Managementsamenvatting (TLDR)

Digitalisering vormt de basis van onze samenleving en economie. Organisaties zijn sneller, flexibeler en internationaal verbonden, maar dezelfde afhankelijkheid maakt ze ook kwetsbaar. Digitale aanvallen, softwarefouten en menselijke misstappen kunnen complete ketens ontwrichten en grote maatschappelijke schade veroorzaken. In dit boek staat daarom niet de techniek op zichzelf centraal, maar de vraag hoe we beveiliging structureel verankeren in onze manier van organiseren en werken.

De kernboodschap is dat informatiebeveiliging geen puur technisch vraagstuk is. Duurzame beveiliging ontstaat als regulering, organisatie en techniek met elkaar in balans zijn. We zien dat incidenten worden beantwoord met méér technologie of méér regels, terwijl de werkelijke oorzaken liggen in cultuur, leiderschap en samenwerking. Onduidelijke verantwoordelijkheden leiden tot afschuifgedrag, een gebrek aan psychologische veiligheid zorgt voor niet tijdig van risico's. En professionals, zoals de CISO, dragen formeel verantwoordelijkheid zonder voldoende mandaat.

Het eerste fundament is regulering. Europese en nationale wetgeving, zoals NIS2, DORA en de Cyber Resilience Act, dwingt organisaties tot structurele aandacht. Maar naleving is slechts het begin: de regels moeten vertaald worden naar gedrag en besluitvorming in de praktijk. Het tweede fundament is organisatie. Heldere taken, verantwoordelijkheden en bevoegdheden maken duidelijk wie mag beslissen en wie moet handelen. Net zo belangrijk is een gezonde werkcultuur, waarin mensen zich veilig voelen om fouten te bespreken en risico's te benoemen. Het derde fundament is techniek. Robuuste systemen, veilige configuraties en moderne concepten als Zero Trust zijn nodig, maar hebben pas effect in een organisatie die ze daadwerkelijk borgt. De afhankelijkheid van leveranciers maakt bovendien dat ook de keten integraal onderdeel van de beveiliging moet zijn.

Andere sectoren, zoals de luchtvaart, laten zien dat veiligheid en kwaliteit niet toevallig ontstaan. Ze zijn het resultaat van systematisch leren, Just Culture en een voortdurende verbetercyclus. Informatiebeveiliging kan dezelfde professionaliseringsslag maken door incidenten niet als eindpunt te zien, maar als startpunt voor leren en verbeteren.

De les voor bestuurders is duidelijk: informatiebeveiliging is geen IT-onderwerp dat men kan delegeren, maar een strategisch thema dat direct raakt aan continuïteit, reputatie en vertrouwen. Bestuurders moeten de toon zetten, prioriteit geven aan een gezonde werkcultuur en ruimte creëren voor structurele verbeteringen. Alleen wanneer mens, organisatie en techniek met elkaar verbonden zijn, wordt beveiliging net zo vanzelfsprekend en waardevol als kwaliteit.

Voorwoord

Toen ik bekend maakte en boek met als werktitel ‘Waarom informatiebeveiliging faalt’ te maken, kwamen er veel reacties los. Het thema raakt mensen. Er zijn veel professionals, die het gesprek over het onderwerp wilden aangaan. Er waren diverse geïrriteerde reacties, omdat het in veel organisaties kennelijk ‘wel goed gaat’. De titel was confronterend, hoorde ik vaak als ik het gesprek aanging. De emotie maakte helder: het thema is iets persoonlijke en ik zou niet bijdragen aan een oplossing.

Maar we kunnen onszelf niet langer wijsmaken dat het wel goed gaat. Zo brengt een slechte software-update de stabiliteit van duizenden ondernemingen in gevaar, zorgt voor het uitvallen van duizenden vluchten en veroorzaakt voor miljarden aan schade. Voor andere softwareproblemen praten we niet meer over miljarden, maar over biljoenen aan schade. Ransomware treft nog altijd veel organisaties, waardoor bedrijven en overheden jarenlange historie kwijtraken en soms zelfs failliet gaan. Bij de introductie van nieuwe wetgeving, die eist dat het basaalste eindelijk geregeld worden, reageren organisaties alsof de ondergang van de wereld is aangekondigd.

