Responsible Disclosure Policy

Bij waterschap Hunze en Aa's vinden wij de veiligheid van onze systemen, maar met name de beveiliging van gegevens van onze inwoners, erg belangrijk. Systemen kunnen door kwetsbaarheden mogelijkerwijs uitvallen (beschikbaarheid), data binnen het systeem kunnen gewijzigd worden (integriteit) en data kunnen toegankelijk worden voor personen die daar niet voor gemachtigd zijn (vertrouwelijkheid). Ondanks onze zorg voor de beveiliging van onze systemen en de daarmee gepaarde investeringen, kunnen wij niet 100% voorkomen dat er toch een zwakke plek is. Om de veiligheid van de gegevens van onze inwoners en andere bedrijfsinformatie te verzekeren, hebben wij een Responsible Disclosure Policy vastgesteld om meldingen te faciliteren.

Het doel van Responsible Disclosure is het bijdragen aan de veiligheid van ICT-systemen en het beheersen van de kwetsbaarheid van ICT-systemen door kwetsbaarheden op verantwoorde wijze te melden en deze meldingen zorgvuldig af te handelen, zodat schade zo veel als mogelijk kan worden voorkomen of beperkt.

Als u een zwakke plek in een van onze systemen heeft gevonden, horen wij dit natuurlijk graag. Ons doel is om zo snel mogelijk maatregelen te treffen tegen deze kwetsbaarheid. Wij willen graag met uw samenwerking en ondersteuning onze gegevens optimaal beschermen. Daarbij hopen wij dat u ons een redelijke termijn gunt voor het verhelpen van de kwetsbaarheid. We houden 60 dagen aan voor verhelpen van een kwetsbaarheid in software en 6 maanden voor oplossen van kwetsbaarheid in hardware.

Wat u van ons kunt verwachten
- Een ontvangstbevestiging van uw melding binnen 3 werkdagen
- Anonimiteit van u, tenzij wetgeving wordt overtreden
- Goed overleg tussen u en ons met betrekking tot het verhelpen van de kwetsbaarheid. U wordt op de hoogte gesteld van onze beoordeling van uw melding en de verdere stappen die in het proces worden genomen
- Een zo spoedig mogelijke verwerking van uw melding
- Een gepast gebaar (cadeaubon), afhankelijk van de volledigheid van de melding en de omvang van de kwetsbaarheid.

Wat wij van u verwachten
- Verantwoordelijkheid voor het eigen handelen
- Een zo spoedig mogelijke melding na het ontdekken van de kwetsbaarheid
- Een melding op een vertrouwelijke manier, om te voorkomen dat anderen toegang krijgen tot deze informatie
- Geen toepassing van social engineering
- Een kwetsbaarheid niet verder te nutten dan noodzakelijk is om de kwetsbaarheid vast te stellen
- Geen gegevens van het systeem te kopiëren, te wijzigen of te verwijderen (een directory listing van het systeem maken mag wel)
- Geen veranderingen in het systeem aanbrengen
- Niet herhaaldelijk toegang tot het systeem nemen of de toegang met anderen delen
- Geen gebruik maken van *brute force* voor toegang tot systemen.
- De kwetsbaarheid pas openbaar maken nadat dit is overeengekomen tussen ons en u. Waarbij alle betrokken organisaties goed zijn geïnformeerd en passende maatregelen hebben kunnen nemen. Openbaar maken van de kwetsbaarheid kan pas na de termijn die wij daarvoor hebben gesteld.
- Geen mogelijke of feitelijke schade aan gebruikers, systemen, data of applicaties toebrengen.
- Geen gebruik maken van een exploit dat data van gebruikers bekijkt, waarbij corruptie van data betrokken is of dat functies van onze diensten kan verstoren.
- Geen port scans uitvoeren op onze netwerkblokken of een DDoS aanval uitvoeren
- In overleg met ons overwegen of een bredere ICT-community op de hoogte moet worden gebracht van de kwetsbaarheid, zoals bijvoorbeeld een melding aan het NCSC.

Inhoud van de melding:

- De volledige gegevens van het beveiligingsprobleem, inclusief de Proof-of-Concept URL, de details van het systemen waar de tests zijn uitgevoerd en een gedetailleerde weergave van de stappen die u heeft genomen
- Op welke manier de zwakke plek kwetsbaar is
    - Authentication/Authorization
    - SQL of XML injection
    - Information leakage
    - Etc.

U kunt bij ons een melding doen via responsibledisclosure@hunzeenaas.nl .

Met vriendelijke groet,

Team Informatieveiligheid