Waardering van de informatiebeveiliging

Hoe de betrouwbaarheid van informatiesystemen
kwantitatiever kan worden gewaardeerd
en de niveaus objectiever kunnen worden bepaald

dr. Clemens H.J. Willemsen

ISBN: 978-94-0367-615-9

Gedrukt en gepubliceerd door: Managementboek

Inhoudsopgave

Lijst van figuren

Lijst van tabellen

1 Inleiding en leeswijzer

Ik richt mij in dit boekwerk op het onderwerp betrouwbaarheid met als componenten beschikbaarheid, integriteit en vertrouwelijkheid (BIV). Het onderwerp vertrouwelijkheid is uitgebreid besproken in mijn voorgaande boek *"Organisatie van de informatiebeveiliging"* [Willemsen][1] maar er is nog genoeg materie om verder op in te gaan als het om het waarderen of het 'meten' van de betrouwbaarheid gaat.

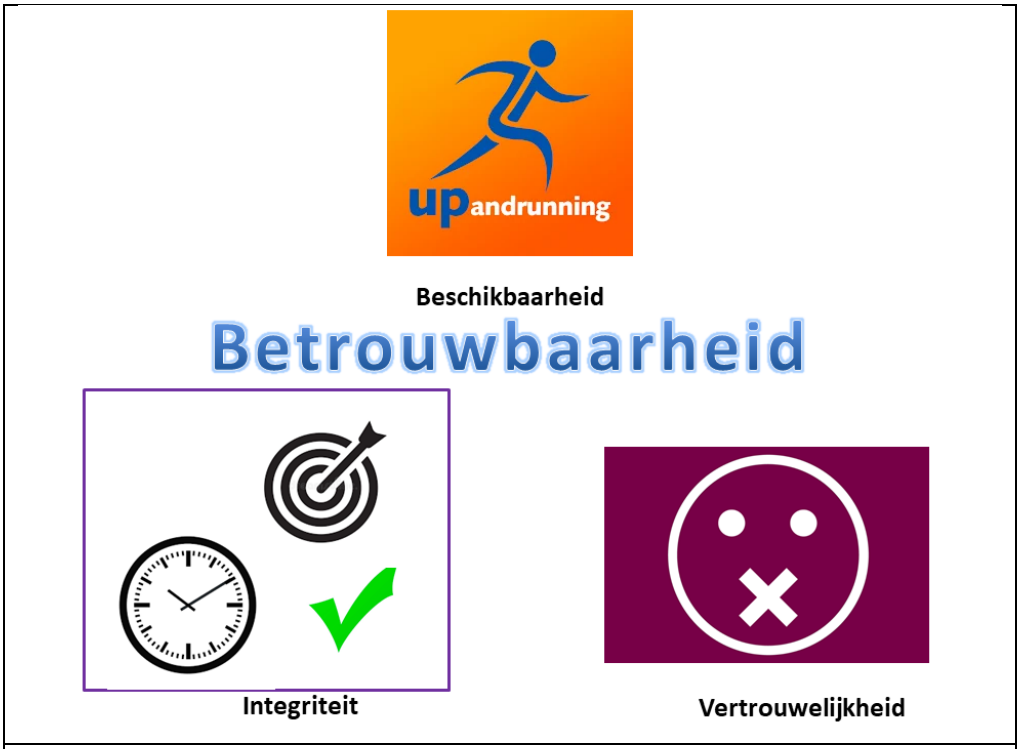

Fig. 1. Onderwerpen van dit boekwerk

Ik ga bewust niet te veel in op de maatregelen die vervolgens genomen kunnen worden om de betrouwbaarheid te waarborgen hetgeen ik verderop onderbouw. "*In de beperking toont zich eerst de meester*" aldus Goethe.

[1] [xx] verwijst naar de literatuurlijst in bijlage 1.

Hoofdstuk 2 gaat in op het doel van dit boekwerk: het kwantitatief maken van de betrouwbaarheid van de informatiebeveiliging. Dat wordt in hoofdstuk 3 per BIV-component uitgesplitst in een beschrijving van de component, de afzonderlijke aspecten, de onderkende niveaus, het meten van de component en de kengetallen. Ook wordt daar ingegaan op mogelijke andere componenten die de betrouwbaarheid zouden kunnen bepalen. Hoofdstuk 4 beschrijft de componenten in samenhang, geeft het proces weer om de niveaus te bepalen en geeft het geheel grafisch weer als een gegevensmodel. Dit mondt uit in een spreadsheet dat kan worden ingevuld en aangepast aan de eigen situatie. Hoofdstuk 5 sluit het geheel af.

2 Betrouwbaarheid kwantitatiever beschreven

De waardering van de betrouwbaarheid van een informatiesysteem is nodig om de werkzaamheden op het gebied van informatiebeveiliging te kunnen prioriteren en in de tijd te kunnen uitzetten met de benodigde financiering daarvan. De beveiliging van een informatiesysteem is nodig om de ongestoorde voortgang van processen mogelijk te maken. Een informatiesysteem in relatie tot een proces ziet er als volgt uit.