Chief Information Security Office-medewerkers (CISO-medewerkers), zeg maar hoofden informatiebeveiliging, hebben een grote kans te worden ontslagen, met een burn-out uit te vallen of zelf maar op te stappen. Gemiddeld zitten ze tussen de 18 en 36 maanden op hun positie. In Nederland bestaat DIVD, Dutch Institute for Vulnerability Disclosure, een stichting met vrijwilligers, die niets anders doet dan organisaties waarschuwen voor zwakheden in ICT die ze publiekelijk zien. Alleen al in Nederland bedraagt het aantal datalekken (dat wordt gemeld), jaarlijks enkele tienduizenden. Uit eigen praktijk weet ik dat sommige bedrijven en overheden er niet voor terugdeinzen de wet te overtreden en ervoor kiezen domweg niet te melden. Besef daarbij dat datalekken alleen incidenten zijn met persoonsgegevens en dat het werkelijk aantal informatiebeveiligingsincidenten veel groter is.

Er zijn initiatieven van organisaties, die al meer dan 20 jaar lijsten maken. Lijsten gevuld met de meest voorkomende beveiligingsfouten in allerhande software. Let wel: dezelfde fouten, die keer op keer worden gemaakt en al jaren zeer veel voorkomend zijn. En het oplossen vergt soms niet meer dan minuten of uren werk. Je zou denken dat je dat met een checklist kunt voorkomen, maar dan hoor je regelmatig dat we geen vinkenlijstjes zouden moeten afwerken. Als Albert Einstein nog had geleefd dan had dit verschijnsel waarschijnlijk een tweede definitie van krankzinnigheid kunnen zijn. Laten we het bij Alberts eerste houden: ‘blijven herhalen wat je doet en toch een andere uitkomst verwachten’.

Checklists en eisen uit regulering kunnen slechts het begin vormen. Echte informatiebeveiliging is een integraal onderdeel van goed en behoorlijk bestuur, ondersteunt de bedrijfsstrategie en zorgt ervoor dat groei en innovatie zonder onnodige hinder kunnen plaatsvinden. De CISO kan hierin adviseren en monitoren dat dit op de juiste manier plaatsvindt, maar de bestuurder is verantwoordelijk.

Dit boek is je hulp bij de zoektocht naar een oplossing voor deze problematiek langs de lijn van eerst de diagnose stellen om vervolgens over een behandeling te kunnen nadenken. Heel verrassend: het kan echt én het moment is perfect. Grote incidenten in de zomer van 2025 bij het Openbaar Ministerie en het Clinical Diagnostics maken pijnlijk duidelijk dat bij een incident ondanks het uiterst minimalistisch communiceren er veel basale zaken rond beveiliging slecht geregeld zijn. Dat we het thema echt moeten oppakken en dat dat meer is dan een beentje bijtrekken.

Wet- en regelgeving dwingen organisaties in toenemende mate om informatieveiligheid structureel en aantoonbaar op orde te hebben, zowel op Europees als nationaal niveau. Dat moet zelfregulering faalt en de dreiging neemt toe.

Wet- en regelgeving bepaalt zo voor een groot deel hoe informatiebeveiliging vorm krijgt. Dat is inmiddels een constante (en groeiende) factor, waar we niet omheen kunnen, omdat nakoming van juridische voorschriften van existentieel belang kan zijn voor organisaties. Niemand wil boetes krijgen, dwangsommen opgelegd krijgen, uit zijn ambt worden gezet of onder curatele worden geplaatst. De bestuurder moet informatiebeveiliging passende aandacht geven. Dat doe je organisatorisch, terwijl en de techniek het vervolgens goeddeels moet inkleuren. Dat maakt informatiebeveiliging ROT: regulering, organisatie en techniek met de mens centraal.

