TNO Cert profiel

1. Document informatie

1.1. Datum laatste wijziging

Dit is versie 1.0 van 30-1-2020.

1.2. Distributielijst voor kennisgevingen

Dit profiel is up-to-date op de locatie aangegeven in 1.3.

E-mail notificatie van updates worden verstuurd naar:

- Alle leden TNOCert
- SURFcert

Voor vragen over updates kunt u zich richten tot het TNOCert e-mailadres.

1.3. Locaties waar dit document kan worden gevonden

De huidige versie van dit profiel is altijd beschikbaar op http://www.tno.nl/cert

2. Contact informatie

2.1. Naam van het team

Volledige naam: TNO IT Security Coordination
Korte naam: TNOCert
TNOCert is het CERT of CSIRT team voor TNO in Nederland.

2.2. Adres

TNO
Information Services
Security, Risk & Compliance manager
Postbus 96800
2595 DA Den Haag
Nederland

2.3. Tijdzone

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

2.4. Telefoonnummer

+31 88 8667100

2.5. Faxnummer

Niet beschikbaar.

2.6. Overige telecommunicatie

Niet beschikbaar.

2.7. E-mailadres

Organisatie-TNO-ITSecurity@tno.nl

Dit adres kan gebruikt worden om alle beveiligingsincidenten die betrekking hebben op de TNOCert opdrachtgever te melden, waaronder het auteursrecht, spam en misbruik..

2.8. Publieke sleutels en encryptie informatie
Op dit moment wordt er geen versleutelde e-mail ondersteund.

2.9. Teamleden
Er wordt geen informatie gegeven over de TNOCert teamleden in het openbaar.

2.10. Overige informatie
TNOCert is geregistreerd door SURFcert.

2.11. Klanteningangen
Normale gevallen: gebruik TNOCert e-mailadres.
Kantoortijden: maandag-vrijdag, 09:00-17:00 (behalve op Nederlandse feestdagen).
Noodgevallen: stuur e-mail met EMERGENCY in de onderwerpregel.

3. Charter

3.1. Missie
De missie van TNOCert is het coördineren van de oplossing van IT-security- incidenten in verband met de opdrachtgever van TNOCert (zie 3.2), en om te voorkomen dat dergelijke incidenten zich voordoen.

3.2. Opdrachtgever
De opdrachtgever voor TNOCert is TNO in Nederland. Deze bestaat uit:

- Nederlandse organisatie voor toegepast-natuurwetenschappelijk onderzoek TNO
- Ten minste het domein: tno.nl
- De volgende IP reeksen: 134.221.0.0/16, 139.63.0/16, 192.87.96.0/24.

3.3. Organisatie
TNOCert is een onderdeel van Nederlandse organisatie voor toegepast- natuurwetenschappelijk onderzoek TNO.

3.4. Autoriteit
Het team coördineert veiligheidsincidenten namens zijn opdrachtgever en heeft geen verderstrekkend gezag. Van het team wordt echter ook verwacht dat ze operationele aanbevelingen doen. Dergelijke aanbevelingen kunnen omvatten, maar zijn niet beperkt tot het blokkeren van adressen of netwerken. De implementatie van deze aanbevelingen is niet een verantwoordelijkheid van het team, maar alleen van degenen aan wie de aanbevelingen gedaan worden.

4. Beleid

4.1. Soorten incidenten en de mate van ondersteuning
Alle incidenten worden beschouwd als normale prioriteit, tenzij ze worden aangeduid als EMERGENCY. Een incident kan worden gemeld bij TNOCert als EMERGENCY, maar het is aan TNOCert om te beslissen over het handhaven van deze status.

4.2. De samenwerking, interactie en doorgifte van informatie
ALLE inkomende informatie wordt vertrouwelijk behandeld door TNOCert, ongeacht de prioriteit.

Informatie die kennelijk gevoelig is, wordt alleen gecommuniceerd en opgeslagen in een beveiligde omgeving, indien nodig met behulp van encryptie-technologieën. Bij het melden van een incident van gevoelige aard gelieve dit expliciet aan te geven, bijvoorbeeld met behulp van het label SENSITIVE in het onderwerpveld van de e-mail.

TNOCert ondersteunt het Information Sharing Traffic Light Protocol (ISTLP - https://www.trusted-introducer.org/ISTLPv11.pdf). Informatie die verstrekt wordt met de tags WHITE, GREEN, AMBER of RED zal op passende wijze worden behandeld.

TNOCert zal gebruik maken van de door u verstrekte informatie om te helpen incidenten op te lossen, zoals alle CERTs doen. Dit betekent dat standaard de informatie zal worden verspreid aan de betrokken partijen, maar alleen op een need-to-know basis en indien mogelijk geanonimiseerd.

Als u bezwaar wilt maken tegen dit standaard gedrag van TNOCert, maak dan duidelijk wat TNOCert kan doen met de informatie die u verstrekt. TNOCert zal voldoen aan uw beleid, maar zal u ook duidelijk maken indien dat betekent dat TNOCert niet kan handelen op basis van de verstrekte informatie.

TNOCert werkt alleen samen met rechtshandhaving hetzij in de loop van een officieel onderzoek - wat betekent dat een gerechtelijk bevel aanwezig is - hetzij in het geval dat een opdrachtgever verzoekt TNOCert mee te werken aan een onderzoek. Wanneer een gerechtelijk bevel afwezig is, zal TNOCert alleen informatie delen op een need-to-know basis.

4.3. Communicatie en authenticatie

Zie hierboven 2.8. In gevallen waarin er twijfel bestaat over de authenticiteit van de informatie of de bron behoudt TNOCert zich het recht voor om deze te verifiëren, gebruik makende van wettelijke middelen.

5. Services

5.1. Incident response (triage, coördinatie en oplossing)

TNOCert is verantwoordelijk voor de coördinatie van IT veiligheidsincidenten met betrekking tot de opdrachtgever (zoals gedefinieerd in 3.2). TNOCert behandelt dus zowel de triage als de coördinatie aspecten. Het oplossen van incidenten wordt overgelaten aan de verantwoordelijke beheerders binnen de organisatie, maar TNOCert zal op aanvraag ondersteuning en advies leveren.

5.2. Proactive activiteiten

TNOCert adviseert de opdrachtgever proactief met betrekking tot de recente zwakke plekken en trends in hacking / cracking.
TNOCert adviseert de opdrachtgever op het gebied van computer- en netwerkbeveiliging. Dit kan zowel proactief in spoedeisende gevallen of op verzoek geschieden.
Beide rollen zijn rollen van consultancy: TNOCert is niet verantwoordelijk voor de uitvoering.

6. Incidentmelding formulieren

Niet beschikbaar. Bij voorkeur rapport in platte tekst via e-mail of gebruik de telefoon.

7. Disclaimers

TNO generieke disclaimer met betrekking tot e-mail communicatie is hier beschikbaar: http://www.tno.nl/emaildisclaimer.