Nathalie Claes

GEHACKT, WAT NU?

Bescherm je bedrijf tegen cybercriminelen

PELCKMANS

Inhoud

Dankwoord

Al jaren loop ik rond met het idee om een boek te schrijven, maar ik had geen idee hoe eraan te beginnen. Het was een Mount Everest, die niet te beklimmen leek. Met de hulp van Laurence Verwee ben ik er toch in geslaagd om de nodige stappen te zetten. Bedankt, Laurence, om me af en toe een liefdevolle schop onder de kont te geven en me te motiveren om door te zetten.

Een boek schrijven gaat ten koste van tijd die je anders met je gezin zou spenderen. Een speciaal woord van dank is dan ook zeker op zijn plaats voor mijn dochter, Myrthe, die me af en toe heeft moeten missen omdat ik met mijn neus in mijn eigen boek zat. Ook zonder mijn partner Johan, die me, wanneer de moed me in de schoenen zakte, iedere keer weer omhoog praatte, zou dit boek er niet zijn.

Daarnaast wil ik mijn mentoren en onderwijzers bedanken, die me door de jaren heen hebben begeleid, geïnspireerd en gevormd. Hun wijsheid en kennis hebben me niet alleen professioneel vooruitgeholpen, maar hebben me ook het zelfvertrouwen gegeven om aan dit avontuur te beginnen. Ook mijn klanten, die waardevolle input hebben geleverd door hun inzichten en ervaringen met me te delen, verdienen mijn oprechte dank. Zonder hun dagelijkse uitdagingen en vragen had dit boek misschien een andere vorm aangenomen.

Een bijzonder woord van dank gaat uit naar mijn proeflezers. Jullie eerlijke feedback en kritische opmerkingen hebben me geholpen om mijn ideeën scherper te formuleren en mijn verhaal duidelijker over te brengen. Dankzij jullie geduld en constructieve input heb ik dit boek naar een hoger niveau kunnen tillen.

En ten slotte gaat mijn grootste dank uit naar mijn ouders. Jullie hebben me alle kansen gegeven om mezelf te ontwikkelen en me door de jaren heen onvoorwaardelijke steun geboden. Jullie geloof in mij heeft me altijd aangemoedigd om mijn dromen na te jagen, en daar ben ik eeuwig dankbaar voor.

Inleiding

Cyberdreigingen zijn overal en zijn dagelijkse realiteit geworden, in alle types van bedrijven, al komen enkel de 'grote gebeurtenissen' in het nieuws. Als ondernemer of manager heb je waarschijnlijk wel eens nagedacht over de beveiliging van je digitale omgeving. De kans is groot dat je denkt: bij mij gebeurt dat niet of mijn bedrijf is toch niet interessant genoeg voor hackers. De realiteit is dat cybercriminelen niet discrimineren op basis van grootte of type bedrijf; ze zoeken naar zwakke schakels. Elk bedrijf, hoe klein ook, kan een aantrekkelijk doelwit zijn. Het kan letterlijk iedereen overkomen. De vraag is dus niet óf, maar wannéér je er slachtoffer van wordt. Misschien vraag je je af of je wel genoeg doet om je bedrijf te beschermen, of je twijfelt over waar je moet beginnen. Herken je deze zorgen? Dan ben je niet alleen. Veel ondernemers worstelen met deze vragen, en dat is precies waarom ik dit boek heb geschreven. Informatieveiligheid is niet alleen een IT-kwestie; het is een essentiële verantwoordelijkheid van iedereen in je bedrijf.

De meeste ondernemers zien cybersecurity als een ver-van-hun-bedshow, iets wat vooral met techniek te maken heeft en door de IT-afdeling wordt geregeld. Maar de realiteit is anders: het is een menselijke kwestie, waarbij de grootste risico's meestal voortkomen uit menselijk gedrag, zoals klikken op een verkeerde link of delen van gevoelige informatie. Jouw medewerkers, klanten en zelfs leveranciers kunnen allemaal onbedoeld bijdragen aan de kwetsbaarheid van je bedrijf.

