INFORMATIE
BEVEILIGINGS
DIENST

Informatiebeveiliging en de lijnmanager - Wat is uw rol?

Informatiebeveiliging, dat is toch de verantwoordelijkheid van de CISO? Die aanname staat gelijk aan de verwachting dat een voetbaltrainer zelf doelman, spelverdeler en spits is van het team dat hij traint. Iedereen begrijpt dat dit niet kan. De CISO verantwoordelijk houden voor de beveiliging van informatie is even onjuist. Informatiebeveiliging is in de eerste plaats de verantwoordelijkheid van de lijnmanager. Waarom de lijnmanager en niet de CISO? En hoe komt de CISO dan wel in beeld bij informatiebeveiliging? Die vragen beantwoorden we in deze factsheet.

Informatiebeveiliging wordt bereikt door een geschikte verzameling maatregelen in te zetten om met risico's om te gaan, in die zin is het niet anders dan andere risico's voor de bedrijfsvoering waar u ook verantwoordelijk voor bent. Het primaire uitgangspunt voor het bepalen van de benodigde beveiligingsmaatregelen is risicomanagement. Het is uw rol als lijnmanager afwegingen te maken in hoeverre risico's acceptabel zijn. U kent het te beveiligen werkproces en de te beschermen informatie uiteindelijk het best.

Risico's

Afhankelijk van het bedrijfsproces bestaan er risico's rondom informatie(systemen). Informatiebeveiliging gaat over het beheersen van risico's rondom: Beschikbaarheid (Doet het systeem het? Zijn de gegevens er als ze nodig zijn)? Integriteit (Kloppen de gegevens? Zijn deze juist, actueel en volledig? Worden de gegevens alleen gewijzigd door mensen die daartoe gerechtigd zijn?) Vertrouwelijkheid (Zijn gegevens alleen zichtbaar voor mensen die daartoe gerechtigd zijn?)

Voorbeelden van risico's zijn: Een systeem valt uit door een langdurige stroomstoring of internetstoring. Inwoners ontvangen de verkeerde correspondentie door foutieve adresgegevens Een vertrouwelijk collegestuk belandt bij de lokale media

1. Hoe bepaal ik de risico's?

De uiteindelijke doelstelling van informatiebeveiliging is een ongestoorde bedrijfsvoering. Als lijnmanager wilt u voorkomen dat informatie in verkeerde handen komt of dat verkeerde informatie in het systeem wordt verwerkt. Het is uiteraard ook van belang dat het systeem waarmee u informatie verwerkt beschikbaar is. Wie mag informatie raadplegen en wie mag gegevens verwerken? En wanneer moet het systeem in ieder geval beschikbaar zijn? Dat zijn vragen die u als lijnmanager moet beantwoorden. De antwoorden zijn de basis voor een ongestoorde bedrijfsvoering door het toepassen van passende beveiligings-maatregelen.

2. Hoe bepaal ik wat een acceptabel beveiligingsniveau is?

Een belangrijke taak van de lijnmanager is om aan te geven welke mate van vertrouwelijkheid verbonden is aan de gegevens, die in het informatiesysteem worden verwerkt. Op basis van de classificatie van informatie worden de risico's bepaald die aan het werken met (of verwerken van) de gegevens verbonden zijn. Een voorbeeld: de BRP bevat vertrouwelijke, authentieke persoonsgegevens, die binnen de gemeentelijke organisatie verplicht worden gebruikt. Dat vereist maatregelen, die waarborgen dat de in de BRP vastgelegde gegevens altijd juist en actueel zijn, maar dat de toegang tot de gegevens niet onbeperkt is.

3. Hoe vul ik mijn verantwoordelijkheid in?

Uw verantwoordelijkheid als lijnmanager voor informatiebeveiliging begint bij het tonen van voorbeeldgedrag. Als u informatiebeveiliging niet serieus neemt, zullen uw medewerkers geen aanleiding zien om zelf wel bewust met informatiebeveiliging om te gaan. Het bevorderen van deze bewustwording is een integraal onderdeel van uw managementtaak. Het hanteren van een gedragscode en het benoemen van beveiligingsbewustzijn als te beoordelen gedragsaspect kan u verder helpen uw verantwoordelijkheid voor informatiebeveiliging in te vullen.

4. Wat gaat er mis als ik niets doe?

Een gebrekkige informatiebeveiliging kan een effectieve bedrijfsvoering in de weg staan. Misschien gaan de maatregelen te ver, waardoor uw medewerkers zich gehinderd voelen in hun werk. Of misschien schieten ze tekort, waardoor gegevens eenvoudig in verkeerde handen kunnen komen. U verliest in ieder geval grip op het proces waarvoor u verantwoordelijk bent. Informatiebeveiliging moet niet van buitenaf worden opgelegd, maar onderdeel zijn van de dagelijkse praktijk. Dat kan alleen als u als lijnmanager uw verantwoordelijkheid ten aanzien van informatiebeveiliging neemt. U weet als geen ander welke risico's bestaan ten aanzien van uw bedrijfsproces en de gebruikte gegevens in de praktijk van alledag. Informatiebeveiliging gaat iedereen aan binnen de organisatie. De CISO speelt een belangrijke rol als deskundige op het gebied van informatiebeveiliging en als coördinator van de binnen de gemeente te treffen beveiligingsmaatregelen. Maar de verantwoordelijkheid ligt te allen tijde bij u als lijnmanager.

Hoe kan de CISO u helpen?

- Door u te helpen om beveiligingsrisico's gestructureerd in beeld te brengen.
- Door te adviseren over een multidisciplinair team met inhoudelijke kennis, systeem- en applicatiekennis om na te denken over de te treffen beveiligingsmaatregelen.
- Door te adviseren bij de classificatie van informatie.
- Door te adviseren over maatregelen om de beschikbaarheid, vertrouwelijkheid en integriteit van informatie(systemen) te waarborgen.
- Door ondersteuning te leveren bij het vergroten en handhaven van het veiligheidsbewustzijn van medewerkers.

VNG Realisatie