Mededeling over de betrouwbaarheid van de Overstapservice Onderwijs

Onlangs heeft Infoseccon BV een rapport over het geautomatiseerde systeem van Overstapservice Onderwijs (OSO) uitgebracht.

Infoseccon BV is een onafhankelijke consultancy expert organisatie op het gebied van risicomanagement en informatiebeveiliging. Door de toegenomen complexiteit, de afhankelijkheid en risico's van de automatisering is een gedegen informatiebeveiliging noodzakelijk om de risico's te kunnen beheersen en het vertrouwen in informatie-uitwisseling van leerling-gegevens tussen scholen onderling in de OSO omgeving te borgen. Wet en regelgeving vereisen ook maatregelen aan organisaties om zich hieraan te conformeren. Belangrijk uitgangspunt is hierbij ook het creëren van vertrouwen bij de gebruikers en toezichthouders betreffende de omgang met private gegevens van de leerlingen.

Infoseccon BV heeft in 2011 de opdracht van het OSO Projectmanagement gekregen om het informatiebeveiligingsbeleid te definiëren met betrekking tot de kaders voor ontwerp en inrichting van de Overstapservice Onderwijs. Bovendien werd gevraagd om beveiligingsadvies te geven en onderzoek te verrichten naar de beveiliging van de implementatie van het OSO, waaronder de beveiliging van de applicaties en infrastructuur en de organisatie van deze beveiliging in het OSO Traffic Center.

Voor de technische beveiligingstesten is Comsec Consulting BV ingehuurd. Comsec heeft meerdere penetratietesten uitgevoerd op de uitvoering en de werking van het Traffic Center binnen OSO en de applicatie MijnELD (annex MijnOSO).

Het onderzoek is uitgevoerd op basis van volledige toegang tot de genoemde applicaties en infrastructuur maar ook vanaf het internet zonder geautoriseerde toegang. Daarbij heeft er beoordeling van relevante documentatie en interviews met betrokken medewerkers plaatsgevonden. Tevens zijn de fysieke locaties bekeken waar de applicaties en de infrastructuur zich bevinden.

In de huidige oplossing van OSO is er alleen sprake van een zg. doorgeefluik, en vindt er geen bewerking plaats in het Traffic Center van leerling-gegevens. Bewerking vindt uitsluitend plaats bij de scholen, waarmee deze verplicht zijn de eisen van de Wet Bescherming Persoonsgegevens (WBP) te volgen. De te volgen beveiligingsmaatregelen door OSO dienen echter wel de Wet op de Computercriminaliteit te honoreren. OSO heeft gekozen voor het volgen van de eisen gesteld in het Voorschrift Informatiebeveiliging Rijksdienst, en de NEN-ISO/IEC 27002 waardoor realisatie tot stand komt.

Consultants van zowel Infoseccon BV als van Comsec Consulting BV hebben de informatiebeveiliging van OSO zwaar op de proef gesteld en adviezen ter verbetering gegeven voor zowel de organisatorische maatregelen als de technische opzet van applicaties en infrastructuur.

In vergelijking met organisaties met een overeenkomstige grote en aard van werkzaamheden scoort OSO bovengemiddeld qua beveiligingsbewustzijn. De organisatie achter OSO werkt er voortdurend aan om de risico’s optimaal te beheersen en te verminderen waar noodzakelijk. Hierbij wordt opgemerkt dat de totale verantwoordelijkheid voor de beveiliging over het geheel van scholen en OSO via organisatie van maatregelen geregeld dient te zijn. De conclusie uit het onderzoek ten aanzien van de OSO onderdelen geldt alleen mits door de andere delen aan de WBP eisen wordt voldaan. Met andere delen wordt bedoeld de scholen, de software leveranciers van het leerling administratiesysteem (LAS) en anderen die gekoppeld worden aan OSO.

Inleiding

De elektronische uitwisseling van leerling-gegevens tussen scholen brengt risico's met zich mee en het moet voldoen aan de vigerende wet en regelgeving. Om informatiebeveiliging risico's te beheersen, controle mogelijk te maken en te voldoen aan de eisen gesteld in wet- en regelgeving moeten er maatregelen van organisatorische en technische aard worden uitgevoerd.

