RFC2350

Het BNG-CERT is opgezet met behulp van de door de Network Working Group van de IETF.org opgestelde richtlijn RFC2350.

Document informatie

- **Versie**: 1.0
- **Datum laatste update**: 05-03-2025
- **Datum laatste review**: 28-02-2025
- **Distributielijst notificaties update**: Notificaties voor distributie van dit document worden niet verstrekt. Neem voor informatie contact op met het BNG-CERT e-mailadres.
- **Locatie publicatie van dit document**: https://www.bngbank.nl/veiligheid.

Contact informatie

- **Team naam**: 'BNG-CERT', Computer Emergency Response Team van BNG
- **Adresgegevens**: BNG Bank N.V.
  T.a.v. BNG-CERT
  Postbus 30305
  2500 GH Den Haag
  Nederland
- **Tijdzone**: BNG-CERT hanteert Central European Time (CET), inclusief daylight saving Time (DST). GMT+0100 in de winter en GMT+0200 in de zomer.
- **Telefoonnummer**: +44 1736 802 045 (PagerDuty)
- **Facsimile nummer**: geen
- **Andere telecommunicatie**: geen
- **Publieke sleutels en encryptie**: BNG-CERT gaat gebruik maken van PGP voor encryptie en digitale ondertekening.
- **Teamleden**: De BNG-CERT teamleden zijn niet publiekelijk bekend, de teamleden maken zich bekend bij het contact wanneer een security incident zich voordoet.
- **Contact informatie**: BNG-CERT is van 08:00 tot 18:00 bereikbaar op +44 1736 802 045 (PagerDuty), ondersteuning buiten deze tijden gebeurt op basis van best effort. Het BNG-CERT is per email bereikbaar op bng-cert@bngbank.nl.
- **Additionele contact informatie**: valse-email@bngbank.nl.

Charter BNG-CERT

Definitie CERT

Een Computer Emergency Response Team (CERT) is een gespecialiseerd team van ICT-professionals, dat in staat is snel te handelen in het geval van een beveiligingsincident met computers of netwerken. Het doel is om schade te reduceren en snel herstel van de dienstverlening te bevorderen.

Missie Statement

De missie van het BNG-CERT is het minimaliseren van de impact bij een incident of schade als gevolg van een (cyber) aanval of digitale inbraak.

Doelgroep (constituenten)

De doelgroep van het BNG-CERT is geheel BNG, inclusief externe leveranciers die een cruciale rol spelen in de verwerking van BNG data.

Doelen

De doelen van het BNG-CERT zijn:

- Eerste punt van contact en de verbindende factor te zijn bij informatiebeveiligingsincidenten;
- Direct kunnen acteren bij informatiebeveiligingsincidenten op het gebied van computer en netwerk;
- Het bundelen van technische en functionele expertise van BNG medewerkers bij de afhandeling van een informatiebeveiligingsincident;
- Schade te reduceren en snel herstel van de dienstverlening te bevorderen;
- Het bijdragen aan het informatiebeveiligingsbewustzijn bij BNG.

Governance & Mandaat

Het BNG-CERT is onderdeel van de BNG organisatie en staat onder directe besturing van het BNG Cyber Defense Center. Het Executive Committee van BNG heeft de oprichting, rol en mandaat van het BNG-CERT vastgesteld.

Bevoegdheden

Het BNG-CERT registreert incidenten op het gebied van informatiebeveiliging en coördineert de afhandeling hiervan. Het BNG-CERT werkt samen met de verantwoordelijke medewerkers en afdelingen, indien nodig ook die van haar leveranciers en klanten en heeft een adviserende rol. Echter, als de omstandigheden daarom vragen, heeft het BNG-CERT het mandaat om maatregelen te nemen die passend zijn om een incident adequaat af te handelen.

Policies

Type incidenten: BNG-CERT acteert op alle informatiebeveiligingsincidenten die plaatsvinden binnen haar doelgroep met de focus op:

- Cyber-gerelateerde incidenten en dreigingen;
- Datalekken;
- Ransomware;
- Abuse, zoals phishing, spam, virussen en malware.

Samenwerking en het delen van informatie: Informatie aangeboden aan BNG-CERT zal, indien noodzakelijk, confidentieel of hoger worden behandeld en zal niet worden gedeeld met derde partijen zonder toestemming vooraf, tenzij verplicht door wetgeving. BNG-CERT hanteert het Traffic Light Protocol (TLP) in de communicatie met externe partijen.

Communicatie en authenticatie: BNG-CERT heeft de voorkeur voor communicatie per e-mail. BNG-CERT gaat gebruik maken van PGP sleutels voor encryptie en digitale ondertekening van vertrouwelijk verkeer. De BNG-CERT publieke sleutel zal binnenkort gepubliceerd worden op de publieke PGP sleutelservers.

Services

Incident triage: Alle incidenten worden geregistreerd en beoordeeld op impact en prioriteit. In de triage zal worden bepaald:

- Wie zijn de belanghebbenden bij het incident;
- Wat is de ervaring van de incidentmelder;
- Wat is de ernst van het incident;
- Wat zijn de tijdbeperkingen van het incident.

Incident coördinatie: Gedurende de looptijd van het incident wordt de oorzaak van het incident bepaald, de relevante contacten gelegd met interne en externe belanghebbenden en indien nodig het escalatieproces in werking gesteld.

Incident afhandeling: Het BNG-CERT biedt ondersteuning door coördinatie tussen de relevante partijen, externe intelligence, evaluatie, rapportage en eventuele vervolgactiviteiten.

Incident rapportage

Na het oplossen van een incident zullen alle betrokken partijen worden geïnformeerd. De volgende gegevens moeten minimaal worden opgenomen in de communicatie:

- Een korte beschrijving van het incident;
- Overzicht van uitgevoerde acties en de bijbehorende resultaten;
- De belangrijkste bevindingen en aanbevelingen.

Disclaimer

BNG-CERT kan de juistheid en beschikbaarheid van alle informatie niet volledig garanderen. Het BNG-CERT aanvaardt geen enkele aansprakelijkheid voor schade ontstaan door afwezigheid of onjuistheid van de geboden informatie.