EU-SEC helpt auditors

10 september 2019

André Kloot

Open grenzen, dat was een belangrijke missie van de EU. Open grenzen om de economische ontwikkeling van de lidstaten te versnellen. En dat heeft de lidstaten geen windeieren gelegd. De economische ontwikkeling maakt onderlinge samenwerking over de grenzen heen veel eenvoudiger door het afschaffen van tariefmuren en door het vrije verkeer van mensen en goederen mogelijk te maken. Als je het geluk hebt om binnen het Schengen-gebied te blijven, dan ben je het concept 'grens' eigenlijk allang vergeten. Ook in de virtuele wereld merken we niets van grenzen. Wij versturen vanaf het begin van het internettijdperk pakketjes met data heen en weer en dankzij het TCP-protocol hoeven we ons geen zorgen te maken. Het pakketje komt wel aan.

Maar juist op dit gebied blijken er toch forse grenzen te bestaan. Dankzij de wet- en regelgeving op het gebied van informatiebescherming, en dan met name op het gebied van privacybescherming, is er feitelijk niet zonder meer sprake van vrij dataverkeer. Er is sinds vorig jaar binnen Europa weliswaar één GDPR, maar elke lidstaat heeft die moeten inpassen in eigen wetgeving.

Op het gebied van informatiebeveiliging is er geen eenduidigheid die vrij verkeer op een transparante manier mogelijk maakt. Europese regelgeving ontbreekt, en ook toezichthouders richten zich op de eigen landelijke wetten en regels. Daar waar in de fysieke wereld samenwerking en ketencontracten binnen de EU prima samengaan en daar waar organisaties uit de verschillende lidstaten over elkaars grenzen heen producten en diensten kunnen afzetten, leveren de virtuele grenzen grote problemen op.

Denk maar aan de volgende casus: de Nederlandse overheid wil diensten van een cloud serviceprovider (CSP) aanbesteden, maar die CSP moet dan voldoen aan de vigerende wet- en regelgeving. In casu de AVG en BIO (Baseline Informatiebeveiliging Overheid, voorheen de BIR, Baseline Informatiebeveiliging Rijksdienst). Bij voorkeur moet die CSP ook ISO27001 gecertificeerd zijn en een ISAE3402-verklaring hebben. Een volstekt logische set eisen. Maar wel een set eisen waar een CSP uit bijvoorbeeld de Tsjechische Republiek niet aan kan voldoen: die kent namelijk de BIO niet en als die CSP al ISO27K gecertificeerd is, dan zegt dat eigenlijk alleen dat er een ISMS bestaat, niet of die partij ook BIO-compliant is. Of dat dan ook resulteert in de noodzakelijke passende beveiligingsmaatregelen voor clouddiensten ten behoeve van de Nederlandse overheid

is daar niet zomaar uit af te leiden. Oftewel: door het stellen van de betreffende eisen zou je, met een beetje een kritische blik, kunnen stellen dat de Nederlandse overheid het buitenlandse partijen onmogelijk maakt om aan de Nederlandse overheid clouddiensten te leveren. Marktbescherming. En dat geldt natuurlijk niet alleen voor de Nederlandse overheid, maar dat geldt voor alle lidstaten. Iedere staat heeft een eigen setje regels, waarmee feitelijk de buitenlandse concurrentie wordt buitengesloten.

Een tweede obstakel in de internationalisering en voor de verdere groei van digitalisering, is de toenemende eis van toezichthouders om permanent in staat te zijn de betrouwbaarheid van geautomatiseerde verwerkingen te kunnen vaststellen. Waar een bank tien jaar geleden de primaire processen nog volledig in eigen hand had en de systemen in eigen rekencentra draaiden, is de transitie naar uitbesteding hedentendage in volle gang. En daar waar overheden nog strikte eigen reguleringen hanteren, maken financiële instellingen al op grote schaal en wereldwijd gebruik van CSP's. Zij kennen geen grenzen meer. Waar vroeger de auditors ter plekke konden meekijken, is dat nu niet meer haalbaar. In de cloud bestaat dat niet meer. Over de landsgrenzen heen kan een toezichthouder ook niet in de cloud kijken, terwijl de financiële instellingen daar wel op grote schaal aanwezig zijn.

Beide problemen hebben te maken met de noodzaak van een Cloud Service Provider om aan te kunnen tonen *in control* te zijn op het gebied van security. Maar zowel de afzonderlijke lidstaten, als de afzonderlijke toezichthouders schermen hun eigen zeggenschap af. De landsgrenzen beperken daarmee voor CSP's nog steeds de mogelijkheid om over grenzen diensten aan te kunnen bieden. Dat gaat in tegen het gedachtengoed van de EU, namelijk het wegnemen van handelsbarrières. Het wegnemen van deze in control-barrières is dan ook de belangrijkste drijfveer achter het EU-SEC programma.

