een kwetsbaarheid brengt MYOBI het bedrijf € 250 in rekening.

Onderzoeker legt de informatie over kwetsbaarheid vast

De onbekende onderzoeker start een draaiboek CVD "vastleggen informatie over de kwetsbaarheid". Omdat hij zich geregistreerd heeft bij MYOBI, krijgt hij daar toegang toe. De onderzoeker nodigt de CVD-coördinator van het bedrijf uit kennis te nemen van de geconstateerde kwetsbaarheid. Veelal heeft de CVD-coördinator de rol van Bedrijfsproces-coördinator.

[2] Nb:

- Iedereen die acteert op het MYOBI Vertrouwensnetwerk onderschrijft de TTP-policy (dus ook de onbekende onderzoeker). Hierdoor kunnen partijen gebruik maken de vertrouwensdiensten.
- Een onbekende onderzoeker kan velerlei gemotiveerd zijn kwetsbaarheden aan bedrijven te melden. Tegelijkertijd is een onbekende onderzoeker voorzichtig. De onderzoeker wil het bedrijf leren kennen, informatie wensen over de feitelijke situatie en afspraken maken over vervolgstappen. Wetende dat de vertrouwde derde partij de identiteit van de onbekende onderzoeker kent, kan het bedrijf met de onbekende onderzoeker informatie uitwisselen en afspraken voorbereiden. Als er voldoende vertrouwen tussen partijen ontstaat kunnen partijen overeenkomsten sluiten.

De CVD-coördinator

De CVD-coördinator van het bedrijf is de persoon die kan inschatten – eventueel na overleg – wat de ernst is van de melding en welke rolhouders van het bedrijf betrokken moeten worden. Ook kan de CVD-coördinator bepalen of er externe professionals ingeschakeld moeten worden. De CVD-coördinator bepaalt de strategie voor de afhandeling van de kwetsbaarheid en waakt dat eenieder zijn rol goed en tijdig uitvoert en is verantwoordelijke voor de communicatie, documentatie en rapportage.

Bedrijf maakt afspraken met de onbekende onderzoeker

Het bedrijf en de onderzoeker wensen afspraken te maken over:

- Uitsluiten van juridische procedures;[3]
- Openbaar maken van informatie over de kwetsbaarheid; en
- Erkenning van de onderzoeker.

In een draaiboek worden de bovenstaande onderwerpen afgewerkt en afspraken gemaakt. Na het maken van afspraken kan de onderzoeker zijn pseudoniem opgeven en zijn identiteit bekend maken.

Communicatie

De effectiviteit van de beheersmaatregel CVD beïnvloedt een bedrijf met een gerichte communicatie voor vertrouwde onderzoekers die behoren tot het bedrijfsinformatie ecosysteem en onbekende onderzoekers. Het bedrijf kan in blogs aan onderzoekers vragen (nieuwe) systemen te onderzoeken, meedoen aan hackers bijeenkomsten en kan de waardering uitspreken over het nut van ethische hackers.

Beheren

Het organiseren van CVD kent vele varianten. Bij de implementatie kiest een bedrijf een bepaalde variant dat tijdens de beheerfase aangepast kan worden.

De-escalatie

Bedrijven zijn bereid informatie over kwetsbaarheden in beheersmaatregelen van bedrijfsprocessen openbaar te maken als er passende remedies beschikbaar zijn of zijn getroffen. Het ontbreken van remedies geeft cybercriminelen de kans misbruik te maken van de gedocumenteerde en gepubliceerde kwetsbaarheden. Een CVD tracht een dergelijke situatie vermijden.

Bedrijven ondersteunen hun bedrijfsprocessen – *waarin "by design" beheersmaatregelen zijn opgenomen* – met IT producten en diensten. Een CVD functioneert effectief als het bedrijf met haar IT-leveranciers afspraken heeft gemaakt over het tijdig treffen van aanvullende beheersmaatregelen die een kwetsbaarheid wegneemt. Veelal maken IT-leveranciers gebruik van achterliggende IT-leveranciers (onderaannemers) voor het samenstellen van producten en diensten.

Het door het bedrijf voeren van regie over het wegnemen en publiceren van kwetsbaarheden in beheersmaatregelen is essentieel voor het borgen van de bedrijfscontinuïteit.

[3] Voor een strafrechtelijke procedure geldt dat het bedrijf kan uitspreken in principe geen aangifte bij de politie of het openbaar ministerie te zullen doen. Het bedrijf kan niet uitspreken geen vervolging in te zullen stellen. Dat is immers het primaat van het openbaar ministerie.