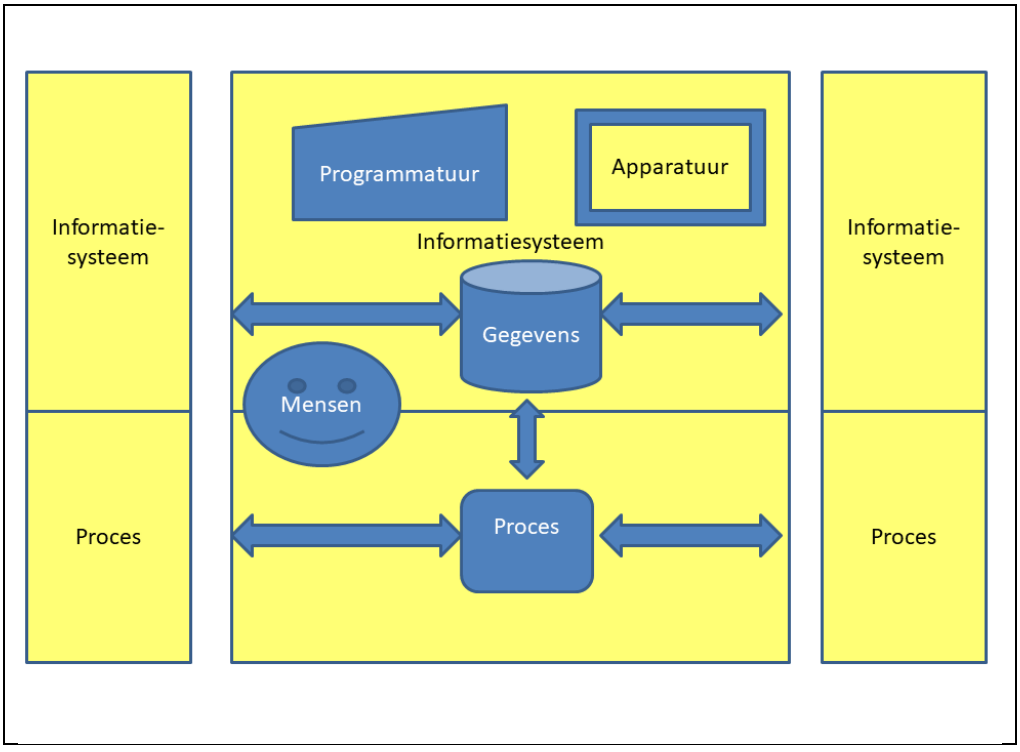

Fig. 2. Informatiesysteem

Het informatiesysteem bestaat uit een samenspel van programmatuur, apparatuur, gegevens en de mens waarmee het proces wordt ondersteund of aangestuurd. Informatiesystemen kunnen onderling gekoppeld zijn en gegevens uitwisselen waarbij processen tal van fysieke of digitale producten kunnen uitwisselen. De mens speelt zowel een rol in het informatiesysteem als gebruiker of beheerder plus de mens is betrokken in het proces als medewerker, afnemer of anderzijds.

Dit boekwerk probeert op een heldere manier de betrouwbaarheid als kernbegrip van informatiebeveiliging te waarderen. Ik gebruik de term 'waarderen' bewust omdat 'classificeren' al is gereserveerd voor het onderscheiden van data naar vertrouwelijkheid. Het bijzondere is dat de begrippen beschikbaarheid, integriteit en vertrouwelijkheid die samen de betrouwbaarheid vormgeven en de basis vormen om systemen te waarderen, veelal kwalitatief zijn omschreven. Daarmee is het bepalen van een vereist niveau van de afzonderlijke componenten en vervolgens via wegingsfactoren de betrouwbaarheid als geheel nog grotendeels kwalitatief en weinig kwantitatief. Een meer kwantitatieve benadering kan mogelijk leiden tot een neutralere of objectievere waardering van de betrouwbaarheid van een informatiesysteem. Daarbij gaat het in dit boek om de gewenste of benodigde betrouwbaarheid (vooraf) en niet zo zeer de maatregelen die genomen moeten worden om een bepaalde betrouwbaarheid te kunnen bereiken (achteraf). Ik herhaal hetgeen ik in [Willemsen, p. 23] over maatregelen heb gesteld en wel: ik ga niet in op de maatregelen die getroffen kunnen worden om een bepaald niveau van betrouwbaarheid te behalen vanwege:

- de keuze van de te nemen maatregelen is niet altijd objectief en het wil niet direct zeggen dat deze voldoende zijn
- de maatregelen zijn tijdgebonden met name vanuit technisch oogpunt
- het valt buiten het doel van dit boekwerk