Voor sommige zaken ben je afhankelijk van derde partijen, maar er is veel wat je zelf kunt doen en hoe je de cirkel van indirecte en zelfs directe invloed kunt vergroten. Dit boek levert handvaten voor die deze noodzakelijke proactiviteit. Dat begint met een hele simpele verandering in houding door het thema niet te zien als belangrijk, maar als motto te nemen: SAFETY FIRST!

Voor iedereen die stelt dat het in zijn of haar organisatie wel goed gaat, ben ik blij als dat waar blijkt te zijn. Daarbij is de vraag, die na een actie bij de politie nog wel eens wordt gesteld toepasselijk: ‘is het goed gegaan of is het goed gedaan’? Dit boek beoogt te helpen met in plaats van laatste en vormt daarmee een onmisbaar onderdeel van de oplossing.

Brenno de Winter,

Noordwijkerhout, zomer 2025

Leeswijzer

Informatiebeveiliging is een breed, multidisciplinair vakgebied dat primair bestaat uit informatietechniek, organisatiekunde en recht. Daarom behandelt dit boek een waaier aan thema's: van juridische kaders en normen tot risicomanagement, organisatorische inrichting, training en awareness, cultuur, technologische ontwikkelingen en psychologische mechanismen. Iedere invalshoek is belangrijk om het geheel te begrijpen en in de praktijk effectieve beveiliging te realiseren.

Dit boek is geschreven voor iedereen die een rol speelt in informatiebeveiliging: bestuurders die eindverantwoordelijk zijn, toezichthouders die willen begrijpen waar ze op moeten letten, en security officers die met de uitvoering belast zijn. De inhoud is breed, omdat informatiebeveiliging niet alleen een technisch, maar ook een organisatorisch, juridisch en menselijk vraagstuk is.

De opzet is bewust zo gemaakt dat de lezer selectief kan lezen. Bestuurders vinden vooral richting en reflectie in de hoofdstukken over governance, zorgplicht en cultuur. Voor security officers en CISO's zijn juist de hoofdstukken over risicomanagement, implementatie en maatregelen praktisch toepasbaar. Daarmee is dit boek geen roman die van begin tot eind gelezen moet worden, maar een naslagwerk waaruit je kunt halen wat op dat moment nodig is.

Door het boek heen vind je uitgebreide voorbeelden die in grijs gemarkeerde kaders zijn geplaatst. Deze illustreren hoe theorie zich vertaalt naar praktijk. Ze maken het boek geschikt voor zowel verdiepende bestudering als thematisch lezen.

Tot slot is dit boek goed te gebruiken als naslagwerk. De hoofdstukken zijn thematisch opgebouwd en zelfstandig leesbaar. Via de inhoudsopgave of het register kun je snel vinden wat voor jouw vraagstuk relevant is. Het maakt niet uit of je nu studeert, adviseert, bestuurt of verantwoordelijk bent voor de uitvoering: dit boek wil je helpen met overzicht, inzicht en praktische houvast.

Bij het refereren aan de ISO-norm, specifiek in de context van dit boek dan refereer ik aan de ISO27001:2022 standaard. Er zijn vele normen en standaarden voor verschillende domeinen (kwaliteit, milieu, enzovoort), maar deze stelt informatiebeveiliging centraal.

Als ik kijk naar luchtvaart vanuit 'safety first' gaat dit louter over de mechanieken rond veiligheid. Nadrukkelijk zegt dit boek niets over service concepten of financiële modellen uit die sector. Dat zijn fascinerende ontwikkelingen voor een ander type boek. Mij gaat het kijken naar werkende mechanismen voor dataveiligheid.

1. Niet meer te berekenen voordeel

Managementsamenvatting

Informatietechnologie speelt een cruciale rol in het dagelijks functioneren van organisaties en onze maatschappij. Technologie bespaart veel tijd, geld en werkdruk, bijvoorbeeld in de gezondheidszorg. Een eenvoudige afspraak bij de huisarts verloopt tegenwoordig grotendeels digitaal, wat zorgt voor tijdwinst, minder fouten en betere dienstverlening. De afhankelijkheid van IT maakt organisaties echter kwetsbaar. Als systemen falen, kunnen de gevolgen ernstig en zelfs existentieel zijn. Daarom is goede informatiebeveiliging essentieel als randvoorwaarde voor een betrouwbare en functionerende samenleving.

