SECURITY EN GDPR/AVG

COMPLIONS-GRC ZOEKT PARTNERS DIE DE KLANT IN CONTROL WILLEN LATEN ZIJN

**Ron Boscu &
Frans Broekhof**

In deze uitgave van ChannelConnect staan security en de AVG/GDPR centraal. Het eerste is in vertrouwde handen van leveranciers met in de regel een lang trackrecord. Het tweede wordt opmerkelijk vaak opgepakt door bedrijven die minder lang actief zijn. Een uitzondering op dat laatste is CompLions-GRC uit Deventer. Met de directie, Ron Boscu en Frans Broekhof, werd gesproken over die bijzondere positie en uiteraard de eigen dienstverlening.

door: Rashid Niamat | fotografie: Andrea Bartosova

Medeoprichter en huidig sales director Ron Boscu begint het gesprek en gaat daarvoor terug in de tijd. “In 2005 was ik medeverantwoordelijk voor drie datacenters. In die tijd kwamen de eerste vragen van klanten die wilden weten of wij onze zaken wel goed voor elkaar hadden. Het draaide specifiek om informatiebeveiliging en kwaliteit. Die klanten gaven ook aan dat ze dit niet meer in contracten en SLA’s vastgelegd wilden zien. Zij wilden namelijk de zekerheid dat de opdrachtnemer objectief gemeten de zaken voor elkaar had. Met andere woorden: ze vroegen om certificeringen.” Als eersten waren dat overheden, enterprises en de zorgsector. Boscu voorzag dat die trend zich zou doorzetten. Ook kleinere organisaties, zoals datacenters, zijn immers vaak essentiële schakels in waardeketens en zouden er vroeg of laat mee te maken krijgen.

Boscu beschrijft verder hoe toen de certificerings- en audittrajecten verliepen. Het was bijna uitsluitend de business van de grote consultancybureaus die enterprisetarieven hanteerden voor strikt genomen te kleine bedrijven die geen alternatief hadden. Belangrijk was tevens dat die consultants te weinig deden om de bedrijven de vereiste kennis en middelen te verschaffen. Er was weliswaar sprake van tooling, software waarmee de processen beschreven en gecontroleerd konden worden, maar die was er puur voor de auditors.

Start van CompLions

Die praktijkervaring en zoals hij zegt frustratie deden Boscu besluiten zelf tooling te gaan ontwikkelen, specifiek bedoeld voor met name mkb en mkb+. In 2008 werd CompLions opgericht. De eisen waaraan de tooling moest voldoen, waren helder. Boscu: “Onze visie en missie kwamen tot uitdrukking in de slogan, te leveren op basis van het ‘fixed price & fixed date’-principe. Daaraan verbonden was de belofte geen vendor-lock-in of andere afhankelijkheid te creëren. We gingen mensen leren vissen in plaats van ze elke keer een vis te geven.”

Ron Boscu

‘We leren mensen vissen in plaats van ze elke keer een vis te geven’

CompLions heeft weliswaar vanaf de start gefocust op mkb en mkb+, maar ondertussen nemen ook er andere sectoren en segmenten de dienstverlening af. Overheden, zorginstellingen en enterprises zijn overtuigd van de voordelen en behoren inmiddels tot de klantenkring. Zij kiezen voor CompLions-GRC onder andere omdat ze merken dat de periodieke audits eigenlijk niet voldoen. Die momentopnames zijn niet geschikt om aan te tonen dat men permanent in control is. Die traditionele manier van werken, met het inschakelen van externe partijen en die rapportages laten maken, wordt als te traag, te star en te duur ervaren. “Als je weet dat dat speelt in de boardrooms en je ziet wat de trackrecord van CompLions-GRC is, dan begrijp je ook waarom ik enthousiast over dit bedrijf ben. We hebben een enorme markt voor ons liggen en dan is er ook nog de AVG/GDPR waaraan iedereen uiterlijk 25 mei 2018 moet voldoen.”

AVG/GDPR van gedoe naar gemak

“De AVG/GDPR betekent dat iedereen inzichtelijk moet maken welke concrete maatregelen zijn getroffen om aan de verordening te voldoen”, zegt Boscu. “Het is echter niet alleen een momentopname. Er moet sprake zijn van een compleet overzicht, dossiervorming dus. Dat is vanzelfsprekend met onze GRC-tooling mogelijk en het is geïntegreerd. Dat komt door onze ‘Map Once, Comply to Many’-aanpak. Alles wat je hebt gedaan om bijvoorbeeld aan de actuele ISO27001-certificeringseisen te voldoen, wat ook voor de AVG/GDPR relevant is, laat onze tooling direct zien. Het toont aan waarom je met tooling beter uit bent dan met de traditionele methodieken waarbij voor elk traject weer een nieuwe certificeringsdeskundige en daarna auditor moet langskomen. AVG/GDPR-compliant worden met onze tooling betekent geen gedoe meer en dubbel werk maar gemak.” »

CompLions werd zo de eerste aanbieder in Nederland van dat soort GRC (Governance, Risk en Compliancy) tooling, ontwikkeld voor ondernemers uit het mkb en mkb+. Met deze tooling krijgen de ondernemers niet alleen optimaal inzicht of ze aan de eisen voor bijvoorbeeld kwaliteit en informatiebeveiliging voldoen. Het maakt ook continue kwaliteitsverbetering volgens de PDCA-cyclus (Plan Do Check Act) een stuk makkelijker door te voeren. Verder vergen periodieke audits door derden minder tijd en daarmee minder kosten omdat er permanent en op uniforme wijze wordt bijgehouden wat relevant is voor een groot aantal certificeringen en andere kwaliteitseisen (naast ISO en NEN onder andere nog BIG en ISAE3402).

