Beschrijving maatregelen Informatie beveiliging centrale omgeving

Versie:	2.1
Datum:	november 2017
Status:	Concept

Inhoud

Inleiding

Doelstelling

De doelstelling van dit document is de klanten te informeren (die van diensten gebruik maken van de centrale hosted omgeving) over de maatregelen die Accensys heeft getroffen in het kader van informatiebeveiliging.

Streven hierbij is om de klant een globaal inzicht te verschaffen in de wijze waarop deze beveiliging is opgezet zonder hierbij specifieke informatie, die mogelijk voor een aanval op deze omgeving gebruikt kan worden, vrij te geven.

Informatiebeveiliging

Accensys heeft informatiebeveiliging hoog in het vandaal staan. Het is een centraal thema bij alle wijzigingen en verbeteringen die wij aan onze bedrijfsprocessen doorvoeren. Met periodiek geplande interne beveiligingsaudits controleren wij de status van informatiebeveiliging. Deze status wordt getoetst aan de norm ISO 27001. De verbeterpunten uit de audits worden opgenomen in de continue cyclus van maatregelen voor informatiebeveiliging die onder dagelijks beheer van de directie valt en elke twee jaar door een ISO 2700X bevoegde externe instantie wordt getoetst.

Algemene verordening gegevensbescherming (AVG)

25 mei 2018 zal de nieuwe wet AVG de huidige wet voor privacywetgeving vervangen. Deze wet bevat regels voor het verwerken van persoonsgegevens. Accensys heeft voor naleving van deze nieuwe wetgeving een verwerkersovereenkomst opgesteld waarin Accensys aangeeft wat de maatregelen zijn die zijn getroffen om compliant te zijn.

Management samenvatting

De hosted diensten van Accensys worden geleverd vanuit de centrale hosted omgeving van Accensys. Deze centrale omgeving is opgebouwd in het data center waar een ruimte(kooi) met redundante toegangslijnen wordt gehuurd. De inrichting van en het beheer op deze omgeving ligt bij supportdesk Accensys.

De basis componenten waarop de centrale omgeving is opgebouwd zijn veiligheid, beschikbaarheid en schaalbaarheid.

Dit document is bedoeld voor klanten die een hosted dienst afnemen van Accensys waar klant- en persoonsgegevens mee zijn gemoeid. De aandacht zal derhalve vooral gericht zijn op de beveiliging.

BEVEILIGING

Toegang tot de omgeving

De hostingdiensten betrekt Accensys bij het top-tier, ISO gecertificeerd data center van Leaseweb. Het data center is gevestigd bij EvoSwitch, één van Nederlands meest geavanceerde data center op dit moment.

U wilt aan uw klanten, aandeelhouders en andere belanghebbenden kunnen bewijzen dat de compliance in orde is, om zorgen over kwesties als cyberveiligheid en de continuïteit van de onderneming te verzekeren. Bij Leaseweb wordt nauw samengewerkt met EY, EY CertifyPoint en ComSec Consulting, met als resultaat ISO 27001-, PCI DSS-, SOC 1-, HIPAA- en NEN 7510-assurancerapporten en -certificaten die u garanderen dat de infrastructuur, gegevensverwerking en beveiliging voldoen aan de laatste normen. U kunt precies zien wat er allemaal onder de rapporten en certificaten valt door de 'bouwstenen' van het LeaseWeb Trust Model te bekijken.
Hier vindt u de certificaten en assurancerapporten die wij hebben behaald:

ISO 27001
ISO (International Organization for Standardization) 27001 is de internationale veiligheidsnorm die gebruikt wordt om de bescherming van gevoelige data te toetsen.

PCI DSS
De PCI DSS (Payment Card Industry Data Security Standard)-zorgt ervoor dat gevoelige informatie op een veilige manier kan worden verwerkt en is bedoeld om organisaties te helpen bij de proactieve bescherming van de accountgegevens van hun klanten. Ons certificeringsproces werd uitgevoerd door Comsec Consulting

Fysieke toegangsbeveiliging EvoSwitch

De apparatuur die wordt gebruikt voor de centrale omgeving van Accensys staat in het bovenstaand beschreven data center. Een aantal punten rond de fysieke beveiliging worden hieronder kort weergegeven

Alleen toegang voor geautoriseerde personen

Het is alleen mogelijk om toegang te krijgen tot dit data center wanneer een persoon door ons is geautoriseerd. Zonder aankondiging van een bezoek is toegang onmogelijk. Bij een bezoek is identificatie verplicht.

