Windesheim

Windesheim CSIRT

Computer Security Incident Response Team

(RFC2350)

2 december 2016

Beschrijving en missie statement van de Windesheim CSIRT inclusief alle contact informatie

Windesheim

Inhoudsopgave

1 Document informatie

1.1 Versie informatie

Laatste versie: 2 december 2016.

1.2 Distributielijst voor updatemeldingen

Melding van updates worden gepubliceerd via ShareNet

1.3 Locatie waar het document te vinden is

De laatste versie van het document is te vinden op ShareNet.
URL: https://infosite.windesheim.nl/Pages/Melden-van-misbruik-ICT-voorzieningen.aspx
Tevens is dit document geplubliceerd op.
URL: https://www.windesheim.nl/beveiliging
Zorg ervoor dat u altijd de laatste versie gebruikt

2 Contact Informatie

2.1 Naam van het team

Windesheim CSIRT : het Windesheim computer security incident response team

2.2 Adres

Bezoekadres
Windesheim CSIRT
Dienst Bedrijfsvoering
ICT Bedrijf
Campus 2-6
8017 CA Zwolle
Nederland

Postadres
Windesheim CSIRT
Dienst bedrijfsvoering
ICT Bedrijf
Postbus 10090
8000 GB Zwolle
Nederland

2.3 Tijdzone

Amsterdam (GMT +0100, en GMT +0200 van april t/m oktober)

2.4 Telefoonnummers

+31 88 469 90 70 (tijdens kantooruren)
Vragen naar ICT bedrijf - Windesheim CSIRT.

2.5 Faxnummer

2.6 Overige Telecommunicatie

2.7 E-mail adressen

CSIRT@windesheim.nl
security@windesheim.nl
abuse@windesheim.nl
cert@windesheim.nl

Deze mailboxen wordt door de CSIRT functionaris van dienst uitgelezen.

2.8 Public Keys en andere encryptie informatie

2.9 Teamleden

Coördinator van het CSIRT team is de Coördinator Infrastructuur. CSIRT diensten worden gedraaid door medewerker die bereikbaarheidsdienst heeft. De security officer wordt door CSIRT team geïnformeerd en staat het team bij met advies. Indien nodig worden een juridisch adviseur en communicatie adviseur toegevoegd aan het team. In crisis situaties wordt teruggevallen op het crisisbeheersplan van Windesheim en kunnen andere deskundigen ingeschakeld worden.

2.10 Overige Informatie

2.11 Aanspreekpunten voor klanten

De voorkeursmethode om de CSIRT te bereiken is via e-mail CSIRT@windesheim.nl .E-mail die naar dit mail adres gestuurd wordt, wordt door de functionaris van dienst uitgelezen. Wanneer het noodzakelijk is dat er direct actie wordt ondernomen zet dan “URGENT” in het onderwerp.

Wanneer het niet mogelijk is (of beveiligingstechnisch onwenselijk is) e-mail te gebruiken dan kan de CSIRT ook telefonisch benaderd worden via de Servicedesk ICT tel 088-4699070. Zij geven het bericht door aan de CSIRT. Mocht het om een vertrouwelijke kwestie gaan dan kan verzocht worden om direct door te verbinden met de Windesheim CSIRT. De Servicedesk is bereikbaar gedurende kantooruren (maandag t/m vrijdag 8.00 – 17.00). De werktijden van de CSIRT zijn in z’n algemeenheid ook beperkt tot deze kantooruren.

3 Handvest

3.1 Missie

Het doel van de Windesheim CSIRT is in eerste instantie om Windesheim te ondersteunen bij het oplossen en voorkomen van incidenten op het gebied van computer- en netwerkbeveiliging.

We onderscheiden 3 deelgebieden:

- Preventie

- Detectie
- Correctie

Het Windesheim CSIRT houdt zich met name bezig met (coördinatie van) detectie en correctie en draagt bij aan preventie door middel van aanbevelingen ten aanzien mogelijke kwetsbaarheden en bedreigingen.

Windesheim CSIRT heeft als taak beveiligingsincidenten te signaleren en te coördineren bij de bestrijding ervan. Het ziet toe op het wegnemen van de oorzaak en herstel van de schade.

