# Coördinated Vulnerability Disclosure

## Wat is Coordinated Vulnerability Disclosure?

Regelmatig worden kwetsbaarheden in ict-producten en ict-diensten ontdekt. Ook in de ict-omgeving van jouw school kunnen zwakke plekken of misconfiguraties sluipen. Coordinated Vulnerability Disclosure (CVD) draagt bij aan het beheersen van de kwetsbaarheid van ict-systemen en maakt de systemen veiliger.

Met een CVD-proces kun je de kwetsbaarheden op verantwoorde wijze melden aan jouw school of schoolbestuur. Het is belangrijk om goed contact met de melders te houden, deze melders worden ook beveiligingsonderzoekers of goedwillende/ethische hackers genoemd.  Zo spreek je bijvoorbeeld af of en wanneer de gevonden kwetsbaarheid en de oplossing (patch) openbaar gemaakt mogen worden. Daarom raden we aan om na te denken over een CVD-proces en het beleid van jouw school of schoolbestuur vast te leggen. Op deze manier kan schade zoveel mogelijk worden voorkomen of beperkt.

## Voor wie is dit document bedoeld?

De doelgroep van dit document is de IBP-medewerker of adviseur: jij gaat aan de slag om bestuurders en andere betrokkenen in beweging te krijgen, elk vanuit hun eigen verantwoordelijkheid. Ook coördineer je de uitvoering van de werkzaamheden. De IBP'er is niet inhoudelijk eigenaar van het onderwerp, maar vaak wel een geschikte procescoördinator.

## Stappenplan voor het zelf opzetten van een CVD-proces


### Stap 1: Opstellen van een CVD-beleid.

Begin met het definiëren van de doelen van je CVD-beleid:
- Bepaal de scope van systemen die binnen het beleid vallen.
- Stel vast welke technieken de melders (niet) mogen gebruiken.
- Leg vast hoe meldingen verwerkt worden.

Maak duidelijk aan de melders hoe je als school omgaat met melders, bijvoorbeeld met betrekking tot het respecteren van hun anonimiteit, de berichtgeving en mogelijke (financiële) beloningen voor het doen van een melding. Door 'spelregels' vast te stellen verlaag je de drempel voor een melder om een kwetsbaarheid of fout te melden.

In de bijlage staat een voorbeeld Coordinated Vulnerability Disclosure-beleid van een fictieve school, als aanvulling op de CVD-leidraad van het Nationaal Cyber Security Centrum (NCSC)[1]. De tekst uit het voorbeelddocument in de bijlage kun je eenvoudig aanpassen en overnemen om direct te gebruiken.

### Stap 2: Publiceren van CVD-beleid

Nadat je beleid is opgesteld, maak je dit toegankelijk en zichtbaar. Dit is een voorbeeld van hoe je dit doet: https://www.kennisnet.nl/responsible-disclosure De link plaats je dan onderaan bij je cookiestatement, privacyverklaring, disclaimer etc. Op de websitepagina van de school waarop je dit beleid publiceert, plaats je ook een invulformulier of een exclusief mailadres voor het melden van een kwetsbaarheid.

### Stap 3: Maken en publiceren van een security.txt bestand

Naast het publiceren van het CVD-beleid op je website is het gebruikelijk om het CVD-beleid en contactgegevens in een security.txt-bestand te publiceren. Dit zorgt ervoor dat melders op een standaardplek kunnen kijken en het verlaagt de drempel om iets (geautomatiseerd) te melden. Een security.txt-bestand is opvraagbaar via het pad /.well-known/security.txt op het bijbehorende domein.

[1] https://www.ncsc.nl/contact/documenten/publicaties/2019/mei/01/cvd-leidraad

Een voorbeeld hiervan staat op https://www.kennisnet.nl/.well-known/security.txt. Je kunt je eigen security.txt genereren op https://securitytxt.org.

Met de tool *Internet.nl* kun je testen of het security.txt bestand van je organisatie correct is.

#### Stap 4: Capaciteit

Reserveer interne capaciteit om meldingen effectief en tijdig te behandelen. Zorg voor een specifiek team of afdeling met expertise om meldingen correct te verwerken.

#### Stap 5: Meldingen verwerken

Zorg voor een proces voor het ontvangen en valideren van meldingen. Stuur bij ontvangst direct een bevestiging aan de melder. Vaak moet een melding worden doorgezet naar een it-leverancier. Zorg dus voor een manier om de voortgang van een melding bij te houden.

#### Stap 6: Probleem oplossen

Na validatie van een melding onderneem je actie om de kwetsbaarheid aan te pakken. Houd de melder op de hoogte van de voortgang en eventuele oplossingen.

#### Stap 7: Terugkoppeling

Communiceer transparant naar de melder over de voortgang en oplossingen. Open communicatie versterkt het vertrouwen en bevordert de samenwerking.

Overweeg ook het opzetten van een ’Hall of Fame’ om melders te erkennen voor hun bijdragen. Zeker voor (buitenlandse) hackers die een carrière in cybersecurity opbouwen is erkenning die ze kunnen delen (al dan niet publiek) een belangrijke motivatie.

