Passend Onderwijs IJmond

RESPONSIBLE DISCLOSURE VOOR MEDEWERKERS

Bij Samenwerkingsverband Passend Onderwijs IJmond (SWV PO IJmond), 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 heeft 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 info@passendonderwijsijmond.nl of telefonisch contact op te nemen met onze FG, Jessica Bunnik;
- 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 nodig zijn.

Wij zeggen toe dat:

- Wij reageren binnen 3 werkdagen op uw melding met onze beoordeling van de melding en een verwachte datum voor een oplossing;
- Als u zich aan bovenstaande voorwaarden heeft gehouden zullen wij geen juridische stappen tegen u ondernemen met betrekking tot de melding*;
- Wij behandelen uw melding vertrouwelijk en zullen uw persoonlijke gegevens niet zonder uw toestemming met derden delen tenzij dat noodzakelijk is om een wettelijke verplichting na te komen. Melden onder een pseudoniem is mogelijk;
- Wij houden u op de hoogte van de voortgang van het verhelpen van de kwetsbaarheid;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam 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.

Passend Onderwijs IJmond

* 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 SWV PO IJmond 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.

Cc/by/3.0 NL

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door SWV PO IJmond,
versie mei 2018

Responsibledisclosure.nl is een initiatief dat is ontstaan vanwege het wederzijdse gebrek aan vertrouwen tussen veel hackers met goede bedoelingen en instellingen met lekke systemen. Dit gebrek aan vertrouwen heeft voor veel onnodige schade gezorgd. Met duidelijke afspraken hoop ik een samenwerking te bevorderen waar hackers, instellingen én de mensen wiens gegevens in de talloze databases staan die op het internet zijn aangesloten.

Hackers die gedreven door nieuwsgierigheid lekken vinden bevinden zich vaak in een juridisch grijs gebied. Ook al hebben ze geen kwade bedoelingen is het vaak niet aantrekkelijk om de instelling te informeren over de lek. Het gebeurd vaak dat instellingen meldingen niet oppikken, slecht communiceren met de melder of zelfs ontkennen dat er een probleem is. In meer extreme gevallen kan het zelfs voorkomen dat een melder te maken krijgt met strafrechtelijke gevolgen. Het is dan ook begrijpelijk dat veel hackers niet de moeite nemen om lekken te melden.

Veel instellingen zijn niet ingericht om om te gaan met meldingen van buitenaf. Meldingen blijven liggen bij een klantenservice die getraind is om mensen gerust te stellen in plaats van onderbouwde kritiek mee te nemen. Wanneer een lek bekend wordt zijn verantwoordelijkheden binnen de organisatie niet duidelijk waardoor slechte beslissingen genomen worden.

Wanneer bedrijven nadenken over hoe ze omgaan met beveiligingslekken en dit duidelijk naar buiten communiceren weten hackers beter waar ze aan toe zijn wanneer ze een lek willen melden. Dit voorkomt onzekerheid en paniek aan beide kanten en beperkt schade zoveel mogelijk. Door deze tekst en uitleg beschikbaar te stellen hoop ik zoveel mogelijk bedrijven en hackers te helpen.