AUDIT MAGAZINE

ARTIKELEN | 1 OKTOBER 2020

OPEN GRENZEN IN DE CLOUD

Auteur: Tekst Drs. André Koot RE

Leestijd: 6 min

Dit artikel is eerder gepubliceerd op deitauditor.nl.

Open grenzen, dat was een belangrijke missie van de EU. 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 binnen het Schengengebied blijft, dan ben je het concept 'grens' eigenlijk allang vergeten. Ook in de virtuele wereld merken we niets van grenzen.

Maar dat blijkt een enorme misvatting. Dankzij wet- en regelgeving op het gebied van informatie- en privacybescherming, is er helemaal geen sprake van vrij dataverkeer. 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.

Geen eenduidigheid

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 nationale wetten en regelgeving. Bijvoorbeeld: 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). En bij voorkeur ISO27001 gecertificeerd zijn en een ISAE3402-verklaring hebben. Een volstrekt logische set eisen. Maar wel een set eisen waar een CSP uit bijvoorbeeld de Tsjechische Republiek niet aan kan voldoen: die kent de BIO niet en als die CSP al ISO27K gecertificeerd is, dan zegt dat eigenlijk alleen dat er een Information Security Management System (ISMS) bestaat, niet of die partij ook BIO-compliant is.

Of die CSP de noodzakelijke passende beveiligingsmaatregelen voor clouddiensten voor de Nederlandse overheid levert, is daar niet zomaar uit af te leiden. Het stellen van de genoemde eisen betekent in de praktijk dat de Nederlandse overheid het buitenlandse partijen onmogelijk maakt om clouddiensten te leveren aan de Nederlandse overheid. Met andere woorden, er is sprake van 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 is de eis van toezichthouders om het mogelijk te maken dat zij permanent de betrouwbaarheid van geautomatiseerde verwerkingen kunnen vaststellen. Waar een bank tien jaar geleden de primaire processen nog volledig in eigen hand had en de systemen in eigen rekencentra draai-den, is de transitie naar uitbesteding vandaag de dag 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. Waar vroeger de auditors of toezichthouders ter plekke konden meekijken, is dat in de cloud niet meer haalbaar.

En toch moet een cloud service provider aan kunnen tonen in control te zijn op het gebied van security. De landsgrenzen beperken voor CSP's nog steeds de mogelijkheid om over grenzen diensten aan te kunnen bieden. Dit staat haaks op het gedachtegoed van de EU, namelijk het wegnemen van han-delsbarrières. Het wegnemen van deze barrières is dan ook de belangrijkste drijfveer achter het EU-SEC programma.

EU-SEC

Het EU-SEC programma is onderdeel van het Horizon2020-innovatieprogramma van de Europese Commissie. De doelstelling van dit project is om de blokkades op het gebied van audit en certificeringen te identificeren en weg te nemen. Blokkades ontstaan vooral door de verschillen tussen de wetten en regelgeving van de verschillende lidstaten.

De Cloud Security Alliance (CSA) heeft samen met acht andere partijen (onder andere Nixu) een consortium opgericht om binnen het Horizon2020-programma een certificerings-raamwerk voor clouddiensten te ontwikkelen. Het consortium is in 2017 begonnen met de eerste van zeven deelprojecten, namelijk de requirements-analyse. Namens Nixu was ik de programmamanager voor dit project. In dit project zijn de security- en privacyeisen alsmede eisen op het gebied van auditing, met name ten aanzien van 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 ten aanzien van auditors afgestemd zijn. Hierdoor wordt hergebruik van al uitgevoerde rapportages en certificeringen mogelijk gemaakt.

Cloud controls matrix

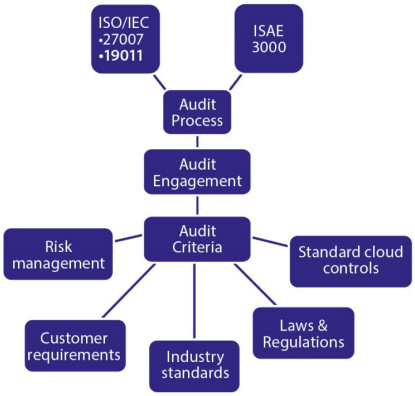
Als basisraamwerk is gebruikgemaakt van de cloud controls matrix (de CCM) van de CSA. Dit instrument is al langer bekend en de CSA heeft op basis hiervan het security trust assurance and risk (STAR) programma opgezet en daarbinnen het STAR-register ontwikkeld. Binnen STAR kunnen CSP's zich laten opnemen als ze op basis van:

- een eigen verklaring kunnen aangeven dat ze voldoen aan CCM;
- een extern auditverslag (door een STAR-auditor) kunnen aangeven dat ze voldoen aan CCM;
- een continuous auditingattestatie kunnen aangeven dat ze voldoen aan CCM.

Op basis van de geïnventariseerde requirements is een multi party recognition framework (MPRF) en een continuous auditing based certification (CABC) aanpak met een controlarchitectuur opgezet en zijn tools (door)ontwikkeld om de audits te kunnen faciliteren. Het control framework bevat onder meer verschillende soorten auditmethoden voor bijvoorbeeld ISO27000-achtige certificeringen en voor ISAE3000-achtige certificeringen.

Auditoptiek

Op het gebied van auditing leverde dat interessante inzichten op. Er werden verschillende auditkaders beoordeeld (inclusief de relevante ISO-standaarden) en er zijn eisen ten aanzien van het auditproces, de bewijsvoering, maar ook eisen ten aanzien van de auditor en de auditorganisatie geanalyseerd (zie *figuur 1*).