Het EU-SEC programma is onderdeel van het Horizon2020-innovatieprogramma van de Europese Commissie. In 2016 heeft de Commissie een competitie georganiseerd voor projecten op het gebied van een certificering voor producten en diensten. De doelstelling van dit project is te identificeren wat de verschillen, maar vooral de overeenkomsten, tussen de wetten en regels van de verschillende lidstaten zijn.

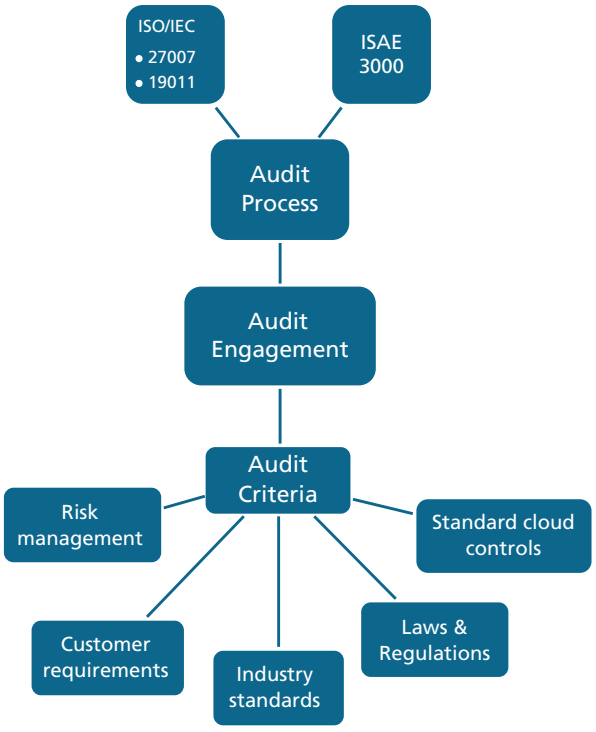
De Cloud Security Alliance heeft samen met acht andere partijen (onder andere Nixu) een consortium opgericht om binnen het Horizon2020-programma een certificeringsraamwerk voor clouddiensten te ontwikkelen. Na de gunning van de innovatieopdracht aan het consortium, is het project in 2017 begonnen met de eerste van zeven deelprojecten, namelijk de requirementsanalyse. Namens Nixu was ik de programmamamager voor deze eerste track. Daarbij werden de security- en privacyeisen alsmede eisen op het gebied van auditing, Multi-Party Recognition (MPR) en Continuous Auditing geïnventariseerd. MPR betekent dat voor het uitvoeren van audits of

certificeringen gebruik kan worden gemaakt van al aanwezige audits en certificeringen en dat over de grenzen heen de eisen aan auditors afgestemd zijn. Hierdoor wordt hergebruik van al uitgevoerde rapportages en cerificeringen mogelijk gemaakt. Als basisraamwerk is gebruikgemaakt van de Cloud Controls matrix (de 'CCM') van de Cloud Security Alliance (CSA). Dit instrument is al langer bekend en de CSA heeft op basis hiervan het STAR-register ontwikkeld. Binnen STAR kunnen CSP's zich laten opnemen als ze:

- op basis van een Eigen Verklaring kunnen aangeven dat ze voldoen aan CCM;
- op basis van een extern auditverslag (door een STAR-auditor) kunnen aangeven dat ze voldoen aan CCM;
- op basis van een Continuous Auditing attestatie kunnen aangeven dat ze voldoen aan CCM.

Op basis van de geïnventariseerde requirements is een *control framework* met een control architectuur opgezet en zijn tools (door)ontwikkeld om de audits te kunnen faciliteren. Het control framework bevat onder meer verschillende soorten auditmethoden voor bijvoorbeeld ISO27K-achtige certificeringen en voor ISAE3000-achtige certificeringen.

Zeker op het gebied van auditing leverde dat interessant materiaal op. Want zoals wij wel weten, is auditing niet zomaar afvinklijsten afwerken. Methodisch gezien is er wel meer te onderzoeken. Zo werden verschillende auditkaders beoordeeld (inclusief de ISO-standaarden terzake) en zijn eisen ten aanzien van het auditproces, de bewijsvoering, maar ook eisen ten aanzien van de auditor en de auditorganisatie geanalyseerd.



