RFC2350

Version 1.2

Last Updated 16/12/2019

TLP: WHITE

1. About This Document

The document describes the operation of the National Cyber Security Center (NCSC) Hungary according to RFC2350.

1.1 Date of Last Update

This version was published at 2019.09.30.

1.2 Distribution List for Notifications

Changes to this document will not be shared through an email list or any other way.

1.3 Locations where this Document can be found

The current version of this document is available from the https://nki.gov.hu website.

1.4 Document Authenticity

This document has been signed with our PGP key. It is available on the https://nki.gov.hu website.

2. Contact Information

2.1 Name of the Team

National Cyber Security Center (NCSC) Hungary - Incident Response Team

2.2 Address

Special Service for National Security

1399 Budapest 62. Pf.: 710/37.

Hungary

2.3 Time Zone

Central European Time / Central European Summer Time

UTC+0100 / UTC+0200

2.4 Telephone Number

+36 (1) 336 4833 / +36 (30) 344 0704

2.5 Facsimile Number

+36 (1) 336 4886

2.6 Other Telecommunication

Not available

2.7 Electronic Mail Address

csirt@nki.gov.hu

2.8 Public Keys and Encryption Information

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v2

mQSuBFIoiGsRDACVhkpWR7iGTvpcLofe4217OGtaup9dYb2EbB0LcZgzcQ2b+dSa
MgK7dRaDHyTAcAZ4GChHxSU/eB4wbfsa4c8V0Swh98zb6fF/Uq1TnHCzD9pPKFx5
BRkhl6xYnInx81PT0tGDmgRibFyZDyOAxrpxCPiQorI1Pi0LHpNJAslx40jRcEP8
+t6buAj+TTUYi/Ge8h2GYhMRjdwDvLAblyYLKViv8vmY7epZPmw0/4b5s923hu2D
hzycf8xrhyRbY8Hn6FyFtsn9t7GgJRBqW8f004KOv7xZvjwGVRtzu/Hp6255QC5V
vkh9FKQC2AvVKEu4wVp32II12Yd44D2E4kbDyIHwQTcU6gsWcPEAT0U94V+rYJ4X
TZclPQqdZleahGs4vof3d2x7bn8p3az8onWcsllrNQ4hSDeRs/kXQSRp6yAzHEsd
GRzaLcKXu/SOdkM5rozK4qfHJOZTNa5cd3AtCokF5uafPyruq+kumnU1eDYj+wt0
Ol9EfPHU2u3Wq48BANmAMt2ME9LwmtGae/rsA6wxx1sQDaxyg1vMg3Jur2NHC/9u
hYvIUaNgEDFaFu/54MFNMTq4nlJMXp8wbS6qSqVgozsjHNMpc2mbdpoL04hHNiIW
