National Cyber Security Centre
Ministry of Justice and Security

Operational Framework NCSC-NL

Version March 21, 2019

Turfmarkt 147
2511 DP The Hague
Postbus 117
2501 CC The Hague
www.ncsc.nl

Introduction

The National Cyber Security Centre of The Netherlands (NCSC-NL) has, in order to prevent or limit the failure of the availability or the loss of integrity of information systems of vital operators and the Dutch central government, as well as in order to further strengthen the digital resilience of Dutch society, the duty to assist, inform and advise these operators and others in and outside the Netherlands on threats and incidents with respect to their information systems. In order to fulfil these duties, the NCSC-NL is the central information hub and centre of expertise for cyber security in the Netherlands. On an international level, NCSC-NL is the Dutch point of contact in the field of ICT threats and cyber security incidents. NCSC-NL is also a key figure in the operational coordination at a major ICT crisis and the Computer Emergency Response Team (CERT) for the Dutch central government and operators of vital infrastructures.

NCSC-NL is a separate agency under the Secretary General of the Ministry of Justice and Security. The National Coordinator for Security and Counterterrorism (NCTV) is commissioner for NCSC-NL.
This document, called operational framework, brings together the agreed basic principles and conditions under which NCSC-NL operates.

Goal and Tasks

NCSC-NL is a key-player in enhancing the resilience of the Netherlands in the digital domain. The goal is to realize a safe, open and stable information society by sharing knowledge, providing insight and pragmatic advice.

Target Group

The primary target group of NCSC-NL is the Dutch central government and operators in the vital infrastructure. Vital infrastructure is infrastructure that is crucial for the proper functioning of Dutch society. Examples of vital infrastructure are energy, water and telecom.

Remits and Act

The Dutch "Security of Network and Information Systems Act" (Nov. 09, 2018) lays down the duties for the Minister of Justice and Security with regards to the promotion and safeguarding of the security and integrity of electronic information systems that are of vital importance to Dutch society, as well as the information systems of the Dutch central government, including an obligation for previously defined operators to report serious breaches in the security of those systems . This Act also governs the legitimacy of the processing of personal data by the Minister for the fulfillment of these duties.

The Minister of Justice and Security has delegated the effectuation of these duties to NCSC-NL through the Organizational Decree of the Ministry ("Organisatiebesluit Justitie en Veiligheid" (02-05-2019)).

Additionally, NCSC-NL is subjected to information security legislation, including the Dutch Data Protection Act (and from May 2018, the EU General Data Protection Regulation), as well as the information security

policies of the Ministry of Justice and Security and of NCSC-NL itself. The policies are part of the review and audit cycle by the Dutch Government.

Activities

Within the remits and legal boundaries of NCSC-NL, the main activities of NCSC-NL are:

a. assisting operators of central government and vital infrastructures in taking measures to safeguard or restore the availability and reliability of their products or services;
b. informing and advising these operators and others in and outside the Netherlands on threats and incidents with respect to the information systems referred to in the opening words;
c. conducting analyses and technical research for the benefit of the duties set out under a and b, following the threats and incidents referred to under b or indications thereof.

The NCSC also plays a crucial role in crisis-management (in case of an IT-related crises) and stimulates public-private partnerships, as well as other collaboration efforts, with regards to information sharing. All activities are provided on an obligation of best effort and no firm service level agreement is established for public services.

Response to threats and incidents

NCSC-NL is constantly working on preventing and responding to cyber-attacks. This is done by scanning numerous sources on the internet. This consequently provides NCSC-NL with continuous insight into current threats. Incident Response provides NCSC-NL with content for the fulfilment of its duties and contributes to increasing the Dutch society's ability to defend itself in the digital domain, and consequently to creating a safe, open and stable information society .

Perception and action prospects

NCSC-NL ensures that the primary target groups are equipped with tactical and strategic knowledge and substantive perspective for action. Both in the short term, for example, in the field of crises, incidents and threats, and in the long term, via, for example, best practices, lessons learned, presentations and whitepapers. In this regard, NCSC-NL provides specialist insight into developments, threats and risks in the field of cyber security. If possible these specialist insights are made public on www.ncsc.nl, in order to share information with more stakeholders than just the primary target group.