Herken je het gevoel van overweldiging als het gaat om de complexiteit van informatieveiligheid? Voelt het ook vaak alsof de mensen van je IT-afdeling een totaal andere taal spreken? Of voel je je onzeker over de stappen die je moet nemen om je digitale assets te beschermen?
Dan is dit boek voor jou. Laten we samen deze uitdagingen aanpakken, zodat je met vertrouwen je bedrijf kunt beschermen tegen de voortdurende dreigingen in de digitale wereld.

Ik heb dit boek geschreven vanuit mijn ervaring als Chief Information Security Officer (CISO), Data Protection Officer (DPO) en externe auditor. Al meer dan 20 jaar help ik bedrijven om grip te krijgen op hun informatieveiligheid. Door de jaren heen heb ik bedrijven van verschillende groottes en in diverse sectoren geholpen die allemaal dezelfde fundamentele fouten maakten: ze onderschatten de risico's, vertrouwden te veel op technologie zonder een solide strategie of dachten dat informatieveiligheid uitsluitend een taak voor de IT-afdeling was. Mijn drijfveer om dit boek te schrijven is het delen van mijn kennis en ervaringen om ondernemers en managers te helpen begrijpen wat er echt nodig is om je bedrijf te beschermen. Ik ben ervan overtuigd dat iedereen, met de juiste kennis en hulpmiddelen, de kracht heeft om zijn bedrijf te beveiligen tegen cyberdreigingen. Dit boek is een praktische gids, bedoeld om je stap voor stap mee te nemen in de wereld van informatieveiligheid, zodat je niet alleen begrijpt wát je moet doen, maar ook waarom.

Het uiteindelijke doel van dit boek is simpel: ik wil je helpen je bedrijf beter te beveiligen, een veilige toekomst voor je bedrijf te garanderen en je weer in controle te laten voelen. Het beschermen van je bedrijf tegen cyberdreigingen kan overweldigend lijken, maar met de juiste aanpak en hulpmiddelen is het haalbaar. Dit boek biedt je de kennis en de tools om proactief aan de slag te gaan met informatieveiligheid. Het is mijn missie om je niet alleen te informeren, maar vooral ook in staat te stellen om zelfverzekerd beslissingen te nemen die je bedrijf veiliger maken. Jij hebt de kracht om de veiligheidscultuur binnen je bedrijf te versterken, en ik ben hier om je te laten zien hoe. Bovendien is dit boek geschreven in begrijpelijke, normale mensentaal, zonder ingewikkeld jargon, zodat ook jij, zonder uitgebreide IT-kennis, alles eenvoudig kunt begrijpen en toepassen.

Wat kun je verwachten van dit boek? Niet alleen krijg je inzicht in de tactieken van hackers en de zwakke punten van je eigen bedrijf, maar je leert ook hoe je een robuuste veiligheidscultuur creëert. Dit boek helpt je om…

- inzicht te krijgen in de acht meest voorkomende manieren waarop hackers bedrijven aanvallen, van phishing en *baiting* tot *insider threats* en *supply chain attacks*;
- praktische stappen te zetten om je bedrijf te beschermen, inclusief tips voor training van je medewerkers en het opzetten van effectieve beveiligingsmaatregelen;
- een veiligheidscultuur te creëren binnen je bedrijf waarin iedereen, van de directie tot de werkvloer, zijn verantwoordelijkheid neemt voor informatieveiligheid;
- mensen samen te brengen en te enthousiasmeren voor een veilige bedrijfscultuur;

- je bedrijf weerbaarder te maken tegen de constante dreiging van cyberaanvallen, zodat je niet alleen reactief bent, maar vooral proactief je risico's beheert;
- de complexiteit van wet- en regelgeving rond informatieveiligheid te begrijpen, zoals de Cyber Resilience Act, NIS2 en de AI Act, en hoe je kunt voldoen aan de eisen die deze wetten stellen.

Door dit boek te lezen, krijg je niet alleen antwoorden op je vragen, maar ook de kennis en het vertrouwen om actie te ondernemen. Je ontdekt dat informatieveiligheid niet alleen gaat over dure software of technische termen, maar vooral over de mensen in je bedrijf en hoe zij met informatie omgaan. Meer rust, meer controle en een sterker beveiligd bedrijf zijn de beloningen voor je inspanningen. Dit boek geeft je de tools om deze doelen te bereiken.