we754G11G6kj/4MZchZuRl0kkTVjzwNc/jQGDTHjuZkclVi8RvgVX8wKjZTL77mH
Usvj1RNz3oOF6RciY5b/zmiMHxZ5x2e1LaPN0cBWV7lNPYXrBj0CcXB0C9OZHWEY
xppfnJwG41GQVP26fOUyqSS4VInL17e4l6/BdYEQturnG/A3Qc9jWeu2kjbIdpWI
8ES4CqWbE/+YKjG93UdyQf9a8iZtQx/2w2RWfPLvIzf/yJ/QWe1FzZREqK+rpz+V
uZ1UdvmWGE9nsEy6VDrNW1TJTeOf03+grhJop4GBQPtaPS+h22o/Q7x8oClxqhxg
nbCSSTgG8CYaky4TpdSDtNZkinb5qfHVQCcvKE/w2ZHO+RDhjMcYrK3jdV+WgQeK
gi43kLGs2Z5bNuknak/YoOBH9XArdk1okrZPn2PVi3FPzXF3/7BRJE2QnLB+dBgL
/RGs9vR6bSRXJrOhH1t3WkwlD1duqzgA+5Uo+I/OoTe5Xm1SlVjYjjIkOa8gDZpH
pIHrdfbJ+N/q11jh3D6UjmUbLQUiXuGQyyLQormPu05nAJ8up8R9n/+38nrxMQ7W
3SA6yIKfXr7Tn+63nv33C2gOJW9kiwxino6RBGBROIaN/JwMZTYEPcJ0YLGbMC7D
i3kkRG/64grTQ09Od3FMPZ7qb3/zrhnADsHh1zkvKB0vAVwpd4uPhsJzSipz3o+v
JlSn9vUC7n3n4EMf4MOO8/7xHlQG68qv++EG/XWSn/eAUzYOpVSI9Fru3htD60RI
NU9kpQhvMIBPSD+0RrXCuHl2yv0Xho8GjrR+BFWTJsBv4HYVmOg/QSfFbul6nkN2
XUGtgj0SEd43FVoi7L2w7gV+iTvaNV4ptlzNni5HLyhunShYFiJEfZaJlgd2neSr
ICebcBcleEDJDEu37bQ3YdmmdB9J/EiubXBmxdE2aHboG5+hlmZ3nsuClqMQtpBL
UrQtdGFtYXMua2lzc0Bnb3ZjZXJ0Lmh1IDx0YW1hcy5raXNzQGdvdmNlcnQuaHU+
iHoEEBEIACIFAlhBKKAGCwkIBwMCAheAAhsjBBYCAwECHgEGFQgCCQoLAAoJENTm
ANkdFt/nXN0A/RyE9pdvF5s1SBjlB36oS9MqLBmncsxM2dFzi+SqWL1WAQDFR00Q
amH01BKLAv8hL73L4A/u8NzH9bVa98e4Tmf3erQmVGVhbS1Hb3ZDRVJULUh1bmdh
cnkgPHRlYW1AZ292Y2VydC5odT6IegQTEQgAIgUCUiiIawIbIwYLCQgHAwIGFQgC
CQoLBBYCAwECHgECF4AACgkQ1OYA2R0W3+fE8QEAzUAhTVlwzHJstnAt2qPIeAH3
LlrknFSmT7HZPa8F5F8A/01kceYAupm16YjMVVXtQv9w5s5LUUurusgYAI9exHm7
iEYEEBECAAYFAlKLUtMACgkQU33xXaL9nbxP/QCgwk1XAWfbXtqtrD3EQMOkM0ig
03gAn37L/YHgHHbMpOQ914uFE7WFVgcziJEEExEIADkCGyMGCwkIBwMCBhUIAgkK
CwQWAgMBAh4BAheAFiEEYBtxqDONUYFYqWeI1OYA2R0W3+cFAl3c4I8ACgkQ1OYA
2R0W3+cRCAD+I+KqDktITJYJxK/799T6FvukddQKm47LRNFyxC2OTmkA/10j//46
/qXGAFdY0UawY7pVgdXs/GF8IbFoxBwP7QF/tCtab2x0w6FuIERvcm9zemkgPHpv
bHRhbi5kb3Jvc3ppQGdvdmNlcnQuaHU+iHoEEBEIACIFAlhBJ/kGCwkIBwMCAheA
AhsjBBYCAwECHgEGFQgCCQoLAAoJENTmANkdFt/nW04BAJCVCwZ4u+LLQEGwZv6q
