PRESENTATION

NEXT GENERATION SECURITY SOLUTIONS - NESTOR

ACCORDING TO THE RFC 2350 STANDARD

Next Generation Security Solutions s.r.o.
U Uranie 954/18, 170 00 Prague 7, Czech Republic
Tel: 237 836 950
info@ngss.cz | www.ngss.cz

Identifying information

Next Generation Security Solutions s.r.o.

Company headquarters:	U Uranie 954/18, 170 00 Prague 7, Czech Republic
Company ID:	06291031
Tax ID:	CZ06291031

Company registered in the Trade Register in Prague, file section C, insert 279627

Website:	www.ngss.cz www.soc247.cz

Contact persons:

Radim Navrátil
Head of IT Security
Tel: +420 237 836 950
Email: rnavratil@ngss.cz

Jaromír Žák
Director
Email: jzak@ngss.cz

Contents

1. NEXT GENERATION SECURITY SOLUTIONS – NESTOR (NESTOR)

This document contains a description of the NEXT GENERATION SECURITY SOLUTIONS NESTOR (hereinafter NESTOR) team according to the RFC 2350 standard. It provides basic information about the NESTOR team, ways to contact them, their responsibilities and services offered.

Last updated

This is version 4, from December 1, 2023.

Distribution list for notifications

There is no distribution list for notifications. Please send any specific questions or comments to NESTOR.

Places where this document can be found

The current version of this NESTOR description document is available on the website of Next Generation Security Solutions s.r.o. (https://www.soc247.cz), where it can also be downloaded.

2. Contact information

Team name

NEXT GENERATION SECURITY SOLUTIONS NESTOR (abbreviated as NESTOR)

Address

Next Generation Security Solutions s.r.o. - NESTOR

Metropolitan Building

U Uranie 954/18

170 00 Prague 7

Czech Republic

Time zone

CET, Central European Time (UTC +1, from the last Sunday in October to the last Sunday in March);

CEST, Central European Summer Time (UTC +2, from the last Sunday in March to the last Sunday in October).

Telephone number

+420 237 836 950

Fax number

Not available

Other communications

Not available

Electronic mail addresses

To report an incident, please use nestor@ngss.cz

For other communications, please use the address nestor@ngss.cz

Public keys and encryption information

To report an incident, as well as for other communications, please use this key:

User ID: NESTOR <nestor@ngss.cz>

Fingerprint: 7593 D6A4 BF64 3467 22D2 8BB4 9318 D86F 1954 C4B1

PGP KeyID: 0x1954C4B1

Team members

The leader of the NESTOR team is Radim Navrátil. A complete overview of NESTOR team members is not publicly available. During official incident resolution communications, team members will identify themselves to the other party with their full names.

Management and supervision are provided by the team leader.

Additional information

General information on NESTOR can be found at www.soc247.cz

Contact with the public

E-mail is the preferred method of contact to the NESTOR team.

Incident reports and related questions should be sent to nestor@ngss.cz. This will create a report in our system.

If it is not possible to use e-mail (or otherwise inappropriate for security reasons), you can contact the NESTOR team by phone.

The NESTOR team's working hours are generally limited to normal working hours (08:0017:00 from Monday to Friday, except on public holidays).

3. Statutes

Mission

The NESTOR team aims to help protect the information infrastructure of its clients and partners. Our goal is to help them to effectively face security challenges, to react to incidents, coordinate steps to resolve them and to prevent them effectively.

Target group

Our target group is primarily clients of Next Generation Security Solutions s.r.o.

We focus on state institutions, commercial, contributory, and non-profit companies.

Classification

NESTOR is part of Next Generation Security Solutions s.r.o., which is its operator.

Qualifications

NESTOR works in the private sector within the bounds of Czech and European legislation.

NESTOR plans to cooperate with system administrators and users within private and public sector institutions.

4. Principles

Incident types and support levels

The NESTOR team is qualified to resolve all types of computer security incidents that have occurred or may potentially occur within its scope.

The level of support provided by the NESTOR team varies depending on the type and severity of the incident or problem, the size of the user community and the resources of the NESTOR team at the time of the incident, but in every case some type of reaction will be provided within one working day. Special attention will be paid to incidents involving critical information infrastructure.

No direct support will be provided to end users. End users are expected to cooperate with their system administrator, network administrator or internet service provider. The NESTOR team will provide them with the necessary support.

The NESTOR is committed to providing information on potential vulnerabilities and, where possible, to provide information to the aforementioned target group about such vulnerabilities before they are exploited.

Cooperation, interaction and access to information

All incoming information is handled securely, regardless of its severity. Information that is visibly highly sensitive will be processed and stored securely, using encryption technology if necessary.

The NESTOR team will use the information provided to it to resolve security incidents. The information will be further distributed to other teams and members only on a need-to-know basis, and anonymously whenever possible.

The NESTOR team operates within the bounds of Czech legislation.

Communication and authentication

Unencrypted e-mails and telephones are considered a sufficiently secure means of communication when transmitting less sensitive data. If it is necessary to send highly sensitive data via e-mail, PGP encryption will be used.

If it is necessary to screen a person before initiating communication, this can be carried out either through existing trust networks (such as TI or FIRST) or other methods such as callback, return mail or (if necessary) face-to-face meetings.

5. Services

Incident response

The NESTOR team's goal is to assist local administrators in resolving technical and organizational aspects of incidents. In particular, it plans to provide assistance or advice with regard to the following aspects of crisis management:

Incident classification

- Assessment of whether the incident is plausible;
- Determining the scope of the incident and its priority.

Incident resolution coordination

- Contacting the parties to the incident to investigate it and then taking appropriate action;
- Facilitating contact with other actors who can help with incident resolution.
- Informing other CERTs and CSIRT teams if necessary;
- Communication with stakeholders and the media.

Incident resolution

- Providing advice on appropriate procedures to local security teams;
- Monitoring the progress of local security teams;
- Providing assistance in evidence gathering and data interpretation.

In addition, the NESTOR team's goals are to collect statistical data on the events that occur within its scope, to provide timely information on possible attacks and to assist in protection against known attacks.

Proactive approach

The NESTOR team collects lists of security contacts for every institution within its scope. These lists are available when needed to resolve security incidents or attacks.

The NESTOR team publishes announcements of serious security threats in order to prevent information and communication technology incidents as much as possible, and thus to reduce their impact to the greatest possible extent.

The NESTOR team processes IoC from available sources and, in the event of a positive finding, ensures the handover of relevant information to the contacts responsible for the affected system.

The NESTOR team also strives to increase awareness of security within its scope.

6. Incident reporting forms

Incident reporting forms are not publicly available. Incidents are reported using encrypted mail using PGP or by phone.

Reports should include information:

- Contact information
- Date and time when the incident was observed
- Description of the event containing all relevant data available

7. Disclaimer

Despite all measures that will be taken in the preparation of information notices, alerts and warnings, the NESTOR team assumes no responsibility for errors, omissions or damages resulting from the use of the information contained therein.