Cybersecurity risico’s bij Amerikaanse bedrijven

In hoeverre volstaat het cybersecurity beleid van Amerikaanse bedrijven om data te beschermen en ingrijpende gevolgen zoals datalekken en ransomware attacks te voorkomen?

Naam: Amine El Yaakoubi

Studentnummer: 609413

Deelproduct: Onderzoeksopdracht Smart Start

Datum: 25-10-2022

Titelpagina

Titel	: Cybersecurity risico’s bij Amerikaanse bedrijven
Ondertitel	: In hoeverre volstaat het cybersecurity beleid van Amerikaanse bedrijven om data te beschermen en ingrijpende gevolgen zoals datalekken en ransomware attacks te voorkomen?
Auteur	: El Yaakoubi, Amine (609413)
Contactgegevens student	: A.ElYaakoubi@student.han.nl / +31 (0) 685484385
Module	: Smart Start (Onderzoeksopdracht)
Opleidingsinstituut	: Hogeschool van Arnhem en Nijmegen
Opleiding	: Bedrijfskunde MER
Docenten	: ten Hove, Witek Bijsterveld, Hubert
Illustratie kaft	: (Goldman, 2021)
Versienummer	: 1.0

Inhoudsopgave

Hoofdstuk 1. Inleiding

1.1 Context

In dit rapport is de uitwerking van mijn onderzoek voor het vak Smart Start opgenomen. In de eerste sprint van het vak Smart Start ben ik opzoek gegaan naar bronnen voor die bij mijn onderzoekvraag horden. Ik voornamelijk via Google Scholar en de databanken van de HAN gezocht. De onderzoekvraag die ik heb bedacht luidt als volgt:

- In hoeverre volstaat het cyber security beleid van Amerikaanse bedrijven om data te beschermen en ingrijpende gevolgen zoals datalekken en ransomware attacks te voorkomen?

Om de onderzoeksvraag te kunnen beantwoorden zijn de volgende subvragen opgesteld:

- Wat zijn de trends en ontwikkelingen op het gebied van effectieve aanpak van cyber security risico's?
- Op welk niveau bevindt het cyber security beleid van Amerikaanse bedrijven zich op dit moment?
- Wat moet er gebeuren bij Amerikaanse bedrijven om het gewenste volwassenheidsniveau t.a.v. van cyber security te bereiken?

1.2 Onderzoeksopzet

Er is uitsluitend gebruik gemaakt van literatuuronderzoek op de onderzoeksvraag te kunnen beantwoorden. Het gaat dus om een kwalitatief onderzoek. Er is gekozen voor deze onderzoeksmethode, omdat er nog weinig bekend is op de invloed van workforce management op de cyber security huishouding van Nederlandse bedrijven. In bijlage 1 is een uitgebreide beschrijving te lezen van de onderzoeksopzet.

1.3 Leeswijzer

In hoofdstuk 2, 3 en 4 wordt in chronologische volgorde antwoord gegeven op de opgestelde deelvragen om de onderzoeksvraag te beantwoorden. In hoofdstuk 5 worden de belangrijkste conclusies beschreven die uit het onderzoek zijn voortgevloeid. Tenslotte is terug te lezen welke bronnen zijn gebruikt en in bijlage 1 hoe het onderzoek precies is opgezet.

Hoofdstuk 2. Wat zijn de trends en ontwikkelingen op het gebied van effectieve aanpak van cyber security risico's?

2.1 Definitie van cybersecurity

Vandaag de dag hebben bedrijven te maken met cyberaanvallen, zoals datalekken, die ingrijpende gevolgen hebben op de bedrijfsvoering. Volgens onderzoek van (IBM, 2018) kost een datalek gemiddeld $3.86 miljoen Amerikaanse dollars. Door deze trend, is cybersecurity en privacy een van de meest kritieke problemen binnen IT-management systemen van bedrijven volgens een rapport uit 2019 van SIM IT Trends (Guerra & Kim, 2020). Ondanks de grote aandacht die er is voor cybersecurity risico's, is een duidelijke definitie van de term nog steeds niet naar voren gekomen in het bedrijfsleven en de literatuur. De reden hiervoor komt doordat de term cybersecurity een containerbegrip is geworden en de interdisciplinaire aard van de term (Craigen et al., 2014). De term cybersecurity roept vooral technische, organisatorische en politieke knelpunten op en het gevolg hiervan is dan ook dat het een uitdaging is om het eens te worden over een uniforme definitie van het woord die alle vakgebieden tevreden stelt. In tabel 1 hieronder zijn twee algemene definities van de term cyber security opgenomen.

