HAN-CERT - RFC 2350

Hogeschool van Arnhem en Nijmegen

Versie: 1.2
Datum: 10 maart 2014

INHOUD

1 Informatie over dit document

Dit document beschrijft het profiel (contactgegevens, diensten, etc.) van het HAN-CERT, het "Computer Emergency Response Team van de Hogeschool van Arnhem en Nijmegen". De structuur van dit document is volgens RFC 2350.

1.1 Datum laatste wijziging

Dit is versie 1.2, gepubliceerd op 10 maart 2014.

1.2 Distributielijst voor mededelingen

Er is geen distributielijst voor mededelingen.

1.3 Locatie waar dit document kan worden gevonden

De meest recente versie van dit document kunt u vinden op http://www.han.nl.

2 Contactinformatie

2.1 Naam van het team

Het "HAN-CERT": het Computer Emergency Response Team van de Hogeschool van Arnhem en Nijmegen.

2.2 Adres

Hogeschool van Arnhem en Nijmegen
Secretariaat ICT, HAN-CERT
Ruitenberglaan 26
6826 CC Arnhem
The Netherlands

2.3 Tijdzone

Het HAN-CERT gebruikt lokale tijd. Dat wil zeggen CET (UTC+1) in de winter en CEST (UTC+2) in de zomer.

2.4 Telefoonnummer

026-3691545

2.5 Faxnummer

026-3658178

2.6 E-mail adres

cert@han.nl

2.7 Website

Het HAN-CERT heeft geen eigen website.

2.8 Publieke sleutel voor communicatie

Het HAN-CERT gebruikt PGP voor beveiligde communicatie. De publieke sleutel zijn beschikbaar op de verschillende public keyservers (bijvoorbeeld op http://wwwkeys.pgp.net).

Key-id: 0x94A1B643

Fingerprint: E064 184F 943D 76C1 01F5 F170 5E47 76FB 94A1 B643

Gebruik de publieke sleutel voor het versleutelen van de berichten die u naar het HAN-CERT stuurt, en onderteken indien mogelijk de berichten met uw eigen sleutel. Het helpt als deze sleutel verifieerbaar is via public keyservers. Berichten van het HAN-CERT zullen in alle gevallen worden ondertekend met de sleutel van het HAN-CERT. De sleutel kan worden gecontroleerd via de public keyservers.

2.9 Teamleden

De leden van het HAN-CERT zijn:

Stefan Arts
Jos Muijzer
Ronny Anneveld
Dave van Ooijen

2.10 Openingstijden

Het HAN-CERT is geopend van maandag tot vrijdag, van 8:30 to 17:00 CET/CEST. Tijdens schoolvakanties is het HAN-CERT niet bereikbaar.

NOODGEVALLEN:
Voor noodgevallen kunt u het beste bellen, of anders e-mailen. Zet in geval van mailen het woord EMERGENCY in het onderwerp.

3 Charter

3.1 Missie

De missie van het HAN-CERT is:

- Het coördineren van het voorkomen en afhandelen van beveiligingsincidenten, welke te maken hebben met de informatievoorzieningen van de Hogeschool van Arnhem en Nijmegen, met het doel om de beschikbaarheid, integriteit en de vertrouwelijkheid van deze informatievoorzieningen te verhogen.

3.2 Bereik

Het HAN-CERT levert haar diensten aan de Hogeschool van Arnhem en Nijmegen. Incidenten kunnen door iedereen worden gemeld, mits ze te maken hebben met de informatievoorzieningen van de Hogeschool van Arnhem en Nijmegen.

3.3 Sponsoring en/of relatie

Het HAN-CERT is onderdeel van de Hogeschool van Arnhem en Nijmegen.

3.4 Bevoegdheden

Bij constatering of vermoeden van misbruik van ICT-voorzieningen is het HAN-CERT bevoegd bewijsmateriaal veilig te stellen en maatregelen te nemen om meer misbruik te voorkomen.

4 Beleid

4.1 Soorten incidenten en ondersteuningsniveau

Het HAN-CERT streeft ernaar binnen één dag te reageren. Alle incidenten krijgen standaard een normale prioriteit, tenzij ze zijn gemarkeerd als EMERGENCY. Een incident kan worden aangemeld als EMERGENCY, maar het HAN-CERT beslist of deze status behouden blijft.

4.2 Samenwerking en vertrouwelijkheid

Alle ontvangen informatie wordt vertrouwelijk behandeld, ongeacht de prioriteit. Gevoelige informatie wordt alleen versleuteld gecommuniceerd. Bij het melden van incidenten die gevoelig liggen, is het verstandig om ook VERY SENSITIVE in het onderwerp erbij te zetten.

Het HAN-CERT zal de verstrekte informatie gebruiken om het beveiligingsincident op te lossen, zoals alle CERT's/CSIRT's doen of zouden moeten doen. Dit kan betekenen dat informatie over het incident verder zal worden gedistribueerd, maar enkel op een need-to-know basis.

Wanneer u bezwaar heeft op de werkwijze van het HAN-CERT, vermeldt dan duidelijk wat het HAN-CERT mag doen met de door u verstrekte informatie. Het HAN-CERT zal aan uw wensen voldoen, maar zal het ook laten weten als het niet kan handelen met de door u verstrekte informatie.

Het HAN-CERT doet alleen aangifte bij de politie, of verstrekt alleen gevoelige gegevens aan derden wanneer het HAN-CERT hiertoe opdracht krijgt van een gezagdrager van de Hogeschool van Arnhem en Nijmegen.

4.3 Communicatie en authenticatie

In alle gevallen waarbij gevoelige informatie is betrokken, wordt het gebruik van PGP aanbevolen. Zie voor meer informatie in 2.9.

5 Diensten

5.1 Incidentenafhandeling

5.1.1 Prioriteitstelling

Het HAN-CERT bepaalt de prioriteit van de gemelde beveiligingsincidenten.

5.1.2 Coördinatie

Het HAN-CERT is verantwoordelijk voor de coördinatie van de afhandeling van de gemelde beveiligingsincidenten.

5.1.3 Probleemoplossing

Het oplossen van een beveiligingsincident wordt overgelaten aan de verantwoordelijke eigenaar van de betreffende informatievoorziening.

5.2 Preventie

Het HAN-CERT informeert en adviseert de Hogeschool van Arnhem en Nijmegen over allerhande zaken die te maken hebben met informatiebeveiliging, zoals nieuwe trends en ontwikkelingen, verbeterpunten en gevonden kwetsbaarheden. Het HAN-CERT doet dit gevraagd of ongevraagd. Het HAN-CERT is niet verantwoordelijk voor de implementatie van beveiligingsmaatregelen.

6 Formulieren

Voor het melden van incidenten zijn geen speciale formulieren beschikbaar.

7 Disclaimer

De informatie in dit document is alleen voor bedoeld voor het vertrekken van informatie. De Hogeschool van Arnhem en Nijmegen is niet verantwoordelijk voor de nauwkeurigheid of volledigheid van de informatie in dit document. De Hogeschool van Arnhem en Nijmegen is niet aansprakelijk voor beschadiging, verlies, persoonlijke schade of wat dan ook, ontstaan uit of gerelateerd aan het gebruik van dit document.