Informatiebeveiligingsbeleid Koninklijke Bibliotheek

Managementsamenvatting

Informatietechnologie (IT) en informatiemanagement (IM) zijn niet meer weg te denken heden ten dage. Bijna alle processen zijn afhankelijk van een goede en ongestoorde werking van IM en IT. Dat geldt net zo zeer voor het primaire proces, alsook voor secundaire processen en ondersteunende processen als financieel management of *human resource management*. Zonder werkende IT geen dienstverlening, geen research, geen productie, geen facturering, geen uitbetaalde salarissen, geen werkende toegangscontrole, enzovoorts.

Als Nationale Bibliotheek wil de KB dat al haar stakeholders kunnen vertrouwen op haar informatievoorziening. In een tijdgewricht met toenemende cybermisdaad, soms zelfs cyberoorlogsvoering, desinformatie en het groeiende risico opgesloten te raken in een informatiebubble van techgiganten als Google en Facebook is de beschikbaarheid van betrouwbare informatiebronnen misschien wel belangrijker dan ooit.

Daarom is evident dat het hoogste management zich verantwoordelijk weet voor IM en IT. Niemand anders dan de directie heeft die eindverantwoordelijkheid. De directie is dan ook niet alleen verantwoordelijk voor de inrichting en de *governance* van IM en IT- maar ook voor de ongestoorde en veilige werking ervan. We hebben het dan over informatiebeveiliging. Dit is het onderwerp van het onderhavige beleid.

Informatiebeveiliging is direct gerelateerd aan de missie en prioriteiten van de organisatie. De mate waarin aandacht besteed wordt aan informatiebeveiliging is afgeleid van de business impact die inbreuken op de informatiebeveiliging kunnen veroorzaken: er ligt dus altijd een *business case* aan ten grondslag. Het middel van de risicoanalyse bestaat ervoor om een inschatting van de risico's en business cases te maken, om daar vervolgens een passende informatiebeveiligingsstructuur en -maatregelen op te kunnen baseren.

Informatiebeveiliging gaat over alle IT- en informatiemiddelen en -processen, waarbij met name 3 aspecten van belang zijn:

1. **Beschikbaarheid**: werken de middelen/processen, zijn ze "in de lucht"?

2. **Integriteit**: is de inhoud van de informatiestromen beveiligd, dat wil zeggen: is het zeker dat er niet mee geknoeid is of kan worden?

3. **Vertrouwelijkheid**: hebben alleen die mensen toegang tot bepaalde informatie die daartoe gemachtigd zijn, en is het voor anderen ontoegankelijk c.q. onleesbaar?

Een aanvullend aspect dat voor alle 3 van belang is, is *controleerbaarheid*: niet alleen "weten" of iets in orde is, maar dat ook achteraf kunnen "verifiëren".

Informatiebeveiliging is géén primair of secundair proces, *géén care business*, maar als we er niets aan doen gaat het wel ten koste van de care business. Informatiebeveiliging is dus een *business enabler* van de eerste categorie. De directie wil dan ook zorgen voor een goede governance, inclusief *auditing* en *feedback*. We noemen dit I-governance. Het is cruciaal en management commitment is daarbij essentieel.

Dit informatiebeveiligingsbeleid wordt daarom door het algemeen Bestuurscollege van de KB vastgesteld, gedragen door de directie en geldt voor de gehele organisatie, en allen die daarbij betrokken zijn in wat voor functie dan ook.

Betrokkenheid van de directie is dus noodzakelijk, maar niet voldoende. Informatiebeveiliging is namelijk nadrukkelijk ieders verantwoordelijkheid binnen de KB. Dit zal worden uitgedragen zowel langs formele weg, als via bewustwordingscampagnes. Een speciale plek is er daarbij voor het lijnmanagement: die heeft de taak om randvoorwaardelijk en curatief toe te zien op goede informatiebeveiliging.

Kortom, informatiebeveiliging zal het best werken wanneer de hele organisatie participeert. Dit is een continu proces. Dit beleid vormt daarvoor het uitgangspunt. Beschreven worden niet alleen de voornoemde aspecten, maar ook welke rollen ingevuld moeten worden, hoe informatiebeveiliging onderdeel is van de *Planning & Control* cyclus, hoe beveiligingsincidenten aangepakt worden (en beter: hoe ze te voorkómen), welke wettelijke randvoorwaarden bestaan, enzovoorts.

Qua rolverdeling springen een aantal cruciale rollen eruit:

· De Coördinator Informatiebeveiliging *(de Corporate Information Security Officer of CISO*) van de KB: een rol op strategisch niveau. De functionaris Coördinator Informatiebeveiliging ressorteert onder de CIO, heeft zo direct toegang tot de directie en draagt geen lijnverantwoordelijkheid. Zijn taak is te waken over informatiebeveiliging, lastige vragen te stellen, auditing voor te bereiden en beleid en aanbevelingen te formuleren.

· ISM: *Information Security Manager* die op tactisch (en operationeel) niveau opereert en daarmee de verbindende schakel vormt tussen het strategische niveau waarop de Coördinator Informatiebeveiliging opereert, en de dagelijkse inrichting en uitvoering van informatiebeveiliging. deze rol is belegd bij de (security) architect van de afdeling Informatiebeleid.

. CSIRT-KB: het *Computer Security Incident Response Team* van de KB, de brandweer van de informatiebeveiliging, die net als de "gewone" brandweer zowel preventief als curatief opereert.