Goede beveiliging betekent niet alleen technische maatregelen treffen, maar vraagt om een bredere aanpak waarbij techniek, organisatie en mensen goed op elkaar aansluiten. Het gaat om risicobeheersing, duidelijke verantwoordelijkheden, bewustzijn onder medewerkers, goede afspraken met leveranciers en partners, crisismanagement en continue verbetering.

Om deze maatregelen effectief te realiseren, is een passend beveiligingsbudget noodzakelijk. Internationale richtlijnen en onderzoeken geven aan dat organisaties tussen de 10% en 15% van hun IT-budget aan informatiebeveiliging zouden moeten besteden, afhankelijk van hun risicoprofiel en grootte. Alleen door informatiebeveiliging gestructureerd en volwassen te organiseren, wordt en blijft het niveau van beveiliging effectief.

Over informatiebeveiliging kun je pas een goed gesprek hebben als we ons realiseren wat de informatietechnologie ons oplevert. Wat hebben we eigenlijk te verliezen als systemen falen of ‘er dingen omvallen’. Pas als we dat op het netvlies hebben, kunnen we kijken naar het bredere plaatje. De technologie is zo verbonden met alles wat we doen dat zowel het functioneren van onze samenleving als de individuele organisaties daarvan afhankelijk zijn. Informatiebeveiliging is geen hobby, geloofssysteem of luxe, maar een noodzakelijke randvoorwaarde.

De opmars van informatietechnologie gaat niet alleen vlot, maar vormt al snel het nieuwe normaal in ons dagelijks leven. Neem een simpele afspraak bij de huisarts, die je online of via een app maakt op het tijdstip en plek die je het beste uitkomt. In een invulveld geef je de samenvatting van je medische probleem en krijg je soms al direct een uitnodiging om bijvoorbeeld bloedwaarden te laten prikken. De uitslagen daarvan vloeien geautomatiseerd door naar het elektronisch patiëntendossier (EPD), waardoor de juiste informatie op de juiste plaats staat. Voor veel diagnoses is dit een efficiënte

route naar een doeltreffende behandeling. In veel gevallen komt daarbij medicatie kijken, die onmiddellijk besteld wordt en zo klaarligt voor de patiënt.

Heel bijzonder lijkt het niet, maar als we even teruggaan naar de jaren 70 en ’80 van de vorige eeuw dan is het al snel duidelijk dat technologie veel in het proces heeft geoptimaliseerd. Voor de afspraak met de huisarts moest eerst gebeld worden met de praktijk. Iets wat een tijdrovende bezigheid kon zijn, omdat veel mensen op hetzelfde moment belden en de telefoonlijn vaak bezet was. De wachtrij bestond eigenlijk alleen voor grote ondernemingen. Eenmaal doorgedrongen tot de assistent moest er een moment in de agenda worden gevonden en dat is het moment waarop de patiënt kon langskomen. In veel gevallen werd de naam letterlijk in de agenda geschreven.

Op gesprek bij de dokter werd het medisch dossier uit het archief (een ladekast) en kon het gesprek beginnen. Als de dokter het zinvol vond om bloed te prikken kwam er een formulier bij dat de dokter handmatig invulde. De scherpere geest plande direct een vervolgafspraak met de dokter. Thuisgekomen werd het weer bellen naar het laboratorium om een afspraak te krijgen. Bij het bloed prikken ging het grotendeels handmatige proces opnieuw verder. Het bloed werd onderzocht en de uitslagen geprint. De post leverde de uitslagen bij de huisarts af. De assistent vulde het papieren dossier aan. Met alle risico’s op fouten of het niet tijdig waarschuwen van de patiënt.

