

Algemene Samenvatting

Modern ondernemerschap wordt in toenemende mate bevorderd dankzij een breed en wereldwijd vertakt netwerk waarin digitale apparaten en diensten communiceren in een hyperverbonden wereld. Voor veel organisaties is de keuze om zich niet bij deze cyberwereld aan te sluiten en eraan deel te nemen een keuze waarmee ze zichzelf beperkingen opleggen. Voor organisaties die besluiten om er wel aan deel te nemen wordt het waarborgen van de continuïteit en integriteit van de digitale infrastructuur echter een steeds grotere uitdaging.

Naast participatie stelt interconnectiviteit deelnemers ook bloot aan partijen die digitale infrastructuren willen ondermijnen, uitbuiten of op andere wijze misbruiken. De exponentiële groei en ontwikkeling van netwerken, datavolumes en digitale apparaten heeft het aantal risico's en kwetsbaarheden sterk vergroot. Professionals die belast zijn met het opzetten van cyberbeveiliging en het bewaken van de cyberveiligheid worden steeds vaker op de proef gesteld door een complex van factoren, waaronder toenemende kwetsbaarheden, veranderende bedreigingen, overwerktheid onder cyberbeveiligingsmedewerkers, overbelasting van het systeem door vaak optredende valse waarschuwingen, uitdagingen bij het vinden van oplossingen en problemen bij het integreren van beveiligingssystemen en gegevens.

Ondanks de groeiende risico's volgen veel organisaties ambitieuze strategieën voor hun digitale ontwikkeling en vooruitgang. Het enorme tempo waarin deze digitale uitbreiding plaatsvindt zorgt er echter ook vaak voor dat een streng veiligheidstoezicht ontbreekt. Beveiligingsprofessionals staan onder druk om het juiste midden te vinden tussen de stijgende vraag naar connectiviteit en de stijgende blootstelling aan opportunistische bedreigingen.

Een van de belangrijkste bestuurlijke uitdagingen bij het beschermen van netwerkinfrastructuren betreft de zich steeds verder ontwikkelende onbalans tussen de technische mogelijkheden waarover aanvallers beschikken en die van verdedigers. Terwijl het aantal dreigingen en kwetsbaarheden toeneemt, is er een oplopend gebrek aan bekwame vakmensen om de risico's die zich voordoen op te vangen en te blijven volgen. Cyberbeveiligingsprofessionals hebben steeds meer moeite om de beveiligingseffecten te ondervangen die worden veroorzaakt door voortdurende groei en technische innovatie.

Al met al hebben bovenstaande factoren gezorgd voor een brede belangstelling in het toepassen van analytische, algoritmische en machinegestuurde methoden waarmee bepaalde aspecten van de steeds groter wordende beveiligingskloof op semiautomatische wijze kunnen worden benaderd. Door aanzwellende bedreigingen, personeelstekorten en een steeds complexer wordende omgeving is er behoefte aan meer geavanceerde, datagestuurde benaderingen. Zo creëert de groeiende druk op cyberbeveiliging een natuurlijk raamwerk voor de eisen die gesteld worden op het gebied van *cybersecurity data science* (CSDS).

CSDS, een discipline die specifiek gericht is op praktijkbeoefenaars, maakt op dit moment een snelle ontwikkeling door op het snijvlak van twee gebieden die van bijzonder groot algemeen en commercieel belang zijn. De professionele praktijk van CSDS komt voort uit de functionele combinatie van twee voorouderlijke domeinen: dit betreft het toepassen van *data science*-methoden om besluitvorming met betrekking tot *cybersecurity* te verbeteren. Als opkomend en hybride metier levert CSDS een reeks nieuwe benaderingen voor het aanpakken van de toenemende uitdagingen op het gebied van cyberbeveiliging. Datawetenschap biedt een scala aan aanbevolen remedies en methoden om een snel veranderend complex van beveiligingsbedreigingen op te sporen, te ontrafelen en af te wenden.

Het CSDS-domein biedt onderdak aan een steeds groter aantal actieve en bekwame professionals en vormt een discipline die is ontstaan vanuit een dynamisch werkveld; het is geen kunstmatig theoretisch platform. In dit opzicht bestrijkt CSDS een opportunistisch werkveld dat zich verder uitbreidt door de bundeling van dringende praktische behoeften (de noodzaak om digitale veiligheidsborging te verbeteren) en zich ontwikkelende analytische methoden (het brede en snelgroeiende scala van benaderingen uit de datawetenschappen en ondersteunende technologieën).