g1cn4x673mz7bJofUG9YSzByAQC5TAXnoD/bNWPIApBE8W92+U2bEOvmgJ0+qZ7i
VfCnuLQwTmVtemV0aSBLaWJlcnbDqWRlbG1pIEludMOpemV0IDx0ZWFtQG5raS5n
b3YuaHU+iJIEExEIADsCGyMFCwkIBwIGFQgJCgsCBBYCAwECHgECF4AWIQRgG3Go
M41RgVipZ4jU5gDZHRbf5wUCXdzgjwIZAQAKCRDU5gDZHRbf5zZDAP9S08NCfrmA
gSUogDT5Z1f2ogoads+oWRQv3Xktm5nHIgD3afN7cpkslCgDmeAkqQzSTaUf5I+i
VVJDtKyoMOormbkEDQRSKIhrEBAA/MdHExYxDrAwFUaw/g32hF53Ofcbokn7tyru
8sT+z5tD55pNZwcOXF3gGs3eRSK2VkPLSck994wjVVj4yirwSIR5LxHgQ8THlLYL
VkexfS/0/bZgIhmUEmR+YWDPodbkIZGVbWHrSx3XbbksBVBfS5BOBoGe8BmrqYbX
Q4H5rrEvXnJgxpiqcXLP8TikC7a3kUr+2f4xJja//Xac9+MxFQCJijxjsxY+tPTo
suwEXq5XLL3Jid6LED1icLMqR8SCbIQvvRSB8arkf8W0biSFl9d0fFgC2SrU/oNE
frwui9W8CgSxDyEH9m/4Q5KYfGTigYgz4421+J0lKQGZWpSDtANn0NIibYJyufMn
T0UnxxBTZ3vydJ2FSTEYoP+JAellmClRAl6/HKQGLLR9MLoP15aI81JgQGcMk12k
1iAy+t5NnSUmttcdKapQ48PXIxLMYAVkgTwoVTcGjSHZ4oPOkDNdiqx8iX8SsUbC
V0RygLoHWDYLe+nx64a6GGTRA5/Umyni8ToMGxd6fGh8bxTv4iIOv+ZW3uOSy8ex
sMtQq7AWqBuG1sLnZn9VjIzzPW90kqDQao2l5a2rk1FY563t0yRZjD9FiAedyyf+
23HkRaO8Mu+x6UqYKlnxmF9Kk+zc3gjpbJXI86FiohY3iYN1G3AEEdDxDkQ/Saan
nUcc4OMAAwUQAMG5PMWDyX9Oie5DXpPzT0coCX0IENjDyrgaXzulCAdml8bRdupO
QueoCSPSPXJITpiQZwcJazV2q9G9Sj2zllDWUFHg0OoiZ0UGD4QC8bTXDDM2Fnes
Aj2SWl/I0zUGUaLAri/yK7ywFt5hruS5XYp3dsloh2zPr88DUbHvIaOO2bfj6/iK
ng/gtpgLy/2EHvEHjTb2N9nD96F/FX0eY6jdvFWc1OI+Fkvc3LqZY1/ZGqkYXgj4
SEz1Z59xcWajIt4p2AMASxQTM3BAHbyW6eAx2FggBLD1ieRIhXv3HTB2wIGGzTO4
H3CWrzl1foGe9MRLQTuB9bJQBHyArXGYVZ69anVvS1VD6HxtAnYZWinovwD20R7z
lTvv+QkhlHpAi6FZ6WKJ+3q4ZQFsNlxX/v/esjlwXTkzMBHNqVeNcEr2Nbodk8HX
zBzJq0jPDoBmaGHyhBvHGGuU5CcPqK7HyPi6iTJ9iC8m5jjaSKnJmtFmMzHviMIG
ZhHEn2oSEvzpIvIF5Z/BRe0hfNW8u0pdPaAmJuBwn/hjqUCZbg9U9PDZl/Ogeosj
5Hp0e4n14l2+3/A9ASQnGvQc967IxQQ3X31CweQbHuGyyXm/4Z4X5xTqq1CvzpcU
7IcxAn/8rYJs3CklBn/Q1IOPvWa2lx6u+OzDvF3weqY60T4BNqgCd8MoiGEEGBEI
AAkFAlIoiGsCGwwACgkQ1OYA2R0W3+f38wD/UIhSIC/BckPxj7KBhp2jtYEfk9wR
Uzj78oga/6hSCbIBAKYrPIcd4Dv7wxaOpJKmyuMp6SXMNn6da3jgtLFz/JKu
=7H6i
```

