Auteur: Valentijn Ishaqsada is bestuurslid PvIB, portefeuille Public Relations & Communicatie, en als consultant actief voor zijn bedrijf ourAlly. Met zijn bedrijf adviseert hij publieke en private organisaties bij de beheersing van hedendaagse uitdagingen rondom informatiebeveiliging en privacy. Valentijn is te bereiken via: valentijnishaqsada pvib.nl.

Titel boek:	**Waardering van de informatiebeveiliging**
Auteur:	**dr. Clemens H.J. Willemsen**
Taal:	**Nederlands**
Bindwijze:	**Paperback**
Aantal pagina s:	**61**
EAN:	**9789403676159**
Prijs:	**€ 17,95**

BOEKREVIEW

Waardering van de informatiebeveiliging

Hoe waardeer je informatiebeveiliging? Wat is de weg naar een objectievere waardering van betrouwbaarheid? Wat schuilt er achter beschikbaarheid, integriteit en vertrouwelijkheid? In het boek Waardering van de informatiebeveiliging neemt auteur dr. Clemens H.J. Willemsen de lezer mee in het onderwerp kwantificering en informatiebeveiliging.

Aspect	Kengetal	Laag	Midden	Hoog
Beschikbaarheid in enge zin	beschikbaarheid	90 (36 dagen niet)	99 (3,6 dagen niet)	99,9 (1 dag niet)
	oftewel in dagen uren	5 8	5 11	7 24
Stabiliteit/ robuustheid	maximaal dataverlies RPO	28 uur	24 uur	18 uur
Continu teit/ herstelbaarheid	maximale hersteltijd RPO/ MTTR	40 uur	16 uur	8 uur
	geprogrammeerde controles	Beperkt	Voldoende	Uitgebreid
Tijdigheid	kritieke momenten	Geen	periode-afsluiting, kortstondige piekperiode	Langdurige piekperiode
Toegankelijkheid bij beperkingen	Belemmeringen	Enkele belemmeringen	Gedeeltelijke belemmeringen	Grote belemmeringen

Figuur 1: Kengetallen voor BIV-factor beschikbaarheid (bron: Waardering van de informatiebeveiliging)

Dr. Willemsen studeerde in 1985 af in de Bestuurlijke Informatica en promoveerde in 2019 aan de Faculteit der Rechtsgeleerdheid van de Tilburg Universiteit. Hij is werkzaam als CISO (Chief Information Security Officer) en beleidsadviseur informatievoorziening bij het ministerie van Justitie en Veiligheid en is in deze functie al jaren betrokken bij informatiebeveiliging en informatievoorziening.

Willemsen opent het boek met de observatie dat informatiebeveiliging tot op heden vaak vanuit een kwalitatief oogpunt wordt benaderd. Hij betoogt dat een juiste waardering van betrouwbaarheid nodig is om werkzaamheden op het gebied van informatiebeveiliging te kunnen prioriteren en in tijd te kunnen uitzetten, met daarbij de benodigde financiering. Een meer kwantitatieve benadering kan tenslotte leiden tot een meer objectieve waardering.

Voor alle informatiebeveiligingsprofessionals zijn de BIV-factoren (beschikbaarheid, integriteit, vertrouwelijkheid) onlosmakelijk verbonden met de betrouwbaarheid van informatiesystemen binnen organisatorische processen. Willemsen stelt echter eerst de vraag of een bredere benadering van andere elementen, naast de welbekende BIV-factoren, niet passend en gerechtvaardigd zou zijn. Diverse bronnen worden voor de beantwoording van deze vraag onderzocht: ISO-standaarden (ISO 25012, 25010, 27000), CoBiT, CIA-triad, 5 Pillars en Nora. In deze uitvoerige bespreking worden de elementen achter deze bronnen beoordeeld op de vraag of deze een rol naast of achter de BIV-factoren zouden kunnen vervullen.
Dan volgt de kwantificering van de BIV-factoren. Voor elk van de drie factoren bestaat dit uit een definiëring, een uiteenzetting en de aanpak waarmee een meting en waardering kan plaatsvinden. Dit geheel voegt dr. Willemsen samen in een **model waarin niveaus (laag, midden, hoog), aspecten en kengetallen samenkomen (zie figuur 1). Door het gebruik van concrete voorbeelden ontstaat zo een uitgebreid en integraal beeld waarmee voor de verschillende BIV-factoren, de achterliggende kwantificering kan worden bepaald.**

Dan volgt een laatste hoofdstuk waarin de BIV-factoren als geheel samenkomen. Willemsen beschrijft op welke manier er sprake is van een mogelijke samenhang tussen de BIV-factoren en de verschillende methoden voor de bepaling van welk niveau voor individuele BIV-factoren passend is. Onder andere de BIO-(toets), het ISACA IT Asset Valuation, Risk Assessment and Control Implementation Model, uickscan Information Security (IS) en de In Control Verklaring komen ter sprake.

Aan de hand van verschillende figuren leidt het traject van de waardering van niveaus naar de waardering van de daadwerkelijke betrouwbaarheid. De methoden worden naast elkaar geplaatst en vergeleken, hetgeen leidt tot een sluitend geheel waarin alle inzichten samenkomen. Als praktisch hulpmiddel levert de auteur online ook nog een spreadsheet aan zodat de lezer zelf met kwantificering aan de slag kan gaan.

Al met al slaagt Willemsen zeker in zijn doel om bruikbare inzichten te geven die helpen bij de objectivering van informatiebeveiliging. Het boek blinkt uit door de abstracte materie concreet te maken, de diverse bronnen die worden besproken en door praktische hulpmiddelen te bieden. Wanneer je aan de slag wil met kwantificering of wanneer je simpelweg nieuwsgierig bent en verdieping zoekt, zul je je bij dit boek goed thuis voelen.

Het boek is onder meer verkrijgbaar via managementboek.nl en de reguliere boekhandel.