3.2 Werkgebied

De doelgroep van de CSIRT zijn alle medewerkers en studenten van Windesheim en heeft betrekking op alle ICT faciliteiten die door het ICT bedrijf worden aangeboden. Alleen apparatuur in eigendom van Windesheim wordt ondersteund.

3.3 Samenwerking / Externe relaties

De Windesheim CSIRT onderhoud contacten met de SURFcert en diverse andere CSIRT's in het Hoger Onderwijs. Verder neemt Windesheim deel in SCIPR, een overleg orgaan voor het Hoger Onderwijs betreffende de meer beleidsmatige kant van informatiebeveiliging.

3.4 Autoriteit

De Windesheim CSIRT valt onder de verantwoordelijkheid van de Manager ICT bedrijf en heeft met betrekking tot de afhandeling van incidenten *volledige bevoegdheid*. Dit houdt in dat de CSIRT gedurende een incident beslissingen kan nemen (bijvoorbeeld om een systeem down te brengen of te isoleren) zonder goedkeuring vooraf van het hogere management. Ook kan de CSIRT (individuen in) de organisatie verplichten bepaalde acties uit te voeren om beveiligingsincidenten het hoofd te bieden.

Waar het gaat om het treffen van preventieve maatregelen om de beveiligingssituatie in de organisatie te verbeteren is er sprake van een *gedeelde bevoegdheid*. In dit geval werkt de CSIRT veel meer samen met de organisatie om invloed uit te oefenen op het besluitvormingsproces betreffende de acties die genomen zouden moeten worden. De CSIRT heeft een stem in de besluitvorming maar beslist in deze dus niet zelf.

De CSIRT verwacht nauw samen te werken met applicatiebeheerders en gebruikers om zoveel mogelijk de autoritaire houding te vermijden. Mocht het echter nodig zijn dan zal de CSIRT niet verzuimen gebruik te maken van de bevoegdheden die haar zijn toebedeeld.

Alle leden van de CSIRT zijn medewerkers van Windesheim, zijn gebonden aan geheimhouding, zijn bekend met en handelen volgens de integriteitcode voor ICT 'ers.

Verder zal er gehandeld worden in overeenstemming met het geldende informatiebeveiligingsbeleid en de ICT reglementen voor medewerkers en studenten.

Medewerkers of studenten van Windesheim die bezwaar willen maken tegen de acties die door de CSIRT ondernomen worden, dienen contact op te nemen met de manager ICT bedrijf.

4 Beleid

4.1 Type incidenten en niveau van ondersteuning

De Windesheim CSIRT is geautoriseerd om alle beveiligingsincidenten die zich voordoen of dreigen voor te doen, aangaande Windesheim, aan te pakken.

Het niveau van ondersteuning dat door de CSIRT geleverd wordt is afhankelijk van het type en de ernst van het incident of geval, de hoeveelheid gebruikers die erdoor getroffen wordt en de beschikbare capaciteit op dat moment.

Indien een incident met hoge prioriteit behandeld dient te worden dient de melder het incident als “URGENT” te labelen. Het CSIRT team behoud zich het recht voor prioriteiten aan te passen.

Incidentmelders krijgen in ieder geval binnen een dag bericht over hoe het incident opgepakt gaat worden.

Niet alle incidenten zullen vanuit de CSIRT zelf opgelost kunnen worden. Specifieke ondersteuning is beschikbaar vanuit ICT en IM. Waar deze ondersteuning ingeschakeld wordt zullen deze personen handelen onder de strikte regels betreffende geheimhouding en integriteit van de CSIRT. Zij zullen daar ook door de betreffende functionaris van dienst op gewezen worden.

Ter voorkoming van incidenten zullen meldingen van mogelijke kwetsbaarheden in de beveiliging door de CSIRT bijgehouden worden en doorgespeeld worden aan de betreffende verantwoordelijken (veelal applicatie-, netwerk- of serverbeheer). De verantwoordelijke instantie zal aan de CSIRT terugmelden wat er met de betreffende melding gebeurd is (noodmaatregelen genomen, kwetsbaarheid verholpen, kwetsbaarheid is geaccepteerd risico).

