Responsible Disclosure

Colofon:
Vastgesteld door de schoolleiding: maart 2025
Ingestemd door MR: 2 april 2025

Inleiding

Wij vinden de veiligheid van onze informatiesystemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen (internet en bijbehorende hardwaren en software) kan het voorkomen dat er toch een zwakke plek (kwetsbaarheid) gevonden wordt. Als er een zwakke plek wordt gevonden horen wij dit graag en zo snel mogelijk. De werkwijze hiervoor is opgenomen in een zogenaamd Responsible Disclosure.

Bij wie melden?

Ziet u een zwakke plek in een ICT-systeem van het LCL? Voelt u zich door deze kennis (mede)verantwoordelijk en wilt u dit bij ons bekend maken? Meld de kwetsbaarheid voordat u dit aan de buitenwereld kenbaar maakt. Zo kan het LCL eerst maatregelen treffen. Een zwakke plek in een ICT-systeem van het LCL kunt u melden via helpdesk@lcl.nl.

Waar u aan moet denken bij Responsible Disclosure

Als u een melding doet van een kwetsbaarheid in een ICT-systeem, denk dan aan de volgende zaken:

- Geef voldoende informatie om het probleem te reproduceren. Zo kan het LCL het probleem zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij ingewikkeldere kwetsbaarheden kan meer nodig zijn;
- Laat contactgegevens (e-mailadres of telefoonnummer) achter zodat het LCL met u contact kan opnemen.
- Doe de melding zo snel mogelijk na ontdekking van de kwetsbaarheid;
- Deel de informatie over het beveiligingsprobleem niet met anderen totdat het is opgelost;
- Ga verantwoordelijk om met de kennis over het beveiligingsprobleem. Verricht geen handelingen die verder gaan dan wat nodig is om het beveiligingsprobleem aan te tonen.

Voldoet u bij uw melding aan deze voorwaarden? Dan verbindt het LCL geen juridische consequenties aan de melding.[1]

Maak geen misbruik van een zwakke plek in een ICT-systeem

Als u een kwetsbaarheid ontdekt, maak hier dan geen misbruik van. Bijvoorbeeld door:

- malware te plaatsen;
- gegevens in een systeem te kopiëren, te wijzigen of te verwijderen (een alternatief hiervoor is een directory listing maken van een systeem);
- veranderingen aan te brengen in het systeem;
- herhaaldelijk toegang te verkrijgen tot het systeem of de toegang te delen met anderen;
- gebruik te maken van het zogeheten ‘bruteforcen’ van toegang tot systemen;
- gebruik te maken van denial-of-service of social engineering.

Wat het LCL doet bij Responsible Disclosure

Heeft u een melding gedaan van een zwakke plek in een ICT-systeem? Het LCL behandelt deze melding als volgt:

- U krijgt binnen 1 werkdag een ontvangstbevestiging van het LCL;
- Het LCL reageert binnen 3 werkdagen op uw melding. Deze reactie bevat een beoordeling van de melding en een verwachte datum voor een oplossing;
- Het LCL houdt u als melder op de hoogte van de voortgang van het oplossen van het probleem;
- Het LCL lost het beveiligingsprobleem zo snel mogelijk op, maar uiterlijk binnen 60 dagen. Het LCL zal samen met u bepalen of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost;

[1] Let op: ons beleid voor Resposible 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 LCL behandelt uw melding vertrouwelijk. Het LCL deelt uw persoonlijke gegevens niet zonder toestemming met derden. Behalve als dit wettelijk of door een rechterlijke uitspraak verplicht is. Het LCL kan, als u dat wilt, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.