'Verbeterde' definitie van cyber security	"De aanpak en acties die samenhangen met veiligheidsrisico managementprocessen gevolgd door organisaties en staten om de vertrouwelijkheid, integriteit en beschikbaarheid van gegevens en activa die in cyberspace worden gebruikt. Het concept omvat: richtlijnen, beleid en verzamelingen van voorzorgsmaatregelen, technologieën, tools en training om de beste bescherming voor de toestand van de cyberomgeving en zijn gebruikers" (Schatz et al., 2017).
	Cybersecurity is het organiseren en verzamelen van middelen, processen en structuren die worden gebruikt om cyberspace en cyberspace-compatibele systemen van voorvallen die de jure niet op één lijn brengt met de facto eigendomsrechten" (Craigen et al., 2014).

Tabel 1. Definitie van cyber security uit literatuur (Guerra & Kim, 2020).

2.2 Opkomst van cyberaanvallen

Cyber security is altijd al een niet eindigende race geweest voor bedrijven, maar de bereidheid om cyber security portfolio's te verbeteren zit in de lift. Bedrijven zijn namelijk nog steeds bezig met investeren in technologie om hun bedrijven op een verantwoorde manier te runnen. Momenteel zijn bedrijven bezig met het inbedden van meer systemen in hun IT/netwerken

voor de ondersteuning van thuiswerken, verbetering van klanttevredenheid en de winstgevendheid van de organisatie verhogen. Deze zaken creëren uiteindelijk juist meer potentiële zwakheden in de IT-systemen van bedrijven.

Bovendien werken cybercriminelen steeds minder op individueel niveau, maar in geavanceerde organisaties die gebruik maken van geïntegreerde tools en de mogelijkheid om gebruik te maken van kunstmatige intelligentie (AI) en machine learning. De omvang van de dreiging voor informatiesystemen blijft hierdoor groeien en geen enkele organisatie blijkt hiervoor immuun te zijn. MKB-bedrijven, multinationals, gemeentes en federale overheden worden steeds vaker geconfronteerd met dergelijke risico's. Boehm et al. (2020) gaan zelfs zo ver in hun analyse, dat de meeste geavanceerde cybercontroles, hoe effectief ze ook zijn, binnen korte tijd achterhaald zullen zijn.

In het huidige cybersecurity landschap moeten bestuursorganen zich twee zaken afvragen:

- Zijn we voorbereidt voor de snelle digitalisatie voor de komende 3 tot 5 jaar?
- Kijken we ver genoeg vooruit om te begrijpen welke gevolgen hedendaagse technologische investeringen hebben op de cyber security van de toekomst?"

In figuur 1 zijn een aantal belangrijke kengetallen op een rijtje gezet om een gedegen antwoord te geven op de bovenstaande vragen.

Figuur 1. Vooruitzichten voor de cybersecurity markt (Boehm et al., 2020).

2.3 Drie cybersecurity trends met grote implicaties

Bedrijven kunnen de knelpunten die zich in de toekomst kunnen voordoen alleen tackelen en beperken door een proactieve en toekomstgerichte houding aan te nemen. Boehm et al. (2022) verwachten dat de drie cybersecurity trends in tabel 1 de komende drie tot vijf jaar grote gevolgen zal hebben voor organisaties over de hele wereld.

Cybersecurity trend	Toelichting
Toegang tot allesomvattende data- en informatieplatforms neemt toe	Mobiele platformen, op afstand werken en andere veranderingen worden steeds meer afhankelijk van de snelle toegang tot integrale datasets en databanken, waardoor de kans op een cyberaanval toeneemt. Zo zal de markt voor webhosting diensten in 2026 $183,18 miljard Amerikaanse dollars waard zijn. Organisaties verzamelen veel gegevens over klanten om koopgedrag te begrijpen en te beïnvloeden om effectiever op de vraag in te spelen. Door het grotere belang van cloud omgevingen worden bedrijven steeds meer verantwoording voor het opslaan, beheren en beschermen van deze gegevens en het onder controle houden van extreme datavolumes. Om dergelijke bedrijfsmodellen te implementeren, hebben bedrijven nieuwe platformen nodig zoals datameren die informatie kunnen verzamelen (zoals de kanaalactiva van leveranciers en partners). Naast het verzamelen van data, centraliseren bedrijven hun data ook steeds meer en verlenen steeds vaker toegang aan een breed scala aan individuen en organisaties (inclusief derden zoals leveranciers). Recente spraakmakende aanvallen maakten gebruik van deze uitgebreide gegevenstoegang van bedrijven. Neem bijvoorbeeld de hack bij Sunburst in 2020. Deze cyberaanval zorgde ervoor dat malware werd verspreid naar klanten tijdens regelmatige software updates.
Hackers gebruiken steeds vaker AI, Machine Learning en andere technologieën voor cyberaanvallen	De doorsnee hacker die alleen te werk gaat, kan vandaag de dag niet meer als grootste bedreiging voor bedrijven worden gezien. Tegenwoordig bestaan er grote criminele organisaties die zich hebbe toegelegd op cyber attacks waarin miljarden dollars worden verdiend (INSUREtrust, 2019) met complete bedrijfsstructuren en R&D-budgetten. Cyberaanvallers gebruiken geavanceerde tools, zoals AI, Machine Learning en automatiseringstechnieken. De verwachting van Boehm et al. (2020) is dat hackers in de komende jaren in staat zullen zijn om de levenscyclus van cyberaanvallen te versnellen en verlengen. Dit betreft het proces van verkenning tot aan de uiteindelijke exploitatie van systemen. Een goed voorbeeld is de geavanceerde malware Emote, wat vooral gebruikt wordt tegen banken. Emote staat

