Beveiliging van het TransFollow platform

Gebruikers van het TransFollow platform die vrachtbrieven of zendingsberichten invoeren, brengen daarmee belangrijke bedrijfsinformatie in. Deze bedrijfsinformatie mag alleen zichtbaar zijn voor bevoegden. In dit document worden de maatregelen uiteen gezet die zijn genomen op het gebied van beveiliging van het systeem en van uw gegevens. Aan bod komen vragen als: welke standaarden en procedures zijn in TransFollow toegepast; welke afspraken heeft TransFollow gemaakt met leveranciers; hoe bewaakt TransFollow de toegang tot het systeem. Ook worden aspecten als beschikbaarheid, kwaliteit van de organisatie en wetgeving beschreven.

1. Inleiding

Via het TransFollow-platform kunnen gebruikers op een veilige en betrouwbare manier vrachtbrieven of zendingsberichten aanmaken, versturen, wijzigen en inzien. Belangrijke maatregelen ter beveiliging van de data zijn:

- toegangsbeheer;
- fysieke bescherming van de servers in het datacenter;
- bewaking van de continuïteit ;
- algemene beveiliging van de applicatie;
- de korte levenscyclus van de vrachtbrieven en zendingsberichten.

Ook is de organisatie, die TransFollow beheert, volgens ISO 27001 ingericht. De juridische betrouwbaarheid van het systeem is getoetst aan wet- en regelgeving betreffende de vrachtbrief en betreffende elektronisch handelsverkeer.

2. Beveiliging van de data

Beveiliging van de toegang tot de data

Toegang tot de data (registratiegegevens, vrachtbrieven, zendingsberichten) is gekoppeld aan de account van gebruiker. Alleen de gebruiker bepaalt, welke andere gebruikers de gegevens kunnen inzien of wijzigen. Het TransFollow-platform beperkt de mogelijkheid om wijzigingen in vrachtbrieven aan te brengen. Op het moment dat een gebruiker (afzender, vervoerder of geadresseerde) zijn handtekening zet is verder wijziging door die gebruiker niet mogelijk.

Alle data van het platform worden opgeslagen op een tweetal servers van een *hosting* partij. Dat betekent dat de fysieke infrastructuur wordt ingezet om meerdere cloudsystemen te faciliteren. Met de hostingpartij is overeengekomen, dat het TransFollow platform alleen toegankelijk is voor klanten met een TransFollow-account. Bij noodgevallen zijn er procedurele afspraken dat de hostingpartij slechts in samenwerking met Beurtvaartadres toegang kan worden verleend tot de omgeving, de applicatie en de data. Ook met de bedrijven, die TransFollow hebben gebouwd, zijn afspraken gemaakt, wanneer en hoe zij toegang hebben tot de broncode van de applicatie en de door gebruikers ingevoerde gegevens.

Data zijn niet beschikbaar voor derden.

Beveiliging van de handtekening

Wachtwoorden en handtekeningen worden met versleutelingsalgoritmes en geavanceerd sleutelbeheer zodanig beveiligd, dat *hacken* vrijwel uitgesloten kan worden. Met deze beveiliging voorkomt TransFollow het lekken van data naar ongeautoriseerde personen.

Fysieke beveiliging

De beveiliging van de servers, waarop alle data van TransFollow worden opgeslagen is juridisch vastgelegd in een Service Level Agreement (SLA) met de hosting partij, CloudVPS. De praktische uitvoering van de SLA voorziet in een noodvoorziening voor de datacenters voor situaties waarin de reguliere stroom uitvalt. Uiteraard is gezorgd voor koeling van de ruimtes van de servers, volgens de eisen van de brandweer. Toegang tot de gebouwen waarin de servers zijn opgesteld is alleen mogelijk als aan de toegangsprocedure is voldaan. Tenslotte maakt het TransFollow-platform gebruik van twee verschillende locaties voor de servers. De locaties zullen altijd op minimaal vijf kilometer afstand van elkaar verwijderd zijn.