Het uitdijende professionele CSDS-domein wordt gekenmerkt door nieuwheid, snelle veranderingen en complexiteit. Dit betreft zowel technische en methodologische contexten alsook organisatorische kaders. Als professie in wording mist CSDS echter de kenmerken die horen bij volwassen beroepen. Een gebrek aan standaarden en vastgelegde optimale handelwijzen, een *overkoepelend theoretisch model*, beperkt de mogelijkheid om personeel op te leiden, om inspanningen ten behoeve van bepaalde programma's in goede banen te leiden, om nauwkeurigheid te garanderen en tenslotte om de mate van effectiviteit te monitoren. Naarmate de CSDS-inspanningen toenemen, zullen theoretische lacunes uit de aard der zaak meer beperkingen gaan opleveren wanneer beoefenaars steeds vaker geconfronteerd worden met tegenstrijdige opvattingen over de juiste aanpak.

Een systematische bestudering van het CSDS-veld laat een lacune in het onderzoek zien, een lacune waarop dit onderzoek zich richt. Door een beter begrip te ontwikkelen van de huidige uitdagingen en door werkmethoden op het gebied van CSDS nog verder te verbeteren, legt dit onderzoek een basis voor de groei en ontwikkeling van het CSDS-domein. Met behulp van een systematische gap-analyse is gekeken – en vergeleken – waar de CSDS-discipline zich momenteel bevindt (*as-is*), waar het zich ontwikkelt in termen van overheersende trends en gewenste praktijken (*to-be*) en waar organisaties verdere ontwikkeling moeten stimuleren om gaten en tekortkomingen aan te pakken (*gap-diagnose*). De resultaten vormen zo een afgebakend kader met daarin een reeks eisen en aanbevolen remedies voor frequent terugkerende professionele CSDS-praktijken.

Op basis van de eindresultaten wordt met deze dissertatie een geïntegreerd onderzoeksrapport geleverd dat gericht is op praktische probleemoplossingen met als doel om de ontwikkeling van het nieuwe vakgebied te ondersteunen. Dankzij een stevig fundament op het gebied van het managen van informatiesystemen (MIS) biedt het onderzoek een systematische, gemengde methode-verkenning van CSDS als een vakgebied in wording.

De studie is opgezet als gefaseerd probleemoplossend onderzoek en omvat drie onderzoeksfasen waarin een brug geslagen wordt tussen diagnostisch onderzoek (achtergrond, mening en gap-analyse) en probleemoplossing op het gebied van ontwerpwetenschap:

- I. *Fase I - Diagnostische achtergrondanalyse (probleemanalyse)*: via literatuuranalyse komen uitdagingen aan het licht met betrekking tot CSDS-professionalisering en worden de belangrijkste methodologische concepten van CSDS afgebakend.
- II. *Fase II - Diagnostisch opinieonderzoek (interviewonderzoek) en gap-analyse (gemengde methode)*: door middel van interviewonderzoek en een kwantitatieve resultatenanalyse komen drie belangrijke lacunes in de CSDS-praktijk naar voren.
- III. *Fase III – Oplossingen voor ontwerpwetenschap-gerelateerde problemen*: gerichte aanbevelingen worden gedaan om CSDS-hiaten aan te pakken met behulp van een probleemoplossend ontwerpproces.

Voor wat betreft de integratie van de drie bovengenoemde fasen zorgt de literatuuranalyse (Fase I) voor het afbakenen van concepten die de introductie van CSDS kunnen vergemakkelijken, het onderzoek van een stevige basis voorzien en onderzoekers stimuleren en informeren. Interviewonderzoek ondersteund door kwantitatieve analyse (Fase II) zorgt er vervolgens voor dat

belangrijke lacunes onderscheiden worden die de CSDS-praktijk kunnen verstoren. De gecombineerde resultaten uit de eerste twee fasen leggen dan een basis voor het oplossen van ontwerpproblemen (Fase III). Op deze manier kunnen ontwerpvoorstellen (latente ontwerpen) geformuleerd en aanbevolen worden om daarmee de belangrijkste hiaten aan te pakken die in Fase II zijn geïdentificeerd. Resultaten worden gepresenteerd als praktische processen om zowel de CSDS-praktijk als de professionele theorie te versterken. De hieruit voortvloeiende voorgestelde remedies kunnen worden beschouwd als nieuwe MIS-onderzoeksbijdragen die van belang zijn voor het bevorderen van CSDS-praktijk.