	erom bekend dat het de aard van zijn aanvallen kan veranderen. In 2020 maakte hackers met Emote gebruik van AI en machine learning technieken om de effectiviteit van aanvallen te vergroten en het verbeteren van het geautomatiseerde proces van phishing mails. Geavanceerde technologieën zorgen ervoor dat bekende vormen van cyberaanvallen, zoals ransomware en phising, steeds vaker voorkomen. Onder andere cryptocurrencies en Ransomware as a Service (RaaS) hebben de kosten voor het uitvoeren van ransomeware aanvallen aanzienlijk verlaagd. Sterker nog sinds 2019 is het aantal ransomeware aanvallen ieder jaar verdubbeld in aantal. Verder veroorzaken andere gebeurtenissen ook een piek in het aantal ransomeware aanvallen. Tijdens de eerste golf van COVID-19, van februari 2020 tot maart 2020, steeg het aantal ransomware aanvallen in de wereld met maar liefst 148 procent. Tenslotte steeg het aantal phishing aanvallen van januari tot februari 2020 met 510 procent (Carlson, 2021).
Continue groei van regelgeving voor cybersecurity en kritieke kloven tussen middelen, kennis en talent zal cybersecurity in de toekomst ontstijgen	Veel organisaties hebben onvoldoende talent, kennis en expertise op het gebied van cyberbeveiliging. Daarnaast groeit dit tekort in rap tempo. Over het algemeen heeft cyber risicomanagement geen gelijk trend aangehouden met de ontwikkeling van digitale en analytische transformaties van IT-systemen. Ook weten bedrijven niet zo goed hoe ze digitale risico's moeten identificeren en beheren. Deze uitdaging wordt door overheden en wetgevers vergroot door de toenemende richtlijnen op het gebied van cybersecurity capaciteiten van bedrijven. Verder hebben bedrijven ook te maken met strengere regelgeving foor de toenemende privacy problemen en spraakmakende datalekken die in de media verschijnen.

Tabel 1. Drie cybersecurity trends met grote implicaties (Boehm et al., 2022).

Hoofdstuk 3. Op welk niveau bevindt het cybersecurity beleid van Amerikaanse bedrijven zich op dit moment?

3.1 Introductie

In het afgelopen jaar heeft de wereld zijn leerstellingen getrokken uit de coronapandemie. In het bedrijfsleven worstelen bedrijven met een balans vinden tussen remote werken vanaf thuis en bedrijfscultuur in stand houden. Op technisch niveau, worden de vele voordelen van een cloud architectuur gewogen tegen de uitdaging om de complexiteit van cloud services te managen. Het zal nog jaren duren voordat de impact van de pandemie zichtbaar is voor de cybersecurity van bedrijven, maar de huidige veranderingen in het technische landschap wijzen op een herstructurering van de bestaande cybersecurity aanpak van bedrijven (CompTIA, 2022).

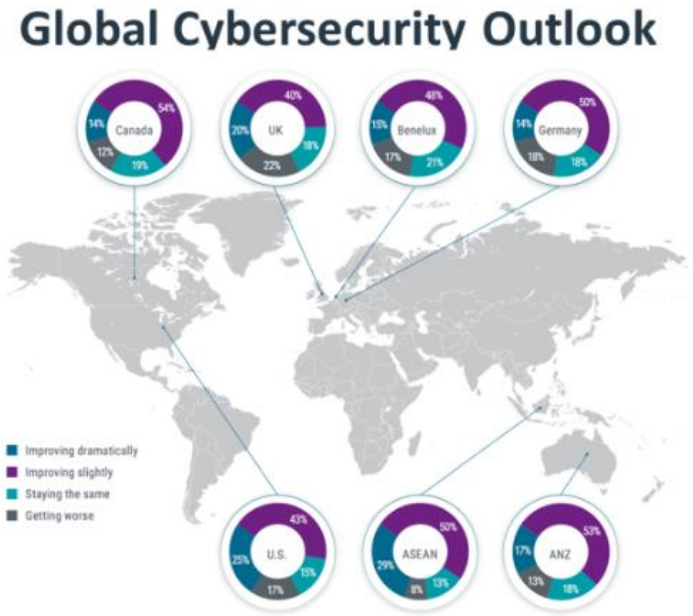
Wat ook uit de pandemie is gebleken, is dat symptomen van bedrijfsuitdagingen vaak makkelijker te identificeren en behandelen dan zogenaamde ‘root causes’. Deze uitdagingen hebben uiteraard verschillende gevolgen voor de bedrijfsstrategie, maar het meest prominente voorbeeld dat deze conclusie bevestigd kan binnen de cyber security worden teruggevonden. Amerikaanse bedrijven zijn zich maar al te bewust van het zwakke cybersecurity beleid dat er op wordt nagehouden wanneer zij worden gehackt door cybercriminelen. Meestal wordt na een evaluatie na de aanval duidelijk welke processen en tools de desbetreffende cyberaanval hadden kunnen voorkomen of mitigeren. Echter identificeren dezen evaluaties meestal niet de onderliggende problemen die kunnen leiden tot een andere cyberaanval in de nabije toekomst.

