Coordinated Vulnerability Disclosure

Voorheen Responsible Disclosure
ISO 27001:2017

Safeguard

DEEL 1. BETEKENIS EN DOEL

1.1 Betekenis Coordinated Vulnerability Disclosure (CVD)

Coordinated Vulnerability Disclosure (CVD), of voorheen responsible disclosure genoemd, is het op een verantwoorde wijze openbaar maken van ICT-kwetsbaarheden of incidenten. Hierbij werken de melder en Safeguard B.V. met elkaar samen. Een ieder kan een CVD-melding doen bij de support afdeling van Safeguard B.V. waarna Safeguard B.V. de kans heeft om de kwetsbaarheid op te lossen.

Voor meer informatie kan de informatie van het NCSC worden geraadpleegd.

1.2 Doel inzet CVD

Het doel van het CVD is het verhogen van de veiligheid van ICT-systemen door kennis over ICT-kwetsbaarheden te delen. Wij kunnen kwetsbaarheden dan verhelpen, voordat deze actief misbruikt zullen worden door derden. Hierdoor kan de schade zoveel mogelijk worden voorkomen of beperkt.

1.3 Beleid

De samenwerking opzoeken met de gebruikers kan ons helpen om de algehele beveiliging van systemen te verbeteren. Voorop staat dat stakeholders zich over en weer houden aan de gemaakte afspraken over het melden van ICT-kwetsbaarheden. Ons beleid voor CVD is erop gericht om ter goeder trouw gedane melding van kwetsbaarheden niet te bestraffen, maar juist te belonen. Dit betekent dat Safeguard B.V. geen aangifte doet als door de melder is voldaan aan de volgens het CVD beleid geldende spelregels.

Safeguard B.V. reserveert interne capaciteit en richt een proces in om adequaat op meldingen te kunnen reageren. Zo hebben wij onze support afdeling aangewezen om deze meldingen in ontvangst te nemen.

1.3 Communicatie

Het CVD beleid van Safeguard B.V.wordt kenbaar gemaakt via onze algemene website www.safeguardapp.nl .

DEEL 2 – DE COORDINATED VULNERABILITY DISCLOSURE (CVD)

Heeft u een kwetsbaarheid in onze systemen ontdekt? Laat het ons zo snel mogelijk weten!

Wij vinden de veiligheid van onze systemen, ons netwerk en onze producten zeer belangrijk. Daar doen wij veel voor. Zo zijn wij ISO 27001 gecertificeerd en hebben wij een integraal beveiligingsbeleid. Ondanks dat wij heel veel zorg besteden aan informatieveiligheid, kan het voorkomen dat u een zwakke plek ontdekt. Wij willen dan zo snel mogelijk maatregelen kunnen nemen om deze zwakheden of kwetsbaarheden op te lossen. Heeft u een kwetsbaarheid ontdekt? Laat het ons dan zo snel mogelijk weten!

Onze contactgegevens

Email: support@safeguardapp.nl
Tel: +31 (0) 85 902 1090
Email Security Officer: gertjan@safeguardapp.nl

Beleid

Wij hanteren voor meldingen de zogenaamde 'Responsible disclosure' of 'CVD' principes. Dat betekent dat wanneer u verantwoord handelt en indien u netjes omgaat met de gevonden kwetsbaarheden, wij dit waarderen en ook graag belonen. Wanneer u als melder op enigerlei wijze een kwetsbaarheid heeft geconstateerd kunt u een bijdrage leveren aan de veiligheid van onze ICT-systemen. U meldt de kwetsbaarheid aan ons zodat wij deze kwetsbaarheid kunnen (laten) verhelpen en openbaar maken. U erkent hiermee dat
u een belangrijke maatschappelijke bijdrage kunt leveren, door kwetsbaarheden op gecoördineerde wijze en in samenwerking met ons openbaar te maken.