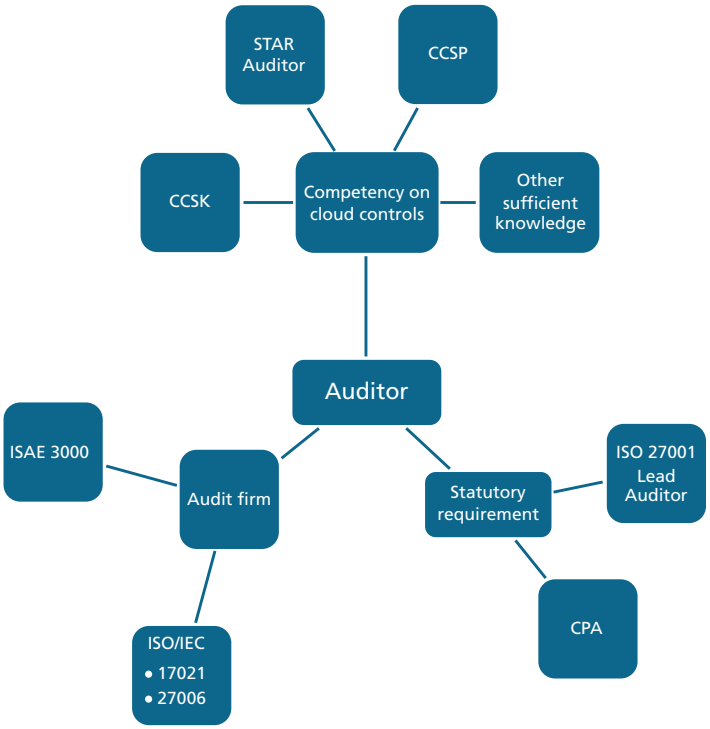
Figuur 1: Standaardaanpak voor auditing Information Security Management Systems

Gaandeweg de analyse werd duidelijk dat het uitvoeren van een ISO27K-audit in belangrijke mate afwijkt van het uitvoeren van een ISAE3402-audit. De belangrijkste bevindingen:

Het auditproces (gebaseerd op toepassing van ISO27007) is grotendeels hetzelfde, maar het grootste verschil is dat bij op ISAE3000 gebaseerde audits er een historisch bewijs van de effectiviteit van de werking van de beheersmaateregelen gedurende een bepaalde tijd (bijvoorbeeld twaalf maanden) moet worden geleverd.

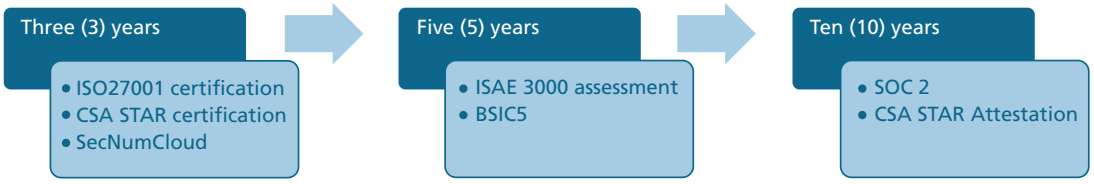
Gedurende het onderzoek kon ook worden geconstateerd dat materiekennis op het gebied van cloudsecurity bij de auditor onmisbaar is. Cloudsecurity kent namelijk diverse gelaagdheden, die je onder de noemer supplychain kunt vatten: een *cloud service sonsumer* kan bijvoorbeeld een SaaS-dienst afnemen, denk aan een HRM-systeem. Daarbij zal de afnemer eisen stellen aan de dienstverlener, onder andere ten aanzien van bijvoorbeeld privacy en security. Maar het probleem is dat een SaaS-provider zelf ook weer diensten van andere providers kan afnemen, zoals platformen of (gevirtualiseerde cloud-) infrastructuren en zelfs ook andere SaaS-oplossingen. De supply chain gedachte houdt in dat het voor de eindklant niet mag uitmaken hoe de dienst wordt geleverd, als maar wordt voldaan aan de eisen. Maar de eindklant moet dan ook wel het inzicht kunnen krijgen om te kunnen beoordelen of op alle niveaus aan eisen wordt voldaan. In EU-SEC wordt de gedachte van supply chain toegepast.

Een auditor die cloud security-projecten beoordeelt, moet deze structuren ook kennen en snappen. Om deze reden worden in het kader van EU-SEC cloud security bekwaamheidseisen toegevoegd aan het kennispallet van de auditor. Het gaat concreet om certificeringen als CCSK en STAR Auditor (beide van de CSA), CCSP (ISC2) en, momenteel nog ongedefinieerd, overige relevante kennis. Maar daarbij zou te denken zijn aan wat binnen Norea-termen gebruikelijk is als kennis- en ervaringseisen. EU-SEC beschouwt de auditor in deze context:



Figuur 2: Context van de auditor

Ook ten aanzien van bijvoorbeeld *audit evidence* worden eisen geïnventariseerd. En ook dat bleek complexer dan op voorhand gedacht. Vanuit verschillende kaders, wetten en regels, maar ook vanuit verschillende belanghebbenden bleken verschillen te bestaan. Op zich is het feit dat er verschillen bestaan niet heel erg, maar zeker in het kader van MPR (Multi-Party Recognition) is het essentieel om in ieder geval de bewijsvoering eenduidig te hebben. In onderstaande afbeelding is een korte analyse van deze eisen te zien.