De digitale transformatie van het bedrijfsleven, wat wordt gedreven door cloud computing en remote werken, dwingt bedrijven om een nieuwe aanpak te bedenken voor cybersecurity. Toch gaat is het niet zo makkelijk om uit te voeren; het volledig implementeren van een nieuwe strategie gaat gepaard met ingrijpende veranderingen zowel op financieel als technisch gebied. Hoewel cybersecurity een van de meest prominente problemen blijft voor moderne bedrijven, zullen achterhaalde visies op IT en een slecht begrip van de bedreigingen in het cybersecurity landschap het lastig maken om nieuwe IT-strategieën in te implementeren.

3.2 Onderzoek van CompTIA

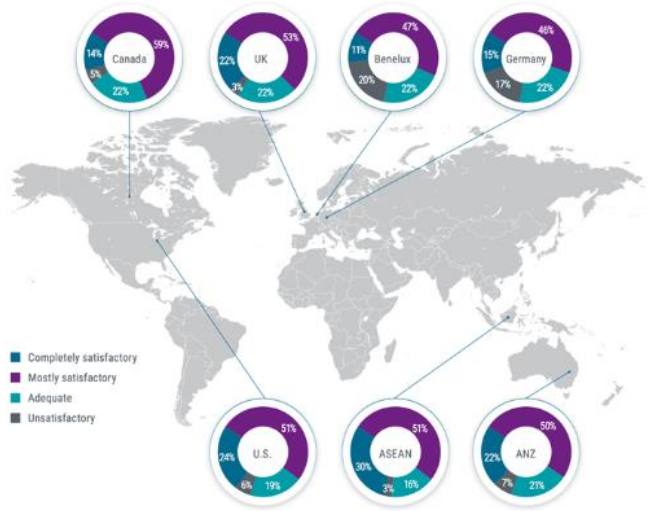
CompTIA (2022) heeft een onderzoek uitgevoerd naar de status van cybersecurity over de wereld, waarbij 7 geografische regio’s in de wereld hebben geparticipeerd. Dit onderzoek heeft een reeks aan economische en technische factoren in kaart gebracht om het cybersecurity volwassenheidsniveau te bepalen. Alle 7 regio’s zijn het er unaniem over eens dat cybersecurity een belangrijk probleem is op de agenda van bedrijven. Over het algemeen kan worden gesteld dat op dit moment cybersecurity (dit is inclusief de organisaties van cybercriminelen, overheidsreacties op cybercriminaliteit en de tools om te reageren op cybercriminaliteit) een relatief langzame ontwikkeling door maakt. Vooral in ontwikkelde gebieden, zoals de Verenigde Staten (VS) en het Verenigd Koninkrijk, alhoewel sommige individuen en instanties in deze gebieden beweren dat er drastische verbeteringen worden doorgevoerd. Zoals in figuur 2 is af te lezen zegt het zelfde percentage mensen dat ze geloven dat de situatie rond cybersecurity juist verslechterd. Aangezien dit onderzoek van CompTIA (2022) zich vooral richt op de Amerikaanse sector, zijn de jaarlijkse cybersecurity cijfers

meegenomen in het onderzoek. Er valt daardoor te concluderen dat alle respondenten uit de VS die een verbetering zagen in het cybersecurity landschap licht afnam van 69% naar 68%.



Figuur 2. Staat van cybersecurity in 7 verschillende wereldregio's (CompTIA, 2022).

Om zaken dichter bij huis te brengen, is de visie van individuele bedrijven in Amerika ook niet al te best. Terwijl de meerderheid van de respondenten in iedere regio het gevoel had dat de cybersecurity van hun bedrijf voldoende was, was er een kleiner aantal respondenten dat de cybersecurity situatie van hun bedrijf als uitstekend ervoer. Over alle regio's gezien vinden respondenten dat er ruimte voor verbetering is. In de Verenigde Staten steeds de tevredenheid over cyber security ieder jaar van 70% naar 75% in 2022. In figuur 3 is te zien wat de resultaten uit andere regio's zijn op organisatieniveau.



Figuur 3. Staat van cybersecurity op organisatieniveau (CompTIA, 2022).

