Elkerliek ziekenhuis profiel

Dit profiel van Elkerliek-CERT is opgesteld volgens RFC-2350.

For English please see page 4-5-6.

1. Document informatie

1.1. Datum van de laatste update

Dit is versie 1.2 van 10-08-2021.

1.2. Distributielijst voor kennisgevingen

Dit profiel wordt bijgehouden in het interne kwaliteitsmanagementsysteem en gepubliceerd op de in 1.3 genoemde locatie.
De updates worden per e-mail verstuurd naar alle Elkerliek-CERT leden.

Vragen over updates kunt u richten aan het e-mailadres van Elkerliek-CERT:
Elkerliek-CERT@elkerliek.nl

1.3. Plaatsen waar dit document kan worden gevonden

De huidige versie van dit profiel is altijd beschikbaar op
https://www.elkerliek.nl/Elkerliek/Contact/Disclaimer-website.html

2. Contactgegevens

2.1 Naam van het team

Volledige naam: Elkerliek-CERT
Elkerliek CERT is het CERT of CSIRT team voor Elkerliek ziekenhuis Helmond/Deurne/Asten/Gemert in Nederland.

2.2. Adres

Elkerliek ziekenhuis
Elkerliek CERT
Afdeling ICMT
Postbus 98
NL - 5700AB Helmond
Nederland

2.3. Tijdzone

GMT+1 (GMT+2 met DST of zomertijd, die begint op de laatste zondag van maart en eindigt op de laatste zondag van oktober)

2.4. Contactgegevens

Telefoon
Van 8.00 tot 17.00 uur kunt u onze helpdesk bellen op +31(0)492-595900 en na 17.00 uur tot 8.00 uur +31(0)492595900 en kies voor de menuoptie.

E-mail
Geen spoedgevallen: Elkerliek-CERT@elkerliek.nl . Dit adres kan gebruikt worden om alle veiligheidsincidenten te melden gerelateerd aan het Elkerliek-CERT, inclusief auteursrechtkwesties, spam en misbruik. Regelmatige responstijden: Maandag-vrijdag, 08:00-17:00 uur (behalve op feestdagen in Nederland).

Spoedgevallen: stuur uw e-mail met SPOED in de onderwerpregel. Wij gebruiken beveiligde e-mail indien nodig voor de communicatie. Bij het melden van een incident met een ernstig vertrouwelijk karakter, gelieve dit expliciet te vermelden, bijvoorbeeld door gebruik te maken van het label VERTROUWELIJK in het onderwerpveld van de e-mail, en indien mogelijk ook met behulp van versleuteling.

2.5. Andere telecommunicatie

Niet beschikbaar.

2.6. Teamleden

Over de teamleden van Elkerliek-CERT wordt geen informatie in het openbaar verstrekt. De Elkerliek-CERT team leden worden geselecteerd uit diverse geledingen van de Elkerliek ICMT-professionals.

2.7. Melden van kwetsbaarheden (CVD)

Specifieke informatie over het melden van kwetsbaarheden is te vinden op:
https://www.elkerliek.nl/elkerliek/contact/disclaimer-website.html

3. Doel

3.1. Missieverklaring

De missie van Elkerliek-CERT is het coördineren van het oplossen van ICMT-beveiligingsincidenten met betrekking tot Elkerliek en haar omgeving (zie 3.2), en om dergelijke incidenten te helpen voorkomen.
Voor de wereld is Elkerliek-CERT de ingang van het Elkerliek met betrekking tot ICMT security incident response. Alle ICMT beveiligingsincidenten (inclusief misbruik) met betrekking tot het Elkerliek ziekenhuis kunnen bij Elkerliek-CERT worden gemeld.

3.2. Stakeholder omgeving

De stakeholders van Elkerliek-CERT is Elkerliek ziekenhuis en instellingen die verbonden zijn met het Elkerliek ziekenhuisnetwerk, met alle gerelateerde medische medewerkers, medewerkers van Elkerliek en leveranciers.

3.3. Positionering

Elkerliek-CERT is onderdeel van ICMT, de IT-afdeling van Elkerliek ziekenhuis.

3.4. Autoriteit

Elkerliek-CERT coördineert namens Elkerliek ziekenhuis beveiligingsincidenten en heeft geen bevoegdheid die verder reikt dan dat. Van Elkerliek-CERT wordt echter verwacht dat het operationele aanbevelingen doet in het verloop van hun werk. De uitvoering van dergelijke aanbevelingen valt niet onder de verantwoordelijkheid van het team, maar alleen van degenen aan wie de aanbevelingen zijn gedaan.