Voor mensen met een chronische aandoening, zoals diabetes, is de winst die we met technologie kunnen behalen nog groter. In plaats van dat de huisarts steeds dezelfde medicatie of hulpmiddelen moet voorschrijven, kun je als patiënt zelf via het portaal aangeven dat je voorraad zo goed als op is. De huisarts hoeft alleen een digitaal vinkje te zetten om de bestelling goed te keuren. Dat scheelt ongelooflijk veel telefoontjes en dubbel werk. Zeker nu de zorg kampt met tekorten aan dokters en assistenten, zie je direct hoe deze digitale zelfredzaamheid tijd en geld bespaart, terwijl de kwaliteit van zorg behouden blijft.

Veel van de zich herhalende handelingen zijn inmiddels vervangen door IT-processen. De telefoongesprekken om een simpele afspraak te maken en die door de assistent in de agenda van de arts te zetten, worden in veel gevallen nu door de patiënt in de agenda gezet via een online boeking. Beide partijen beschikken nu over dezelfde informatie en de kans op fouten neemt af. De integratie tussen systemen neemt medewerkers veel werk uit handen. De arts is beter voorbereid en de processen lopen vooral veel sneller.

Wat deze efficiëntie oplevert, is moeilijk in getallen uit te drukken. Het is nu mogelijk meer mensen te bedienen met hetzelfde team aan mensen. De kans op het maken van administratieve fouten is fors afgenomen, processen lopen sneller en de effectiviteit

neemt toe. Voor het voorbeeld met de huisarts is dat een belangrijk gegeven, omdat de druk op huisartsen sinds de jaren 70 enorm is toegenomen. Nederland is gegroeid van veertien miljoen naar achttien miljoen mensen, de huisarts heeft meer taken gekregen doordat de eerstelijnszorg centraler is komen te staan, er zijn regionale tekorten aan huisartsen en door de vergrijzing neemt die druk toe. Zonder informatietechnologie, zouden dit soort belangrijke rollen nog veel sneller tegen capaciteitsgrenzen aanlopen. Dat is precies wat IT in brede zin doet voor onze maatschappij en economie: het bespaart tijd, vermindert de werkdruk, maakt processen betrouwbaarder en verhoogt daarmee de productiviteit en het serviceniveau in talloze sectoren.

Uit onderzoek blijkt dat IT vaak een belangrijk deel van de productiviteitsgroei voor zijn rekening neemt. In bepaalde periodes schat het Centraal Plan Bureau (CPB) dat IT goed was voor 20 tot 40% van de groei in Nederland. Internationaal gezien laten vergelijkbare studies van de OESO en economen als Bart van Ark en Dale Jorgenson zien dat de VS en andere Europese landen enorme productiviteitswinst haalden uit IT, met name in de jaren negentig en de vroege jaren 2000.

Toch is er geen universeel ‘eindbedrag’ te noemen. IT is zo verweven in alle sectoren dat het lastig is om precies te isoleren waar de ene innovatie begint en de volgende ophoudt. Denk alleen al aan het voorbeeld van de huisarts: je hebt de software van de praktijk, de systemen van het laboratorium, de systemen van de zorgverzekeraar en de IT-voorzieningen van de patiënt thuis. Alle deelsystemen beïnvloeden elkaar en vormen gezamenlijk het eindresultaat. Laat even doordringen dat de voordelen van IT economisch gezien zo groot zijn dat we het niet meer kunnen berekenen[1].

Als we het over informatiebeveiliging hebben dan is dit wel waar het om draait: we moeten iets beschermen dat onlosmakelijk verbonden is geworden met onze way of life, onze economie en ons bestaan. Informatiebeveiliging gaat over het borgen van dat samenspel van systemen, processen en organisatorisch functioneren. Het raakt nagenoeg iedere betrokken organisatie op het moment dat het verkeerd gaat. Het is de noodzakelijke randvoorwaarde voor je organisatie om te kunnen functioneren en te kunnen overleven. De mens is daarbij overigens niet te vergeten. Die is niet een losse factor, maar speelt bij ieder onderdeel een rol als spil. De mens staat bij alles centraal.

