Responsible Disclosure

Hoe kan men een zwakke plek in een ICT-systeem van het Christiaan Huygens College (CHC) melden (Responsible Disclosure)?

Een zwakke plek in een ICT-systeem van CHC, kunt u melden aan systeembeheer van CHC. U kunt dit melden via de e-mailadressen:
Frits Philips lyceum-mavo: helpdesk@fritsphilips.eu
Huygens Lyceum: ict.hl@huygenslyceum.nl
Olympia (incl. Onderwijsbureau): helpdesk@huygenscollege.nl

Meld de kwetsbaarheid voordat u dit aan de buitenwereld kenbaar maakt. Zo kan CHC eerst maatregelen treffen. Dit heet Responsible Disclosure. Ook wordt de term Coördinated Vulnerability Disclosure (CVD) wel gebruikt.

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 CHC 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 CHC 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 CHC geen juridische consequenties aan de melding.

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, wijzigen of 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 Christiaan Huygens College doet bij Responsible Disclosure

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

- U krijgt binnen 1 werkdag een ontvangstbevestiging van CHC.
- CHC reageert binnen 3 werkdagen op uw melding. Deze reactie bevat een beoordeling van de melding en een verwachte datum voor een oplossing.
- CHC houdt u als melder op de hoogte van de voortgang van het oplossen van het probleem.
- CHC lost het beveiligingsprobleem zo snel mogelijk op, maar uiterlijk binnen 60 dagen. CHC zal samen met u bepalen of en hoe over het gemelde probleem wordt bericht. Berichtgeving vindt pas plaats nadat het probleem is opgelost.
- CHC biedt een beloning als dank voor de hulp.
- CHC behandelt uw melding vertrouwelijk. CHC deelt persoonlijke gegevens niet zonder toestemming van u met derden. Behalve als dit wettelijk of door een rechterlijke uitspraak verplicht is. CHC kan, als u dat wilt, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.

Maart 2019