Zelf een Computer Security Incident Response Team (CSIRT) opzetten

Je kunt zelf een Computer Security Incident Response Team (CSIRT) opzetten voor je instelling. Zo'n team handelt beveiligingsincidenten in netwerken af. SURFcert ondersteunt het opzetten van een CSIRT in je instelling.

Verantwoordelijk voor instellingsnetwerk

Je kunt een lokaal team op verschillende manieren opzetten. CSIRT's in verschillende organisaties kunnen daardoor verschillende verschijningsvormen hebben. De overeenkomst tussen alle CSIRT's die geregistreerd staan bij SURF is dat ieder CSIRT verantwoordelijk is voor het instellingsnetwerk, inclusief de daar aan gekoppelde (afdelings)netwerken.

Blauwdruk voor opzetten van een CSIRT (RFC 2350)

Wanneer je zelf een CSIRT gaat opzetten voor je instelling, is het belangrijk om op gestandaardiseerde wijze te werk te gaan, wat betreft opzet, structuur en werkwijze. Dit vergemakkelijkt het operationele interne werk van een CSIRT, en het komt ook de samenwerking met andere CSIRT's ten goede.

Er is een goede blauwdruk beschikbaar vanuit de standaarden voor internet(gebruik), waarmee je op een gestructureerde manier een CSIRT kunt opzetten: RFC 2350. Je kunt deze gebruiken als basis voor verdere invulling binnen je eigen organisatie.

Naar de blauwdruk voor het opzetten van een CSIRT

Registratie bij SURFcert

Heb je de CSIRT opgezet en voldoet het aan de administratieve eisen, dan kun je het team registeren bij SURFcert via cert@surfcert.nl of +31 88 787 30 00. Vanaf dat moment is het CSIRT zichtbaar in de index van de bij SURFcert aangesloten teams.

CSIRT's wereldwijd

Er zijn een groot aantal CSIRT's wereldwijd:

CSIRT's in Nederland

- Nationaal Cyber Security Centrum (NCSC) voor alle overheidsinstellingen. Voor burgers en kleine MKB's is er een waarschuwingsdienst.
- KPN-CERT voor alle klanten van de KPN.

CSIRT's in Europa en daarbuiten

- Trusted Introducer (TI): lijst van TF-CSIRT leden (waaronder SURFcert), een Europese organisatie van Incident Response en Security Teams.
- FIRST: lijst van FIRST-leden (waaronder SURFcert), een internationale organisatie van Incident Response en Security Teams.

Deel je security-kennis in de SURFcommunity

De SURF Community van Incident Response Teams (SCIRT) is de groep van leden van CSIRT's van op SURF aangesloten instellingen. SCIRT i s de plek waar je actuele security-uitdagingen kunt bespreken en de laatste tips en trucs kunt uitwisselen.

Training: leer hoe je een CSIRT opzet en beheert

Tijdens de training TRANSITS leer je hoe je een Computer Security Incident Response Teams (CSIRT) opzet en runt. Er zijn trainingen voor beginnende security-medewerkers (TRANSITS 1) en een voor meer ervaren security-medewerkers (TRANSITS 2).

Bekijk de agenda voor actuele trainingen