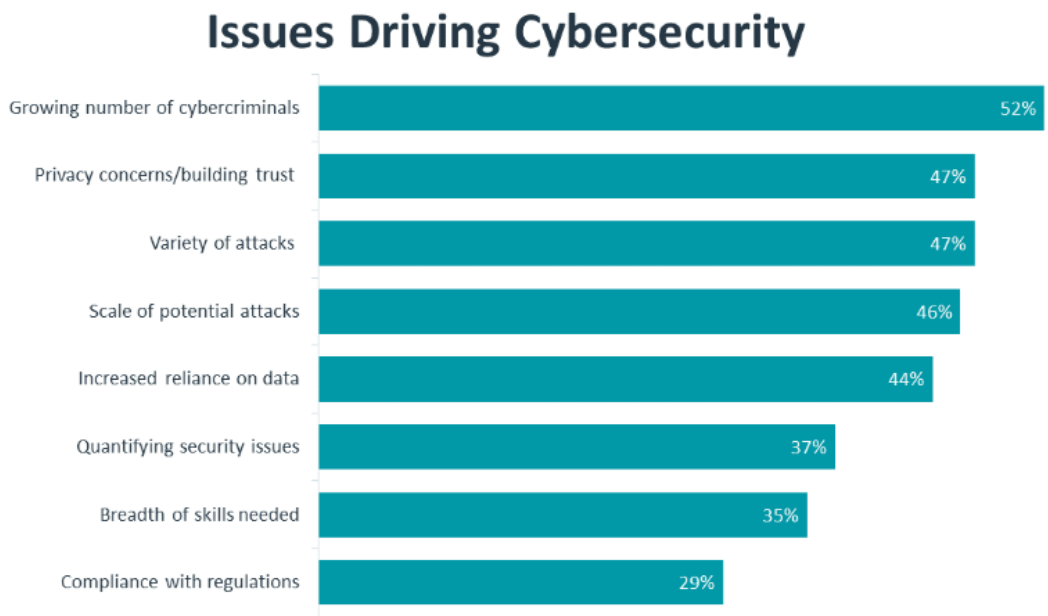
Vooral tijdens de coronapandemie raakte de technische flexibiliteit van Amerikaanse bedrijven in een stroomversnelling door de explosieve toename van internetgebruik en daardoor ook cybercriminaliteit. Deze ontwikkeling heeft de deuren geopend voor Amerikaanse bedrijven om flexibelere cybersecurity portfolio's op te bouwen op lange

termijn. Tegelijkertijd heeft deze ontwikkeling ervoor gezorgd dat Amerikaanse bedrijven in een positie zijn gekomen waarin traditionele visies op cybersecurity achterhaald zijn geworden en niet meer effectief zijn. Volgens CompTIA (2022) zouden bedrijven er goed aan doen door individuele problemen rond cybersecurity niet meer afzonderlijk aan te pakken. In plaats hiervan zouden bedrijven hun business model zo moeten aanpassen dat alle lagen binnen de organisatie worden geïnformeerd over cybersecurity beslissingen die worden genomen.

3.3 Analyse van de markt

Het vakgebied cybersecurity reageert in zekere mate op hoe de Information Technology (IT) van het bedrijfsleven zich ontwikkelt. De behoefte voor cybersecurity is immers alleen het geval als bepaalde technologieën zijn geïmplementeerd. Deze dynamiek is in de afgelopen jaren sterk toegenomen binnen het bedrijfsleven. Onder andere Amerikaanse bedrijven hebben de neiging om sterk in te zetten op het verbeteren van technologie binnen de organisatie, maar cybersecurity niet als prioriteit mee te nemen in de verbetering hiervan.

Naast het feit dat cybersecurity de ontwikkeling van IT volgt, kan worden gesteld dat het binnen het huidige cybersecurity landschap draait om complexiteit. IT-processen en strategieën zijn over de jaren heen steeds complexer geworden met de introductie van cloud computing en mobiele softwaresystemen. Dit gegeven heeft er toe geleid dat Amerikaanse bedrijven door de toename van facetten binnen het managen van cybersecurity de dreiging van cybercriminaliteit is toegenomen. Volgens een enquête van CompTIA (2022) zijn twee van de top drie grootste problemen binnen cybersecurity het stijgende aantal cybercriminelen en de stijgende variëteit in cyberaanvallen. In figuur 4 hier onder zijn de belangrijkste problemen die uit de enquête naar voren zijn gekomen samengevat in een staafdiagram.



Figuur 4. Cybersecurity problemen binnen de markt (CompTIA, 2022).

Hoofdstuk 4. Wat moet er gebeuren bij Amerikaanse bedrijven om het gewenste volwassenheidsniveau t.a.v. van cyber security te bereiken?

Een hoofdstuk twee is in kaart gebracht de huidige trends en ontwikkelingen zij op het gebied van cybersecurity. Om het gewenste volwassenheidsniveau te beschrijven zal in dit hoofdstuk worden beschreven, wat bedrijven kunnen doen om effectief te reageren op de genoemde trends in tabel 1 van hoofdstuk 1.

