Protocol verantwoord melden beveiligingslekken (responsible disclosure)

Stichting Interconfessioneel (rk/pc) Voortgezet Onderwijs in het Gooi

1 Protocol verantwoord melden beveiligingslekken (responsible disclosure)

Bij SIVOG vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks de 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 om die zo mogelijk te dichten. Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te beschermen.

Wij vragen u:

- Uw bevindingen te melden door te mailen naar privacy@sivog.nl of telefonisch contact op te nemen met het hoofd Bedrijfsvoering, bereikbaar via het algemeen nummer van Willem de Zwijger College 035 – 692 76 00;
- 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 met een ontvangstbevestiging en nemen contact met u op over het verdere proces;
- Wij zullen in overleg met u afspraken maken over de termijnen van bekendmaking, afhankelijk van de tijd die nodig is voor het herstel van de kwetsbaarheid. Voor software is een redelijke termijn 60 dagen, voor hardware 6 maanden. Als een kwetsbaarheid moeilijk of niet is op te lossen of indien er (te) hoge koste mee zijn gemoeid kunnen melder en SIVOG besluiten om de kwetsbaarheid niet openbaar te maken.
- 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 proces van verhelpen van de kwetsbaarheid;
- In berichtgeving over het gemelde probleem zullen wij, indien u dit wenst, uw naam vermelden als de ontdekker. Wij streven ernaar 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.
- Wij kunnen in overleg met u afspreken om de bredere ict-gemeenschap te informeren over de kwetsbaarheid, als het aannemelijk is dat de kwetsbaarheid ook op andere plaatsen aanwezig is.

* 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

handelingen uitvoert die volgens het strafrecht strafbaar zijn. Het feit dat de school 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.