Om het leesgemak te verhogen en ervoor te zorgen dat je de informatie kunt toepassen, is elk hoofdstuk van dit boek opgebouwd uit verschillende delen. Ieder hoofdstuk begint met een herkenbare situatie of een verhaal, vaak gebaseerd op echte gebeurtenissen. Daarna volgt een uitleg van de specifieke dreiging en waarom het belangrijk is om deze serieus te nemen. Vervolgens biedt ieder hoofdstuk praktische tips en stappen die je kunt nemen om je bedrijf te beschermen, aangevuld met voorbeelden uit de praktijk. De voorbeelden die ik in het boek gebruik komen zowel uit België en Nederland als uit de Verenigde Staten en andere werelddelen. Deze structuur helpt je om de informatie niet alleen te begrijpen, maar ook toe te passen in je dagelijkse bedrijfsvoering. Ik heb ervoor gekozen om deze aanpak te gebruiken omdat het belangrijk is dat je niet alleen leest over de dreigingen, maar ook begrijpt hoe je ze in de praktijk kunt aanpakken. Achteraan het boek vind je checklists per hoofdstuk die je kunt gebruiken bij de implementatie in jouw organisatie.

Twijfel je nog of je dit boek moet lezen? Laat me je dan inspireren om die eerste stap te zetten: de bescherming van je bedrijf begint met kennis. Elke dag dat je wacht, loop je risico, maar door te investeren in je eigen kennis en die van je team, kun je je bedrijf een veilige toekomst bieden. Cyberaanvallen stoppen niet, maar jij kunt ervoor zorgen dat jouw bedrijf voorbereid is. Begin vandaag met het versterken van je informatieveiligheid en lees dit boek. Neem meteen de eerste stap naar een veiliger bedrijf en ontdek hoe je met vertrouwen door de uitdagingen van de digitale wereld kunt navigeren. Samen maken we jouw bedrijf sterker en weerbaarder tegen cyberdreigingen. *Let's get started!*

HOOFDSTUK 1

Informatieveiligheid heeft niks met IT te maken

In de huidige digitale wereld is het niet de vraag óf je als ondernemer met informatieveiligheidsproblemen te maken krijgt, maar wanneer. Dat is een realiteit waar veel kmo's zich onvoldoende van bewust zijn. 'Bij mij gebeurt dat niet' is een veelgehoorde uitspraak, maar helaas ook een gevaarlijke misvatting. Juist kmo's zijn interessante doelwitten voor cybercriminelen, omdat zij vaak denken niet interessant genoeg te zijn en daardoor minder goed beveiligd zijn.

Veel bedrijven staan er niet bij stil welke risico's ze dagelijks lopen. Ik kan zo uit de losse pols meer dan 300 verschillende soorten risico's opsommen die, in een gemiddeld bedrijf, de vertrouwelijkheid (*Confidentiality*), de integriteit (*Integrity*) en de beschikbaarheid (*Availability*) van gegevens kunnen bedreigen. Dit wordt vaak afgekort als de CIA-triade. Voor een hacker is jouw bedrijf slechts één doelwit tussen vele, maar voor jou kan een enkele aanval rampzalige gevolgen hebben.

Een hacker ziet jouw bedrijf als een potentieel goudmijntje. Ze gaan massaal e-mails versturen en aanvallen uitvoeren totdat ze een zwakke plek vinden. Zodra dat gebeurt, word jij een doelwit. En niet alleen IT komt onder vuur te liggen. Hr, Finance, Marketing en Sales zijn allemaal aantrekkelijke targets vanwege de waardevolle informatie die ze beheren. De meeste bedrijven besteden onvoldoende aandacht aan de risico's en denken vaak dat het allemaal wel losloopt.

