Noorderpoort Responsible Disclosure

Ons beleid voor responsible disclosure is geen uitnodiging om ons bedrijfsnetwerk uitgebreid actief te scannen om zwakke plekken te ontdekken. Wij monitoren ons bedrijfsnetwerk zelf.

Wij willen graag met u samenwerken om onze gebruikers en onze systemen beter te kunnen beschermen.

WIJ VRAGEN U:

1. Uw bevindingen te mailen naar cert@noorderpoort.nl. Versleutel de bevindingen indien mogelijk met de PGP-sleutel van Noorderpoort CERT om te voorkomen dat de informatie in verkeerde handen valt. Per email wordt één Responsible disclosure geaccepteerd.

2. Voldoende informatie te geven om het probleem te reproduceren zodat wij het zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid (POC) voldoende, maar bij complexere kwetsbaarheden kan meer nodig zijn.

3. Contactgegevens achter te laten zodat het Noorderpoort CERT met u in contact kan treden om samen te werken aan een veilig resultaat. Laat minimaal een e-mail adres of telefoonnummer achter.

4. De informatie over het beveiligingsprobleem niet met anderen te delen totdat het is opgelost.

5. Verantwoordelijk om te gaan met de kennis over het beveiligingsprobleem door geen handelingen te verrichten die verder gaan dan noodzakelijk is om het beveiligingsprobleem aan te tonen.

Wij nemen uw melding altijd serieus en gaan elk vermoeden van een kwetsbaarheid uitzoeken, ook zonder ‘bewijs’.

VERMIJD DUS IN ELK GEVAL DE VOLGENDE HANDELINGEN:

1. Het plaatsen van malware.

2. Het kopiëren, wijzigen of verwijderen van gegevens in een systeem (een alternatief hiervoor is het maken van een directory listing van een systeem).

3. Het aanbrengen van veranderingen in het systeem.

4. Het herhaaldelijk pogen toegang tot het systeem verkrijgen of de toegang delen met anderen.

5. Het gebruik maken van het zogeheten “bruteforcen” van toegang tot systemen.

6. Het gebruik maken denial-of-service of social engineering.

WAT WIJ BELOVEN:

1. Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ICT-systeem van Noorderpoort aan bovenstaande voorwaarden voldoet, zullen wij geen juridische consequenties verbinden aan deze melding.

2. Wij behandelen een melding vertrouwelijk en delen persoonlijke gegevens, niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.

3. In onderling overleg kunnen wij, indien u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.

4. Wij sturen zo spoedig mogelijk een ontvangstbevestiging.

5. Wij reageren zo spoedig mogelijk op een melding met onze beoordeling van de melding en een verwachte datum voor een oplossing.

6. Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.

7. 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.