Toegang tot systemen
Eenmaal binnen kan een bezoeker alleen toegang krijgen tot de ruimte waarvoor deze is geautoriseerd. Binnen deze ruimte is alle apparatuur in afgesloten kasten geplaatst.

Derden
Wanneer derden fysieke toegang moet worden verleend tot de systemen van de centrale serveromgeving (bijvoorbeeld een engineer bij een storing op een systeem) wordt deze ten allen tijden begeleid door een medewerker van Accensys.

Netwerk beveiliging
Uiteraard is er ook netwerk toegang tot de diverse systemen. Hieronder volgt een beschrijving van de belangrijkste maatregelen die Accensys heeft genomen om deze toegang te controleren en te beveiligen.

Beveiligde verbindingen
Accensys kiest er voor om alle toegang tot de systemen van de centrale omgeving over beveiligde verbindingen te laten verlopen. In principe ondersteunen we alleen de nieuwste protocollen en wordt het gebruik van verouderde of gecompromitteerde protocollen onmogelijk gemaakt.
Wanneer het slechts een uitgaande verbinding betreft zullen wij hier een uitzondering op maken. Bij inkomende verbindingen wordt er een specifieke risicoanalyse voor gemaakt.

Netwerkapparatuur
Accensys maakt gebruik van A-merk netwerkapparatuur die wanneer nodig van updates worden voorzien. Op deze apparatuur is proactieve monitoring ingeregeld.

Afscherming binnen het netwerk
Binnen het netwerk op de centrale omgeving worden alleen de noodzakelijke verbindingen toegestaan. Vanaf een systeem wat van buitenaf benaderbaar is, kan bijvoorbeeld nooit toegang worden gekregen tot de systemen waarop Accensys backups van gegevens opslaan.

Externe scans
Periodiek worden onderdelen van de netwerk infrastructuur door hierin gespecialiseerde bedrijven gecontroleerd. Uitkomsten hiervan worden gebruikt om verbeteringen in de beveiliging door te voeren

Toegang tot gegevens

Gegevens van klanten worden gesegmenteerd per klant opgeslagen. In de inrichting is vastgelegd dat een klant geen toegang kan krijgen tot gegevens van andere klanten. Bij Accensys is vooraf bekend welke medewerker van de klant geautoriseerd is om deze toegang tot de eigen klantgegevens waar nodig door Accensys aan te laten passen. Verzoeken die wij ontvangen deze rechten aan te passen van niet geautoriseerde medewerkers (van de klant), worden altijd eerst besproken met de geautoriseerde medewerkers (van de klant).

Medewerkers van Accensys hebben alleen toegang tot gegevens van een klant voor zover dat uit hoofde van hun functie nodig is.

Authenticatie van gebruikers

Eindgebruikers

Gebruikers kunnen op basis van een gebruikersnaam en wachtwoord toegang krijgen tot de systemen en gegevens waarvoor ze geautoriseerd zijn. Indien gewenst of vereist kan er gekozen worden voor authenticatie op een hoger beveiligingsniveau, bijvoorbeeld door middel van *two factor authenticatie* (2FA).

Authenticatie medewerkers van Accensys

De toegang tot het netwerk van Accensys voor medewerkers vindt plaats met behulp van 2FA.

Bescherming tegen virussen en malware

Virus en malware scanners

Accensys maakt gebruik van een modern virus- en malwarescanner welke meerdere keren per dag wordt geupdate met de nieuwste definities. Elk bestand word zowel bij het schrijven als het openen gecontroleerd door deze scanner.
Daarnaast draaien er periodieke scans om opgeslagen bestanden, welke een eerder onbekende bedreiging bevatten, alsnog te isoleren

Updates van operating systemen

Accensys zorgt er voor dat alle operating systemen waar nodig worden voorzien van de laatste updates en patches. Deze updates vinden, waar mogelijk, buiten kantoortijden plaats. De klant wordt vooraf geïnformeerd over de onderhoudswerkzaamheden.
Wanneer de aard van de bedreiging hiertoe aanleiding geeft kan een patch of update per direct worden geïnstalleerd. Uiteraard wordt ook hier de klant vooraf geïnformeerd.

Updates van overige software

Ook alle overige software wordt regelmatig voorzien van patches en updates, afhankelijk van de beschikbaarheid door de fabrikant/leverancier van deze software.

