gemeente
SCHIERMONNIKOOG

OMRIN

Schiermonnikoog, 31 oktober 2025

Geachte heer, mevrouw,

Zoals u in de verschillende kranten heeft kunnen lezen, is Omrin slachtoffer geworden van een ransomware aanval. De aanval is direct opgemerkt en er zijn maatregelen genomen om verdere escalatie te voorkomen. Helaas zijn er toch gegevens buit gemaakt. Zo bleek dat de hackers op 28 oktober buitgemaakte gegevens op het “darkweb” hebben gepubliceerd; een illegaal, afgesloten deel van het internet dat alleen toegankelijk is via speciale software. De informatie is dus niet zichtbaar op gewone websites of via Google.

Ook heeft Omrin samen met externe cyberbeveiligingspecialisten (Fox IT) een onderzoek ingesteld naar de oorzaak, impact en omvang van de aanval en de geraakte gegevens. Via dit onderzoek komt langzaam maar zeker meer informatie over de buitgemaakte gegevens naar voren. Daarom sturen wij u nu deze brief.

Gegevens inwoners, bedrijven en huiseigenaren Schiermonnikoog
Bij het onderzoek is een bestand gevonden met daarop de namen, adressen en BSN-nummers van inwoners van Schiermonnikoog en van eigenaren van recreatiewoningen op Schiermonnikoog. Ook bevatte het document RSIN-nummers en adresgegevens van bedrijven op het eiland. Emailadressen of telefoonnummers stonden niet in het bestand. Wij betreuren dit incident ten zeerste en bieden u onze oprechte excuses aan voor het ongemak en de zorgen die dit kan veroorzaken.

Mogelijke risico’s
Het buitmaken van deze gegevens brengt risico’s met zich mee, waaronder:
- **Identiteitsfraude:** Met een combinatie van naam, adresgegevens en een BSN kunnen kwaadwillenden zich voordoen als u, bijvoorbeeld bij het openen van rekeningen of het aanvragen van diensten.
- **Phishing en oplichting:** U kunt benaderd worden met verzoeken die lijken te komen van betrouwbare instanties.

Wat kunt u doen?
Wij adviseren u om de volgende stappen te nemen:
- Let op verdachte communicatie: Wees alert op e-mails of brieven waarin om persoonlijke gegevens wordt gevraagd.
- Controleer uw gegevens: Houd uw bankafschriften en andere accounts goed in de gaten op ongebruikelijke activiteiten.
- Meld identiteitsfraude: Bij vermoeden van misbruik kunt u contact opnemen met de Fraudehelpdesk via fraudehelpdesk.nl of neem contact op met gemeente Schiermonnikoog.
- Maak een registratie aan bij het Centraal Meldpunt Identiteitsfraude (CMI) via www.rvig.nl/cmi (melding doen bij het CMI). Dit kan helpen bij het voorkomen van verdere schade. Heeft u hulp nodig bij de registratie neem dan contact op met de gemeente Schiermonnikoog.

Wat heeft Omrin gedaan?
Samen met externe cyberbeveiligingspecialisten (Fox IT) heeft Omrin direct gehandeld, zo zijn hun servers vergrendeld en geïsoleerd en er is een forensisch onderzoek ingesteld naar de oorzaak, impact en omvang van de aanval en de geraakte gegevens. Het forensisch onderzoek wordt uitgevoerd door Fox-IT.

Wat heeft de gemeente Schiermonnikoog gedaan?
De gemeente Schiermonnikoog heeft het datalek gemeld bij de Autoriteit Persoonsgegevens en is nauw betrokken bij het onderzoek dat door Omrin wordt uitgevoerd. Daarnaast zijn de beveiligingsmaatregelen aangescherpt en worden de medewerkers extra geïnformeerd over gegevensbescherming.

Heeft u nog vragen?
Als u na het lezen van deze brief nog vragen heeft over de ransomware aanval, neem dan gerust contact op met gemeente Schiermonnikoog via datalek@schiermonnikoog.nl. Ook kunt u contact opnemen met onze Functionaris Gegevensbescherming via fg@leeuwarden.nl. Op www.schiermonnikoog.nl vindt u actuele informatie.

Nogmaals onze oprechte excuses voor dit incident. De gemeente Schiermonnikoog en Omrin doen er alles aan om de gevolgen van dit incident zoveel mogelijk te beperken en u zo goed mogelijk te ondersteunen en te blijven informeren.

Met vriendelijke groet,

Ineke van Gent
burgemeester gemeente Schiermonnikoog

John Vernooij
directeur Omrin