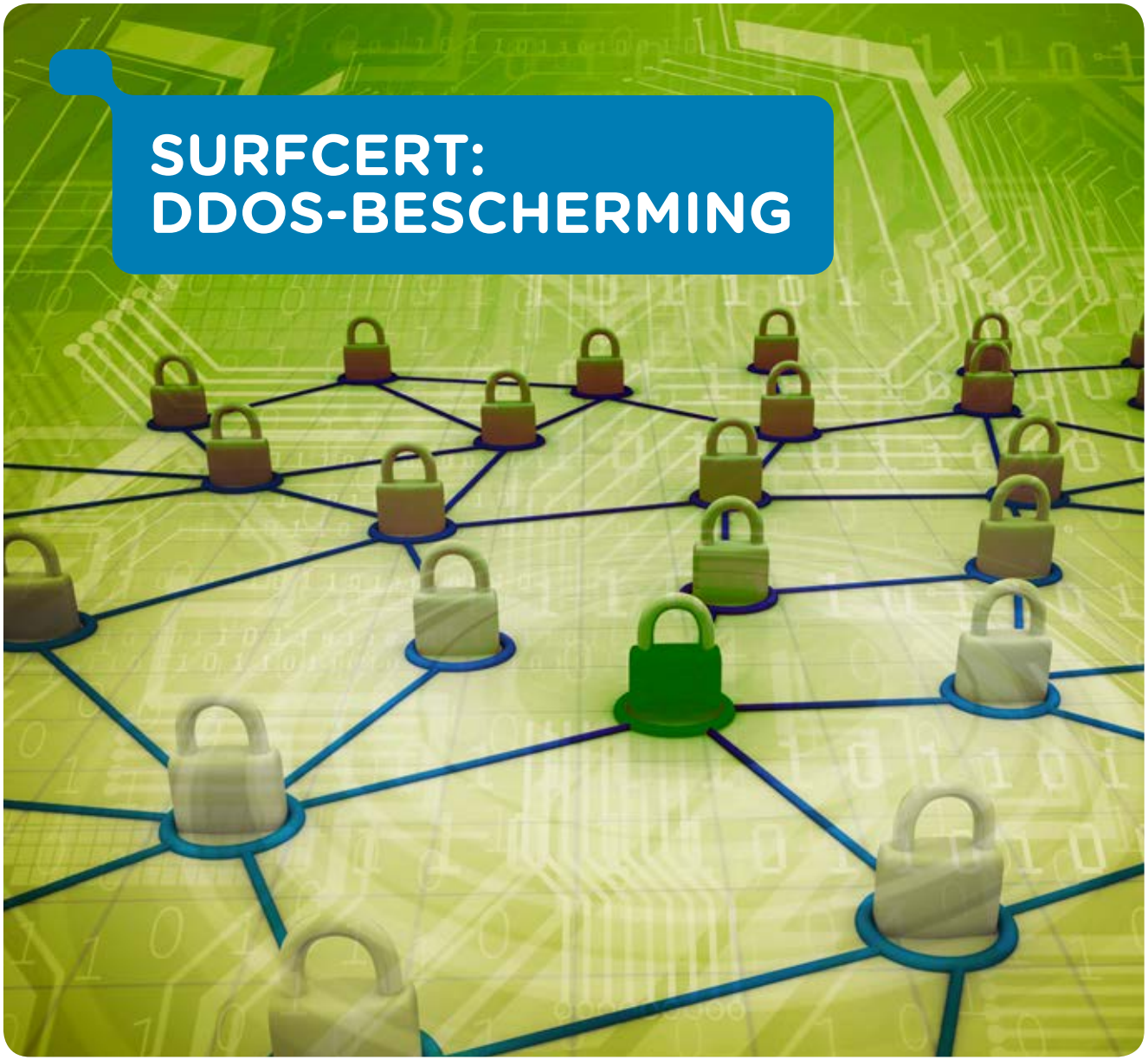

SURFCERT: DDOS-BESCHERMING

SURFCERT 2017
WWW.SURF.NL/SURFCERT

SURF NET

OP SURFNET AANGESLOTEN INSTELLINGEN HEBBEN STEEDS VAKER TE MAKEN MET ZOGENAAMDE DISTRIBUTED-DENIAL-OF-SERVICE (DDOS) AANVALLEN. SURFCERT IS CONTINU ACTIEF OM DE OVERLAST VAN DEZE AANVALLEN TE MINIMALISEREN EN ZO JE INSTELLING BETER TE BESCHERMEN.

