Melden van beveiligingslekken door derden (Coordinated Vulnerability Disclosure)

1. Doel

St. Antonius Ziekenhuis hecht veel belang aan de veiligheid van zijn informatiesystemen en (medische) apparatuur: deze zijn cruciaal voor patiëntenzorg, onderwijs en onderzoek. Ondanks onze inzet voor de beveiliging hiervan kan het voorkomen dat er toch sprake is een zwakke plek in het systeem, een zogenaamde kwetsbaarheid. Als een externe partij toch zo'n kwetsbaarheid ontdekt dan hoort het St. Antonius Ziekenhuis dit graag zo snel mogelijk, zodat zo snel mogelijk maatregelen getroffen kunnen worden. Wij werken graag met externen samen om onze gebruikers en onze systemen nog beter te kunnen beschermen.

2. Definities en afkortingen

Term	Betekenis
Externe	Een partij (natuurlijk persoon of organisatie) waarmee het St. Antonius Ziekenhuis geen (contractuele) afspraken heeft.

Afkorting	Betekenis
CVD	Coordinated Vulnerability Disclosure

3. Toepassingsgebied

Het beleid is van toepassing op het melden van beveiligingslekken in informatiesystemen van het St. Antonius Ziekenhuis door derden waarmee geen (contractuele) afspraken bestaan. Medewerkers, contractanten en leveranciers volgen het normale beleid gegevensbescherming en informatiebeveiliging inclusief de daarvoor beschreven procedures voor het melden van incidenten.

4. Beleid

Voor het veilig melden van kwetsbaarheden hanteert het St. Antonius Ziekenhuis een *Coordinated Vulnerability Disclosure (CVD) beleid*, dat in dit document is beschreven.

5. Verantwoordelijkheden, bevoegdheden

-

6. Procedures

6.1. Zoeken naar beveiligingslekken

Bij het zoeken naar kwetsbaarheden gelden de volgende regels:

- Ons CVD-beleid is geen uitnodiging voor externe partijen om onze systemen en bedrijfsnetwerk uitgebreid en actief te scannen op kwetsbaarheden. Dit doet het St. Antonius Ziekenhuis zelf al.
- Het is niet toegestaan om aanval(len) te doen op de fysieke beveiliging van onze locaties en gebruik te maken van social engineering, distributed denial of service (DDOS), spam, brute-force-aanvallen en/of applicaties van derden.

6.2. Omgaan met een gevonden beveiligingslek

Heeft een externe een kwetsbaarheid gevonden, dan vragen we hem/haar zich te houden aan de volgende regels:

- Maak geen misbruik van de geconstateerde kwetsbaarheid, bijvoorbeeld door meer data te downloaden dan nodig is om het lek aan te tonen of door gegevens van derden in te zien, te verwijderen of aan te passen.
- Vermoedt u dat u via een kwetsbaarheid medische gegevens kunt inzien? Probeer dit dan niet zelf uit maar laat dit door ons vaststellen.
- Deel uw bevindingen niet met anderen, voordat het is opgelost.

- Wis alle vertrouwelijke gegevens die u heeft verkregen, na het dichten van het lek direct.

6.3. Melding maken van een beveiligingslek

Als een externe een kwetsbaarheid heeft gevonden, horen wij dit graag zo snel mogelijk. Zo kunnen wij tijdig passende maatregelen kunnen treffen. Een externe kan als volgt een melding doen:

- De externe meldt zijn/haar bevindingen bij voorkeur door een e-mail te sturen naar fg@antoniusziekenhuis.nl**.**
- De externe melder geeft voldoende informatie, zodat we het probleem kunnen nabootsen. Op die manier kunnen wij het probleem zo snel mogelijk oplossen. Meestal is het IP-adres of de URL van het getroffen systeem en een omschrijving van de kwetsbaarheid voldoende, maar bij complexere kwetsbaarheden is soms meer informatie gewenst/noodzakelijk.
- Anoniem of onder pseudoniem melden is mogelijk. Het is goed te weten dat het St. Antonius Ziekenhuis in dit geval geen contact kan opnemen over de melding, de vervolgstappen en de voortgang van het oplossen van het probleem.

6.4. Opvolgen van het beveiligingslek

- St. Antonius Ziekenhuis behandelt de melding vertrouwelijk. Daarnaast delen wij de persoonlijke gegevens van de melder niet met derden zonder toestemming van de melder, tenzij dit wettelijk verplicht is.
- De melder krijgt een ontvangstbevestiging van de melding. Daarna ontvangt hij/zij binnen 5 werkdagen een reactie met een beoordeling van de melding.
- Wij houden de melder op de hoogte van de voortgang van het oplossen van het probleem. We streven ernaar om alle problemen zo snel mogelijk op te lossen rekening houdend met het concrete risico dat het probleem met zich meebrengt.
- Samen met Marketing & Communicatie overleggen we over de meerwaarde van een eventuele publicatie van het opgeloste probleem. In berichtgeving over het gemelde probleem vermeldt St. Antonius Ziekenhuis, als de melder dit wenst, de naam van de melder.
- Als dank voor de hulp van de melder, biedt St. Antonius Ziekenhuis een beloning aan. Deze beloning varieert en is afhankelijk van de ernst van het beveiligingsprobleem en de kwaliteit van de melding.

NB: Er bestaat een kans dat een externe melder tijdens het onderzoeken van de kwetsbaarheid handelingen verricht die volgens het strafrecht strafbaar zijn. Wanneer de externe melder zich aan de onderstaande regels van ons CVD-beleid heeft gehouden, dan hebben wij geen reden om juridische consequenties te verbinden aan de melding. Het Openbaar Ministerie (OM) behoudt altijd het recht zelf te beslissen of de externe melder strafrechtelijk vervolgd wordt. Het OM heeft hierover een richtlijn gepubliceerd (https://www.om.nl/documenten/brochures/cybercrime/map/map1/coordinated-vulnerability-disclosure).

7. Verwijzingen

Gebaseerd op licentietekst afkomstig van http://responsibledisclosure.nl/ (Floor Terra)