2017 Quick scan self-assessement - uitbesteding en informatiebeveiliging m.b.t. alarmcentralediensten

Vraag	Ja	Nee	N.V.T.	Toelichting/bewijsvoering
Beschikt u over een geldige ISAE3402 certificering?				
Zo niet, staat er gepland dit binnen nu en 12 maanden gerealiseerd te hebben?				
Zo wel, betreft dit een ISAE3402 type 1 of type 2 certificering?				
Zo wel, bent u bereid het ISAE scope document met ons te delen?				
Indien u ISAE3402 type 1 certificering heeft, heeft u gepland type 2 certificering te behalen? En zo ja, wanneer.				
Beschikt u over een geldige ISO27001 certificering?				
Zo niet, staat er gepland dit binnen nu en 12 maanden gerealiseerd te hebben?				
Zo wel, bent u bereid het scope document van de ISO27001 certificering met ons te delen?				
Heeft u met uw leveranciers de informatiebeveiligingseisen om risico's te verlagen die verband houden met de toegang van de leverancier tot de bedrijfsmiddelen van de organisatie, contractueel overeengekomen en gedocumenteerd?				
Beschikken al uw medewerkers, die toegang hebben tot informatie zoals door ons aangeleverd of door u via onze verzekerden verkregen, over een getekende geheimhoudingsverklaring en VOG verklaring?				

Heeft u als organisatie m.b.t. bedrijfscontinuïteit (o.a. datarecovery, power, co-locatie, mensen, financieel) alle benodigde en passende beheersmaatregelen geëffectueerd?				
Zo ja, bent u bereid de genomen beheersmaatregelen met ons te delen?				
Zo niet, welke beheersmaatregelen ontbreken nog?				
Heeft u een vastomlijnd proces voor het signaleren en registreren van incidenten op het gebied van informatiebeveiliging?				
Heeft u een security officer binnen uw bedrijf? Zo ja, graag de contactgegevens in de toelichting.				
Heeft u in de afgelopen 24 maanden wel eens te maken gehad met een informatiebeveiligingsincident?				
Heeft u beleid op gebied van functiescheiding en autorisatieniveaus binnen uw operationele en financiële systemen?				
Wordt er informatie uitgewisseld tussen de verschillende systemen binnen en buiten uw bedrijf?				
Is deze uitwisseling beveiligd op basis van geaccepteerde standaarden (zoals sftp, TLS)?				
Heeft u nog andere zaken te melden die van belang kunnen zijn voor het verkrijgen van inzicht in de mate waarin u voorziet in beheerste uitbesteding en/of informatiebeveiligingsrisico's?				
Zo ja, graag toelichting.				

FAQ

Vraag: Mijn leverancier heeft alle vragen m.b.t. certificeringen met “NEE” beantwoord, lopen wij nu een verhoogd risico?
Antwoord: Dat is niet met ja of nee te beantwoorden. Beschikt uw leverancier niet over bepaalde certificaten dan kan het nog steeds een prima partner zijn om mee samen te werken. Er rust dan een zwaardere verplichting op u als uitbestedende opdrachtgever om zich ervan te vergewissen dat bijv. informatiebeveiliging goed is georganiseerd. Niet iedereen beschikt over de expertise om dit op een goede manier te onderzoeken. Het is ook goed mogelijk dat uw leverancier alle maatregelen op het juiste niveau heeft geïmplementeerd, het is alleen niet onafhankelijk vastgesteld. Het wel of niet onafhankelijk vaststellen doet aan de maatregel zelf immers niks af.

Vraag: Mijn leverancier heeft wel certificaten maar heeft op andere vragen “NEE” als antwoord, hoe kan dat?
Antwoord: Het kan goed zijn dat bepaalde risico’s voor uw leverancier op een andere wijze zijn beoordeeld en er daarom geen beheersmaatregelen zijn genomen, de auditor deze afweging accordeert en uw leverancier voor certificering in aanmerking komt. In zo’n geval kunt u vragen naar het “scope-document”. Daarin staat beschreven welke scope de certificering heeft en vaak leest u daarin ook welke afwegingen er zijn gemaakt. Bent u het eens met deze afweging dan is er weinig aan de hand. U kunt als opdrachtgever uiteraard ook altijd extra eisen overeenkomen als u dat nodig vindt. Er dient wel opgemerkt te worden dat de items in deze quick scan dusdanig basaal zijn dat het op zijn minst opmerkelijk is wanneer gecertificeerde organisaties de overige items met “NEE” beantwoorden.

Vraag: Zijn we niet enorm aan het doorschieten m.b.t. eisen rondom uitbesteding en informatiebeveiliging?
Antwoord: We kunnen ons dat gevoel in eerste instantie goed voorstellen. Wanneer er langer stilgestaan wordt bij de impact die het heeft op u als opdrachtgever en uw klant als gebruiker van de service dan wordt die mening meestal snel bijgesteld. Er geldt immers: RISICO = IMPACT X VERSCHIJNINGSKANS. Het is een onderdeel geworden van de hedendaagse professionele bedrijfsvoering.

Vraag: Welke kosten zijn hier wel niet mee gemoeid?
Antwoord: Hoewel dit voor elke organisatie anders ligt, zijn de kosten niet gering. Denk niet alleen aan de certificeringskosten (jaarlijkse audits, etc.) maar ook aan de arbeidsuren die gepaard gaan met de interne controle, beheren van processen op interne en externe ontwikkelingen, steeds stijgende eisen door voortschrijdende technieken en bedreigingen. Realiseer u wel dat deze kosten allemaal in het niet vallen wanneer uw klant of klantgroep benadeeld is door een datalek of de opgelopen merkschade wanneer u groot in de krant komt te staan.

Vraag: Waarom stellen jullie deze quick scan ter beschikking?
Antwoord: Wij zien dat er nog ruimte voor verbetering is in de mate waarin gekeken wordt naar de risico’s die gepaard gaan met samenwerken met een alarmcentrale. Wij realiseren ons dat wanneer er onverhoopt dingen fout gaan dit waarschijnlijk zijn weerslag heeft op allerlei eisen die dwingend worden opgelegd. Wij zijn van mening dat het voor iedereen beter is dit voor te zijn en de zaken gewoon goed te regelen, pro-actief.