Denial-of-Service: systemen overladen met dataverkeer

Bij een Denial-of-Service-aanval worden systemen, online diensten en/of de infrastructuur aangevallen door deze te overladen met dataverkeer. Dit kan ten koste gaan van de bereikbaarheid. Een Denial-of-Service-aanval kan van een enkel systeem afkomstig zijn maar ook van meerdere systemen tegelijkertijd: dit wordt een Distributed-Denial-of-Service-aanval (DDoS) genoemd. Momenteel zijn de meeste DoS-aanvallen distributed van karakter.

Wat doet SURFcert?

SURFcert helpt instellingen bij het analyseren en onschadelijk maken van allerlei soorten aanvallen. Om de impact van (D) DoS-aanvallen te minimaliseren, hebben we momenteel de volgende verkeersbeperkende instrumenten: de ‘wasmachine’ en netwerkfilters. SURFcert zet deze alleen in na overleg met, en op verantwoording van je instelling. Er kan immers sprake zijn van gewenst verkeer, bijvoorbeeld van een populaire videoserver.

Wasmachine

SURFcert kan met de ‘wasmachine’ bij een lopende aanval snel en voor beperkte duur ingrijpen. De wasmachine leidt het verkeer naar het aangevallen IP-adres om en ontdoet

het van ongewenst verkeer waardoor (een deel van) de aanval afgevangen wordt. Zo wordt een volgelopen SURFinternet-aansluiting snel weer vrijgemaakt.

Netwerkfilters

Deze gerichte filters in het SURFnet-netwerk beschermen preventief tegen enkele veel voorkomende aanvallen. Ze zetten een maximum op verkeer via een aantal protocollen die bij (D)DoS-aanvallen veel misbruikt worden. SURFcert plaatst deze filters op verzoek van de instelling, of adviseert zelf deze te plaatsen tijdens of na een (D)DoS-aanval.

Wat kun je doen?

Bij een aanval

Zodra je aangevallen wordt, neem dan contact met het alarmnummer van SURFcert dat 24/7 bereikbaar is: 06 - 22 92 35 64.

Preventief

Neem contact op met SURFcert om het plaatsen van preventieve filters bespreken. Wij raden je daarnaast aan ook zelf beschermingsmaatregelen te treffen. SURFcert biedt namelijk geen bescherming tegen alle soorten aanvallen. Met name aanvallen op applicatieniveau worden niet afgevangen met netwerkfilters. Uiteraard kun je SURFcert hiervoor om advies vragen.

Daders opsporen

Aanvallen technisch analyseren en onschadelijk maken is een deel van de oplossing. Ook opsporing van de daders is belangrijk en helpt toekomstige aanvallen, zeker vanuit je eigen netwerk, te voorkomen. Probeer daarom de veroorzakers te vinden en indien mogelijk ter verantwoording te roepen, eventueel met hulp van buitenaf.

Tarief

Je betaalt niets extra voor de (D)DoS-bescherming van SURFcert. Dit is onderdeel van de reguliere dienstverlening van SURFcert en valt daarmee onder de vaste aansluitvergoeding van SURFnet.

MEER INFORMATIE OVER SURFCERT:
www.surf.nl/surfcert

CONTACT:
SURFnet Klantsupport
(088 - 787 30 00 of
klantsupport@surfnet.nl)

SURFnet
www.surf.nl/surfnet