[1] Dit hebben bijvoorbeeld Nicolas G. Carr in Harvard Business review geprobeerd in 2003 en in zijn boek uit 2004 ‘Does IT matter?’. Ook de econoom en Nobelprijswinnaar Robert Solow (“You can see the computer age everywhere but in the productivity statistics.”), Erik Brynjolfsson (MIT) 1990, Shoshana Zuboff (1988, In the Age of the Smart Machine en later Surveillance Capitalism 2019) en Manuel Castells (The Information Age, 1996–1998) beschrijft dat informatie de kern wordt van de economie zelf.

Faalt de techniek door inbraak, verstoring of een andere nare samenloop van omstandigheden dan ondermijnt dat de voordelen op zo'n manier dat het voortbestaan van organisaties in het geding kan komen. Inmiddels wordt binnen Europa goed begrepen dat de risico's verder gaan dan een enkele organisatie, maar grote uitwerking op andere bedrijven of zelfs de hele samenleving kunnen hebben. Daarom heeft de wetgever mechanismen voor het geval de risico's te groot worden. Via toezichthouders en rechtbanken kan worden ingegrepen, waardoor transparantie afdwingbaar wordt, systemen kunnen worden stilgelegd, een toezichthouder soms zelfs rechtstreeks kan ingrijpen, een bestuurder onder een vorm van curatele kan worden geplaatst of zelfs uit zijn functie kan worden ontheven.

IT is voor iedere organisatie een onmisbaar middel geworden om de doelen te halen. Het vormt een integraal onderdeel van de strategie van de organisatie. Daarbinnen is informatiebeveiliging randvoorwaardelijk om te kunnen borgen dat op IT gesteund kan worden. Wordt aan die voorwaarde niet voldaan dan kunnen de gevolgen voor organisaties existentieel bedreigend zijn.

Ongekende schade

Iets anders, waaruit de waarde en afhankelijkheid van software en de enorme impact op de economie blijkt, is af te leiden uit het ontwikkelen van software. De digitale transformatie van organisaties gaat gepaard met aanzienlijke risico's. IT-projecten, die bedoeld zijn om efficiency te verhogen en concurrentievoordeel te creëren, eindigen vaak in kostbare mislukkingen met verstrekkende gevolgen. De schade van gefaalde IT-projecten reikt veel verder dan alleen budgetoverschrijdingen en vertragingen.

De Standish Group, een toonaangevende onderzoeksorganisatie op het gebied van IT-projectmanagement, publiceert sinds 1994 het Chaos Report dat de prestaties van IT-projecten analyseert. Hun onderzoek, gebaseerd op ongeveer 50.000 projecten uit verschillende marktsegmenten, toont een schokkende realiteit.

Volgens het recentste Chaos Report van 2020 slaagt slechts 31% van alle IT-projecten volledig. Dit betekent dat deze projecten op tijd, binnen budget en met alle geplande functionaliteiten worden opgeleverd. 50% van de projecten overschrijdt de deadline en het budget, terwijl 19% van alle projecten volledig wordt geannuleerd voordat ze worden voltooid.

Bij grotere projecten zijn de cijfers nog alarmerender. Voor IT-projecten met een budget van meer dan tien miljoen dollar (ongeveer 9,2 miljoen euro) bedraagt het succespercentage wereldwijd slechts 7%. Een verbijsterende 36% van deze grote projecten faalt zo dramatisch dat het systeem nooit in gebruik wordt genomen.

In Nederland is de situatie bijzonder zorgwekkend. Het parlementaire onderzoek uit 2014 naar IT-projecten binnen de overheid, toonde aan dat de Nederlandse overheid jaarlijks 4 tot 5 miljard euro verliest aan falende IT-projecten. Dit bedrag komt overeen met ongeveer 1% van het Nederlandse BBP, wat neerkomt op enkele honderden euro's per jaar per inwoner.

Op Europees niveau zijn de verliezen niet minder dramatisch al ontbreekt het wel aan recente cijfers. Marktonderzoekbureau en adviesbureau Gallop becijferde over 2004 dat de kosten van gefaalde IT-projecten in de Europese Unie € 142 miljard bedroegen. Dit enorme bedrag illustreert de systematische aard van het probleem dat zich uitstrekt over alle EU-lidstaten.

