PIJLER 4

Veilige data

Deelnemende banken delen hun transactie- en klantgegevens alleen met TMNL en niet met elkaar. Ook zijn er IT-beveiligingsmaatregelen volgens de hoogste normen getroffen om de gegevens te beschermen, die worden gecontroleerd door onafhankelijke partijen. Denk hierbij bijvoorbeeld aan pseudonimisering, dataencryptie en toegangsbeveiliging. Alleen medewerkers die de data nodig hebben voor het uitoefenen van hun functie hebben toegang.

Wat doet TMNL om de veiligheid van data te waarborgen?

TMNL stelt alles in het werk om de veiligheid van data te waarborgen. De data die TMNL van de banken ontvangt en verwerkt zijn volgens de hoogste standaard beveiligd. Ook zorgt TMNL ervoor dat privacygevoelige gegevens niet herleidbaar zijn naar de klant.

Hoe ontvangt TMNL de data en hoe wordt deze beveiligd?

Bij de data-overdracht is de data versleuteld net als de verbinding waarover de data verstuurd wordt. TMNL controleert met een digitale handtekening of de data daadwerkelijk van de bank afkomstig is en of deze ongewijzigd is voordat zij deze versleutelde data per

bank opslaat in een aparte, beveiligde en versleutelde database. Toegang tot deze data om analyse te doen is alleen mogelijk vanuit een streng beveiligde en volledig afgeschermde omgeving. Daarnaast legt TMNL elke datahandeling vast zoals het opvragen of verwerken van gegevens.

Voldoet TMNL aan de internationale securitystandaarden en wie controleert dat?

TMNL heeft een Information Risk Management Framework, dat is gebaseerd op vijf vertrouwensprincipes: Security, Beschikbaarheid, Integriteit van verwerking, Vertrouwelijkheid en Privacy. In het framework worden alle beveiligingsmaatregelen van TMNL beschreven, inclusief hun doel en werking, om zo de risico's op bijvoorbeeld dataverlies te beperken. Een externe auditor controleert het framework regelmatig en controleert daarnaast ook of TMNL alle beschreven beveiligingsmaatregelen uitvoert.

Wie heeft toegang tot de data en hoe wordt dit gemonitord?

Alleen vooraf geselecteerde TMNL-medewerkers hebben toegang tot de versleutelde transactiedata. Zij zijn gescreend en hebben een geheimhoudingsverklaring en een gedragscode ondertekend. Elke datahandeling, zoals een zoekactie, wordt vastgelegd en is altijd herleidbaar naar een TMNL-medewerker.

Wat doet TMNL om zich te beschermen tegen aanvallen van buitenaf?

TMNL gebruikt de nieuwste en meest betrouwbare technologieën voor de best mogelijke beveiliging. Naast alle beschreven beveiligingsmaatregelen in het Information Risk Management Framework en de periodieke audit door een externe en onafhankelijke partij voert TMNL elk half jaar en bij grote wijzigingen technische beveiligingstesten uit, zoals penetratietesten. Een onafhankelijk team controleert of de omgeving op de juiste en veiligste manier is geconfigureerd om te voorkomen dat hackers binnen kunnen komen.

Daarnaast voert een team van de beste ethische hackers periodiek zogenaamde 'red-teaming'-aanvallen uit. Het TMNL-securityteam moet deze aanval dan detecteren en blokkeren. TMNL gebruikt de learnings om de beveiliging van het platform verder te verbeteren. Dit is een continu proces.

TMNL heeft 5 belangrijke pijlers die altijd ten grondslag liggen aan alles wat ze zegt en doet.

Lees meer op tmnl.nl