Amsterdamse Hogeschool voor de Kunsten

AHKCERT profile

Ferry de Jong (ICT Manager)

12 April 2010

Contents

AHKCERT profile

Established according to RFC-2350.

1. Document Information

1.1 Date of Last Update

This is version 1.5 of 12 April 2011.

1.2 Distribution List for Notifications

This profile is kept up-to-date on the location specified in 1.3.
E-mail notification of updates are sent to:
All AHK security team members
All AHKCERT constituents

AHKCERT has been registered by SURFcert (http:/ /cert.surfnet.nl/), the internationally acknowledged CERT for the Research and Education community in The Netherlands.
Any specific questions or remarks please address to the AHKCERT mail address.

1.3 Locations where this Document May Be Found

The current version of this profile is always available on the de www.ahk.nl website at http://www.ahk.nl/fileadmin/cert/rfc-2350.pdf.

2. Contact Information

2.1 Name of the Team

Full name: (NL)	Amsterdamse Hogeschool voor de Kunsten Computer Emergency Response Team
Full name: (UK):	Amsterdam School of the Arts Computer Emergency Response Team
Short name:	AHKCERT

AHKCERT is the CERT or CSIRT team for the 'Amsterdamse Hogeschool voor de Kunsten (Amsterdam School of the Arts)' (AHK) in The Netherlands**.**

2.2 Address

Dutch
AHK
Afdeling ICT, AHKCERT
Markenplein 1
NL-1011 MV Amsterdam
Nederland

English
AHK
IT department, AHKCERT
Markenplein 1
NL-1011 MV Amsterdam
The Netherlands

2.3 Time Zone

GMT+1 (GMT+2 with DST or Summer Time, which starts on the last Sunday in March and ends on the last Sunday in October)

2.4 Telephone Number

+31 20 5277752 (ICT helpdesk of the AHK)

2.5 Facsimile Number

+31 20 527 7456 (ICT/CERT and ICT fax)
Note: this is not a secure fax.

2.6 Other Telecommunication

Not available.

2.7 Electronic Mail Address

security@ahk.nl
This address can be used to report all security incidents to which relate to the AHKCERT constituency, including copyright issues, spam and abuse.

2.8 Public Keys and Encryption Information

PGP is currently not supported for secure communication.
An AHKCERT public PGP key is not yet available on the public keyservers.
For highly sensitive/confidential information, AHKCERT can establish phone contact.

2.9 Team Members

No information is provided about the AHKCERT team members in public.

2.10 Other Information

- See the AHKCERT webpages http://www.ahk.nl/cert.
- AHKCERT is registered by SURFcert (see http://www.surfnet.nl/nl/Thema/surfcert/teams/Pages/CERTteams.aspx). This registration is conditional – one of the conditions is making this RFC-2350 profile available and keeping it up-to-date.

2.11 Points of Customer Contact

Regular
Regular cases: use AHKCERT e-mail address.

Regular response hours: Monday-Friday, 09:00-17:00 (except public holidays in The Netherlands, last week July, first week August and the period between Christmas and first Monday after New Year).

Emergency
EMERGENCY cases: use AHKCERT phone number with back-up of mail address for all details (putting EMERGENCY in subject line is recommended). The AHKCERT phone number is available at regular response hours. The helpdesk employee (not an AHKCERT team member) forward the request directly to the members of the AHKCERT team.

3. Charter

3.1 Mission statement

The mission of AHKCERT is to resolve IT security incidents related to their constituency (see 3.2), and to prevent such incidents from occurring.

3.2 Constituency

Amsterdam School of the Arts (AHK) and institutions connected to AHK network, with all related students.

AHK IP-range 145.102.112.0/20 (SURFnet).
AHK domein: ahk.nl

145.102.112.0/22
DMZ, Backbone (for routing between the 6 faculties), VPN, Management, inbound NAT, outbound NAT

145.102.112.116/22
Account or sign on network (students and employees)

145.102.112.124/22
Wireless network

145.102.112.120/22
Not used

3.3 Alumni and employees. Sponsorship and/or Affiliation

AHKCERT is embedded in the ICT department of the AHK.

3.4 Authority

AHKCERT coordinates and resolves security incidents on behalf of AHK and has no authority reaching further than that. AHKCERT is however expected to make operational recommendations in the course of its work. Such recommendations can include for instance blocking addresses or networks. The implementation of such recommendations is a responsibility of AHK ICT department.

4. recommendations were made. Policies

4.1 Types of Incidents and Level of Support

All incidents are considered normal priority unless they are labeled EMERGENCY. AHKCERT itself is the authority that can set and reset the EMERGENCY label. An incident can be reported to AHKCERT as EMERGENCY, but it is up to AHKCERT to decide whether or not to uphold that status.

4.2 Co-operation, Interaction and Disclosure of Information

ALL incoming information is handled confidentially by AHKCERT, regardless of its priority.

Information that is evidently sensitive in nature is only communicated and stored in a secure environment, if necessary using encryption technologies. When reporting an incident of sensitive nature, please state so explicitly, e.g. by using the label SENSITIVE in the subject field of e-mail, and if possible using encryption as well.

AHKCERT supports the Information Sharing Traffic Light Protocol (ISTLP – see https://www.trusted-introducer.org/links/ISTLP-v1.1-approved.pdf) - information that comes in with the tags WHITE, GREEN, AMBER or RED will be handled appropriately.

AHKCERT will use the information you provide to help solve security incidents, as all CERTs do. This means that by default the information will be distributed further to the appropriate parties – but only on a need-to-know base, and preferably in an anonymised fashion.

If you object to this default behavior of AHKCERT, please make explicit what AHKCERT can do with the information you provide. AHKCERT will adhere to your policy, but will also point out to you if that means that AHKCERT cannot act on the information provided.

AHKCERT does not report incidents to law enforcement, unless national law requires so. Likewise, AHKCERT only cooperates with law enforcement EITHER in the course of an official investigation – meaning that a court order is present – OR in the case where a constituent requests that AHKCERT cooperates in an investigation. When a court order is

absent, AHKCERT will only provide information on a need-to-know base.

4.3 Communication and Authentication

See 2.8 above.
In cases where there is doubt about the authenticity of information or its source, AHKCERT reserves the right to authenticate this by any (legal) means.

5. services

5.1 Incident Response (Triage, Coordination and Resolution)

AHKCERT is responsible for the coordination of security incidents somehow involving their constituency (as defined in 3.2). AHKCERT therefore handles both the triage and coordination aspects. Incident resolution is left to the responsible administrators within the constituency – however AHKCERT will offer support and advice on request.

5.2 Proactive Activities

AHKCERT pro-actively advises their constituency in regard to recent vulnerabilities and trends in hacking/cracking.
AHKCERT advises the ICT department of the Amsterdam school of the Arts (AHK) on matters of computer and network security. It can do so pro-actively in urgent cases, or on request.
Both roles are roles of consultancy: AHKCERT is not responsible for implementation.

5.3 Incident reporting Forms

Not available. Preferably report in plain text using e-mail - or use the phone.

5.4 Disclaimers

None.