RFC2350

Het PGGM-CERT is opgezet volgens de richtlijnen als beschreven in de RFC2350, uitgegeven door de Network Working Group van de IETF.org

Document informatie

- **Versie**: 1.0
- **Datum laatste update**: 01-03-2017
- **Distributielijst notificaties update**: Notificaties voor distributie van dit document worden niet verstrekt. Neem voor informatie contact op met het PGGM-CERT e-mailadres.
- **Locatie publicatie van dit document**: https://www.pggm.nl/Paginas/Veiligheid.aspx

Contact informatie

- **Team naam**: "PGGM-CERT", Computer Emergency Response Team van PGGM
- **Adresgegevens**: PGGM
  T.a.v. PGGM-CERT
  Postbus 117
  3700 AC Zeist
  Nederland
- **Tijdzone**: PGGM-CERT hanteert Central European Time (CET), inclusief daylight Saving Time (DST). GMT+0100 in de winter en GMT+0200 in de zomer.
- **Telefoonnummer**: (030) 277 72 40
- **Facsimile nummer**: geen
- **Andere telecommunicatie**: geen
- **Publieke sleutels en encryptie**: PGGM maakt gebruik van PGP voor encryptie en digitale ondertekening
- **Teamleden**: De PGGM teamleden zijn niet publiek bekend, de teamleden maken zich bekend bij het contact wanneer een security incident zich voordoet.
- **Contact informatie**: PGGM-CERT is van 08:00 tot 18:00 bereikbaar op: (030) 277 72 40, ondersteuning buiten deze tijden gebeurt op basis van best effort. Het CERT is per email bereikbaar op CERT@pggm.nl
- **Additionele contact informatie**: valse-email@pggm.nl; informatiebeveiliging@pggm.nl

Charter CERT

Missie Statement

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

Doelgroep (constituenten)

De doelgroep van de PGGM-CERT is geheel PGGM

Doelen

De doelen van het PGGM-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 PGGM medewerkers bij de afhandeling van een informatiebeveiligingsincident
- Schade te reduceren en snel herstel van de dienstverlening te bevorderen
- Het promoten van het informatiebeveiligingsbewustzijn bij PGGM

Sponsors

Het PGGM-CERT is onderdeel van de PGGM organisatie en staat onder directe besturing van het PGGM Security & Quality Office. Het Executive Committee van PGGM heeft de oprichting, rol en bevoegdheden van PGGM-CERT en de inrichting van PGGM-CERT vastgesteld.

Bevoegdheden

Het PGGM-CERT registreert incidenten op het gebied van informatiebeveiliging en coördineert de afhandeling hiervan. Het PGGM-CERT werkt samen met de verantwoordelijke medewerkers, indien nodig ook die van haar leveranciers en klanten, en heeft een adviserende rol. Echter, als de omstandigheden daarom vragen, heeft PGGM-CERT de bevoegdheid om maatregelen te nemen die passend zijn om een incident naar behoren op te lossen. Dit conform de crisis management structuur binnen PGGM.

Policies

Type incidenten: PGGM-CERT acteert op alle informatiebeveiligingsincidenten die plaatsvinden of dreigen plaats te vinden binnen haar doelgroep met de focus op:

- Cyber-gerelateerde incidenten en dreigingen
- Datalekken
- Geconstateerde kwetsbaarheden (responsible disclosure)
- Abuse, zoals phishing, spam, virussen

Samenwerking en het delen van informatie: Informatie aangeboden aan PGGM-CERT zal vertrouwelijk worden behandeld en zal niet worden gedeeld met derde partijen zonder toestemming vooraf, tenzij verplicht door de wet. PGGM-CERT hanteert het Traffic Light Protocol in de communicatie met externe partijen.

Communicatie en authenticatie: PGGM-CERT heeft de voorkeur voor communicatie per e-mail. PGGM-CERT maakt gebruik van PGP sleutels voor encryptie en digitale ondertekening van vertrouwelijk verkeer. De PGGM-CERT publieke sleutel is gepubliceerd op de publieke sleutelservers.

Services

Incident triage: Alle incidenten worden geregistreerd en beoordeeld op impact en prioriteit. De triage functie is verantwoordelijk voor het uitzetten van het incident aan de juiste mensen en het bewaken van de voortgang.

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 PGGM-CERT lost zelf geen incidenten op. PGGM-CERT biedt ondersteuning door coördinatie tussen de relevante partijen, externe intelligence, evaluatie, rapportage en eventuele vervolgactiviteiten.

Incident rapportage

Er zijn geen speciale formulieren beschikbaar gesteld om een incident te melden.

Disclaimer

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