```
-----END PGP PUBLIC KEY BLOCK-----
```

2.9 Team Members

Information about the team members cannot be published.

2.10 Other Information

General information about NCSC Hungary can be found at: https://nki.gov.hu

2.11 Points of Customer Contact

The suggested method of contacting the NCSC Hungary is via e-mail to csirt@nki.gov.hu.

Please use our cryptographic keys above to ensure integrity and confidentiality.

2.12 Business Hours

The hours of operation are generally restricted to regular business hours (07:30-16:00 Monday to Thursday, 07:30-13:30 on Friday) except public holidays.

2.13 Emergency Procedure

Reporting an incident is possible by telephone 24/7.

3. Charter

3.1 Mission Statement

Our Mission:

NCSC Hungary's goal is to assist the development of the Hungarian information society, by making the use of computers and the Internet safer.

Our Vision:

NCSC Hungary builds on strong national and international cooperation, to develop a knowledge base, which could be used in this new field of security: the protection of e-services are supervised by a professional team capable of providing quick intervention and effective assistance.

Our goal is to make the Internet secure, to develop a world-class security and information base, and to become a publicly accessible forum for Internet and computer security.

3.2 Constituency

NCSC Hungary provides services for the entire Hungarian government administration and the municipalities. The security of computer systems in particular the government backbone system owned by the government and critical infrastructures receive special attention from our organization. NCSC Hungary is also the responsible CSIRT for all sectors mentioned in the Directive (EU) 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (NIS Directive)

3.3 Sponsorship and/or Affiliation

NCSC Hungary operates within the organization of the Special Service for National Security (SSNS), under the direction and control of the Minister of Interior. NCSC Hungary is the Hungarian government’s network and information security center. Its task is provide network and information security support to the entire Hungarian government administration and the local municipalities. The center has a vital role in Hungary's critical information infrastructure protection. NCSC Hungary also acts as a knowledge base for IT professionals and the Hungarian public.

NCSC Hungary is member in the following organisations.

- FIRST (since 30. of May 2006.)
- Trusted Introducer (since 14. of February 2006)
- NIS CG
- CSIRTs Network
- Meridian Process
- Central European Cyber Security Platform

3.4 Authority

The NCSC Hungary expects to work cooperatively with system administrators within its constituency, and, insofar as possible, to avoid authoritarian relationships. However, if necessary and requested by a constituent, NCSC Hungary may assist in initiating legal proceedings.

4. Policies

4.1 Types of incidents and level of support

NCSC Hungary is authorized to address all types of computer security incidents which occur, or threaten to occur, in Hungary. The level of support given by NCSC Hungary will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and NCSC Hungary's resources at the time, though in all cases some response will be made within one working day. Computer security incidents at organizations registered at NCSC Hungary will always receive priority over incidents at unregistered organizations.

4.2 Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from NCSC Hungary, NCSC Hungary acknowledges its indebtedness to, and declares its intention to contribute to, the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites where necessary, NCSC Hungary will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from NCSC Hungary. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

Information being considered for release will be classified as follows:

Private user information is information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons. Private user information will not be released in identifiable form outside NCSC Hungary, except as provided for below. If the identity of the user is disguised, then the information can be released freely (for example to show a sample .cshrc file as modified by an intruder, or to demonstrate a particular social engineering attack).

Intruder information is similar to private user information, but concerns intruders. While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking an incident.

Private site information is technical information about particular systems or sites. It will not be released without the permission of the site in question, except as provided for below.

Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds if they are available. Vulnerability information will be released freely, though every effort will be made to inform the relevant vendor before the general public is informed.

Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users. Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.

Statistical information is embarrassing information with the identifying information stripped off. Statistical information will be released and used in publications and other educational papers.

Contact information explains how to reach system administrators and CSIRTs. Contact information will not be released freely, except where the contact person or entity has requested that this not be the case. If NCSC Hungary has reason to believe that the dissemination of this information would not be appreciated, will deny to release any contact information.

Potential recipients of information from NCSC Hungary will be classified as follows:

Registered members of NCSC Hungary are entitled to information which pertains to the security of their own computer systems, even if this means revealing "intruder information", or "embarrassing information" about another system. For example, if account aaaa is cracked and the intruder attacks account bbbb, user bbbb is entitled to know that aaaa was cracked, and how the attack on the bbbb account was executed. User bbbb is also entitled, if she or he requests it, to information about account aaaa which might enable bbbb to investigate the attack. For example, if bbbb was attacked by someone remotely connected to aaaa, bbbb should be told the provenance of the connections to aaaa, even though this information would ordinarily be considered private to aaaa. Registered members of NCSC Hungary are entitled to be notified if their computer systems are believed to have been compromised.

Unregistered constituents of NCSC Hungary will receive no restricted information, except where the affected parties have given permission for the information to be disseminated.

Statistical information may be made available to the constituents of NCSC Hungary. There is no obligation on the part of NCSC Hungary to report incidents to the community, though it may choose to do so; in particular, it is likely that NCSC Hungary will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

