TNO Cert profile

1. Document information

1.1. Date last amendment

This is version 1.0 from 30-1-2020.

1.2. Distribution list for notifications

This profile is up-to-date at the location indicated in 1.3.

Email notification of updates are sent to:

- All members TNOCert
- SURFcert

For updates questions, please address the TNOCert email address.

1.3.Locations where this document can be found

The current version of this profile is always available on http://www.tno.nl/cert

2. Contact information

2.1. Team name

Full name: TNO IT Security Coordination
Short name: TNOCert

TNOCert is the CERT or CSIRT team for TNO in the Netherlands.

2.2. Address

TNO
Information Services
Security, Risk & Compliance manager
Postbus 96800
2595 DA The Hague
Netherlands

2.3. Time zone

GMT +1 (GMT +2 during daylight saving time, which starts on the last Sunday of March and ends on the last Sunday of October)

2.4. Phone number

+31 88 8667100

2.5. Fax Number

Unavailable.

2.6. Other telecommunications

Unavailable.

2.7. Email address

Organisatie-TNO-ITSecurity@tno.nl

This address can be used to report all security incidents related to the TNOCert client, including copyright, spam and abuse..

2.8. Public keys and encryption information
At this time, no encrypted email is supported.

2.9. Team members
No information is given about the TNOCert team members in public.

2.10. Other information
TNOCert is registered by SURFcert.

2.11. Customer entrances
Normal cases: use TNOCert email address.
Office hours: Monday-Friday, 09:00-17:00 (except on Dutch holidays).
Emergencies: Send emergency email in the subject line.

3. Charter

3.1. Mission
TNOCert's mission is to coordinate the solution of IT security incidents related to the constituency of TNOCert (see 3.2), and to prevent such incidents from occurring.

3.2. Client
The client for TNOCert is TNO in the Netherlands. This consists of:

- Dutch organisation for applied-scientific research TNO
- At least the domain: tno.nl
- The following IP series: 134.221.0.0/16, 139.63.0/16, 192.87.96.0/24.

3.3. Organization
TNOCert is part of a Dutch organization for applied scientific research TNO.

3.4. Authority
The team coordinates IT security incidents on behalf of his client and has no far-going authority. However, the team is also expected to make operational recommendations. Such recommendations may include, but are not limited to blocking addresses or networks. The implementation of these recommendations is not a responsibility of the team, but only of those to whom the recommendations are made.

4. Policy

4.1. Types of incidents and the degree of support
All incidents are considered normal priority unless they are referred to as EMERGENCY. An incident can be reported to TNOCert as an EMERGENCY, but it is up to TNOCert to decide on maintaining this status.

4.2. The cooperation, interaction and transmission of information
All incoming information is treated confidentially by TNOCert, regardless of priority.

Information that is apparently sensitive is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting a sensitive incident, please explicitly indicate this, for example using the SENSITIVE label in the subject field of the email.

TNOCert supports the Information Sharing Traffic Light Protocol (ISTLP - https://www.trusted-introducer.org/ISTLPv11.pdf). Information provided with the WHITE, GREEN, AMBER or RED tags will be treated appropriately.

TNOCert will use the information you provide to help resolve incidents, as all CERTs do. This means that by default the information will be disseminated to the parties involved, but only on a need-to-know basis and if possible anonymized.

If you want to object to this standard behavior of TNOCert, make it clear what TNOCert can do with the information you provide. TNOCert will comply with your policy, but will also make it clear to you if it means that TNOCert cannot act on the basis of the information provided.

TNOCert is only cooperating with law enforcement either in the course of an official investigation - meaning a court order is present - either in the event that a client requests TNOCert to cooperate with an investigation. When a court order is absent, TNOCert will only share information on a need-to-know basis.

4.3. Communication and authentication

See 2.8 above. In cases where there is doubt about the authenticity of the information or the source, TNOCert reserves the right to verify it, using legal means.

5. Services

5.1. Incident response (triage, coordination and solution)

TNOCert is responsible for coordinating IT safety incidents related to the client (as defined in 3.2). TNOCert therefore handles both triage and coordination aspects. Solving incidents will be left to the responsible administrators within the organization, but TNOCert will provide support and advice on request.

5.2. Proactive activities

TNOCert proactively advises the client regarding recent weaknesses and trends in hacking/cracking. TNOCert advises the client in the field of computer and network security. This may be done proactively in urgent cases or on request.
Both roles are roles of consultancy: TNOCert is not responsible for the execution.

6. Incident notification forms

Unavailable. Preferably report in plain text via email or use the phone.

7. Disclaimers

TNO generic disclaimer regarding email communication is available here:
http://www.tno.nl/emaildisclaimer.