EUROPESE WETGEVING EN RICHTLIJNEN

Bovendien zien we vanuit Europa ook meer en meer wetgeving die tot stand komt, mede door de constante verandering op het vlak van informatieveiligheid. Een van de belangrijkste ontwikkelingen is de Cyber Resilience Act, die als doel heeft de digitale weerbaarheid van producten met digitale elementen te versterken door

middel van duidelijke veiligheidsnormen. Deze wetgeving verplicht bedrijven om aan specifieke beveiligingsnormen te voldoen, wat niet alleen de algehele veiligheid verbetert, maar ook het vertrouwen van consumenten en zakenpartners versterkt.

Daarnaast is er de NIS2-richtlijn, een herziening van de oorspronkelijke NIS-richtlijn (Network and Information Security), die veel verder gaat in het versterken van de beveiliging van netwerken en informatiesystemen binnen de Europese Unie. De NIS2-richtlijn legt strengere eisen op aan bedrijven en organisaties, met name in sectoren die van essentieel belang zijn voor de economie en de samenleving, zoals energie, transport, gezondheidszorg en digitale infrastructuur. Bedrijven moeten nu proactief beveiligingsmaatregelen implementeren en regelmatig risicoanalyses uitvoeren om de continuïteit van hun diensten te waarborgen. Bovendien valt ook de hele toeleverancierskeketen mee onder de NIS2-wetgeving. Dus zelfs al val je niet direct onder het toepassingsgebied van de richtlijn, de kans is groot dat je er toch, door de nadruk op de toeleverancierskeketen, mee in aanraking zult komen. De NIS2-wetgeving is in oktober 2024 in voege getreden.

De AI Act richt zich op de regulering van kunstmatige intelligentie binnen de Europese Unie. Deze wetgeving stelt duidelijke regels en richtlijnen voor het gebruik van AI, met als doel de ethische en veilige toepassing ervan te garanderen. Voor bedrijven betekent dit dat ze zorgvuldig moeten nadenken over hoe ze AI integreren in hun producten en diensten en dat ze ervoor moeten zorgen dat hun AI-systemen transparant, betrouwbaar en vrij van vooroordelen zijn.

Andere relevante wetgevingen omvatten de Algemene Verordening Gegevensbescherming (AVG), die sinds 2018 van kracht is en strikte regels stelt aan de verwerking en bescherming van persoonlijke gegevens. De AVG heeft een brede impact op bedrijven van alle groottes, die nu verplicht zijn om zorgvuldige maatregelen te nemen om de privacy van hun klanten te waarborgen.

Deze toenemende wetgevingsdruk dwingt bedrijven om hun informatieveiligheidsstrategieën te herzien en te versterken. Bovendien zijn er bovenop de algemeen geldende wet- en regelgeving ook sectorspecifieke regels, zoals de DORA-wetgeving. Het naleven van deze wetten vereist investeringen in technologie, processen en opleiding, maar biedt ook kansen om het vertrouwen van klanten te winnen en de bedrijfscontinuïteit te waarborgen. Het is evident dat bedrijven die deze wetgevingen serieus nemen en proactief stappen ondernemen om te voldoen

aan de regelgeving, zichzelf beter positioneren in een steeds complexere en risicovollere digitale wereld.

DE OPKOMST VAN AI EN HET DOMINO-EFFECT

Een belangrijk aspect dat vaak over het hoofd wordt gezien, is het domino-effect. Een enkele zwakke schakel kan leiden tot een kettingreactie van problemen.

Even uitleggen aan de hand van een concreet voorbeeld: een *supply chain attack*, ofwel een aanval op de toeleveringsketen. Stel je voor dat jouw bedrijf, net als de meeste bedrijven, afhankelijk is van verschillende leveranciers en partners om te kunnen functioneren. Dat kunnen leveranciers van software, hardware of zelfs diensten zijn. Een *supply chain attack* vindt plaats wanneer een hacker een zwakke plek bij een van je leveranciers gebruikt als een ingang om jouw bedrijf aan te vallen.