Uit een risico analyse is bepaald dat het grootste risico de dreiging is van het openbaar worden van vertrouwelijke leerling-gegevens. Daarmee onder andere verlies van vertrouwen veroorzakend in het gebruik van de Overstapservice Onderwijs, en het creëren van publieke commotie ten nadele van het Ministerie van Onderwijs en Wetenschappen en de scholen. De aard van de verstuurde schoolinformatie legt hoge eisen op het gebied van vertrouwelijkheid neer. Het is slechts voor speciaal daarvoor geautoriseerde gebruikers toegestaan informatie uit te wisselen via het Traffic Center, alvorens de uitwisseling van de leerlingdossiers tussen de scholen onderling plaats vindt. De scholen dienen het identiteitsbeheer op gebruikersniveau, autorisatie en authenticatie zelf herleidbaar te regelen.

Daarnaast kan de beschikbaarheid van uitwisseling worden bedreigd, echter gezien de eisen aan tijdigheid is dat meer lastig vanuit gebruiksoverwegingen dan dat het een directe bedreiging voor de toepassing is. Het Traffic Center zelf slaat geen leerling dossiers op. De beschikbaarheid van die dossiers ligt binnen het verantwoordelijkheidsgebied van de scholen.

Het waarborgen van integriteit, volledigheid, juistheid en tijdigheid van de leerling-gegevens is zeer hoog. De datastroom die plaats vindt tussen de school en het Traffic center mag niet gemanipuleerd kunnen worden. Het gaat hier immers om de controle op de authenticiteit van de scholen en de controle of de scholen geautoriseerd zijn om persoonsinformatie uit te wisselen.

De juridische status is geregeld in de wetgeving en onderlinge afspraken tussen de partijen en vormt als zodanig geen bedreiging, waardoor aanvullende technische of organisatie maatregelen niet nodig zijn.

Al in een vroeg stadium heeft de Overstapservice Onderwijs organisatie zich gerealiseerd dat Informatiebeveiliging onderdeel uit zou moeten maken van het totale proces. Mede door de Privacy wetgeving, deze stelt eisen aan het werken met persoonsgebonden gegevens, is al in vroeg stadium nagedacht over Informatiebeveiliging. Tweeledig, het uitvoeren van de eisen voortvloeiend uit de Wet Bescherming Persoonsgegevens, organisatorisch door het aanmelden en opstellen van een wettelijk kader waarbinnen gewerkt moet worden, en het opstellen van een beveiligingsplan.

Aan het Overstapservice Onderwijs project zijn hoge eisen gesteld met betrekking tot het waarborgen van de vertrouwelijkheid van de verbindingen tussen de diverse hostingpartijen en de toegang tot de schoolinformatie in het Traffic center. Adviezen hierover zijn tijdens het project voortdurend bijgesteld naar aanleiding van de gewijzigde inzichten sinds het oorspronkelijke advies, waarin nog sprake was van een controleslag die OSO zou doen op de kwaliteit van de leerlingdossiers. In de huidige implementatie van het Traffic center is er geen enkele bemoeienis meer met leerlingdossiers en wordt uitsluitend gekeken naar de authenticiteit van de aanbiedende en afnemende onderwijsinstellingen.

Op basis van deze uitgangspunten is de gegevensclassificatie bepaald en zijn de bijbehorende maatregelen geïmplementeerd in het project. Als uitgangspunt voor het Beveiligingsplan is uitgegaan van ISO 2700X in een aan de organisatie grootte aangepaste

versie. Dit heeft geresulteerd in een aantal technische en organisatorische maatregelen conform de van de Informatie Beveiligingsstandaard ISO 27002 afgeleide invulling van maatregelen opgenomen in het beveiligingsplan van Overstapservice Onderwijs.

Opdracht, werkgebied en werkwijze

De doelstelling van de opdracht aan Infoseccon en Comsec Consulting voor de uitvoering van de informatiebeveiligingsaudit respectievelijk technische beveiligingstesten was:

- Bepalen of de Overstapservice Onderwijs organisatie voldoet aan de eisen die voortvloeien uit de Wet Bescherming Persoonsgegevens en de 'best practices' conform ISO 27002 (Code voor Informatiebeveiliging);
- In welke mate zijn de onderdelen; intentie, implementatie en uitvoering van de informatie beveiligingsprocessen volwassen uitgevoerd;
- Een weergave van de status quo van zowel processen als de systemen en toepassingen met aanbevelingen ter verbetering waar noodzakelijk geacht.

Het onderzoek naar de beveiliging van de informatiesystemen welke door OSO en derde partijen worden gebruikt en beheerd betrof de eigen OSO omgeving. De audit omvatte alleen het werkgebied en de daarbij behorende ICT processen waar OSO verantwoordelijk voor is en waar OSO een mogelijke rol in speelt. Het betrof niet de Primair Onderwijs scholen of de Voortgezet Onderwijs scholen als gebruikers van deze service. Ook de leerling-administratiesystemen zelf en toegang hiertoe vielen buiten de opdracht.