Met het uitvoeren van probleemoplossend onderzoek ligt de wetenschappelijke focus van deze studie op het strikt onderscheiden van diagnostische patronen en op een strikte onderbouwing hiervan in een nieuw en complex domein. De empirische kernelementen in dit proces bestaan uit interviewonderzoek, vergelijkende literatuuranalyse en tekstanalyse. Dit wordt verder ondersteund door op literatuur gebaseerde, deductief afgeleide concepten die als leidraad fungeren voor ontwerpaanbevelingen. Deductieve en inductieve methoden worden geïntegreerd om daarmee, op een manier die abductief genoemd kan worden, een reeks *best practices* af te leiden en aan te bevelen voor toepassing in het CSDS-veld.

Een belangrijk punt van aanbeveling dat uit dit onderzoek naar voren komt betreft de conclusie dat cybersecurity niet louter als een serie kunstmatige, technische oplossingen moet worden gezien, maar veeleer als een *wetenschappelijk fenomeen*, wil er in de ontwikkeling van het cybersecurity-domein vooruitgang geboekt worden. Traditioneel gezien wordt er vanuit de cybersecuritywereld op elke nieuwe uitdaging instinctief gereageerd met technische oplossingen, een aanpak die als risico heeft dat zich een spel ontwikkelt met de naam 'whack-a-mole', een vicieuze strijd zonder einde en zonder winnaar. In deze dissertatie wordt een reeks methoden en processen geschetst om in het licht van CSDS een strengere wetenschappelijke discipline, en dus theorievorming, aan te houden tijdens activiteiten die gericht zijn op cyberbeveiliging.

Theoretische Bijdragen

De onderzoeksresultaten leveren een brede bijdrage op academisch, theoretisch en methodologisch gebied:

1. Er is met deze studie, gezien vanuit een MIS-perspectief, systematisch inzicht verkregen in de uitdagingen en beste werkmethoden voor het zich ontwikkelende CSDS-domein; hiermee is een lacune in het huidige onderzoek aangepakt.
2. De beoordeling van de professionele wasdom en rijpheid van CSDS die is gemaakt aan de hand van een gestructureerd model heeft hiaten aan het licht gebracht die professionalisering van CSDS dwarsbomen. Dit model kan mogelijk breder ingezet worden voor het beoordelen van andere opkomende IT-gerelateerde beroepen.
3. Een functionele beoordeling van de CSDS-praktijk laat zien dat het veld van cruciaal diagnostisch belang is bij het bepalen van datawetenschappelijke handelwijzen die tot doel hebben om uitdagingen op het gebied van cyberbeveiliging aan te pakken. Dit benadrukt het belang van een theoretisch model voor de CSDS-praktijk.
4. Er is een CSDS-literatuurcorpus samengesteld van 33 omvangrijke wetenschappelijke werken. Deze zijn beoordeeld en er is een vergelijkende analyse gemaakt van de belangrijkste thema's.
5. Betekenisvolle methodologische concepten op het gebied van datawetenschap die van bijzonder belang zijn voor het CSDS-domein zijn aan de orde gesteld en van kaders voorzien.
6. Door de nieuwe mix van kwantitatieve methoden zoals die zijn toegepast in het interviewonderzoek zijn nieuwe benaderingen naar voren gekomen voor het analyseren van interviewgegevens.
7. De uitkomsten van de gap-analyse die is gemaakt voor de interviews laten drie hiaten in het centrale CSDS-domein zien die van belang zijn voor zowel onderzoekers als professionals in de praktijk: deze

hiaten betreffen gegevensbeheer, wetenschappelijke processen en domeinoverschrijdende samenwerking.

8. Op basis van de gevonden hiaten in het CSDS-domein is een reeks procesoplossingen afgeleid. Deze oplossingen worden aanbevolen om de ontwikkeling van het opkomende veld te ondersteunen.
9. De gap-remedies die voortvloeien uit het probleemoplossende ontwerpproces vormen tezamen een raamwerk van gerichte aanbevelingen om het theoretisch model voor CSDS te versterken.
10. De verzamelde gap-remedies vormen een reeks gestructureerde benaderingen waarmee een strengere empirische, theoretische en wetenschappelijke nauwkeurigheid betracht kan worden in het cyberbeveiligingsonderzoek.