The public at large will receive no restricted information. NCSC Hungary communicates with the public mainly through its website https://nki.gov.hu/. Members of the public may find vulnerability, statistical, and contact information, other public data, and news on NCSC Hungary's website. Any concerns about, or objections to information published on NCSC Hungary's website should be addressed to the NCSC Hungary team at sajto@nki.gov.hu.

The computer security community will be treated the same way the general public is treated. While members of NCSC Hungary may participate in discussions within the computer security community, such as newsgroups, mailing lists (including the full-disclosure list "Bugtraq"), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed to any level of detail, any examples taken from NCSC Hungary experience will be disguised to avoid identifying the affected parties.

Other sites and CSIRTs, when they are partners in the investigation of a computer security incident, will in some cases be trusted with confidential information. This will happen only if the foreign site's bona fide can be verified, and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Such information sharing is most likely to happen in the case of sites registered at NCSC Hungary, unless they have objected to such information exchange at registration.

For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other system administrators and CSIRTs. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

Vendors will be considered as foreign CSIRTs for most intents and purposes. NCSC Hungary wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without most intents and purposes the permission of the affected parties.

Law enforcement officers will receive full cooperation from NCSC Hungary, including any information they require to pursue an investigation, in accordance with the law.

NCSC Hungary uses the Traffic Light Protocol (TLP) as described in FIRST Standards Definition and Usage Guidance (https://www.first.org/tlp/).

While handling Classified Information (including National, International, EU, NATO or other), NCSC Hungary will act in accordance of the Act CLV of 2009. on the Protection of Classified Information

4.3 Communication and Authentication

In view of the types of information that NCSC Hungary will likely be dealing with, telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP encryption will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission or encrypted channels should be used during the transfer.

Where it is necessary to establish trust, for example before relying on information given to NCSC Hungary, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, along with telephone call-back or e-mail mail-back to ensure that the party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures (in particular PGP is supported).

4.4 Reaction Time

NCSC Hungary will its best to have all reported incidents managed in a timely manner. During office hours we will start our incident handling process within 6 hours, while during duty period (weekends and holidays) we start our activities within 24 hours. In case of urgent matters, or issues with specific importance, or in case of serious incidents (as described in NIS Directive) NCSC Hungary will start the incident handling process within 2 hours.

5. Services

5.1 Incident Response

NCSC Hungary will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

Investigating whether indeed an incident occurred.

Determining the extent of the incident.

5.1.2. Incident Coordination

Determining the initial cause of the incident (vulnerability exploited).

Facilitating contact with other sites which may be involved.

Facilitating contact with law enforcement, if necessary.

Making reports.

Composing announcements to users, if applicable.

5.1.3. Incident Resolution

Analyzing and if possible removing the vulnerability.

Securing the system from the effects of the incident.

Collecting evidence where criminal prosecution, or community disciplinary action, is contemplated.

In addition, NCSC Hungary will collect statistics concerning incidents which occur within or involve its constituency, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of NCSC Hungary's incident response services, please send e-mail as per section 2.7 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.

5.2 Proactive Activities

Intrusion Detection Services

NCSC Hungary 's intrusion detection service can keep a watchful eye on a client's system and can give you an early alert about successful virus or hacker attacks, thus security issues can be handled, before they become a serious problem.

Security Audits

NCSC Hungary offers security audits on information technology systems. We will provide valuable information in determining the risk related to any specific IT system or we can actually perform the risk assessment of a supported organization. Such an assessment can find the balance between maximizing security and minimizing costs, resulting in substantial savings. NCSC Hungary will help its clients get ready for the worst by providing business continuity and disaster recover planning solutions, so when a problem disrupts normal business operations, they will be among the first ones to get back on their feet.

Development of Security Applications

NCSC Hungary can also be commissioned to install, configure, maintain or even develop security applications. Our experts can evaluate the security of software applications, hardware, or IT services to help supported organizations choose the best products available.

Malware Analysis

Malicious code can reduce work efficiency and system security, but only an expert can determine the threat of a software or document for an IT system. Any software, document or other suspicious code sent to NCSC Hungary will be analysed by our experts to find malicious code.

Technology Watch

IT security tools are developing at a fast pace, keeping up with upcoming threats. NCSC Hungary can determine the need for a new security tool, and develop effective deployment methods for its clients.

Security Consultancy

NCSC Hungary, with the support of its external experts, can give advice on any security issue to its clients. The 70-30 rule is still effective, which means that most Security threats are coming from inside the organization, NCSC Hungary can provide educational materials and hold training sessions for their constituents, so employees and managers become part of the security, instead of being a security risk.

Notification of Incident:

Computer security incidents should be reported to csirt@nki.gov.hu.

5.3 Awareness Raising Services

During its awareness raising duty, NCSC Hungary is performing different types of activities. NCSC Hungary issuing a weekly newsletter about security, we are giving lectures, presentations to our constituents as well as performing hidden Social Engineering activates upon request. We are also publishing vulnerability and malware descriptions, alerts and warnings.

6. Incident Reporting Forms

The Incident reporting form is available on https://nki.gov.hu. Incidents or related information can be reported via email on csirt@nki.gov.hu or via the phone on +36 (1) 336 4833.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, NCSC Hungary assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.