Beschikbaarheid

Omdat logistieke processen dag en nacht doorgaan, dient TransFollow- 24/7 beschikbaar te zijn. Door een pakket van redundant uitgevoerde systemen, back-upschema's en monitoring wordt de kans op uitval geminimaliseerd. De software ondersteunt diverse offline (offline wil zeggen, dat er geen internet bereik is) scenario's voor de elektronische handtekening, waaronder de mogelijkheid om op het scherm te tekenen ('sign-on-glass'). Het gebruik van TransFollow kan erg fluctueren en daarmee de beschikbaarheid (zoals performance) beïnvloeden. Door de flexibiliteit van de hosting infrastructuur kan heel snel opgeschaald worden en daarmee is beschikbaarheid gegarandeerd.

Om beveiligingsrisico's tijdig te kunnen signaleren worden zowel de individuele componenten als het platform als systeem gemonitord en geanalyseerd. Er zijn gerichte procedures opgesteld die zorgdragen voor opvolging bij problemen en calamiteiten.

Applicatiebeveiliging en audits

Bij de ontwikkeling van TransFollow is voortdurend aandacht besteed aan de beveiliging van de applicatie en de data. De applicatie is vóór en tijdens het ontwikkelproces voortdurend getoetst aan uitgebreide kwaliteitscriteria vanuit onder andere de ISO 25010 norm, waarbij betrouwbaarheid, bruikbaarheid, compatibiliteit, efficiency, onderhoudbaarheid en overdraagbaarheid centraal staan. De kans op misbruik van de code is verder geminimaliseerd door alle componenten individueel én als een integraal systeem te toetsen.

Het datamodel van TransFollow is gericht op veiligheid en betrouwbaarheid, omdat gebruikers in hun bedrijfsvoering volledig moeten kunnen rekenen op de beschikbaarheid van hun vrachtbrieven en zendingsberichten. In de applicatie zijn validaties op invoergegevens, integriteitcontroles en gedetailleerde log-mechanismen gebouwd. TransFollow maakt gebruik van bewezen communicatiestandaarden, die het risico op verlies van data zeer klein maken.

Deze communicatiestandaarden worden op correcte implementatie getoetst. ISO 27002 voorziet in een jaarlijkse audit. Ook tijdens de ontwikkeling is de software meerdere keren gecontroleerd door middel van code reviews. Tenslotte voert een gespecialiseerd bureau software penetratietests (hackerstests) uit.

Databeveiliging

De levenscyclus van de data in het TransFollow-platform is nauwkeurig gedefinieerd. De data van vrachtbrieven en zendingsberichten zullen maximaal twee weken worden bewaard. De data worden zodanig vernietigd, dat reproduceren onmogelijk is. Er is een duidelijke definitie van eigenaarschap van de data en er zijn technische procedures die borgen dat er geen data kunnen worden gekopieerd tussen omgevingen en netwerken. De procedures voor toegang tot de productie data zijn zo ver beperkt dat ook TransFollow geen toegang hiertoe heeft.

Vanuit perspectief van de gebruiker kan het noodzakelijk zijn om gegevens langer te bewaren. Daarom adviseren wij klanten om in eigen beheer gegevens (bijvoorbeeld de TransFollow-vrachtbrief) minimaal één jaar, maar liever nog zeven jaar te bewaren. TransFollow zal bedrijven daartoe in de gelegenheid stellen door een verzegeld PDF-bestand (certified) beschikbaar te stellen aan partijen. Zo kan een partij het verzegelde PDF-bestand, in geval er een schadeclaim gesteld moet worden, aan de verzekeraar ter beschikking stellen als bewijsmateriaal. De vrachtbrief wordt verzegeld direct nadat de ontvanger zijn eventuele opmerkingen op de vrachtbrief heeft geplaatst en voor ontvangst heeft getekend. Na verzegeling hebben partijen twee weken de tijd om het verzegelde PDF-bestand te downloaden. Ook kunnen klanten kiezen om de gegevens te archiveren bij TransFollow. In het archief van TransFollow (tegen betaling) zullen de vrachtbrieven voor een periode van 7 jaar bewaard worden. Voor het archief zijn dezelfde voorzieningen ter beveiliging getroffen als voor de rest van het TransFollow-platform. Het archief is in beheer bij dezelfde hosting leverancier.