Zaken doen met partners (bijvoorbeeld klanten, medewerkers, leveranciers en onderzoekers) die de TTP-policy onderschrijven en behoren tot het bedrijfsinformatie ecosysteem geeft comfort over de goede intenties van de partners en als er toch onduidelijkheden zijn het de-escaleren op basis van mediation. Dit wil niet zeggen dat een gang naar de rechter is geblokkeerd. First Lawyers advocaten onderhouden het juridische model van de-escalatie.

Organisations and vulnerability disclosure

Source: ENISA study on the economics of vulnerability disclosure

Businesscase

De bedrijfsleiding vraagt met behulp van een bewustwordings- en trainingsprogramma CVD aan het management en de medewerkers aandacht voor het effectief organiseren informatieveiligheid, in het bijzonder Coordinated Vulnerability Disclosure (CVD). Wat is de reden om dat te doen?

Voor elke bedrijfssituatie is de noodzaak en de aanpak voor het organiseren van informatieveiligheid anders. Organisaties met een beperkte bedrijfsomvang zullen een sectoraal programma kiezen en bedrijven met enige omvang zullen een bedrijfsspecifiek programma wensen. Voor elk bedrijfstype is het belangrijk dat vanuit het perspectief van de bedrijfsleiding, het management en de medewerkers een businesscase wordt samengesteld voor het effectief organiseren van CVD.

In het algemeen geldt dat het niet organiseren van CVD leidt tot onbekende aansprakelijkheids- en kostenrisico's die de bedrijfscontinuïteit bedreigen. Het wel organiseren van CVD brengt bescheiden kosten met zich mee en meer zekerheid

over de continuïteit van de bedrijfsvoering. Wij gebruiken de ENISA-studie voor het benoemen van kosten en opbrengsten:

Kosten

- Omzetafhankelijke licentie voor het gebruik van het MYOBI Vertrouwensnetwerk;
- Implementatie- en beheerkosten; en
- Kosten op afroep van externe professionals met technische, organisatorische en of juridische kennis en ervaringen (loodgieterscontracten).

Opbrengsten

- Met behulp van kennis- en verandermanagement de bewustwording en kennis bij het management en de medewerkers op het vlak van informatieveiligheid, in het bijzonder CVD, verhogen en verankeren. **Waardepropositie**: *uitbouwen van de bereidheid bij het management en medewerkers de informatieveiligheid te borgen door proactief actie te ondernemen als de informatieveiligheid in het geding is*;
- Effectieve communicatie en marketing gericht op onbekende onderzoekers die kwetsbaarheden in de infrastructuur en of toepassingen hebben gevonden. **Waardepropositie**: *zekerheid over de robuustheid van de infrastructuur en toepassingen die toegang kunnen geven tot bedrijfs- en persoonsgegevens (inclusief bedrijfsgeheimen)*;
- Het bedrijf maakt – met behulp van smart contracting – effectieve afspraken met partners (bijvoorbeeld klanten, externe en interne medewerkers en leveranciers) en onbekende onderzoekers over het organiseren van de aansprakelijkheden die voortvloeien uit CVD. **Waardepropositie**: *beperken en beheersbaar maken van de aansprakelijkheids- en kostenrisico's, afwerken van geconstateerde kwetsbaarheden in infrastructuren en of toepassingen*;
- Het bedrijf organiseert de informatieveiligheid effectiever en kostenefficiënter. **Waardepropositie**: *bewustzijn en kennisontwikkeling, effectieve afspraken met partners, en CVD leveren de randvoorwaarden voor een betere en kostenefficiëntere organisatie informatieveiligheid;*
- De-escalatie bij het afwerken van beveiligingsincidenten en datalekken op basis van het mediationreglement uit de TTP-policy dat van toepassing is vanwege de in de CVD-verklaring opgenomen vertrouwensrol van MYOBI. **Waardepropositie**: *het beperken van de aansprakelijkheids- en kostenrisico's bij het afwerken van geconstateerde kwetsbaarheden;*
- Voorkomen dat criminele organisaties kwetsbaarheden benutten met als resultaat dat het bedrijf wordt afgeperst. **Waardepropositie**: *de aansprakelijkheids- en kostenrisico's beperken bij het afwerken van geconstateerde kwetsbaarheden.*

Neem contact op met onze sales-afdeling

Een gebruiker van het vertrouwensnetwerk is met behulp van het bewustwordings- en trainingsprogramma CVD in staat CVD voor de organisatie te organiseren. Het komt voor dat het aan capaciteit ontbreekt de implementatie en of het beheer te bemensen. Wij bespreken graag met u de mogelijkheden van uitbesteden van werkzaamheden.

sales@myobi.eu

+31 (0) 70 362 18 07

REGISTREER

myobi.eu/nl