De zichtbaarste schade van mislukte IT-projecten manifesteert zich in directe financiële verliezen. Onderzoek van onder andere onderzoeksbureau McKinsey toont aan dat grote IT-projecten gemiddeld 45% boven het budget uitkomen en 7% langer duren dan gepland, terwijl de Oxford University becijferde dat ze 56% minder waarde leveren dan voorspeld. In sommige gevallen kunnen de budgetoverschrijdingen oplopen tot 200% tot 400% van het oorspronkelijke budget, wat deze projecten tot 'black swan[2]'-gebeurtenissen maakt die de toekomst van organisaties kunnen bedreigen.

De werkelijke schade draait om meer dan de investering in de projecten. Mislukte IT-projecten veroorzaken vaak ernstige operationele verstoringen. Het voorbeeld van Birmingham City Council illustreert dit pijnlijk: na implementatie van een nieuw gefaald Oracle ERP-systeem in april 2022 kon de gemeente haar financiën niet meer beheren. Ondanks handmatige interventies volgde een faillissement in september 2023. Organisaties die afhankelijk zijn van IT-projecten voor het behalen van hun strategische doelstellingen ondervinden een dubbele klap als deze projecten falen. Niet alleen worden de verwachte voordelen niet gerealiseerd, maar concurrenten die wel succesvol digitaliseren, kunnen een onoverbrugbare voorsprong opbouwen.

Mislukte IT-projecten, vooral die met hoge zichtbaarheid, kunnen leiden tot ernstige reputatieschade. Dit kan investeerders en kredietverschaffers afschrikken, waardoor

[2] Een Black Swan is een onverwachte en zeldzame gebeurtenis met ingrijpende gevolgen, die vooraf vrijwel onmogelijk te voorspellen lijkt maar achteraf vaak als verklaarbaar wordt gezien. Je kunt denken aan denk aan financiële crises, pandemieën, de Eerste Wereldoorlog of grote digitale aanvallen. Het begrip, geïntroduceerd door Nassim Nicholas Taleb, benadrukt hoe zulke schokken buiten de normale aannames en modellen vallen, terwijl hun impact enorm kan zijn. Het dwingt organisaties rekening te houden met onzekerheid en veerkracht, in plaats van uitsluitend te vertrouwen op lineaire risico-inschattingen.

de toegang tot kapitaal voor toekomstige projecten wordt beperkt. Het verlies aan vertrouwen van stakeholders kan langdurige gevolgen hebben voor de organisatie.

De gevolgschade van softwarefalen is wereldwijd enorm en loopt in de biljoenen euro's per jaar. Recente onderzoeken benadrukken dat de directe én indirecte kosten van slechte softwarekwaliteit en softwarestoringen exponentieel zijn toegenomen. In de Verenigde Staten bedroegen de kosten van slechte softwarekwaliteit in 2022 minimaal $ 2,41 biljoen (ongeveer € 2,2 biljoen) becijfert de Standish Group. Zij onderzochten 50.000 mislukte projecten. In dit cijfer zitten kosten van digitale criminaliteit (cybercrime), beveiligingsincidenten door softwarelekken, operationele softwarestoringen, downtime, kosten van mislukte IT-projecten en 'technical debt' (technische schuld ofwel achterstallig onderhoud en verouderde systemen). Maar als grootste kostenpost zijn operationele verstoringen goed voor een schadepost van $1,56 biljoen (circa €1,34 biljoen) zoals in 2020 blijkt uit een rapportage van BGC.

Wereldwijd zijn de kosten nog hoger. De verwachte schade door digitale criminaliteit, vaak mogelijk gemaakt door softwarefouten, wordt voor 2025 in het Cybersecurity Ventures-rapport geschat op $ 10,5 biljoen (circa € 9 biljoen). Dit komt doordat er naast directe financiële verliezen indirecte gevolgen zijn, zoals reputatieschade en verlies van klantvertrouwen, productiviteitsverlies door uitval van systemen, juridische claims en boetes bij datalekken of niet-naleving van regelgeving en natuurlijk verhoogde operationele kosten door noodreparaties en herstelmaatregelen.

