INFORMATION SECURITY

In veel organisaties zijn er feitelijk geen fysieke processen meer. Alles wat de organisatie ingaat en uitgaat en alles wat de organisatie in beweging zet, zijn virtuele data. Soms is er nog sprake van een papierstroom, maar ook dat neemt snel af. Sinds de Coronacrisis zijn zelfs vergaderingen steeds vaker digitaal. Dat betekent dus ook dat al deze processen tot stilstand kunnen komen als de digitale infrastructuur wordt aangevallen. Informatiebeveiliging moet daarom een essentieel onderdeel zijn van de governance en het risicomanagement. Maar het is wel een onderdeel dat om specifieke deskundigheid én visie vraagt. Lees hier onze visie op Information Security.

INTEGRATIE IN DE GOVERNANCE

Chaos is de vijand van security. Informatiebeveiliging verschilt van andere vormen van risicobeheersing door de complexiteit van ICT-systemen, de omvangrijkheid van normenkaders en de vereiste kennis. Het is een specifieke tak van sport, maar een gestructureerde aanpak blijft evenzeer essentieel. Onze kennis en ervaring op het gebied van governance en risicobeheersing kunnen u helpen om structuur en overzicht te brengen. Vanuit onze achtergrond hanteren wij een logische aanpak die uitgaat van processen, risico's en controls (interne controleraamwerk) en een vertaling van risicobereidheid en normenkaders naar een helder plan van aanpak.

Deze logische en heldere aanpak zorgt voor meer inzicht en een beter bewustzijn, waardoor het bestuur meer grip gaat krijgen op informatiebeveiliging.

SPECIFIEKE DESKUNDIGHEID

Voordat wij met onze dienstverlening zijn gestart, zijn we eerst gaan studeren. Onze collega's zijn opgeleid met een HBO- opleiding in Security Management, als CISA en we studeren verder, onder meer voor certificering als CISM (certified information securitymanager). Ook werven we technische expertise en desnoods huren we onderdelen in.

Vanuit InAudit Information Security nemen we kennis en ervaring serieus en zullen we hierin blijven investeren. Onze deskundigheid is anders dan van veel technisch georiënteerde specialisten. Voor ons zijn zaken als uw normenkader, uw informatiebeveiligings-beleid, risicoanalyse en interne beheersing het vertrekpunt. De techniek volgt daaruit.

EEN PRAKTISCHE AANPAK: FIRST THINGS FIRST

Door onze aanpak die begint met het informatie-beveiligingsbeleid en de risicoanalyse die daaruit volgt kunnen we vrij snel de juiste prioriteiten vooropstellen en voorkomen we dat er veel tijd en geld verdwijnt in een soort 'technology push' van securityproducten. Na (grote) incidenten zijn dit vaak de belangrijkste vragen:

1. Is er een effectieve incident response geregeld (en werkt deze) ?
2. Zijn er effectieve back-up en recovery procedures zodat snel kan worden herstart ?
3. Wanneer is het incident ontstaan en is dit tijdig gesignaleerd ?
4. Was de toegangsbeveiliging effectief (gegeven de risicobereidheid van de organisatie) ?

Als grote incidenten naar buiten komen en de oorzaken daarvan, dan blijken toch vaak betrekkelijk eenvoudige zwaktes doorslaggevend te zijn geweest. Daarom is daar onze aanpak op gericht: "first things first".

HELDERE COMMUNICATIE

De wereld van de governance-organen en de wereld van de ICT-technologie hebben soms moeite om elkaar te verstaan. Met name in de hoek van de technologie met zijn stormachtige ontwikkelingen en vele afkortingen is het als bestuurder het gevoel te hebben 'in control' te zijn. Daarin heeft de CISO een belangrijke rol. De CISO moet de taal van beide werelden spreken en het bestuur aan de hand van eenvoudige presentaties en rapportages laten zien waar de organisatie staat qua volwassenheid.

FOCUS OP BEWUSTZIJN EN DE MOTIVATIE VAN MENSEN

"Het grootste IT-beveiligingsrisico zit tussen het toetsen-bord en de bureaustoel". Hoewel hier best nog wel wat op te dingen is, is het zeker zo dat de menselijke factor bij veel incidenten doorslaggevend blijkt te zijn. Daarbij denken we overigens niet alleen aan medewerkers, maar ook aan bestuurders die verzuimen om voldoende te investeren in informatiebeveiliging. Binnen InAudit zijn ook gedragsdeskundigen werkzaam die u kunnen helpen met het verbeteren van het risicobewustzijn en het vertalen van beveiliging naar bewuster en veiliger gedrag.

De CISO (Chief Information Security Officer) is de risicomanager op het gebied van informatie- beveiliging. Bent u op zoek naar een parttime CISO? Lees hier onze oplossing.

ONZE CISO BRENGT DE ONAFHANKELIJKE BLIK VAN BUITEN

InAudit Information Security richt zich op het leveren van deze expertise. Wij kunnen de CISO-rol voor uw organisatie invullen, deskundig, onafhankelijk en met een nuchtere blik van buiten. Hiertoe werven we mensen met relevante expertise en investeren we in de opleiding van onze mensen. Onze achtergrond in governance en bekendheid met normenkaders zorgt ervoor dat we op heldere wijze kunnen communiceren met zowel de bestuurlijke laag als met de IT-specialisten. Tegelijk investeren we ook in kennis en ervaring met de techniek, zodat we ook een goede gesprekspartner zijn voor de IT-specialisten binnen uw organisatie (of daarbuiten als u dit heeft uitbesteed).

PARTTIME CISO

Voor veel kleinere organisaties is de CISO-functie geen fulltime functie, bovendien gaat een goede CISO zich er vervelen. Wellicht leent de volwassenheid van de organisatie ten aanzien van informatiebeveiliging zich ook nog niet voor een CISO. Juist voor deze organisaties kunnen wij een prima service verlenen en zorgen dat er wel de nodige expertise in huis komt, zodat er stappen voorwaarts kunnen worden gezet, zonder daarvoor enorme investeringen zijn vereist.

MEER INFORMATIE

Wilt u meer weten over information security voor uw organisatie? Neem vrijblijvend contact op met onze information security specialist Annebeth Groen via marketing@inaudit.nl

InAudit
Information Security

In Audit
Information Security

Annebeth Groen BBA
Information Security Specialist

"Omdat de informatie binnen uw organisatie het waard is!"