Bijdragen aan de Managementpraktijk

De resultaten van dit onderzoek zijn van belang voor verschillende partijen in het professionele, commerciële en publieke domein. De belangrijkste belanghebbenden zijn onder andere praktijkbeoefenaars die actief zijn op het gebied van beveiliging, datawetenschap en CDS, cyberbeveiligingsstewards, organisatiemanagers, planners en strategen, softwarebedrijven, servicebedrijven, gouvernementele en non-gouvernementele organisaties en tenslotte (militaire) inlichtingendiensten.

Door het in kaart brengen van de uitdagingen waarmee CSDS geconfronteerd wordt en door het voorschrijven van praktische remedies en aanbevolen oplossingen vormt dit werk een leidraad voor diegenen die gericht zijn op het stimuleren van professionele CSDS-praktijken en het bevorderen van de algehele effectiviteit van cybersecurity. Dit geldt ook voor belanghebbenden die zich bezighouden met de planning van programma-implementaties. Specifieke bijdragen in dit verband zijn de volgende:

1. Het geïntegreerde rapport biedt een uitgebreide en diepgaande analyse van de hiaten waarmee CSDS als vakgebied wordt geconfronteerd en het biedt richtlijnen voor de toekomstige ontwikkeling van dit gebied. Het rapport bepleit ook een aantal oplossingen als manier om het theoretisch model van CSDS verder te vervolmaken en zo het professionaliseringsproces te bevorderen.
2. In het rapport wordt CSDS gedefinieerd als een hybride domein en een ontluikende professie. CSDS is voortgekomen uit de samensmelting van behoeften op het gebied van cyberbeveiliging en data science-methoden; dit geschiedde als reactie op de toenemende economische en organisatorische druk die samenhangt met de effecten van een snelle digitale uitbreiding en ontwikkeling. In termen van management wordt de mogelijkheid geschapen om deze transformatie te beheersen en te bevorderen door middel van een gestructureerd begrip van de brede dynamiek die ten grondslag ligt aan de opkomst van CSDS.
3. Begeleiding op basis van interviews met actieve CSDS-beoefenaars laat zien dat het noodzakelijk is om menselijke en technische middelen te integreren en op elkaar af te stemmen via organisatorische processen. De resultaten geven aan dat resourcecoördinatie, gegevensbeheer en wetenschappelijke methoden samen zouden moeten komen om zodoende CSDS als een functioneel organisatieproces te bevorderen. Dit betekent dat er voor CSDS meerdere en overlappende processen nodig zijn, met name cyclische gegevensverkenningen en wetenschappelijke vraagstellingen.
4. De drie CSDS-hiaten die zijn onderscheiden – gegevensbeheer, wetenschappelijke processen en domeinoverschrijdende samenwerking – sluiten globaal aan bij de MIS-focusgebieden technologie, proces en organisatie. Een belangrijke constatering in dit verband betreft de mate waarin deze hiaten elkaar overlappen: ontwerpoplossingen en aanbevolen remedies die in de conclusie worden

gepresenteerd laten zien dat datamanagement en wetenschappelijke processen elkaar wederzijds versterken.

5. In het ideale geval vergemakkelijken en stimuleren CSDS-programma's sociale processen die verband houden met kennisuitwisseling, creatie en validatie. Toezicht door leidinggevenden is noodzakelijk om data science in een programmatisch kader te vatten, een inspanning die zowel organisatorisch als methodologisch en technisch van aard is. Er worden passende aanbevelingen gegeven om dergelijke programmatische toepassingen mogelijk te maken.
6. De beschreven best practices op het gebied van CSDS bieden een reeks methoden om fenomenen te meten, betere beslissingen te nemen, bedreigingen op te sporen, risico's te beheersen en processen te optimaliseren. Deze verzameling best practices schetst een beeld van de ideale CSDS-praktijk. Gezamenlijk vormen de adviezen en oplossingen een basis voor een model waarmee de wasdom van CSDS bepaald kan worden. Volwassenheidsindicatoren zijn nuttig voor managers bij het benchmarken van mogelijkheden en bieden een gestructureerde basis voor gap-analyse en strategische planning.