## Verder lezen

- NCSC (2019) Leidraad Coordinated Vulnerability Disclosure (CVD)
- NCSC (2023) Handreiking security.txt | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)

# Bijlage 1: CVD beleid

## Coördinated Vulnerability Disclosure

<pas de blauwe tekst aan, zodat deze aansluit bij het beleid van jouw onderwijsinstelling>

Onze school <schoolnaam> hecht veel belang aan de beveiliging van haar systemen. Ondanks alle voorzorgsmaatregelen blijft het mogelijk dat er een zwakke plek in de systemen zit. Wanneer je een zwakke plek in één van onze systemen ontdekt, vernemen wij dit graag van je. Dan kunnen wij snel gepaste maatregelen nemen. Door het maken van een melding verklaar je je akkoord met onderstaande afspraken over Coordinated Vulnerability Disclosure en zal <schoolnaam> je melding conform onderstaande afspraken afhandelen.

## Wij vragen het volgende van je:

- Mail je bevindingen naar <e-mailadres>. Versleutel de bevindingen indien mogelijk met <versleutelingsmethodiek> om te voorkomen dat de informatie in verkeerde handen valt.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. 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 krijgen graag tips die ons helpen het probleem op te lossen. Beperk je daarbij wel graag tot verifieerbare feiten die betrekking hebben op de door jou geconstateerde kwetsbaarheid. We hebben geen behoefte aan reclame voor specifieke (beveiligings)producten.
- Als je je contactgegevens achterlaat, kunnen we contact met je zoeken om samen te werken aan een veilig resultaat. Laat minimaal één e-mailadres of telefoonnummer achter.
- Dien de melding alsjeblieft zo snel mogelijk in na ontdekking van de kwetsbaarheid.

## De volgende handelingen zijn niet toegestaan:

- Het plaatsen van malware, noch op onze systemen noch op die van anderen.
- Het zogeheten ’bruteforcen’ van toegang tot systemen, behalve als dat noodzakelijk is om aan te tonen dat de beveiliging op dit vlak ernstig tekortschiet. Dat wil zeggen als het heel eenvoudig is om met openbaar verkrijgbare en betaalbare hardware en software een wachtwoord te kraken waarmee het systeem ernstig kan worden gecompromitteerd.
- Het gebruikmaken van social engineering.
- Het openbaar maken of aan derden verstrekken van informatie over het beveiligingsprobleem voordat het probleem is opgelost.
- Het verrichten van handelingen die verder gaan dan wat strikt noodzakelijk is om het beveiligingsprobleem aan te tonen en te melden. In het bijzonder waar het gaat om het verwerken (waaronder het inzien of kopiëren) van vertrouwelijke gegevens waar je door de kwetsbaarheid toegang toe hebt gehad. In plaats van een complete database te kopiëren, kun je normaliter volstaan met bijvoorbeeld een directorylisting. Het wijzigen of verwijderen van gegevens in het systeem is nooit toegestaan.
- Het gebruikmaken van technieken waarmee de beschikbaarheid en/of bruikbaarheid van het systeem of services wordt verminderd (DoS-aanvallen).
- Het op wat voor (andere) wijze dan ook misbruik maken van de kwetsbaarheid.

## Wat je mag verwachten:

- Wanneer je aan alle bovenstaande voorwaarden voldoet, zullen wij geen strafrechtelijke aangifte tegen je doen en ook geen civielrechtelijke zaak tegen je aanspannen.
- Als blijkt dat je een bovenstaande voorwaarde hebt geschonden, kunnen wij alsnog besluiten om gerechtelijke stappen tegen je te ondernemen.

- Wij behandelen een melding vertrouwelijk en delen je persoonlijke gegevens niet met derden zonder jouw toestemming, tenzij wij daar volgens de wet of een rechterlijke uitspraak toe verplicht zijn.
- Wij delen de ontvangen melding altijd met het CERT voor het funderend onderwijs. Zo zorgen we ervoor dat scholen hun ervaringen op dit vlak met elkaar delen.
- In onderling overleg kunnen we, als je dit wenst, je naam vermelden als de ontdekker van de gemelde kwetsbaarheid. In alle andere gevallen blijf je anoniem.
- Wij reageren binnen <5> werkdagen op een melding met een (eerste) beoordeling van de melding en eventueel een verwachte datum voor een oplossing.
- Wij lossen het door jou gemelde beveiligingsprobleem zo snel mogelijk op. Daarbij streven we ernaar om je goed op de hoogte te houden van de voortgang en nooit langer dan <90> dagen te doen over het oplossen van het probleem. Wij zijn daarbij vaak wel mede afhankelijk van toeleveranciers.
- In onderling overleg met elkaar kan worden bepaald of en op welke wijze over het probleem wordt gepubliceerd, nadat het is opgelost.
- Wij kunnen je een beloning bieden als dank voor je hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van een erkenning van jouw bijdrage tot een bedrag van maximaal <50> euro. Het moet hierbij wel gaan om een nog onbekend en serieus beveiligingsprobleem.

Met dank aan Floor Terra voor zijn voorbeeldtekst op responsiblediscloSure.nl.

School CERT | 08-10-2024

Voor ondersteuning: support@kennisnet.nl / 0800 321 22 33
Voor vragen over het School-CERT: cert@kennisnet.nl