Duthler Associates
law, ICT & organisation

White paper

Organiseren Coordinated Vulnerability Disclosure (CVD)

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 liggen. 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 relatie met het bedrijf voorwaarden willen stellen.

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

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 deze whitepaper bespreken wij een plan van aanpak en de ondersteuning hierbij.

Plan van aanpak

Bewustwording

Het introduceren van CVD vereist dat de bedrijfsleiding en de sleutelfunctionarissen die hierbij betrokken moeten worden een gelijk kennisniveau hebben van CVD en de invoering hiervan willen ondersteunen. Een informatieverstrekking met een gelijk verhaal zorgt ervoor dat een ieder op een gelijk niveau van kennis komt. De acceptatie van de noodzaak om CVD in te voeren kan tijdens een workshop worden gediscussieerd

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. Het digitaal forensisch bureau geeft via haar leeromgeving (tenant) aan haar relaties toegang tot bewustwordings- en trainingsprogramma's vanuit een technisch perspectief. First Lawyers verzorgt ook een dergelijk programma vanuit een bestuurlijk en juridisch perspectief. Desgewenst kunnen First Lawyers en het digitaal forensisch bureau gezamenlijk bewustwordings- en trainingsworkshops verzorgen.

De Contract Board, waarvan First Lawyers lid is, onderhoudt een portfolio met draaiboeken en contracttypen CVD. De advocaten van First Lawyers 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.

Zij kan uiteraard ook professionele ondersteuning inroepen voor een bedrijfsspecifieke implementatie en onderhoud van de CVD.

De voorbereiding bestaat uit:

- Opstellen van een CVD-Beleid;
- Het toewijzen van taken, bevoegdheden en verantwoordelijkheden;
- Het operationaliseren van het beleid naar interne processen en verantwoording hierover;
- Het communiceren van het beleid en de uitwerking hiervan naar medewerkers;
- Het opleiden van betrokken medewerkers;
- Opstellen van de CVD-verklaring. Deze verklaring sluit aan op de TTP-policy 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;
- 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 advocaten van First Lawyers afspreken;
- Het bedrijf maakt met het digitaal forensisch bureau afspraken over de scope en reikwijdte van de werkzaamheden inzake CVD; en
- MYOBI zorgt ervoor dat alle afspraken en documenten 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.

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).

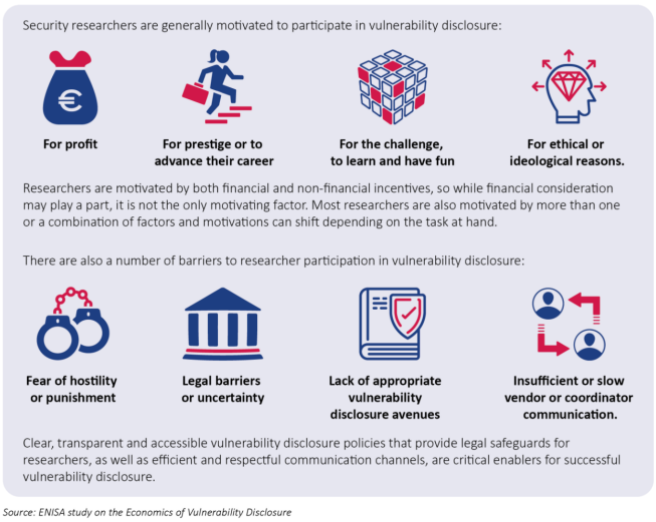
Processen

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 worden onderzocht en op hun risico's voor discontinuïteit worden 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.



Source: ENISA study on the Economics of Vulnerability Disclosure

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, dat 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 een bewustwordings- en trainingsprogramma CVD. De onbekende onderzoeker kan – als hij dat wil - met behulp van een pseudoniem de kwetsbaarheid melden bij het bedrijf.[2]

[2] Nb:

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 bedrijfsprocescoördinator.

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 zoals een professional van het digitaal forensisch bureau of een advocaat. 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.

De bedrijfsprocescoördinator

Vanuit het informatie ecosysteem op het MYOBI Vertrouwensnetwerk starten bedrijven bedrijfsprocessen. Er kunnen verschillende rollen bestaan in een bedrijfsproces, waaronder de rol van bedrijfsproces-coördinator.

Alle informatie in het bedrijfsproces is geencrypt en is slechts toegankelijk voor de deelnemers van het proces. De auditlog van MYOBI geeft inzage in het gebruik van de informatie.

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.

Beheren

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

- 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 leveranciers en bedrijven te melden. Tegelijkertijd is een onbekende onderzoeker voorzichtig. De onderzoeker wil de leverancier en of 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, kunnen de leverancier en of het bedrijf met de onbekende onderzoeker informatie uitwisselen en afspraken voorbereiden. Als er voldoende vertrouwen tussen partijen ontstaat kunnen partijen overeenkomsten sluiten.

[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.

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:

Source: ENISA study on the economics of vulnerability disclosure

Kosten

- Omzetafhankelijke licentie voor het gebruik van het MYOBI Vertrouwensnetwerk;
- Implementatie- en beheerkosten; en
- Kosten op afroep van het digitaal forensisch bureau en advocaten (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, te verhogen en te 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; en

  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.*

Wij zijn graag bereid de door u opgestelde businesscase met u te bespreken.

Duthler Associates
law, ICT & organisation

Afspraak maken en contact

Wilt u meer weten? Neem dan contact op met ons op via de onderstaande gegevens. Of bezoek onze website: www.duthler.nl

Kantoor:

Frankenslag 137

2582 HH Den Haag

+31 (0) 70 392 22 09

info@duthler.nl