De gevolgschade door software falen is niet alleen een kwestie van miljarden, maar loopt wereldwijd in de biljoenen euro's per jaar. Dit onderstreept het belang van investeren in softwarekwaliteit, robuuste beveiliging en goed projectmanagement om deze immense schade te beperken. Het is daarnaast duidelijk dat er een harde link is tussen het ontwikkelen van software en de gevolgen voor informatiebeveiliging.

Een prijskaartje als randvoorwaarde

De randvoorwaardelijkheid van informatiebeveiliging roept de vraag op welke inspanning een organisatie moet doen en wat dat dan moet kosten. Bij het goed beschermen van de organisatie komt veel kijken. Daarbij is het niet voldoende om alleen de handelingen te doen, omdat verschillende wetgeving van de bestuurder vraagt daadwerkelijk te kunnen bewijzen dat er wordt voldaan. Om een serieuze kans op succes te maken is het integraal en gestructureerd organiseren van informatie-beveiliging noodzakelijk. Dit houdt in dat een organisatie meer moet doen dan de techniek op orde krijgen. Goede informatiebeveiliging vraagt om een samenhangend geheel van technische, organisatorische, strategische en menselijke maatregelen die in

samenhang functioneren. Dat betreft veel verschillende activiteiten om dit te organiseren, waarbij het goed is te beseffen wat er zoal moet gebeuren.

Allereerst ligt een stevige basis bij duidelijke governance en compliance ofwel: het omgaan met regulering. Governance bepaalt wat moet gebeuren en hoe dat echt gebeurt volgens de regels. Het begrip governance is het geheel aan structuren, processen en gedragsregels waarmee een organisatie wordt bestuurd, controle en verantwoordelijk wordt georganiseerd.

In de context van informatie betekent dit dat voor iedereen duidelijk is wie verantwoordelijk is voor het beveiligingsbeleid, wie mag beslissen over risico's en maatregelen, hoe naleving wordt gecontroleerd en hoe er gerapporteerd wordt aan het bestuur of externe toezichthouders. Een goede governancestructuur zorgt voor heldere rollen, expliciete besluitvormingsprocessen en voorkomt dat belangrijke besluiten willekeurig of ondoorzichtig (of niet) genomen worden. Zo draagt governance bij aan betrouwbaarheid, integriteit en het effectief functioneren van de organisatie. Dat goed functioneren kan alleen slagen als het bestuur besluiten neemt die de operationele kant opdragen én in staat stellen beveiliging te realiseren.

Naast governance is het van groot belang dat de organisatie haar risico's kent. Zonder dat inzicht is de informatiebeveiliging niet gericht op het halen van de organisatiedoelen. Daarom is risicomanagement essentieel. Dit betekent dat een organisatie dreigingen en kwetsbaarheden continu in kaart brengt, de mogelijke impact daarvan beoordeelt en vervolgens passende maatregelen neemt om deze risico's te beheersen. Dit vraagt om een gestructureerde aanpak en voortdurende aandacht, aangezien nieuwe dreigingen zich snel ontwikkelen.

De uitvoering van informatiebeveiliging kent meerdere dimensies. Technische maatregelen, zoals goede netwerkbeveiliging met firewalls, antivirussoftware, segmenteren van netwerken, segmenteren van functionaliteit, up-to-date houden van omgevingen, monitoren en beveiligen van endpoints, vormen hierbij het fundament.

Naast techniek is organisatie een belangrijk onderdeel. Want goede informatiebeveiliging is niet compleet zonder aandacht voor organisatorische maatregelen. Een mooi voorbeeld is het toegangsbeheer: het moet duidelijk zijn wie welke toegang heeft en waarom. Dit moet periodiek worden geëvalueerd. Het creëren van een sterke bewustzijnscultuur onder medewerkers is essentieel. Veel beveiligingsincidenten vinden hun oorsprong in menselijke fouten, zoals klikken op phishingmails of het onbedoeld lekken van data. Door regelmatig trainingen te geven en medewerkers bewust te maken van risico's, verlaagt een organisatie deze kwetsbaarheid aanzienlijk. Want uiteindelijk staat de mens centraal.