4. Beleid

4.1. Soorten incidenten en niveau van ondersteuning

Alle incidenten worden beschouwd als normale prioriteit, tenzij ze door de afzender als SPOED worden bestempeld en/of na eigen onderzoek. Elkerliek-CERT zelf is de instantie die het SPOED-label kan instellen en resetten. Een incident kan bij Elkerliek-CERT worden gemeld als SPOED, maar het is aan Elkerliek-CERT om te bepalen om die status al dan niet te handhaven.

4.2. Samenwerking, interactie en openbaarmaking van informatie

Alle binnenkomende informatie wordt door Elkerliek-CERT vertrouwelijk behandeld, ongeacht de prioriteit. Informatie die duidelijk vertrouwelijk van aard is, wordt alleen gecommuniceerd en opgeslagen in een beveiligde omgeving, indien nodig.

met behulp van encryptietechnologieën. Wanneer u een incident van vertrouwelijke aard meldt, geef dit dan expliciet aan, bijvoorbeeld door het gebruik van het label VERTROUWELIJK in het onderwerpveld van de e-mail, en indien mogelijk met behulp van versleuteling.
Elkerliek-CERT ondersteunt het Information Sharing Traffic Light Protocol (ISTLP - zie https://www.first.org/tlp/)- informatie die binnenkomt met de tags WIT, GROEN, GEEL of ROOD zal op de juiste manier worden behandeld.
Elkerliek-CERT zal de door u verstrekte informatie gebruiken om te helpen bij het oplossen van beveiligingsincidenten, zoals alle CERTS doen. Dit betekent dat de informatie standaard verder wordt verspreid onder de juiste partijen - maar alleen op een need-to-know basis - en bij voorkeur op een geanonimiseerde manier.
Indien u bezwaar heeft tegen dit standaard gedrag van Elkerliek-CERT, kunt u dat kenbaar maken wat te doen met de informatie die u verstrekt. Elkerliek-CERT zal aan uw wens voldoen, maar zal u er ook op wijzen als dat betekent dat Elkerliek-CERT op basis hiervan niet kan handelen .
Elkerliek-CERT rapporteert geen incidenten aan wetshandhavingsinstanties, tenzij de nationale wetgeving dit voorschrijft. Elkerliek-CERT werkt alleen samen met de wetshandhavingsinstanties als de nationale wetgeving dit voorschrijft - als onderdeel van een officieel onderzoek, wat betekent dat er sprake is van een gerechtelijk bevel of in het geval dat een melder of instantie verzoekt dat Elkerliek-CERT meewerkt aan een onderzoek. Bij afwezigheid van een gerechtelijk bevel zal Elkerliek-CERT alleen informatie verstrekken op een need-to-know basis.

5. Diensten

5.1. Incident Response (Triage, Coördinatie en Oplossing)

Elkerliek-CERT is verantwoordelijk voor de coördinatie van beveiligingsincidenten waarbij Elkerliek op de een of andere manier betrokken is. Elkerliek-CERT behandelt dus zowel de triage- als de coördinatieaspecten. Oplossing van incidenten
wordt overgelaten aan de lijnverantwoordelijken binnen het Elkerliek ziekenhuis of externe partij(en), waarbij Elkerliek-CERT op verzoek ondersteuning biedt en advies geeft.

5.2. Proactieve activiteiten

Elkerliek-CERT adviseert haar stakeholders pro-actief over recente kwetsbaarheden en trends in cybersecurity.
Elkerliek-CERT adviseert Elkerliek ziekenhuis op het gebied van beveiliging in computer- en netwerkvraagstukken. Zij kan dit proactief doen in dringende gevallen, of op verzoek. Beide rollen zijn rollen van advies. Elkerliek-CERT biedt ondersteuning en advies op verzoek.

6. Registratie van incidenten

Incidenten die per post, telefoon of iets anders worden gemeld, worden in Elkerliek centraal geregistreerd om het incidentregistratiesysteem.

7. Disclaimer

Op de website https://www.elkerliek.nl/Elkerliek/Contact/Disclaimer-website.html is een algemene disclaimer opgenomen.

Elkerliek ziekenhuis profile

This profile of Elkerliek -CERT is established according to RFC-2350.

ENGLISH VERSION

1. Document Information

1.1. Date of Last Update

This is version 1.2 of 10-08-2021.