Melders van kwetsbaarheden krijgen wel bericht dat hun melding ontvangen is maar geen bericht óf en wanneer betreffende kwetsbaarheid verholpen is tenzij de melding conform de responsible disclosure procedure verloopt.

4.2 Samenwerking, interactie en openbaarmaking

Communicatie met Windesheim CSIRT vindt plaats op basis van vertrouwelijkheid. Het CSIRT zal dan ook geen inhoudelijk informatie over incidenten of melders daarvan aan derden verstrekken. Informatie over beveiligingsincidenten wordt alleen doorgegeven aan betrokken partijen voor zover relevant en noodzakelijk voor het oplossen van het incident.

Privé gebruikers informatie

Windesheim is gehouden aan de Wet Bescherming Persoonsgegevens en de Algemene verordening Gegevensbescherming. Vertrouwelijke informatie betreffende individuele personen zullen dan ook niet buiten Windesheim beschikbaar gesteld worden zonder schriftelijke vordering van politie en justitie. Uitzondering hierop vormt het op aanvraag van nabestaanden toegang verlenen tot de mailbox van een overledene. (Zie hiervoor het protocol overlijden)

Vanuit de CSIRT zal er alleen monitoring op inhoud van bestanden, mail en surf gedrag van individuele gebruikers zijn wanneer er een sterk vermoeden van misbruik is gemeld. Rapportage over het vermeende misbruik vindt vervolgens alleen plaats aan de instantie die verantwoordelijk wordt geacht voor het nemen van repressieve maatregelen. Naam en toenaam worden alleen bekend gemaakt aan de CSIRT leden die verantwoordelijk zijn voor de oplossing van het betreffende incident. In geanonimiseerde vorm kan vrijelijk over het voorval gerapporteerd worden en kan het voorval in voorbeelden aangehaald worden.

Hackers informatie

Hackers informatie is eigenlijk ook privé gebruikers informatie met dit verschil dat het hier een hacker betreft. Informatie over indringers in systemen wordt niet publiek verspreid maar mag wel intern onder betrokkenen verspreid worden. Alleen in het geval van aangifte wordt deze informatie met politie en justitie gedeeld.

Kwetsbaarheden informatie

Informatie betreffende kwetsbaarheden wordt vrijelijk verspreid waar het gaat om algemene kwetsbaarheden inclusief fixes en workarounds.

Informatie betreffende specifieke kwetsbaarheden in Windesheim systemen wordt in principe niet publiekelijk verspreid. Verspreiding vindt in eerste instantie alleen plaats binnen het ICT bedrijf en richting systeemverantwoordelijken. Communicatie aangaande workarounds zal altijd in overleg met de systeemverantwoordelijke plaats vinden.

Gênante informatie

Gênante informatie of informatie “die iemand in verlegenheid kan brengen” betreft bijvoorbeeld ook een uiting dat een bepaald incident zich heeft voorgedaan en informatie over de omvang en de schade die daarbij ontstaan is. Gênante informatie kan een site betreffen maar ook individuele gebruikers of gebruikers groepen.

Dit soort informatie wordt alleen verspreid als de betrokken gebruikers daar toestemming voor verlenen.

Management informatie

Management informatie mbt aantallen en aard van incidenten wordt naar goeddunken van de manager ICT bedrijf verspreid.

Samenwerking

Windesheim werkt in SURF verband samen met diverse Hoger Onderwijs instellingen. Binnen SCIPR (Surf community voor informatiebeveiliging en privacy) wordt informatie betreffende beveiligingsincidenten wel gedeeld maar alleen anoniem en uitsluitend beschikbaar voor leden van SCIPR. Dit gremium wordt ook gebruikt voor collegiaal overleg betreffende de aanpak van specifieke beveiligingsissues binnen de eigen instelling.