4.1 Reactie op trend 1: ‘zero-trust’ capaciteiten en grote datasets vanuit veiligheidsoverwegingen

Om de cyberbeveiligingsrisico's van on-demand toegang tot integrale gegevens te verminderen, zijn vier cyberbeveiligingstoepassingen vereist: zero-trust architectuur, gedragsanalyse en elastische logbewaking. In de onderstaande tabel zijn de toepassingen uitgebreid toegelicht.

Cyberbeveiligingstoepassing	Toelichting
Zero-trust architectuur (ZTA)	In geïndustrialiseerde landen werkt ongeveer 25% van alle werknemers nu drie tot vijf dagen per week op afstand (McKinsey & Company, z.d.). Hybride werken, verbeterde cloudtoegang en Internet of Things (IoT)-integratie zorgen voor potentiële kwetsbaarheden. Een zero-trust architectuur (ZTA) verschuift de focus van cyberdefensie weg van de statische grenzen rond fysieke netwerken en naar gebruikers, activa en bronnen, waardoor het risico van gedecentraliseerde gegevens wordt verkleind. Toegang wordt nauwkeuriger afgedwongen door nieuw beleid; zelfs als gebruikers toegang hebben tot de gegevensomgeving, hebben ze mogelijk geen toegang tot gevoelige gegevens. Organisaties moeten de invoering van zero-trust toepassingen afstemmen op de potentiële bedreigingen van waarmee ze worden geconfronteerd en op hun zakelijke doelstellingen. Verder zouden bedrijven ook moeten overwegen om een audit uit te voeren om de effectiviteit en dekking van hun zero-trust toepassingen te valideren.
Gedragsanalyse	Werknemers zijn het meest kwetsbaar voor cybersecurity risco’s binnen een organisatie. Analytische software kan verschillende eigenschappen in kaart brengen zoals aantal inlogmomenten en de gezondheid van computers. De software is in staat om afwijkend, opzettelijk en onopzettelijk gebruikersgedrag inzichtelijk te maken. Naast het feit analytische software autorisatie op basis van risico’s mogelijk maakt, kunnen deze tools dus ook preventief werken voor bedrijven.

Elastische logboekbewaking voor grote datasets	Enorme datasets en gedecentraliseerde logboeken, als gevolg van ontwikkelingen zoals big data en IoT, bemoeilijken de uitdaging van het monitoren van gebruikersgedrag. Elastische logboekbewaking is een oplossing op basis van verschillende open-sourceplatforms die, wanneer ze worden gecombineerd, bedrijven in staat stelt om logboekgegevens van overal in de organisatie naar een centrale plek te halen en de gegevens vervolgens in 'real time' te zoeken, analyseren en visualiseren.

Tabel 2. Reacties op trend 1 (Boehm et al, 2020).

4.2 Reactie op trend 2: automatisering gebruiken voor aanpak geavanceerde cyberaanvallen

Om geavanceerdere aanvallen die worden aangestuurd door AI en andere geavanceerde toepassingen tegen te gaan, moeten organisaties een op risico's gebaseerde benadering van automatisering en automatische reacties op aanvallen hanteren. Automatisering moet zich richten op defensieve mogelijkheden zoals tegenmaatregelen van het Security Operations Centre (SOC) en arbeidsintensieve activiteiten, zoals identiteits- en toegangsbeheer (IAM) en rapportage. AI en machine learning moeten gebruikt worden om op de hoogte te blijven van veranderende aanvalspatronen. Ten slotte helpt de ontwikkeling van zowel geautomatiseerde als automatische reacties op ransomware aanvallen het verminderen van de impact van een cyberaanval.

Cyberbeveiligingstoepassing	Toelichting
Implementatie van automatisering gebaseerd op mogelijk risico	Naarmate het digitaliseringsniveau versnelt, kunnen organisaties automatisering gebruiken om processen met een lager risico en routinematige processen af te handelen, waardoor middelen worden vrijgemaakt voor activiteiten met een hogere waarde. Het is van cruciaal belang dat automatiseringsbeslissingen gebaseerd zijn op risicobeoordelingen en segmentatie om ervoor te zorgen dat er niet per ongeluk extra kwetsbaarheden worden gecreëerd. Organisaties kunnen bijvoorbeeld geautomatiseerde patching, configuratie en software updates toepassen op apparaten met een laag risico, maar meer direct toezicht gebruiken voor activa met een hoger risico.
Gebruik maken van defensieve AI en machine learning voor cyber security	Net zoals cyberaanvallers AI en machine learning gebruiken, zullen cyberbeveiligingsteams dezelfde mogelijkheden moeten ontwikkelen en opschalen om voorbereidt te zijn. Met name kunnen organisaties deze technologieën gebruiken om niet-conforme systemen te detecteren en te verhelpen. Beveiligingsteams kunnen ook gebruik maken van machine learning om workflows te optimaliseren, zodat middelen in de loop van de tijd op de meest effectieve manier worden gebruikt.

Tabel 3. Reacties op trend 2 (Boehm et al, 2020).