Improving crisis management

In case of a large cyber security incident or crisis, the NCSC-NL offers operational coordination regarding the response and has, in addition, an advising and informing role towards the National crisis governance structure. In part, ICT crisis management is based on public-private partnerships. Therefore, an advisory

board has been established under the name ICT Response Board (IRB). This is a public-private board in which representatives of vital infrastructure organizations analyze the situation and give an advice to the national decision-making structure. NCSC-NL furthermore prepares its own organization and that of its partners through the preparation and execution of trainings and exercises. For the international partners the NCSC-NL operates as National Point Of Contact and is taking part in international exercises.

Cyber security collaboration

Cyber security is too comprehensive to be managed by a single sector. ICT structures are highly interdependent in the digital community, which makes cooperation essential. Cyber security affects all sectors of the community. Sharing knowledge is of vital importance to be able to recognize threats. To achieve an adequate response, those involved must know how to find each other quickly. The NCSC-NL cooperates on the basis of equality and trust. The various partnerships aim to raise the digital security in the Netherlands.

The NCSC cooperates in the following ways:

- with public parties (government);
- with private parties;
- with professionals in practice, education and academia;
- with international partners.

Partnerships

Within the scope of its legal framework, the NCSC-NL cooperates and collaborates through varying Partnerships:

National partnerships

In the national context, NCSC-NL cooperates with partners like on both a governmental level as well as with private organizations. Examples of these partners are: National Police, General Intelligence and Security Service (AIVD), Military Intelligence and Security Service (MIVD), Radiocommunications Agency Netherlands (AT), Authority for Consumers & Markets (ACM), National Forensic Institute (NFI), Public Prosecutor office (OM), Dutch internet service providers, other incident response teams in The Netherlands, organizations in vital infrastructure, etc. Furthermore NCSC-NL participates in Information Sharing and Analysis Centers (ISAC's) with organizations in the vital infrastructures.

International partnerships

NCSC-NL is part of an extensive network of affiliated organizations, mainly other Computer Emergency Response Teams (CERTs). Since this network is a vital information hub, NCSC-NL considers it just as important to make expertise available to other teams as it is to benefit from the knowledge of the international CERT community.

The aim is to achieve maximum results with minimum means, and international collaboration is one way to realize this. That is why NCSC-NL encourages the development of shared standards and specialization in different areas. Our primary networks:

- CSIRT network - Computer security incident response team network. The NIS directive establishes in article 12 a CSIRTs network "in order to contribute to developing confidence and trust between the Member States and to promote swift and effective operational cooperation". It is "composed of representatives of the EU Member States' CSIRTs and a CSIRT for EU institutions CERT-EU".
- EGC – European Governmental CERTs, in which NCSC-NL holds a prominent position
- FIRST – Forum of Incident Response and Security Teams, which consists of over 400 CERTs worldwide
- TERENA – Trans-European Research and Education Networks Association, lobby of European national academic networks
- I4 – International Information Integrity Institute, a co-operative in the field of security, including private sector participants
- ISF – Information Security Forum, a co-operative in the field of security consisting of various international organizations
- TF-CSIRT - TF-CSIRT provides a forum where members of the CSIRT community can exchange experiences and knowledge in a trusted environment in order to improve cooperation and coordination. It maintains a system for registering and accrediting CSIRTs, as well as certifying service standards.

Point of contact

The NCSC-NL point of contact arrangements have been established to provide a framework for sharing information about serious and time critical computer threats, vulnerabilities or incidents for the constituency.

At all times, urgent incident related information can be shared with NCSC-NL via email to cert@ncsc.nl. Other questions or information can be sent to info@ncsc.nl.
Other relevant contact information is shared in the Trusted Introducer database, the website of FIRST, and RFC2350 info on www.ncsc.nl.

Communication and press

The Ministry of Justice and Security has a press officer, to answer questions of media. NCSC-NL has a corporate communication unit, with close working relationships to the press officer of the Ministry.

Amendments to NCSC-NL operational framework

Amendments to this Operational Framework must be approved by the Head of NCSC-NL.