RESPONSIBLE DISCLOSURE ZYNYO B.V.

Bij Zynyo vinden wij de veiligheid van onze systemen, ons netwerk en onze producten erg belangrijk. Ondanks dat wij heel veel zorg besteden aan security, kan het voorkomen dat een zwakke plek wordt ontdekt. Indien dat het geval is, dan horen wij dit graag zo snel mogelijk, zodat we snel maatregelen kunnen treffen.

Zwakke plekken kunnen op twee manieren worden ontdekt: je loopt ergens per ongeluk tegenaan bij normaal gebruik van een digitale omgeving, of je doet expliciet je best om een zwakke plek te vinden. Gezien de aard van onze dienstverlening, kunnen zwakke plekken uitmonden in datalekken en daarom in te kwader trouw omstandigheden leiden tot ernstige inbreuken op iemands privacy.

Ons Responsible Disclosure-beleid is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen op zwakke plekken. Wij monitoren ons netwerk zelf. Uit verantwoording naar onze klanten willen we niet oproepen tot hack-pogingen op de infrastructuur. Echter, ook hiervoor geldt dat we zo snel mogelijk van u willen vernemen zodra er kwetsbaarheden worden gevonden, zodat wij deze adequaat kunnen verhelpen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:
- Uw bevindingen zo snel mogelijk te mailen naar support@zynyo.com.
- Misbruik de zwakheid niet door bijvoorbeeld het downloaden, veranderen of verwijderen van gegevens. Wij nemen uw melding altijd serieus en gaan elk vermoeden van een kwetsbaarheid uitzoeken, ook zonder ‘bewijs’.
- Deel het probleem niet met anderen totdat het is opgelost.
- Maak geen gebruik van aanvallen op fysieke beveiliging, van social engineering of hacking tools, zoals vulnerability scanners.
- Geef ons voldoende informatie om het probleem te reproduceren, zodat wij het zo snel mogelijk kunnen oplossen. 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 nodig zijn.

Wat wij beloven:
- Wij reageren binnen drie werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen. Een uitzondering hierop is politie en justitie, in geval van aangifte of indien gegevens worden opgeëist.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker.
- Het is helaas niet mogelijk bij voorbaat juridische stappen tegen u uit te sluiten. We willen elke situatie apart kunnen afwegen. We achten ons zelf moreel verplicht om aangifte te doen, bijvoorbeeld bij de Autoriteit Persoonsgegevens, op moment dat we het vermoeden hebben dat de zwakheid of gegevens misbruikt worden, of dat u kennis over de zwakheid met anderen heeft gedeeld. U kunt erop rekenen dat een toevallige ontdekking in onze online-omgeving niet tot aangifte zal leiden.
- Als dank voor uw hulp bieden wij een beloning voor elke melding van een ons nog onbekend beveiligingsprobleem. De grootte van de beloning bepalen wij aan de hand van de ernst van het lek en de kwaliteit van de melding.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen, alle betrokken partijen op de hoogte te houden en wij worden graag betrokken bij een eventuele publicatie over het probleem, nadat het is opgelost.