LEG EERST EEN **GOEDE** BASIS

Eindelijk begint het besef dat een goede informatiebeveiliging cruciaal is voor het succes en voortbestaan van organisaties te groeien. Dat mag ook wel, want vanaf 1 januari 2016 zijn bedrijven verplicht om datalekken te melden wanneer deze nadelige gevolgen hebben voor persoonsgegevens. De Europese Unie werkt op dit moment zelfs aan een nieuwe Europese privacy-verordening die strikte eisen gaat stellen aan organisaties die werken met persoonsgegevens. Boetes tot 100 miljoen euro of 5% van de jaaromzet voor wie zich niet aan de regels houdt zullen ongetwijfeld de aandacht krijgen van veel CEO's en andere topmanagers.

Het zal duidelijk zijn dat we informatiebeveiliging maar beter niet meer aan het toeval overlaten. We doen er verstandig aan om binnen organisaties iemand aan te wijzen die als opdracht meekrijgt de organisatie te ondersteunen bij het minimaliseren van security- en privacy-risico's.

VEEL UITDAGINGEN

Deze persoon wordt vanaf de eerste werkdag geconfronteerd met heel wat uitdagingen. Eentje die ik zelf in de praktijk vaak tegenkom, is dat de juiste achtergrond of expertise ontbreekt. Natuurlijk kan iedereen zich in grote lijnen wel een beeld vormen van de onderwerpen die aangepakt dienen te worden. Maar het borgen van aandacht voor informatiebeveiliging door de gehele organisatie heen, is een behoorlijk uitdagende klus. Zeker als die aandacht ook nog eens vertaald moet worden in concrete maatregelen. Zelfs iemand die wél de nodige achtergrond en expertise bezit, is hier wel even zoet mee.

PRAGMATISCHE AANPAK

Voor veel (vaak kleinere) bedrijven geldt dat er eerst en vooral behoefte is aan een pragmatische aanpak. Daarmee kunnen ze op korte termijn een goede basis leggen en gestructureerd verder bouwen. Een volledige implementatie van NEN-ISO/IEC 27001 en de bijhorende best-practice NEN-ISO/IEC 27002 gaat in veel gevallen te ver. Toch kunnen deze normen wel een goede inspiratiebron vormen. Ze bevatten namelijk wel degelijk goede en voor iedereen bruikbare beheersmaatregelen.

NIEUWE BLOG

Daarom ga ik iedere twee weken op de website van Infosecurity Magazine een blog schrijven waarin ik telkens een beheersmaatregel uit NEN-ISO/IEC 27002 onder de loep neem. Ik probeer dan kort en in begrijpelijke taal toe te lichten wat deze control inhoudt. En wat je in de praktijk kunt doen om er invulling aan te geven. Uiteraard ben je van harte uitgenodigd om ook jouw mening te geven of je ervaringen te delen.

WAAR HEBBEN WE HET OVER?

Bij wijze van aftrap begin ik met een korte uitleg van beide normen. ISO 27001 is een standaard die beschrijft hoe een organisatie ervoor zorgt dat de informatiebeveiliging altijd goed is. Dat gebeurt via een reeks van processen en procedures die ook wel een Information Security Management System (ISMS) wordt genoemd. ISO 27001 beschrijft dus eigenlijk aan welke eisen een goed ISMS dient te voldoen. De achterliggende gedachte is dat wanneer er op de juiste momenten en op de juiste manier aandacht wordt gegeven aan informatiebeveiligingsrisico's, dit continu resulteert in passende maatregelen die het risico tot een acceptabel niveau verlagen.

MAATREGELEN NEMEN

De ISO 27001 geeft in bijlage A een overzicht van een groot aantal organisatorische en technische maatregelen. Deze kunnen genomen worden als het risico hier aanleiding toe geeft. Je zou dus kunnen stellen dat de ISO 27002 een verlengstuk vormt van de ISO 27001. Het is als het ware een handreiking waarin een aantal potentiële maatregelen in detail zijn uitgewerkt zodat je wat te kiezen hebt.

CERTIFICEREN

Het is dus ISO 27001 die er met behulp van een ISMS op toe ziet dat de juiste maatregelen worden geselecteerd en geïmplementeerd. ISO 27002 geeft een opsomming van een flink aantal maatregelen die hierbij ter beschikking staan. Om deze reden is ISO 27001 certificeerbaar, en ISO 27002 niet. Maar vergis je niet. Een auditor kijkt bij certificering van ISO 27001 ook naar de wijze waarop je geselecteerde maatregelen uit de ISO 27002 hebt geïmplementeerd.

Dennis Baaten is eigenaar van Baaten ICT Security en helpt organisaties op organisatorisch en technisch vlak met het opzetten en borgen van een goede informatiebeveiliging