4.3 Reactie op trend 3: integreren van beveiliging in technologieën voor de groeiende regelgeving en kritieke kloven

De toenemende regelgeving en kritieke kloven rondom kennis, talent en expertise van cybersecurity, onderstreept de behoefte om beveiliging binnen technologische toepassingen te embedden zoals ze ontworpen en geïmplementeerd zijn. Daarnaast helpen toepassingen zoals beveiliging als code en software voor de Bill of Materials (BOM) organisaties om beveiligingsmogelijkheden in te zetten en de regelgeving van wetgevers voor te zijn. In tabel 4 zijn de mogelijke reacties op trend 3 uiteengezet.

Cyberbeveiligingstoepassing	Toelichting
Beveiligen van software ontwikkeling	In plaats van cybersecurity als een bijzaak te beschouwen, zouden bedrijven het vanaf het begin het ontwerp moeten inbedden in het ontwerp van software, inclusief het gebruik van een softwarelijst met materialen (zie derde punt 'Bill of Materials'). Een belangrijke manier om een veilige levenscyclus voor softwareontwikkeling te creëren, is door cybersecurityteams in elke ontwikkelingsfase met ontwikkelaars te laten samenwerken. Een andere mogelijkheid is om ervoor te zorgen dat software ontwikkelaars bepaalde beveiligingsmogelijkheden leren die door cybersecurityteams zelf kunnen worden gebruikt (bijvoorbeeld dreigingsmodellering, code- en infrastructuurscanning en statische en dynamische tests). Afhankelijk van de activiteit kunnen sommige beveiligingsteams overstappen op Agile werken. Andere teams kunnen een hybride benadering toepassen op basis van Agile en Kanban.
Infrastructuur en beveiliging als code	Het standaardiseren en coderen van infrastructuur- en besturingstechnische processen kan het beheer van hybride en cloud omgevingen vereenvoudigen en de veerkracht van het systeem vergroten. Deze aanpak maakt processen mogelijk zoals routinematige patching, evenals snelle bevoorrading en het afbestellen van voorraad.
Software van Bill of Materials (BOM)	Naarmate de cybersecurity regelgeving toeneemt, kunnen organisaties de administratieve last verminderen door formeel alle componenten en supply chain relaties die in software worden gebruikt te specificeren. Net als een gedetailleerde Bill of Materials zou deze documentatie open source moeten zijn en zouden componenten van derden in een aparte database opgesomd moeten worden door middel van nieuwe softwareontwikkelingsprocessen, scantools voor codes, industrie standaarden en supply chain vereisten. Naast het verminderen van supply chain risico's, helpt gedetailleerde softwaredocumentatie ervoor zorgen dat cybersecurityteams voorbereidt zijn op vragen van de regelgevende instanties.

Tabel 4. Reacties op trend 3 (Boehm et al, 2020).

Hoofdstuk 5. Conclusie

In dit hoofdstuk worden conclusies getrokken op basis van de beantwoorde deelvragen en wordt een eenduidig antwoord gegeven op de hoofdvraag. Het probleem waar veel Amerikaanse bedrijven tegenaan lopen vandaag de dag zijn de cybersecurity maatregelen die ineffectief zijn en de werkwijze van cybercriminelen die steeds geraffineerder wordt naarmate technologie zich blijft ontwikkelen. De hoofdvraag van deze onderzoeksopdracht luidt als volgt: ‘’In hoeverre volstaat het cyber security beleid van Amerikaanse bedrijven om data te beschermen en ingrijpende gevolgen zoals datalekken en ransomware attacks te voorkomen?’’.

5.1 Cybersecurity als prioriteit

Over het algemeen wordt er nog te weinig aandacht en geld geïnvesteerd in degelijke cybersecurity maatregelen. Dit is mede af te leiden uit het onderzoek van CompTIA (2022), waarin naar voren kwam dat iets meer dan de helft van de Amerikanen tevreden is met het cybersecurity beleid, maar niet volledig tevreden.

Ondanks de grote aandacht die er is voor cybersecurity risico’s, is een duidelijke definitie van de term nog steeds niet naar voren gekomen in het bedrijfsleven en de literatuur. De reden hiervoor komt doordat de term cybersecurity een containerbegrip is geworden en de interdisciplinaire aard van de term. Er zal dus meer aandacht moeten worden geschonken aan het helder definiëren van de term cybersecurity op organisatieniveau zodat cyberbeveiligingsmaatregelen effectiever kunnen worden ingezet.

Daarnaast werken cybercriminelen steeds minder op individueel niveau, maar in geavanceerde organisaties die gebruik maken van geïntegreerde tools en de mogelijkheid om gebruik te maken van kunstmatige intelligentie (AI) en machine learning. De omvang van de dreiging voor informatiesystemen blijft hierdoor groeien en geen enkele organisatie blijkt hiervoor immuun te zijn. MKB-bedrijven, multinationals, gemeentes en federale overheden worden steeds vaker geconfronteerd met dergelijke risico’s.

