Transferpunt Noord Limburg DPIA
Beveiligingsmaatregelen PGAx

Logbestanden
inloggen: datum, tijd en het IP-adres.
Bij een gefaalde inlogpoging: de reden van falen.

Geen registratie uitloggen; gebruikers worden automatisch uitgelogd bij inactiviteit of het veranderen van IP-adres.

Registratie wie welke onderwerpen (Aanmeldingen, Aanpakken of Trajecten) in ziet.
Daarnaast worden alle changes opgeslagen in het audit log.
Deze gegevens worden alleen verwijderd wanneer een onderwerp wordt verwijderd.

Deze gegevens zijn in te zien door senior supportmedewerkers en de senior ontwikkelaars van Ranshuijsen B.V.

Elke gebruiker ziet dat handelingen in het systeem worden geregistreerd.
Zij moeten hier akkoord mee gaan om het systeem te kunnen gebruiken.

Bewaartermijn logbestanden: 12 maanden.

Toegang
Het zaaksysteem PGAx wordt ontsloten via een beveiligde internetserver. Hiervoor is 2-factor authenticatie nodig om toegang te krijgen.

Backups
Intermax maakt dagelijks (maandag t/m zaterdag) een incrementele kopie van alle gewijzigde data die op (managed) servers staan. Daarnaast wordt periodiek een volledig nieuwe back-up van alle data gemaakt. Dit gebeurt op meerdere speciaal daartoe ingerichte servers op harde schijven. Hierbij wordt gebruik gemaakt van Netvault software en Veeam.
De data wordt daarna gekopieerd naar een ander datacenter. Bovendien worden met enige regelmaat zogenaamde snapshots van bepaalde opslagsystemen gemaakt als derde veiligheidsmaatregel. Back-ups worden kruislings tussen twee datacentra uitgewisseld en opgeslagen.

Back-up van de back-up
De back-up is voorzien van een eigen back-up. Deze unieke dienst staat bekend als de back-up van de back-up.
De extra back-up wordt meermaals op geografisch gescheiden locaties wordt opgeslagen. De scheiding kent een afstand van 35 kilometer van de productiedata. Zo ontstaat een geografische scheiding tussen de back-up en productiedata. Het proces wordt met een interval van één keer per week uitgevoerd en kent een Recovery Time Objective (RTO) van zeven dagen. De extra back-up dienstverlening geldt echter uitsluitend voor virtuele omgevingen.

Er worden op regelmatige basis en voor afnemers op verzoek zogenaamde ‘restore tests’ gedaan om te zien of de back-ups nog de vereiste kwaliteit en integriteit hebben.

Fysieke toegangscontrole
Intermax heeft vier niveaus van fysieke toegangsbeveiliging:
het pand, de verdieping, de ruimte en de individuele systeemkasten.

1. Toegang pand: persoonsgebonden proximitycards, biometrische toegangscontrole.

2. Toegang verdieping: persoonsgebonden proximitycards of biometrische toegangscontole met logging, aangevuld met bemande receptie.

3. Toegang sectie verdieping buiten kantoortijden: persoonsgebonden proximitycards met logging, camerabewaking met vastlegging beelden (bewaartermijn 1 maand, volgens wettelijk maximaal toegestane duur).

4. Toegang datacenter: persoonlijke code en biometrische toegangscontrole, camerabewaking met vastlegging beelden (bewaartermijn 1 maand, volgens wettelijk maximaal toegestane duur).
5. Toegang individuele 19" systeemkasten: digitale codesloten.

Uniek per afzonderlijke kast zijn de kritieke netwerkcomponenten afgeschermd van de semi-openbare co-locatieruimte in het datacenter d.m.v. een cage met digitaal codeslot (geldt zowel voor Rotterdam-Spaanse Kubus als voor DCG Delft.

Medewerkers van Ranshuijsen van Loon hebben geen fysieke toegang tot de verschillende bedrijfsruimtes van Intermax.

Netwerkactiviteit controleren
Intermax controleert al het in- en uitgaande http- en smtp-verkeer dat door diens centrale Fortigate cluster loopt op de aanwezigheid van digitale bedreigingen zoals hackers, virussen, wormen en andere digitale bedreigingen ter voorkoming van ongeoorloofde toegang, wijziging, diefstal of beschadiging van persoonsgegevens. Waar nodig wordt het verkeer geschoond van bedreigingen die de continuïteit van de dienstverlening in gevaar zouden kunnen brengen.

De beveiliging van de PGAx server wordt dagelijks pro-actief gecontroleerd d.m.v. de Guardian360 security scan. De core van het netwerk wordt automatisch scherp bewaakt en regelmatig doorgelicht op veiligheid.

Netwerkbeveiliging
Intermax beschikt aantoonbaar over de vereiste beveiligingscertificaten o.a. ISO 2700. Intermax is tevens ISAE 3401 en 3402 gecertificeerd en voldoet aan de GIBIT 2016.

Intermax monitort het netwerk 24/7 o.a. door het Guardian360 Security platform. Intermax is een door Microsoft geautoriseerde Qualified Multitenant Hoster (QMTH). Intermax is aangesloten bij de Nationale Beheersorganisatie Internet Providers (NBIP) en de Dutch Hosting Provider Association (DHPA). Via beide brancheorganisaties neemt Intermax deel aan de Nationale Anti-DDOS Wasstraat ter bestrijding van DDOS aanvallen (NaWas) waardoor binnen enkele minuten DDOS verkeer volautomatisch bestreden kan worden.

Personeelsmanagement
Medewerkers van Ranshuijsen B.V. ondertekenen een vertrouwelijkheidsverklaring en beschikken over een VOG.

Patchmanagement
Bij het afsluiten van het patchcontract wordt er proactief onderhoud van het besturingssysteem van PGAx uitgevoerd. Minimaal 1x per maandag worden beveiligingsupdates geïnstalleerd dan wel bij het verschijnen hiervan. Dit geldt zowel voor Windows als Linux besturingssystemen (hierbij wordt ook regelmatig de kernel bijgewerkt). De te installeren patches kunnen worden gevolgd via de Klantenportal.

Indien een beveiligingslek is gevonden waarvoor (nog) een patch op oplossing is, brengt Intermax advies uit omtrent het minimaliseren van de risico's d.m.v. andere maatregelen.