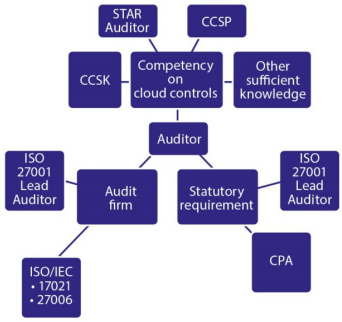


Figuur 1. Standaardaanpak voor auditing Information Security Management Systems

Gaandeweg de analyse werd duidelijk dat het uitvoeren van een ISO27000-audit in belangrijke mate afwijkt van het uitvoeren van een ISAE3402-audit. De auditprocessen zijn grotendeels hetzelfde, maar het grootste verschil is dat bij op ISAE3000 gebaseerde audits een historisch bewijs van de effectiviteit van de werking van de beheersmaatregelen gedurende een bepaalde tijd (bijvoorbeeld twaalf maanden) moet worden geleverd.

Ook werd geconstateerd dat materiekennis op het gebied van cloud security bij de auditor onmisbaar is. De cloud kent namelijk diverse gelaagdheden, die je onder de noemer supply chain kunt vatten: een cloud service consumer kan een software-as-a-service (SaaS) dienst afnemen, denk aan een hrm-systeem. De afnemer stelt eisen aan de dienstverlener, onder andere ten aanzien van privacy en security. Maar deze SaaS-provider kan zelf ook weer diensten van andere providers afnemen, zoals platformen of (gevirtualiseerde cloud) infrastructuren en zelfs ook andere SaaS-oplossingen. De supply-chaingedachte 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 krijgen om te kunnen beoordelen of op alle niveaus aan eisen wordt voldaan.

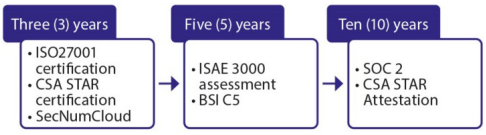
Een auditor die cloud-securityprojecten beoordeelt, moet deze supply-chainconcepten kennen en snappen. Om deze reden worden in het kader van EU-SEC cloud security bekwaamheidseisen toegevoegd aan het kennispallet van de auditor. Het gaat concreet om certificeringen als CCSK en STAR Auditor (beide van de CSA), CCSP (ISC2) maar ook over kennis- en ervaringseisen. Zie *figuur 2* voor hoe de EU-SEC de auditor in deze context beschouwt.



Figuur 2. Context van de auditor

Audit evidence

Ook ten aanzien van bijvoorbeeld audit evidence werden eisen geïnventariseerd. En ook dat bleek complexer dan op voorhand gedacht. Vanuit verschillende kaders, wetten en regels, maar ook vanuit verschillende belanghebbenden bleken aanzienlijke verschillen te bestaan ten aanzien van de bewaartermijnen van bewijs (zie *figuur 3*).



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

Voor auditdoeleinden bestaan geautomatiseerde hulpmidde-len van bijvoorbeeld de CSA (STARWatch) en het Fraunhofer Institut (Clouditor, zie https://github.com/clouditor/clouditor voor de open source communityversie). Vanuit het ontwikkelde raamwerk zijn de tools uitgebreid en binnen de EU-SEC-auditaanpak werden requirements, beheersmaatregelen en tools goed op elkaar afgestemd. Zo zijn voor de CABC-certificeringsfaciliteiten meerdere nieuwe API's (application programming interfaces) ontwikkeld, waardoor auditors in staat zijn om continu, geautomatiseerd, de verwer-king van CSP's te monitoren en auditen.

Pilots

Binnen EU-SEC zijn twee pilots uitgevoerd. Het eerste programma richt zich op het uitvoeren van audits conform de MPRF-methode. Het tweede programma toetst de CABC-aanpak.

Voor MPRF zijn vier pilots uitgevoerd. De resultaten van deze vier pilots zijn zeer bemoedigend. De aanpak stroomlijnt het auditproces wanneer wederzijdse erkenning van beveiligingseisen kan worden gebruikt om het aantal te auditen beveiligingsmaatregelen te verminderen. MPRF stelt de auditor ook in staat om een gecombineerde audit uit te voeren waarbij meerdere standaarden in één audit kunnen worden beoordeeld, door gebruik te maken van hetzelfde bewijs voor gelijkwaardige vereisten in verschillende standaarden. Uit de pilot bleek dat tot 80% minder controlehandelingen hoeven plaats te vinden. Voor CABC is in de pilot vastgesteld dat efficiency en betrouwbaarheid van de geautomatiseerde compliancetests hoger is dan de traditionele aanpak. Handwerk blijft nodig, maar CABC is een geavanceerde aanvulling op de periodieke audit.

'What's in it for me?'

Dat is nog niet helemaal duidelijk, EU-SEC is momenteel nog geen verplichte standaard, 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 wil aantonen in control te zijn, is het EU-SEC waardevol. EU-SEC is nog geen formeel geadopteerde standaard, maar CABC is al erkend binnen EC CSPCert (het nieuwe cloudcertificeringsschema dat door ENISA, dit EU-agentschap dat verantwoordelijk is voor Europese securitykaders, wordt ontwikkeld), ENISA was lid van de raad van advies van EU-SEC.

Op de projectsite van EU-SEC zijn alle relevante documenten te vinden.[1]

Noot

1. www.sec-cert.eu

Over
André Koot is principal consultant bij Nixu en houdt zich 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

Tags: informatiebeveiliging, IT-audit

Bron url: https://auditmagazine.nl/artikelen/open-grenzen-in-de-cloud/