Figuur 3: Bewaartermijnen voor bewijs (in relatie tot verschillende kaders)

Er waren ook al geautomatiseerde hulpmiddelen van bijvoorbeeld de CSA (STARWatch) en het Fraunhofer Institut (Clouditor, zie https://github.com/clouditor/clouditor voor de open source community versie). Vanuit het ontwikkelde raamwerk zijn de tools uitgebreid en binnen de EU-SEC auditaanpak werden de requirements, beheersmaatregelen en tools goed op elkaar afgestemd. Zo zijn voor de Continuous Auditing certificeringsfaciliteiten meerdere nieuwe audit-API's gespecificeerd, waardoor auditors in staat zijn om continu de verwerking van CSP's te monitoren en auditen.

Op dit moment is het programma de pilot-audits aan het afwerken. Vanuit de doelstelling zijn twee pilots ontwikkeld. Het eerste programma richt zich op het uitvoeren van audits conform de MPR-methode. Het tweede programma toetst de Continuous Auditing aanpak.

Het MPR-programma bestond uit vier pilots. De resultaten van deze vier pilots zijn zeer bemoedigend. De EU-SEC methode blijkt goed bruikbaar en levert toegevoegde waarde, onder meer doordat er door hergebruik van al aanwezige rapporten en bewijsstukken tot tachtig procent minder controlehandelingen hoeven plaats te vinden. De belangrijkste randvoorwaarde is wel dat een CSP die in aanmerking wil komen voor een EU-SEC audit zelf volwassen is op het gebied van security. Bij de pilots hadden alle CSP's een ISO27001-certificering.

Continuous Auditing houdt in dat een Cloud Service Provider aan de Cloud Service Consumer permanent inzicht kan (laten) verschaffen in het niveau van dienstverlening door de CSP en ook in het niveau van beveiliging: geautomatiseerde tools kunnen gebruikmaken van API's om de CSP direct te bevragen.

De resultaten van de continuous auditing-pilot zijn momenteel (voorjaar 2019) nog niet in detail bekend.

What's next…

Allemaal mooi en aardig, maar wat heb ik eraan? Dat hangt een beetje af van je rol. Feit is dat vrijwel elke organisatie al gebruikmaakt van clouddiensten. Feit is ook dat er onduidelijkheid bestaat over de stand van zaken op het gebied van compliance en governance. Dus misschien is het niet nu relevant, maar voor de volgende doelgroepen zien we al wel toepassingsmogelijkheden:

- Voor een auditor is het EU-SEC framework een waardevol hulpmiddel. De audit requirements en de aanpak is volkomen in lijn met de vigerende standaarden en de aanvulling met tools voor met name cloudomgevingen is een bruikbare innovatie.
- Voor een provider van clouddiensten die op een efficiënte manier wilt aantonen in control te zijn, is het EU-SEC een interessante optie. Omdat EU-SEC nog in de innovatieprojectfase verkeert, is het nog geen formeel geadopteerde standaard. Maar de consortiumpartners verwachten dat de EU en daarna ook de lidstaten het zullen overnemen. Dat betekent dat een aanbieder van diensten daarop voorbereid kan zijn door gebruik te maken van deze kennis en nu al aan te sluiten op de cloud *controls matrix*.
- Voor aanbesteding van clouddiensten is op dit moment toepassen van de CAIQ-methode van de CSA al bruikbaar, maar voor het inrichten van beheersmaatregelen biedt EU-SEC aanvullende handvatten.

Op de projectsite zijn onder meer de volgende documenten te vinden:

- Requirementsanalyses
- Methodes en architecturen
- Beschrijvingen van tools en aanpak
- Auditrapporten van de pilotaudits
- Mocht je inhoudelijk meer willen weten, aarzel niet om contact op te nemen.

Mocht je inhoudelijk meer willen weten, aarzel niet om contact op te nemen.

André (A) Koot RE | Consultant bij *Nixu*

André Koot houdt zich bij Nixu vooral bezig met Identity & Access Management. Hij is voormalig (hoofd)redacteur van het blad InformatieBeveiliging van het PvIB. Hij is bereikbaar via andre.koot@nixu.com