VERANKEREN MET HET INFORMATIEBEVEILIGINGSBELEID

Dennis Baaten schrijft op InfosecurityMagazine.nl een serie blog posts over ISO 27002:2013. In deze serie (waarvan dit deel 3 is) probeert hij deze norm vooral heel praktisch te maken.

De eerste maatregelen uit de ISO 27002:2013 vind je in de hoofdstuk 5, en deze beschrijven dat er een informatiebeveiligingsbeleid is gedefinieerd dat uitlegt hoe de organisatie haar doelstellingen op het gebied van informatiebeveiliging wil bereiken. Bovendien stelt de norm dat een dergelijk beleid goedgekeurd dient te worden door de directie. Er zal dus een en ander vastgelegd dienen te worden, maar het liefst geen enorme pakken papier.

Ik definieer de term informatiebeveiligingsbeleid als de totale verzameling van documenten die samen beschrijven hoe de organisatie haar informatiebeveiliging heeft geregeld. Dat is dus inclusief documenten zoals standaarden, richtlijnen, processen en procedures waarin onderwerp-specifieke zaken separaat zijn uitgewerkt. Echter, in de praktijk is het document met de titel 'informatiebeveiligingsbeleid' vaak een zogenaamd hoogover document waarmee de directie zich expliciet committeert aan informatiebeveiligingsdoelstellingen. Dit document fungeert dan als kapstok voor andere documenten waarin bepaalde onderwerpen in meer detail zijn uitgewerkt.

De inhoud, opbouw en reikwijdte van een dergelijke document (het informatiebeveiligingsbeleid) kan per organisatie verschillen, maar een aantal onderwerpen zie ik vaak terugkomen. Hieronder een opsomming inclusief een korte toelichting.

1. Intentieverklaring - een beschrijving van de algemene doelstellingen van de organisatie (visie/strategie), en als afgeleide hiervan het belang van informatiebeveiliging. De directie spreekt expliciet haar intentie uit om de beschikbaarheid, integriteit en vertrouwelijkheid op een passend niveau te houden.

2. Definities - geef een toelichting op veelgebruikte termen zoals bijvoorbeeld betrouwbaarheid, integriteit, beschikbaarheid, vertrouwelijkheid, informatiebeveiliging en risicoanalyse.

3. Doelstelling - beschrijf het doel van het document zelf. Bijvoorbeeld het realiseren van betrouwbare dienstverlening waarbij er tegen een acceptabel kostenniveau bescherming wordt geboden tegen interne en externe dreigingen.

4. Besturingsmodel - de wijze waarop de organisatie haar informatiebeveiliging wenst te besturen. Dit is de plek om te verwijzen naar een proces wat voorziet in een plan-do-check-act cyclus waarmee de organisatie borgt dat haar informatiebeveiliging actueel en doeltreffend blijft (Information Security Management System).

5. Verantwoordelijkheden - benoem wie er in de organisatie welke verantwoordelijkheid draagt. Bijvoorbeeld de directie als eindverantwoordelijke, de information security officer als onafhankelijke aanjager en controleur van het beleid, en de informatie-eigenaren als verantwoordelijke voor het implementeren van risicoverlagende maatregelen.

6. Consequenties voor de praktijk - om het wat tastbaarder te maken, kan er nog op grote lijnen iets worden gezegd over de impact van het beleid op de praktijk. Denk bijvoorbeeld aan het bepalen van maatregelen en aanverwante prioriteiten door het uitvoeren van risicoanalyses, de wijze en frequenties waarmee controles zullen worden uitgevoerd, en het belang van bewustwording en opleiding van medewerkers.

Een handtekening onder het document, kun je zien als het noodzakelijke (theoretisch!) commitment van de directie voor het realiseren en onderhouden van een passende informatiebeveiliging. Zonder management commitment loop je vast, en is het trekken aan een dood paard. Niet dat management commitment automatisch betekent dat alles van een leien dakje gaat, maar dan heb je in ieder geval iets om op terug te vallen. Het zal meer dan eens voorkomen dat er discussies ontstaan over te nemen maatregelen in het kader van informatiebeveiliging. Zodra je collega's voelen dat ze het met inhoudelijke argumenten niet van je gaan winnen, proberen ze je 'te pakken' op het proces: ''Waar staat dan dat dit nodig is? Is het management het hier wel mee eens?'' In een dergelijk geval ben je blij als er iets op papier staat waar de directie (hiërarchisch boven het operationeel management) zijn handtekening onder heeft gezet.

BELANG VAN DOCUMENTEREN VAAK ONDERSCHAT

De verborgen boodschap in deze blogpost is eigenlijk dat documenteren en accorderen erg belangrijk is. Niet alleen om discussies te winnen, maar ook omdat je hiermee de directie bewust maakt van haar (wettelijke) verantwoordelijkheden, en om aan medewerkers en andere belanghebbenden (klanten, auditors) uit te kunnen leggen hoe er met informatiebeveiliging om wordt gegaan en waarom dat voor de organisatie belangrijk is.

Kortom, doe jezelf een plezier en schrijf dingen op. Verankeren kan niet zonder documenteren. Als het niet op papier staat, dan bestaat het niet.

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.