Bijvoorbeeld: jouw bedrijf gebruikt een softwarepakket van een externe leverancier voor je dagelijkse bedrijfsvoering. Deze leverancier wordt echter gehackt omdat ze hun beveiliging niet op orde hebben. De hacker plaatst schadelijke code in de software-updates die jouw bedrijf ontvangt. Omdat je het softwarepakket vertrouwt en regelmatig updates installeert, wordt de schadelijke code ongemerkt in je eigen systemen geïnstalleerd. Vanaf dat moment heeft de hacker toegang tot jouw bedrijfsgegevens en kan hij ernstige schade aanrichten.

Het domino-effect komt hier goed naar voren, omdat de zwakke beveiliging van één leverancier kan leiden tot een reeks van problemen binnen jouw bedrijf. Het begint met een aanval op je leverancier, maar de impact verspreidt zich snel naar jouw systemen, en mogelijk zelfs naar je eigen klanten als de situatie niet snel wordt aangepakt. Dat kan leiden tot verlies van data, verstoring van je bedrijfsactiviteiten en ernstige reputatieschade.

Met de opkomst van AI worden deze *supply chain attacks* alleen maar geavanceerder. Hackers kunnen AI gebruiken om sneller en efficiënter zwakke plekken te vinden in de systemen van leveranciers, en om complexere aanvallen uit te voeren die moeilijker te detecteren zijn. AI kan bijvoorbeeld patronen herkennen in netwerkverkeer die wijzen op kwetsbaarheden, of automatisch phishingaanvallen uitvoeren op medewerkers van leveranciers om toegang te krijgen tot gevoelige informatie.

AI wordt steeds vaker gebruikt door cybercriminelen om geautomatiseerde aanvallen uit te voeren, kwetsbaarheden te scannen en zelfs social engineering-technieken te verbeteren. Dit betekent dat bedrijven niet alleen moeten investeren in traditionele beveiligingsmaatregelen, maar ook in geavanceerde technologieën om zich te beschermen tegen AI-gedreven dreigingen.

SOCIAL ENGINEERING

Social engineering is een methode waarbij cybercriminelen mensen manipuleren om vertrouwelijke informatie prijs te geven of acties te ondernemen die schadelijk zijn voor hun bedrijf. In plaats van technische systemen te hacken, spelen aanvallers in op menselijke emoties, zoals nieuwsgierigheid, angst of behulpzaamheid. Dit gebeurt bijvoorbeeld via phishing-e-mails die lijken te komen van betrouwbare bronnen, of door fysieke lokmiddelen zoals besmette USB-sticks.

Het is belangrijk voor bedrijven om te begrijpen hoe AI werkt en hoe het kan worden ingezet om zowel bedreigingen te identificeren als zich te verdedigen tegen aanvallen. Dit omvat het implementeren van AI-gebaseerde beveiligingsoplossingen die anomalieën in netwerkverkeer kunnen detecteren, verdachte activiteiten kunnen identificeren en automatisch kunnen reageren op dreigingen.

Daarnaast moeten bedrijven zich bewust zijn van de ethische implicaties van AI en ervoor zorgen dat hun AI-systemen transparant, verantwoord en vrij van vooroordelen zijn. Dat helpt niet alleen om juridische en reputatierisico's te verminderen, maar draagt ook bij aan het opbouwen van vertrouwen bij klanten en zakenpartners.

Voor bedrijven betekent dit dat ze niet alleen hun eigen beveiliging moeten versterken, maar ook die van hun hele toeleveringsketen. Dat kan door samen te werken met leveranciers om ervoor te zorgen dat zij ook voldoen aan hoge beveiligingsnormen, en door regelmatig audits uit te voeren om de beveiliging van leveranciers te controleren. Daarnaast moeten bedrijven noodplannen hebben om snel te kunnen reageren als er een aanval plaatsvindt, zodat de schade beperkt blijft en de bedrijfscontinuïteit gewaarborgd is.

Ik ervaar vaak in bedrijven dat hier nog veel te weinig bij stil wordt gestaan, dat informatie nog te veel verspreid zit en nergens gedocumenteerd is. Hierdoor spreek ik altijd van een hoge 'bus-factor'. Als één iemand onder een bus terechtkomt, stort het hele huis in. En dat moet je koste wat kost vermijden.