Het onderzoek bestond uit de volgende onderdelen:

A. Logische beveiliging
- Het onderzoeken van de applicatie "MijnELD (annex MijnOSO)" met gebruik van volledige toegangsrechten tot de applicatie als ook vanaf het internet zonder toegangsrechten;
- Het onderzoeken van de webservice en infrastructuur van het Traffic Center in het OSO.

B. Organisatorische beveiliging
- Een audit uitgevoerd op de organisatorische beveiligingsmaatregelen die het OSO projectmanagement genomen heeft om het gewenste niveau van informatiebeveiliging te garanderen. Deze audit heeft tot doel na te gaan of de organisatorische beveiligingsmaatregelen aansluiten bij de taken en bevoegdheden van medewerkers, of de verantwoordelijkheden juist zijn belegd en adequaat worden beheerd.
- Vooraf is vastgesteld dat de audit steekproefsgewijs zal plaatsvinden op een aantal zaken genoemd in het beveiligingsbeleid Traffic Center 1.0 van 23 november 2011. Hierbij is alleen gekeken naar de opzet en het bestaan van de beveiligingsmaatregelen. De werking van de beveiligingsmaatregelen is niet gecontroleerd. De reden hiervan is dat de opdracht tot hosting van het Traffic Center bij de hosting provider Kennisnet en het gebruik van de CRM applicatie bij OfficeHeart nog pas recent gegeven zijn. Het is gewenst beide partijen een redelijke tijd te geven om het beveiligingsbeleid waar het op een ieder van toepassing is te implementeren en daarna een diepgaander heraudit uit te voeren op een nog nader te bepalen tijdstip.

Door middel van interviews, feitenonderzoek en een technische audit werd bepaald of OSO ten opzichte van vergelijkbare organisaties voldoet aan de doelstelling. OSO heeft een aantal processen uitbesteed; deze uitbestede processen vallen onder de

verantwoordelijkheid van OSO en zijn voor de audit dan ook gelijkgesteld aan processen die door medewerkers van OSO worden uitgevoerd.

In de volgende paragraaf wordt ingegaan op de hoofdlijnen van de uitkomsten van het onderzoek.

Bevindingen

Geconstateerd is dat OSO doordrongen is van het feit dat Informatiebeveiliging noodzakelijk is, afgeleid uit het vanaf het begin van het project bezig zijn met Informatiebeveiligingszaken en het opstellen van een beveiligingsplan. De aanleiding daarvoor was tweeledig, namelijk het voldoen aan wet & regelgeving in het bijzonder de Wet Bescherming Persoonsgegevens en gezien de complexiteit, het aantal deelnemers t.w. alle scholen met hun eigen automatiseringsomgeving en applicaties van de leerling-administratiesysteem (LAS) leveranciers als mogelijke risico's. Vanuit audit perspectief kan worden opgemerkt dat de intentie vanuit OSO qua beveiligingsbewustzijn als zeer positief kan worden aangemerkt.

De complexiteit in aanmerking genomen, veel processen en activiteiten worden bij en door derden uitgevoerd, het aantal daarbij betrokken medewerkers, en in vergelijking met gelijkvormige organisaties zijn bij OSO veel informatie beveiligingsmaatregelen geïmplementeerd, processen gecreëerd en verantwoordelijkheden toegekend, echter in de uitvoering van het OSO beveiligingsbeleid dient er nog een aantal maatregelen ter verbetering in de uitvoering van de beveiligingsverantwoordelijkheden genomen te worden. Het OSO projectmanagement heeft aangegeven pragmatisch opvolging te geven aan de aanbevelingen en hiervoor ook overleg gevoerd met Infoseccon.

Zodra de diverse verbeteringsmaatregelen zijn doorgevoerd adviseren wij om een heraudit te laten uitvoeren om te kunnen beoordelen of alle betrokken partijen op alle verbeterpunten dan voldoen aan het OSO beveiligingsbeleid. Voor de definitieve planning van hiervan zullen nog verdere afspraken gemaakt moeten worden.

De werking van de informatiebeveiliging wordt door feiten onderbouwd, wordt gekenmerkt door zichtbaarheid op websites, beschikbare documenten, beveiligingsplan, audit rapportages, etc.

Wat betreft de logische beveiliging van applicaties en systeem- en netwerk infrastructuur zijn uit de technische audit een aantal belangrijke zaken gekomen die voor verbetering in aanmerking komen en inmiddels door OSO werden aangepakt cq. in een vervolgfase worden geïmplementeerd.

