ICT-beveiligingsincident bij LYNX

Amsterdam, 11 november 2026 • Laatst bijgewerkt: 22:00

LYNX heeft een ICT-beveiligingsincident vastgesteld en maatregelen genomen. Bij dit incident heeft een onbevoegde derde toegang verkregen tot persoonsgegevens van een deel van ons klantenbestand.

De onbevoegde derde heeft geen toegang verkregen tot effectenrekeningen van klanten of tot onze handelsdiensten. Portefeuilles en gelden van klanten maakten geen deel uit van het incident. Ook posities, orders en orderhistorie en de gegevens van gekoppelde bankrekeningen zijn beschermd gebleven.

Om welke gegevens gaat het?

Welke en hoeveel gegevens het betreft, verschilt per getroffen klant. Iedere getroffen klant heeft van ons een persoonlijk overzicht ontvangen van de gegevens die het betreft. Het kan gaan om personalia, identificatiegegevens, informatie over de effectenrekening en de financiële situatie van de klant.

De betrokken gegevens zijn ongestructureerd en niet als een samengestelde dataset of database verkregen, maar als losse delen informatie die niet aan elkaar gekoppeld waren. Technisch gezien kunnen deze losse delen informatie wel met elkaar worden gecombineerd.

Wat wij doen

Direct na het vaststellen van het incident heeft ons IT-beveiligingsteam de onbevoegde toegang geblokkeerd en aanvullende maatregelen genomen om onze digitale beveiliging verder te versterken. Zodra vaststond dat het gevoelige klantgegevens betrof, hebben wij de getroffen klanten direct en persoonlijk geïnformeerd.

Wij blijven de situatie nauwlettend volgen en externe cybersecurityspecialisten ondersteunen ons bij het onderzoek naar de toedracht van het incident. In het belang van onze digitale beveiliging en de bescherming van onze klantgegevens zijn wij terughoudend met het delen van details over het incident.

Wij hebben het incident gemeld bij de politie. Ook hebben wij de Autoriteit Persoonsgegevens (AP) en de Autoriteit Financiële Markten (AFM) ingelicht. Wij houden beide autoriteiten op de hoogte van het onderzoek.

Wij adviseren onze klanten alert te blijven

De betrokken gegevens kunnen worden gebruikt om frauduleuze e-mails, telefoontjes of sms-berichten geloofwaardiger te laten lijken. Iemand kan zich bijvoorbeeld voordoen als LYNX of als een andere financiële instelling en daarbij verwijzen naar gegevens die over de klant zijn verkregen.

Wij raden klanten daarom aan extra alert te zijn op onverwachte berichten of telefoontjes over hun rekening of beleggingen.

Wij begrijpen dat dit bericht bij onze klanten zorgen kan oproepen. Dat vinden wij zeer vervelend. Goede dienstverlening aan onze klanten staat bij LYNX centraal. De beveiliging van onze systemen en de gegevens van onze klanten heeft daarbij de hoogste prioriteit. Wij vinden het belangrijk om zorgvuldig te handelen en blijven onze klanten zo duidelijk mogelijk informeren.