SURFcert: 24/7 ondersteuning bij beveiligingsincidenten

SURFcert is het incident response team voor bij SURF aangesloten instellingen. Op deze wiki vind je informatie over onze dienstverlening, en lees je hoe je contact opneemt bij incidenten. Informatie over ernstige kwetsbaarheden of grootschalige incidenten publiceren we hier in de vorm van bulletins en factsheets.

Zoeken in deze wiki

Let op: toegang tot bepaalde informatie is afgeschermd en uitsluitend beschikbaar voor leden van de SCIRT-community, die lid zijn van het bijbehorende SURFconext Team. Meer informatie over SCIRT, en hoe lid te worden vind je op https://surf.nl/scirt. Meen je al lid te zijn van SCIRT maar heb je geen toegang tot de wiki, meld je dan bij lidmaatschap@scirt.nl. (Het heeft geen zin om de knop "toegang aanvragen"/"request access" van de wiki zelf te gebruiken. Toegang tot dergelijke informatie wordt uitsluitend verleend via lidmaatschap van de SCIRT-community.)

Hulp bij incidenten

Roep de hulp in van SURFcert

E-mail: cert@surfcert.nl

Telefoon: +31 6 22 92 35 64 (24/7 bereikbaar)

Vertrouwelijke berichten naar SURFcert sturen?

Gebruik de SURFcert PGP-sleutel om vertrouwelijke berichten naar SURFcert te versturen en om de authenticiteit van de digitale handtekening van SURFcert te verifiëren.

Wat is SURFcert?

Met SURFcert heb je bij beveiligingsincidenten 24 uur per dag, 7 dagen per week ondersteuning van onze deskundigen. Ook kun je met de tools van SURFcert zelf de beveiliging bij je instelling optimaliseren. Zo minimaliseren we samen de overlast van onder andere DDoS-aanvallen.

view Dienstbeschrijving SURFcert (Engels)

view Webpagina over SURFcert op SURF.nl

Privacystatement

view Privacystatement SURFcert

Dienstverlening van SURFcert

DDoS-bescherming

SURFcert helpt DDoS-aanvallen voorkomen en de overlast ervan te minimaliseren. Met Netflow analyseren we verkeersgegevens van en naar je instelling. Zo kunnen we vroegtijdig een netwerkaanval detecteren en de schade beperken. Om de impact van aanvallen op voorhand zo veel mogelijk te minimaliseren, bieden we de volgende anti-DDoS-middelen aan:

- **DDoS filter**
- **DDoS auto-mitigatie**

view Lees meer over DDoS-bescherming

Incidentmeldingen

Elke aangesloten instelling ontvangt meldingen van SURFcert over incidenten in hun netwerk, waarover SURFcert meldingen ontvangt of die ze zelf waarneemt. SURFcert verwacht tijdige en adequate reactie op deze meldingen. De instelling is verantwoordelijk om de contacten hiervoor (het **Site Security Contact** en eventueel een **Security Entry point**) te registreren en up-to-date te houden! Het is tevens mogelijk om machine-leesbare versies van incidentmeldingen te krijgen.

view Lees meer over incidentmeldingen van SURFcert

MISP

Met MISP delen we Indicators of Compromise (IoC's) om aangesloten instellingen te voorzien van specifieke dreigingsinformatie, zodat zij sneller digitale dreigingen waarnemen en benodigde maatregelen kunnen nemen.

view Lees meer over MISP

Zelf een CSIRT opzetten

Een Computer Security Incident Response Team (CSIRT) handelt beveiligingsincidenten in je netwerk af. SURF helpt je met opzetten en professionaliseren van dit team.

view Lees meer over het opzetten van een CSIRT