Responsible disclosure

Bij Unilogic vinden wij de veiligheid van onze systemen erg belangrijk. Ondanks onze zorg voor de beveiliging van onze systemen kan het voorkomen dat er toch een zwakke plek is. Als u een zwakke plek in één van onze systemen heeft gevonden horen wij dit graag, zodat wij zo snel mogelijk maatregelen kunnen treffen. Wij willen graag met u samenwerken om onze klanten en onze systemen beter te kunnen beschermen.

Wij vragen u:

- Uw bevindingen te mailen naar m.lonij@unilogic.nl. Versleutel de bevindingen indien mogelijk met <versleutelingsmethodiek: PGP-sleutel> om te voorkomen dat de informatie in verkeerde handen valt.
- Voldoende informatie te geven om het probleem te reproduceren zodat Unilogic het zo snel mogelijk kan 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.
- Contactgegevens achter te laten zodat Unilogic met u in contact kan treden om samen te werken aan een veilig resultaat. Laat minimaal een email adres of telefoonnummer achter.
- De melding zo snel mogelijk na ontdekking van de kwetsbaarheid te doen.
- De informatie over het beveiligingsprobleem niet met anderen te delen totdat het is opgelost.
- 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.

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 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 u mag verwachten:

- Indien u bij de melding van een door u geconstateerde kwetsbaarheid in een ict-systeem van Unilogic aan bovenstaande voorwaarden voldoet, zal Unilogic geen juridische consequenties verbinden aan deze melding.
- Unilogic behandelt een melding vertrouwelijk en deelt persoonlijke gegevens, niet zonder toestemming van de melder met derden, tenzij dit wettelijk of uit hoofde van een rechterlijke uitspraak verplicht is.
- In onderling overleg kan Unilogic, indien u dit wenst, uw naam vermelden als de ontdekker van de gemelde kwetsbaarheid.
- Unilogic stuurt u binnen 1 werkdag een ontvangstbevestiging.
- Unilogic reageert binnen 3 werkdagen op een melding met de beoordeling van de melding en een verwachte datum voor een oplossing.
- Unilogic houdt de melder op de hoogte van de voortgang van het oplossen van het probleem.
- Unilogic lost het door u geconstateerde beveiligingsprobleem in een systeem zo snel mogelijk, maar uiterlijk binnen 60 dagen, op. In onderling overleg kan worden bepaald of en op welke wijze over het probleem, nadat het is opgelost, wordt gepubliceerd.

- Unilogic biedt een beloning als dank voor de hulp. Afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding, kan die beloning variëren van € 20,- tot maximaal een bedrag van € 300,- aan cadeaubonnen. Het moet hierbij wel gaan om een voor Unilogic nog onbekend en serieus beveiligingsprobleem.

Wij danken u voor de medewerking!