1.2. Distribution List for Notifications

This profile is kept up-to-date in our internal system for quality management and published on the location specified in 1.3 . E-mail notification of updates are sent to all Elkerliek-CERT members

Any questions about updates please address to the Elkerliek-CERT e-mail address: Elkerliek-CERT@elkerliek.nl

1.3. Locations where this Document May Be Found

The current version of this profile is always available on
https://www.elkerliek.nl/Elkerliek/Contact/Disclaimer-website.html

2. Contact Information

2.1. Name of the Team

Full name: Elkerliek-CERT
Elkerliek CERT is the CERT or CSIRT team for Elkerliek ziekenhuis Helmond/Deurne/Asten/Gemert in the Netherlands.

2.2. Address

Elkerliek ziekenhuis
Elkerliek CERT
Department ICMT
P.O Box 98
NL – 5700AB Helmond
The Netherlands

2.3. Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4. Contact

Telephone
+31(0)492-595900. From 8.00 until 17.00 you can call our helpdesk at +31(0)492-595900 and after 17.00 until 8.00 hour +31(0)492-595900 and choose menu option.

E-mail
Regular cases: Elkerliek-CERT@elkerliek.nl. This address can be used to report all security incidents related to the Elkerliek-CERT constituency including copyright issues, spam and abuse.
Regular response hours: Monday-Friday, 08:00-17:00 (except public holidays in the Netherlands).
EMERGENCY cases: send e-mail with EMERGENCY in the subject line.
We use secure e-mail if necessary for communication.
When reporting an incident of severe sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

2.5. Other Telecommunication

Not available.

2.6. Team Members

No information is provided about the Elkerliek-CERT team members in public. The Elkerliek-CERT team members are selected from the ranks of the Elkerliek ICMT-professionals.

2.7. Reporting of Vulnerabilities

Specific details for reporting vulnerabilities can be found at
https://www.elkerliek.nl/Elkerliek/Contact/Disclaimer-website/Coordinated-Vulnerability-Disclosure(English).html

3. Charter

3.1. Mission statement

The mission of Elkerliek-CERT is to coordinate the resolution of ICMT security incidents related to the Elkerliek ziekenhuis constituency (see 3.2), and to help prevent such incidents from occurring.
For the world, Elkerliek-CERT is the Elkerliek interface with regards to ICMT security incident response. All ICMT security incidents (including abuse) related to the Elkerliek Ziekenhuis can be reported to Elkerliek CERT.

3.2. Constituency

The constituency for Elkerliek-CERT is Elkerliek ziekenhuis and institutions connected to the Elkerliek ziekenhuis network, with all related medical staff, Elkerliek employees and suppliers.

3.3. Sponsorship and/or Affiliation

Elkerliek-CERT is part of ICMT, the IT-department of Elkerliek ziekenhuis.

3.4. Authority

Elkerliek-CERT coordinates security incidents on behalf of Elkerliek ziekenhuis and has no authority reaching further than that. Elkerliek-CERT is however expected to make operational recommendations in the course of their work. The implementation of such recommendations is not a responsibility of the team, but solely of those to whom the recommendations were made.

4. Policies

4.1. Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY by the sender and/or after own investigation. Elkerliek-CERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to Elkerliek-CERT as EMERGENCY, but it is up to Elkerliek-CERT to decide whether or not to uphold that status.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by Elkerliek-CERT, regardless of its priority. Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.
Elkerliek-CERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.first.org/tlp/) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.
Elkerliek-CERT will use the information you provide to help solve security incidents, as all CERTS do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymized fashion.

If you object to this default behavior of Elkerliek-CERT, please make explicit what Elkerliek-CERT can do with the information you provide. Elkerliek-CERT will adhere to your policy, but will also point out to you if that means that Elkerliek-CERT cannot act on the information provided.
Elkerliek-CERT does not report incidents to law enforcement, unless national law requires so. Likewise, Elkerliek-CERT only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that Elkerliek-CERT cooperates in an investigation. When a court order is absent, Elkerliek-CERT will only provide information on a need-to-know base.

5. Services

5.1. Incident Response (Triage, Coordination and Resolution)

Elkerliek-CERT is responsible for the coordination of security incidents somehow involving Elkerliek ziekenhuis. Elkerliek-CERT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the Elkerliek ziekenhuis and externally – however Elkerliek-CERT will offer support and advice on request.

5.2. Proactive Activities

Elkerliek-CERT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking. Elkerliek-CERT advises Elkerliek ziekenhuis on matters of computer and network security. It can do so proactively in urgent cases, or on request. Both roles are roles of consultancy: Elkerliek-CERT is not responsible for implementation.

6. Incident reporting Forms

Incidents which are reported by mail, telephone or something else, will be registered in Elkerliek central Incidentregistration system.

7. Disclaimers

On the website https://www.elkerliek.nl/Elkerliek/Contact/Disclaimer-website.html is an overall disclaimer available.