Aanvankelijk werd op het beveiligingsniveau van de applicaties een aantal zwakke plekken geconstateerd. Daarnaast werden er met betrekking tot de infrastructuur ook een aantal beveiligingsproblemen geconstateerd die een mogelijke aanvaller mogelijkheden boden om toegang te krijgen, zelfs vanaf het internet. Evenals bij de applicaties was vanwege het risiconiveau gewenst dat ook deze problemen zo snel mogelijk werden aangepakt, waarvoor door OSO maatregelen genomen zijn om beveiligingsniveau op het vereiste betrouwbare niveau te brengen. Het OSO projectmanagement heeft op basis van de rapportages technische verbetermaatregelen op de diverse bevindingen genomen. Zij heeft deze ook weer laten hertesten door Comsec Consulting, zodat daarmee de risicoproblemen in applicaties en infrastructuur onder controle zijn gekomen om de overstapservice ruim voldoende betrouwbaar te kunnen lanceren en in de ontwikkelingsvervolgfasen van het project verbeteringen verder te optimaliseren conform de gegeven adviezen.

Eindconclusie

Als eindconclusie van de organisatorische audit wordt vastgesteld dat de maatregelen die in het kader van de informatiebeveiliging door alle delen over het geheel van scholen en OSO plaats moeten vinden, inclusief bij en door derden. De conclusie uit het onderzoek ten aanzien van de OSO geldt alleen mits door de andere delen aan de WBP eisen wordt voldaan.

Er is een beveiligingsadvies gevraagd door het OSO projectmanagement waaraan het ontwerp en de implementatie van applicatie/infrastructuur architectuur van OSO getoetst kon en ook in de toekomst kan worden. Wezenlijke veranderingen echter zullen altijd opnieuw geëvalueerd dienen te worden voor eventuele aanpassingen in dat advies.

Er is een beveiligingsplan van waaruit de OSO organisatie procedures heeft afgeleid en gedocumenteerd. Er worden richtlijnen gegeven aan leerlingadministratiesysteem leveranciers met betrekking tot de koppeling aan de OSO. Ook heeft OSO een beveiligingsbewustzijn presentatie laten ontwikkelen om de scholen te wijzen op hun verantwoordelijkheden in het proces rond het gebruik van het overstapdossier en de overstapservice. Bovendien bestaat er als juridisch kader een bewerkerovereenkomst tussen OSO en de scholen om de verantwoordelijkheden op juiste wijze toe te wijzen aan partijen.

Processen en taken zijn toegewezen en de meeste daarvan zijn geïnitieerd en operationeel. Processen dienen nog nader geëvalueerd en geoptimaliseerd te worden waarbij ook verbeteringen op het vlak van beveiligingsverantwoordelijkheden met betrokken derden doorgevoerd dienen te worden door middel van het vastleggen van afspraken in contracten. Een heraudit dient hier te zijner tijd op plaats te vinden.

Geconstateerd wordt dat in verhouding met organisaties van gelijksoortige grootte en dienstverlening OSO in positieve zin presteert. Met uitzondering van een klein aantal nog te verbeteren processen en beveiligingsverantwoordelijkheden door middel van kleine aanpassingen, voldoet OSO aan de in de doelstelling gestelde eisen op organisatorisch informatiebeveiligingsvlak. Als randvoorwaarde wordt hierbij wel gewezen op de eerdere opmerking over de WBP eisen waar door de andere delen aan voldaan dient te worden. Immers, de zwakste schakel kan de keten hier breken.

In alle voorgaande situaties waar door Infoseccon en Comsec Consulting geconstateerd werd dat het vastgestelde beveiligingsniveau te laag was zijn beveiligingsadviezen gegeven aan OSO welke acties ondernomen dienden te worden om dit niveau voldoende te verhogen.

Met dien verstande dat OSO gevolg heeft gegeven aan de uitvoering van de gegeven adviezen op het vlak van de logische en organisatorische beveiliging kan het OSO systeem als voldoende betrouwbaar worden gekenmerkt. Om de effectiviteit en handhaving van deze genomen maatregelen te beoordelen wordt geadviseerd in tweede fase van het project in 2012 een evaluatie van de getroffen verbetermaatregelen weer door Infoseccon cq. Comsec Consulting te laten uitvoeren.

Verdere periodieke audits, beveiligingstesten en beveiligingsadviezen zullen bijdragen tot waarborg van de betrouwbaarheid van de Overstapservice Onderwijs.

Deze verklaring betreffende de informatiebeveiliging van Overstapservice Onderwijs is afgegeven door Infoseccon B.V. op 27 juni 2012.