Governance Risk and Compliancy made easy

Het bedrijf, dat als slogan ‘Governance Risk and Compliancy made easy’ gebruikte, bleek een schot in de roos en het succes bleef niet onopgemerkt. In 2015 bracht een grotere consultancyorganisatie een bod uit op CompLions. Dat leidde ertoe dat in 2016 de consultancytak werd verkocht en de softwareontwikkeling de volledige focus kreeg. Boscu: “We hadden inmiddels een goede reputatie in de markt en een groeiend aantal klanten. Mensen die ermee gewerkt hadden en van werkgever waren gewisseld, vroegen ons of ze de dienst zonder verdere ondersteuning konden afnemen. Ze hadden immers de ervaring al en wisten hoe makkelijk het in gebruik was.” Dat krachtige signaal bevestigde voor CompLions dat het een softwareontwikkelaar moest blijven. Voor ondersteuning en implementaties vertrouwde het op samenwerking met externe partners.

Andere marktsegmenten

In 2017 maakte het bedrijf een doorstart en kwam Frans Broekhof als CEO aan boord. Broekhof, die zijn sporen reeds verdiend had bij tal van andere bedrijven, vertelt waarom hij deze stap maakte. “Het begon uit pure belangstelling, maar al snel was duidelijk dat dit een heel mooi bedrijf is met interessante dienstverlening en enorm veel potentie.”

Continuïteitsregeling

De GRC-tooling van CompLions-GRC wordt aangeboden als een SaaS-oplossing en voor instanties die niet vanuit de cloud kunnen werken is er een on-premise-variant. De SaaS-oplossing is het meest gevraagd. Alle data die de klant nodig heeft om te laten zien dat hij aan de AVG/ GDPR-eisen voldoet staat dan wel extern. Natuurlijk leidt dat tot de vraag hoe hij er zeker van kan zijn daar altijd toegang toe te hebben. Broekhof: "Wij hebben daar veel tijd in geïnvesteerd en zijn tot een voor de sector unieke oplossing gekomen. Er is een aparte stichting opgericht waar de directie van CompLions-GRC geen zitting in heeft. Mocht er onverhoopt een omvangrijk incident zijn waardoor CompLions-GRC niet meer aanspreekbaar is, dan neemt de stichting de werkzaamheden direct over en garandeert zo de continuïteit van de dienstverlening." Met de klanten is deze zogenaamde Escrow-overeenkomst per afzonderlijk contract geregeld. Zij hebben hierdoor de garantie altijd bij de data en de applicatie te kunnen, wat belangrijk is om aan de AVG/GDPR te voldoen en andere eisen vanuit de wetgeving gebaseerd op omgekeerde bewijslast.

'Onze tooling voorkomt dubbel werk'

De aandacht voor continuïteit kan volgens Boscu niet los worden gezien van de aandacht voor de eigen kwaliteit. "De Escrow-regeling lijkt misschien iets dat vooral de enterprise- en overheids-klanten zal aanspreken. Dat is echter niet waarom wij deze stap hebben genomen. Wij willen met de tooling én de dienst-verlening gewoon de beste aanbieder in Nederland zijn." Daarom heeft het bedrijf vanaf de start de Verklaring Omtrent het Gedrag (VOG) verplicht gesteld voor alle medewerkers. Verder wordt de appli-catie volledig in Nederland ontwikkeld en beheerd. De data staat in Nederlandse datacenters die vanzelfsprekend aan alle ter zake doende certificeringen voldoen. Last but not least is CompLions-GRC uiteraard zelf ook o.a. ISO27001 gecertificeerd.

Meer partners

CompLions-GRC heeft een aantal doelstellingen voor de komende periode geformuleerd. Broekhof: "Wij hebben de ambitie, zonder afbreuk te doen aan de hoge kwaliteit, meer klanten te bedienen. Daarvoor kijken we naar extra partners die op zoek zijn naar new business en begrijpen dat AVG/ GDPR een uniek momentum biedt om de dienstverlening uit te breiden. We kijken daarvoor naar vier type bedrijven: accountantskantoren, juridische dienst-verleners, consultants en IT-bedrijven." Wat CompLions-GRC hen biedt is in de woorden van Broekhof een noodzake-lijke vulling van de gereedschapskist waardoor aan de eisen wordt voldaan die een auditor – en in het geval van de AVG/GDPR: de AP – aan rapportages en inzichten stelt.

Broekhof: "We hebben recent onder-zoek laten doen naar het aanbod van AVG/GDPR-oplossingen die aan de Nederlandse markt worden gepresenteerd. Dat leverde een beeld op van een volstrekte wirwar aan deeloplossingen en veel vendor-lock-ins. CompLions-GRC is uit de bus gekomen als één van de weinige aanbieders in deze markt met een transparante dienst die maximaal op integratie en overzichtelijkheid is ingesteld. Verder scoren we goed omdat onze tooling de klant zelf kennis laat opbouwen en behouden."

Boscu en Broekhof nodigen dienst-verleners uit, die de klanten ook 'in control' willen laten zijn en daarvoor op zoek zijn naar degelijke, overzichtelijke tooling, kennis te komen maken met CompLions-GRC. Dankzij de 'Map Once, Comply to Many'-benadering, unieke ervaring en uitgebreide sectorale kennis biedt de GRC-tooling ongekende integratiemogelijkheden en efficiency-verbeteringen. Dat is waar een steeds groter deel van de markt om vraagt en waar voor partners mooie business kansen liggen. «

Frans Broekhof

info@complions.com | 31 (0)570 634 717 | @CompLionsGRC