

Melding beveiligingsprobleem (responsible disclosure)

Bij het Stedelijk Gymnasium Leiden vinden wij de veiligheid van onze informatiesystemen (internet en bijbehorende hardware en software) erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) is. Als jij 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 jou samenwerken om de leerlingen, medewerkers en onze systemen beter te kunnen beschermen.

Wij vragen jou:

- Je bevindingen zo snel mogelijk te mailen naar informatiemanager@gymnasiumleiden.nl; leerlingen kunnen deze ook door geven aan hun mentor. Deze zal de leerling vervolgens in contact brengen met onze afdeling ICT;
- De kwetsbaarheid niet te misbruiken door bijvoorbeeld meer informatie/data te downloaden dan nodig is om het lek aan te tonen of informatie van andere leerlingen, docenten of andere medewerkers in te kijken, te verwijderen of aan te passen;
- De kwetsbaarheid niet met anderen te delen, totdat deze is verholpen en alle informatie die verkregen is via het lek direct na het verhelpen van het lek te wissen;
- Geen gebruik te maken van aanvallen op de beveiliging van de school;
- De school voldoende informatie te geven om het probleem te kunnen vinden 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 meer ingewikkelde kwetsbaarheden kan extra informatie nodig zijn.

Wij beloven dat:

- Je binnen 3 dagen van ons te horen krijgt hoe we de kwetsbaarheid gaan oppakken en wanneer wij hiervoor een oplossing verwachten te hebben;
- Als je de kwetsbaarheid netjes gemeld hebt en via de bovenstaande stappen gehandeld hebt, wij geen melding zullen maken bij de politie*;
- Wij jouw melding vertrouwelijk behandelen en dat jouw persoonlijke gegevens niet zonder jouw toestemming met anderen delen worden, tenzij dit wettelijke verplicht is;
- Wij je op de hoogte houden van de voortgang van het verhelpen van de kwetsbaarheid.
- wij in berichtgeving de naam van de ontdekker zullen vermelden, indien je dit wenst. 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.

* 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 je tijdens jouw 'zoektocht' handelingen uitvoert die strafbaar zijn. Het feit dat het Stedelijk Gymnasium Leiden geen aangifte tegen je zal doen, sluit niet uit dat er een strafrechtelijk onderzoek naar jouw handelen gehouden kan worden dan wel dat je strafrechtelijk kunt worden veroordeeld.

Geschreven door Floor Terra (responsibledisclosure.nl), bewerkt door Kennisnet en Stedelijk Gymnasium Leiden.

MELDINGSFORMULIER ONTDEKKER BEVEILIGINGSINCIDENT STEDELIJK GYMNASIUM LEIDEN
DIT FORMULIER MAILEN NAAR: INFORMATIEMANAGER@GYMNASIUMLEIDEN.NL

1. DATUM/PERIODE VAN HET BEVEILIGINGSINCIDENT/DATALEK:

2. NAAM MELDER (VOOR- EN ACHTERNAAM):

3. FUNCTIE /KLAS:

4. EMAILADRES (BIJ VOORKEUR SCHOOLMAIL, INDIEN LEERLING OF MEDEWERKER):

5. SOORT INCIDENT: VERLIES OF DIEFSTAL:

6. VOND HET INCIDENT BUITEN OF BINNEN SCHOOL PLAATS?

7. KORTE BESCHRIJVING TOEDRACHT:

8. OM WAT VOOR GEGEVENS GAAT HET (WEL OF GEEN PERSOONSgegevens)?

9. WIE IS VERANTWOORDELIJK VOOR HET DATALEK (PERSOON/ORGANISATIE/BEDRIJF)?

10. WELKE ACTIE IS AL ONDERNOMEN?