Back-up

Van de centrale omgeving wordt meerdere malen per dag een back-up gemaakt naar systemen die hiervoor speciaal zijn neergezet binnen de centrale omgeving. Bij calamiteiten kunnen hiermee snel gegevens worden teruggehaald. De retentie op deze system is zeer kort, ten hoogste een aantal dagen.

Dagelijks worden er back-ups gemaakt naar draagbare media. De data op deze media is versleuteld. Deze media worden buiten het data center bewaard in een daarvoor geschikte, afgesloten ruimte. Het transport van deze gegevensdragers wordt gepland door de afdelingsmanager en uitgevoerd door daarvoor geautoriseerde medewerkers en vervolgens gecontroleerd door de manager.
De retentie van deze media is enkele jaren. Door deze lange retentie periode kiest Accensys voor opslag met versleutelde containers per klant te werken. Het verwijderen van data van een klant op meerdere media is mogelijk echter zeer tijdrovend en slecht te controleren op compleetheid.

De containers zijn beveiligd met een encryptiesleutel die bekend is bij de klant en op het systeem wat verantwoordelijk is voor het maken van de back-up. Het is niet mogelijk deze encryptiesleutel op een ander systeem te gebruiken. Accensys draagt zorg voor de authenticiteit van deze encryptiesleutels). Wanneer er voor Accensys een noodzaak is om te beschikken over deze encryptiesleutel zal deze bij de klant worden opgevraagd. Dit is denkbaar wanneer deze back-up server wordt vervangen of wanneer het noodzakelijk is om een back-up op een ander systeem terug te lezen.
Wanneer de klant Accensys verzoekt om de back-up data te verwijderen zal Accensys de encryptiesleutel verwijderen. Hiermee is het dan zonder dat de klant de encryptiesleutel verstrekt niet meer mogelijk om deze gegevens te lezen.

Vernietiging van gegevensdragers

Wanneer gegevensdragers worden uit gefaseerd worden deze altijd eerst voorgoed gewist “gewiped” door medewerkers van Accensys en daarna vernietigd door een hiervoor gecertificeerd bedrijf.

Monitoring

Accensys heeft op de gehele centrale omgeving proactieve monitoring ingericht. Deze monitoring is zowel gericht op het voorkomen van storingen als het detecteren van aanvallen van buitenaf en van binnenuit (door medewerkers van klanten die toegang hebben tot de systemen van klanten).

Interne controle

Accensys heeft een systeem voor interne controles waarbij met regelmaat wordt gecontroleerd of alle afspraken en procedures worden nageleefd.
Een belangrijk onderdeel hiervan is een audit op de toegang die medewerkers hebben tot systemen en gegevens. Wanneer deze toegang niet (meer) noodzakelijk blijft zal deze worden ingetrokken.

Geheimhouding

Medewerkers van Accensys hebben allemaal een geheimhoudingsverklaring getekend. Uiteraard is geheimhouding ook onderdeel van de afspraken tussen Accensys en de klant. De medewerkers van Accensys hebben allen een VOG-verklaring weerlegd bij tekenen van de arbeidsovereenkomst.

Geplande verbeteringen

Two Factor authenticatie (2FA)

Accensys gaat vanaf dit jaar 2FA aanbieden aan de huidige gebruikers. Doelstelling is dat in de tweede helft van 2018 alle gebruikers op 2FA zijn aangesloten.

BESCHIKBAARHEID

Accensys streeft naar een beschikbaarheid van 99,9% waarbij servicevensters niet worden meegenomen in de berekening van deze beschikbaarheid. Hiertoe zijn de systemen binnen de centrale omgeving voorzien van minimaal enkelvoudige redundantie . Op kritieke componenten binnen de centrale omgeving ligt de redundantie een of meerdere niveaus hoger.

Voor grote calamiteiten (bijvoorbeeld bij uitval van het data center) beschikt Accensys over een additionele dienst waarmee de functionaliteit van de centrale omgeving binnen bepaalde tijd weer online kunnen brengen. Deze dienst valt echter buiten de standaard hosting dienst en wordt uitgevoerd, zonder verdere afspraken, op basis van Best Effort. Op verzoek kan voor deze dienst een service level worden afgesproken.

SCHAALBAARHEID

De centrale omgeving is opgebouwd in een geclusterd netwerk. Het toevoegen van extra performance of capaciteit is een kwestie van het toevoegen van hardware. Uit de rapportages van het proactieve monitoring op de omgeving kan worden geconcludeerd of en wanneer er toevoeging van hardware vereist is.