Onze spelregels

- Houd rekening met de proportionaliteit en subsidiariteit van de aanval of inbreuk. Dat wil zeggen dat u in ieder geval niet verder gaat dan noodzakelijk om de kwetsbaarheid aan te tonen, en in eerste instantie de kwetsbaarheid meldt bij de (systeem/informatie) eigenaar. Kunt u bijvoorbeeld bij gegevensrecords? Dan is het voldoende dit aan te tonen middels bijvoorbeeld het meesturen van de eerste regel of kolom.
- Doe de melding direct nadat u deze heeft ontdekt.
- Verstrek voldoende informatie. Stuur het IP-adres of de URL van het getroffen systeem mee, indien bekend.
- Bevestig bij uw melding dat u zich aan het CVD-beleid houdt en zult blijven houden.
- Versleutel de bevindingen indien mogelijk om te voorkomen dat de informatie in verkeerde handen valt.
- Stuur ook uw contactgegevens mee (inclusief naam, e-mailadres en eventueel uw telefoonnummer).
- Ga verantwoordelijk met de door u opgedane kennis om. Deel de informatie over de kwetsbaarheid of het beveiligingsprobleem niet met derden.
- Verwijder op zijn laatst na de afhandeling van de melding alle vertrouwelijke gegevens die zijn verkregen in het onderzoek.

- En, wanneer u een onderzoek doet, ga dan zelf zorgvuldig om met onze systemen en netwerken. Plaats bijvoorbeeld geen malware, wijzig of kopieer zo min mogelijk en alleen indien dit echt noodzakelijk is voor het melden. Verwijder geen informatie in onze systemen.

Onze beloftes

- Wij reageren binnen een redelijke termijn op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- We zullen u laten weten wanneer wij uw melding in goede orde hebben ontvangen en welke opvolging wij daaraan hebben gegeven.
- Wij behandelen uw melding en gegevens vertrouwelijk, tenzij het wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is om uw informatie te verstrekken.
- Of wij overgaan tot publicatie, bespreken wij eerst met u. In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Mochten er meerdere organisaties betrokken zijn, dan is het uitgangspunt dat pas gepubliceerd kan worden als alle organisaties het hiermee eens zijn.
- Wij bieden een beloning als dank voor uw hulp in de vorm van een cadeaubon. Voorwaarde hiervoor is dat het een voor Safeguard B.V.een nog onbekend beveiligingsprobleem betreft.

Wanneer u de melding volgens de procedure doet, dan hebben wij geen reden om juridische consequenties te verbinden aan uw melding. We zullen elke situatie apart afwegen. Houd er rekening mee dat wij hierbij meewegen of er een vermoeden bestaat op misbruik van de zwakheid of onze informatie, of als de kennis over de zwakheid met derden is gedeeld.

Communicatie

De communicatie naar aanleiding van een melding zal als volgt verlopen:

- Nadat u contact heeft opgenomen met Safeguard B.V. nemen wij contact op over de gevonden kwetsbaarheid. Wij vermelden daarbij wat onze reactietermijn zal zijn voor een eerste inhoudelijke reactie.
- Gedurende deze eerste fase kunnen wij met u overleggen wat een indicatie is van de te verwachten oplossingstermijn.
- Wij geven u regelmatig een update. En indien nodig bespreken wij met u hoe we het inlichten van mogelijk ander geraakte organisaties zullen aanpakken.
- Na afloop van de procedure maken wij afspraken met u over (publieke) erkenning en beloning voor het melden. Wij houden daarbij rekening met uw input voor het ontdekkingsproces.

Let op:

De bedoeling van ons CVD-beleid is niet om je uit te nodigen om onze ICT-systemen of netwerken uitgebreid te scannen of te infiltreren om zwakke plekken te ontdekken. Gebruik ook geen “bruteforce”- of “denial-of-service”- of “social engineering” methodes voor toegang tot systemen.

Wij willen wel graag met u samenwerken om onze en uw informatie en onze systemen beter te kunnen beschermen.

Formulier – inhoud vertrouwelijk

Voor- en achternaam	
E-mailadres*	
Telefoonnummer	
Soort kwetsbaarheid*	
Toelichting en samenvatting kwetsbaarheid*	
Waarom is deze kwetsbaarheid het melden waard?	
Welke kans bestaat er op het uitbuiten door een kwaadwillende?	
Welke kans op schade acht u aanwezig?	
Domein of IP-adres waar de melding betrekking op heeft*	
Heeft u nog aanvullende opmerkingen of vragen?	
NAW gegevens voor een eventuele beloning	
- Voeg bijlagen toe -	
- Raadpleeg onze privacyverklaring voor meer informatie over de verwerking van uw persoonsgegevens.	

DEEL 3 – OVERZICHT VAN MELDINGEN

3.1 Overzicht van meldingen in 2020

Het overzicht van meldingen via onze CVD procedure is opgenomen in SmartManSys.

Er zijn geen meldingen gedaan in 2020