Responsible disclosure

Onderwerp: Responsible disclosure
Datum: 28 januari 2019

Het Slingeland Ziekenhuis Doetinchem en Streekziekenhuis Koningin Beatrix Winterswijk vinden het belangrijk dat de systemen die in de ziekenhuizen worden gebruikt veilig zijn. Ondanks dat wij onze systemen met zorg beveiligen, kan er een zwakke plek voorkomen.

Om onze systemen, medewerkers en patiënten beter te kunnen beschermen, werken wij graag met u samen. Als u een zwakke plek in één van onze systemen heeft gevonden, horen wij dit graag van u. Zo kunnen wij zo snel mogelijk aanvullende en/of nieuwe maatregelen treffen om onze systemen beter te beveiligen.

Wij vragen u:

- Uw bevindingen te mailen naar het Slingeland Ziekenhuis, informatiebeveiliging@slingeland.nl, of het Streekziekenhuis Koningin Beatrix, informatiebeveiliging@skbwinterswijk.nl, zonder details in de mail te vermelden. Vermeld in de e-mail wel uw contactgegevens zodat wij met u contact kunnen opnemen om de melding te bespreken, bijvoorbeeld een e-mailadres of telefoonnummer.
- Het probleem niet te misbruiken door bijvoorbeeld meer data te downloaden dan nodig is om het lek aan te tonen of door gegevens van derden in te kijken, te verwijderen of aan te passen.
- Het probleem niet met anderen te delen totdat het is opgelost.
- Alle vertrouwelijke gegevens die u via het lek heeft verkregen direct nadat het lek is gedicht te verwijderen.
- Geen gebruik te maken van aanvallen op fysieke beveiliging, social engineering, distributed denial of service, spam of applicaties van derden.
- Voldoende informatie te geven zodat wij het probleem kunnen achterhalen en zo snel mogelijk kunnen oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende. Bij complexere kwetsbaarheden kan meer informatie nodig zijn.

Wat wij beloven:

- U ontvangt binnen 5 dagen een reactie op uw melding en een verwachte datum voor een oplossing.
- Als u zich aan bovenstaande voorwaarden houdt, verbinden wij geen juridische consequenties aan de melding.
- Wij behandelen uw melding vertrouwelijk en delen uw persoonlijke gegevens niet zonder uw toestemming met derden, tenzij dit wettelijk noodzakelijk is. Melden onder een pseudoniem is mogelijk.
- Wij houden u op de hoogte van de voortgang van het oplossen van het probleem.
- Wij vermelden, indien gewenst, uw naam als ontdekker in de berichtgeving over het gemelde probleem.

Wij streven ernaar om alle problemen zo snel mogelijk op te lossen. Wij worden graag betrokken bij een eventuele publicatie over het probleem, nadat het is opgelost.

Deze tekst beschrijft het responsible disclosure beleid van het Slingeland Ziekenhuis Doetinchem en Streekziekenhuis Koningin Beatrix Winterswijk Ziekenhuis als aanvulling op de leidraad responsible disclosure die het NCSC heeft gepubliceerd.

Uitleg termen

Responsible disclosure - Praktijk van het verantwoord melden van aangetroffen beveiligingslekken. Hierbij worden afspraken gemaakt over hoe beveiligingslek behandeld wordt, bijvoorbeeld dat het lek totdat het verholpen is niet gedeeld wordt met derden en de getroffen partij geen juridische stappen tegen de melder zal ondernemen.

Social engineering - een techniek waarbij een computerkraker computersystemen probeert aan te vallen via de gebruikers van de systemen.

Distributed denial of service = **DDoS-aanvallen** zijn pogingen om een computer, computernetwerk of dienst onbeschikbaar te maken voor de gebruiker.