



stichting voor christelijk primair onderwijs

Model Responsible Disclosure voor medewerkers

Stichting ProCon

Bron

Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet

Bewerkt door:

Stichting ProCon, F.v.A.

Versie	Status	Datum	Auteur	Omschrijving
1.0		17-5-2019		

Vastgesteld door het Bestuur van Stichting ProCon

Versie	Datum	Naam	Functie
		T. Diepeveen	Bestuurder
Handtekening			

Vastgesteld door de GMR van Stichting ProCon

Versie	Datum	Naam	Functie
Handtekening			
Handtekening			

Model Responsible Disclosure voor medewerkers

Bij stichting ProCon vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één van onze systemen hebt gevonden, dan horen wij dit graag, zodat we zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar security@stichting-procon.nl of telefonisch contact op te nemen met de administratie;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of (persoons) gegevens van derden in te kijken, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen totdat deze is verholpen en alle (vertrouwelijke) gegevens die zijn verkregen via de lek direct na het verhelpen van de lek te wissen;
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden;
- Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen verhelpen. Meestal is het IP adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden kan meer informatie nodig zijn.

Wij zeggen toe dat:

- Wij binnen 3 dagen reageren op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Als u zich aan bovenstaande voorwaarden hebt gehouden wij geen juridische stappen tegen u zullen ondernemen met betrekking tot de melding¹;
- Wij uw melding vertrouwelijk behandelen en uw persoonlijke gegevens niet zonder uw toestemming met derden zullen delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk;
- Wij u op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid;
- Wij, in berichtgeving over het gemelde probleem, uw naam, indien u dit wenst, vermelden als de ontdekker. Wij streven er naar om alle problemen zo snel mogelijk op te lossen en wij worden graag betrokken bij een eventuele publicatie over het probleem nadat het is opgelost.

¹ Let op: ons beleid voor responsible disclosure is geen uitnodiging om ons netwerk uitgebreid te scannen om zwakke plekken te ontdekken. Er bestaat een kans dat u tijdens uw onderzoek handeling uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat stichting ProCon geen aangifte tegen u zal doen sluit niet uit dat er een strafrechtelijk onderzoek naar uw handelen gehouden kan worden dan wel dat u strafrechtelijk kunt worden veroordeeld.