5.2 Maatregelen tegen cybercriminaliteit

De belangrijkste maatregelen die Amerikaanse bedrijven in acht moeten nemen om zich beter te kunnen beschermen tegen cyberaanvallen is een tweezijdige aanpak. In de onderstaande bullet points is deze aanpak uitgelegd:

1. Gebruik maken van defensieve AI en machine learning voor cyber security: net zoals cyberaanvallers AI en machine learning gebruiken, zullen cyberbeveiligingsteams dezelfde mogelijkheden moeten ontwikkelen en opschalen om voorbereidt te zijn. Het dus belangrijk dat Amerikaanse bedrijven op de hoogte blijven van hoe cybercriminelen te werk gaan en strategische keuzes te maken over welke systemen meer of minder beveiliging nodig hebben.
2. Gedragsanalyse van systeemgebruik: werknemers zijn het meest kwetsbaar voor cybersecurity risico’s binnen een organisatie. Analytische software kan verschillende eigenschappen in kaart brengen zoals aantal inlogmomenten en de gezondheid van computers. De software is in staat om afwijkend, opzettelijk en onopzettelijk gebruikersgedrag inzichtelijk te maken.

Al met al kan worden geconcludeerd dat de staat van het Amerikaanse cyber security landschap op de goede weg is, maar nog een lange te gaan heeft om cybercriminaliteit op effectieve wijze een halt toe te roepen. Het vakgebied cybersecurity reageert in zekere mate op hoe de Information Technology (IT) van het bedrijfsleven zich ontwikkelt. De behoefte voor cybersecurity is immers alleen het geval als bepaalde technologieën zijn geïmplementeerd. Deze dynamiek is in de afgelopen jaren sterk toegenomen binnen het bedrijfsleven. Onder andere Amerikaanse bedrijven hebben de neiging om sterk in te zetten op het verbeteren van technologie binnen de organisatie, maar cybersecurity niet als prioriteit mee te nemen in de verbetering hiervan. Om dit probleem effectief aan te pakken, moeten Amerikaanse bedrijven ervoor zorgen dat er een duidelijke en vooral actuele visie op IT kenbaar wordt gemaakt binnen de organisatie en via bijvoorbeeld e-learnings een beter begrip onder werknemers wordt gecreëerd van de bedreigingen binnen het cybersecurity landschap.

Literatuurlijst

Boehm, J., Dias, D., Lewis, C., Li, K. & Wallance, D. (2022, 8 augustus). *Cybersecurity trends: Looking over the horizon*. McKinsey & Company. Geraadpleegd op 26 juni 2022, van https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/cybersecurity/cybersecurity-trends-looking-over-the-horizon

Carlson, B. (2021, 7 oktober). Top cybersecurity statistics, trends, and facts. *CSO Online*. Geraadpleegd op 27 juni 2022, van https://www.csoonline.com/article/3634869/top-cybersecurity-statistics-trends-and-facts.html

Craigen, D., Diakun-Thibault, N. & Purse, R. (2014, 30 oktober). Defining Cybersecurity. *Technology Innovation Management Review*, *4*(10), 13–21. https://doi.org/10.22215/timreview/835

CompTIA. (2022, september). *2022 State of Cybersecurity - US | CompTIA*. Geraadpleegd op 24 oktober 2022, van https://www.comptia.org/content/research/cybersecurity-trends-research

Goldman, S. (2021, 15 maart). 5 ways to grow the cybersecurity workforce in 2021. *InsiderPro.* Geraadpleegd op 16 januari 2022, van https://www.idginsiderpro.com/article/3611384/5-ways-to-grow-the-cybersecurity-workforce-in-2021.html

Guerra & Kim. (2020, 8 juli). Cybersecurity: A Definition across Europe and North America. In *AIS eLibrary*. University of North Texas. Geraadpleegd op 26 juni 2022, van https://aisel.aisnet.org/amcis2020/info_security_privacy/info_security_privacy/16/

IBM. (2018, 10 juli). *IBM Study: Hidden Costs of Data Breaches Increase Expenses for Businesses*. IBM Newsroom. Geraadpleegd op 27 juli 2022, van https://newsroom.ibm.com/2018-07-10-IBM-Study-Hidden-Costs-of-Data-Breaches-Increase-Expenses-for-Businesses

INSUREtrust. (2019, 14 januari). *Cybersecurity: Hacking Has Become a $300 Billion Dollar Industry*. Geraadpleegd op 27 juni 2022, van https://insuretrust.com/2019/01/14/cybersecurity-hacking-has-become-a-300-billion-dollar-industry/

McKinsey & Company. (z.d.). *Global surveys of consumer sentiment during the coronavirus crisis*. Geraadpleegd op 2 juli 2022, van https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/global-surveys-of-consumer-sentiment-during-the-coronavirus-crisis

Schatz, D., Bashroush, R. & Wall, J. (2017). Towards a More Representative Definition of Cyber Security. *The Journal of Digital Forensics, Security and Law*, *12*(8), 53–74. https://doi.org/10.15394/jdfsl.2017.1476