Onafhankelijkheid databeheerder

Beurtvaartadres, als eigenaar van het TransFollow platform, is een onafhankelijke organisatie. Beurtvaartadres stelt zich ten doel om de logistieke keten te faciliteren bij het uitwisselen en bewaren van gegevens over logistieke transacties. In dat kader is het TransFollow-platform ontwikkeld. Zowel bij de ontwikkeling als het beheer van TransFollow is maximaal aandacht besteed aan veiligheid en betrouwbaarheid. Beurtvaartadres ziet dit als haar verantwoordelijkheid in het belang van de logistieke branche. Het gebruik van data voor andere doeleinden ziet zij als zeer ongewenst. Afscherming en vernietiging van gedateerde data heeft dan ook hoge prioriteit op technisch, operationeel en contractueel gebied.

3. Management en Organisatie

Bij de ontwikkeling en het beheer van het TransFollow-platform is een groot aantal bedrijven en organisaties betrokken. Beurtvaartadres stelt hoge eisen aan de procesinrichting van de interne organisatie en die van haar partners. Beurtvaartadres is ISO 27001 gecertificeerd en voldoet daarmee aan internationale informatiebeveiligingsrichtlijnen. TransFollow wordt beheerd in een organisatie waar processen zijn ingericht voor wijzigingen, het testen van de software en de distributie van de software naar eindgebruikers. Deze processen kennen een duidelijke scheiding van verantwoordelijkheden. Toetsing vindt plaats op basis van een planning- en controlcyclus. Bovendien laat Beurtvaartadres op regelmatige basis risicoanalyses uitvoeren op de kwetsbare delen van de processen.

Functionele wijzigingen op het platform gaan via een Change Advisory Board, waarin vertegenwoordigers van alle betrokken partijen participeren. Opgeleverde wijzigingen worden in een

zorgvuldig gedefinieerd release management proces in productie genomen. Ook hier zijn vertegenwoordigers van diverse partijen betrokken.

Het TransFollow-platform en de beheersorganisatie zijn gebaseerd en getoetst op internationale standaarden op het gebied van procesinrichting (ISO9001:2000 en ISO 20000), software ontwikkeling (ISO 25010), informatiebeveiliging (ISO 27001 en ISO 27002) en fraude identificatie.

4. Wetgeving

Wij hebben de volgende wetgeving geïdentificeerd, waaraan het TransFollow-platform moet voldoen:

- Wetgeving over de vrachtbrief;
- Wetgeving over elektronische handelen inclusief de elektronische handtekening;
- Wetgeving omtrent de bescherming van persoonsgegevens.

Samen met juristen, gespecialiseerd in vervoerrecht en ICT-recht zijn de eisen geformuleerd, waaraan het TransFollow-platform volledig voldoet.

TransFollow wordt bij de lancering alleen voor binnenlands vervoer gebruikt. Zodra de wettelijke mogelijkheid zich voordoet, dat wil zeggen wanneer een aangrenzend land het e-protocol van het CMR-verdrag ratificeert of wanneer een aan Nederland grenzend land elektronische vrachtbrieven voor binnenlands vervoer toestaat, zal TransFollow ook voor grensoverschrijdend vervoer of voor gebruik in het buitenland geschikt gemaakt worden. Voor multimodaal vervoer is het systeem op dit moment niet geschikt.

Ook de papieren vervoerder kan gebruik maken van het systeem, omdat het systeem mogelijk maakt dat de vrachtbrief wordt ‘overgedragen’ aan een volgende vervoerder.

De opslag van data van TransFollow is ondergebracht bij een Nederlandse hosting partij die gebruik maakt van datacenters op Nederlands grondgebied. Dat betekent dat het Nederlands recht van toepassing is. Contractueel is afgedwongen dat de data en de applicatie niet overgedragen mogen worden aan buitenlandse overheden.

5. Ten slotte

Mocht u nog vragen hebben over de beveiliging van TransFollow, neemt u dan contact op met TransFollow, telefoonnummer 088-55 22 582.