4.3 Communicatie en Authenticatie

Het CSIRT meldpunt is momenteel gelokaliseerd in F2.20. Indien de aard van de melding daarom vraagt zal de CSIRT functionaris van dienst het gesprek in een andere afsluitbare ruimte voortzetten. Bij het voeren van gesprekken met melders of gesprekken over incidenten zal de CSIRT altijd rekening houden met mogelijk meeluisteren van anderen.
Alle CSIRT leden hebben de beschikking over een mobiele telefoon.

De voorkeur methode van communicatie is via email.

5 Diensten

5.1 Incident respons

Windesheim CSIRT ondersteunt de afhandeling van beveiligingsincidenten en neemt hierbij zowel de technische als organisatorische aspecten voor haar rekening.

5.1.1 Incident prioritering

- Onderzoek of er zich inderdaad een incident heeft voorgedaan.
- Inschatten impact.
- Prioriteit toekennen op basis van geschatte impact.

5.1.2 Incident coördinatie

- Inschakelen van de juiste functionarissen (applicatiebeheer, juridisch adviseur, communicatieadviseur).
- Oorzaak achterhalen.
- Onderhoud van contacten met “eigenaar” getroffen omgeving.
- Communicatie naar gebruikers (indien van toepassing).

5.1.3 Incident afhandeling

- Beperken van de gevolgen van het incident.
- Oorzaak wegnemen.
- Dader achterhalen tbv het nemen van disciplinaire maatregelen op basis van ICT reglement of het verzamelen van bewijs tbv aangifte.
- Evalueren van kans op herhaling en advisering ten aanzien van te nemen maatregelen in relatie tot kosten en risico.

Windesheim CSIRT zal ook statistische informatie verzamelen mbt incidenten om zo de organisatie te kunnen voorzien van beveiligingsadviezen.

De doelgroep van de Windesheim CSIRT kan gebruik maken van deze dienst middels de contactpunten zoals beschreven in 2.8.

5.2 Proactief

Windesheim CSIRT coördineert en onderhoud de volgende diensten:

Informatie dienst

- CSIRT beschikt over een lijst van alle functionele en technische (applicatie)beheerders, inclusief alle contact gegevens.

Bewaken kwaliteit van de monitoring door Infrastructuur

- Infrastructuur monitort (de beschikbaarheid van) verschillende services :
  - Verbindingen
  - Hardware in serverruimte en patchruimtes
  - Bandbreedte gebruik /netwerkverkeer
  - Authenticatieomgeving (incl. mislukte inlogpogingen)
- Infrastructuur zorgt dagelijks voor de back-up.

Audit

- Op regelmatige basis zal de CSIRT een beveiligingsscan uitvoeren op het netwerk. De resultaten hiervan zullen vertrouwelijk behandeld worden en alleen medegedeeld worden aan de betrokken partijen.

Archivering

- De CSIRT houdt een register bij van beveiligingsincidenten. De informatie in dit register is vertrouwelijk van aard en zal ook als zodanig behandeld worden.

6 Incident rapportage formulier

Intern kunnen incidenten online gemeld worden via https://serviceplein.windesheim.nl

7 Disclaimer

Onderstaande algemene disclaimer die uitdrukking geeft aan de vertrouwelijkheid en “need-to-know” basis van specifieke informatie kan gebruikt worden in de communicatie. Deze disclaimer kan aangepast worden aan de aard van het incident en de personen/organisaties die daarbij betrokken zijn.

<start disclaimer>
*Deze informatie ontvangt u vanwege uw betrokkenheid bij een incident dat afgehandeld wordt door CSIRT Windesheim (*https://infosite.windesheim.nl/Pages/Melden-van-misbruik-ICT-voorzieningen.aspx*). Deze informatie dient strikt vertrouwelijk behandelt te worden. Kopieën van deze informatie (elektronisch of hard copy) moeten op een dusdanige manier opgeborgen worden dat anderen hier geen ongeautoriseerde toegang toe hebben. Wanneer het nodig is deze informatie in het kader van incident afhandeling verder te verspreiden dan dient dit op*

individuele basis te geschieden waarbij u ook weer gebruikt dient te maken van deze disclaimer. Tevens dient u een kopie hiervan aan de CSIRT Windesheim te sturen.

<eind disclaimer>