BELEGGEN

Cybersecurity: de investering van de toekomst.

Tekst **Lieven Beullens**

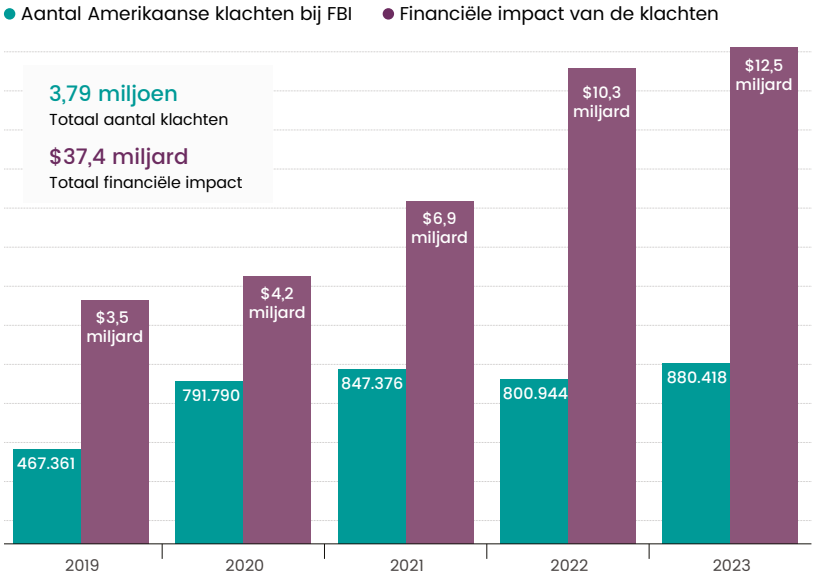
In onze reeks beleggingsthema's bespreken we in deze editie de cybersecurity sector meer in detail. Dit is een snel veranderende sector waar jaarlijks honderden miljarden euro's en dollars naartoe vloeien. In het aansluitende artikel bespreken we enkele posities uit onze portefeuille waarmee we inspelen op deze sector.

Investeringen in cybersecurity zijn hoogstnoodzakelijk en hier kan moeilijk op bespaard worden. Wereldwijd worden steeds meer aanvallen gerapporteerd en de negatieve gevolgen van inbreuken stijgen sterk. Ook de Duvel-brouwerij Moortgat kreeg hier recent mee te maken waardoor de productie enkele dagen plat lag. Volgens een studie van de Amerikaanse FBI is het aantal gerapporteerde aanvallen in de Verenigde Staten sinds 2019 bijna verdubbeld tot 880.000 aanvallen. De totale omvang van de geleden schade is zelfs bijna vervierdubbeld tijdens dezelfde periode tot 12,5 miljard USD (grafiek 1).

Mensen gebruiken steeds meer verschillende technologische toestellen en deze vormen allemaal een potentiële bedreiging.

Grafiek 1: Evolutie van aantal Amerikaanse klachten van cyberaanvallen bij FBI en financiële impact

Bron: FBI IC3 Rapport



Tabel 1: De belangrijkste hedendaagse cybersecurity niches

1. Netwerkbeveiliging
Beveiliging die de toegang tot het (bedrijfs)netwerk controleert.

2. Applicatie beveiliging
Beveiliging van specifieke software programma's.

3. Databeveiliging
Encryptie van data om te voorkomen dat (gevoelige) data openbaar gemaakt kunnen worden.

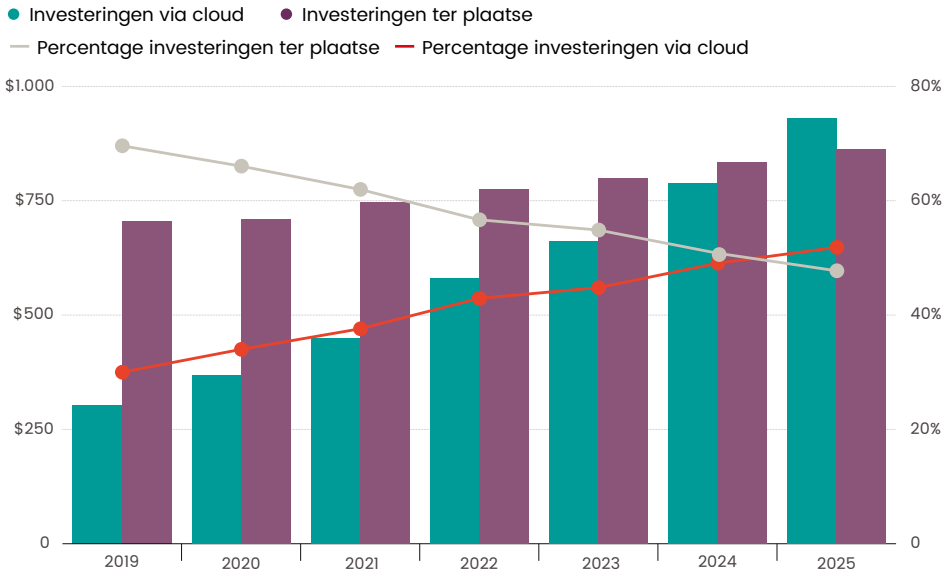
4. Endpointbeveiliging
Werknemers gebruiken niet alleen desktops, maar ook laptops, smartphones en tablets. Zelfs huishoudapparaten kunnen geconnecteerd zijn en dienen dus beveiligd te worden.

5. Identiteitsbeveiliging
Beperken van toegang op persoonsniveau.

6. Cloudbeveiliging
Beveiliging van alle applicaties die gebruik maken van de cloud.

7. Internetbeveiliging
Beveiliging van browsers, websites en mails

Grafiek 2: Evolutie van uitgaven voor investeringen ter plaatse vs via de cloud
Bron: Morningstar



Bovendien heeft ook de evolutie naar meer werken vanop afstand een belangrijke impact. Werknemers kunnen nu met diverse toestellen en van overal ter wereld inloggen op het bedrijfsnetwerk. Elk van deze toegangen en toestellen dient beveiligd te worden.

Door de snelle verandering van het landschap het laatste decennium zijn stevige investeringen noodzakelijk. Waar bedrijven vroeger enkel moesten investeren in een goede beveiliging van hun bedrijfsnetwerk, is de huidige situatie veel complexer. Met een traditionele netwerkbeveiliging komen bedrijven niet ver meer. De meeste aanvallen maken niet langer gebruik van traditionele malware waarbij virussen verspreid worden. Volgens het Global Threat Report van CrowdStrike richten meer dan 75% van de aanvallen zich op andere tactieken zoals het stelen van data en het stelen van identiteitsgegevens (wachtwoorden en bankgegevens). Het aantal aanvallen via de cloud is op een jaar tijd met meer dan 75% gestegen. In tabel 1 enkele van de belangrijkste hedendaagse cybersecurity niches.

Veel concurrentie

Her en der schoten er de laatste jaren wereldwijd verschillende start-ups als paddenstoelen uit de grond om in te spelen op specifieke niches binnen de sector. Dit heeft geleid tot een zeer competitieve sector. Sommige van deze spelers richten zich op één aspect van de beveiliging, andere spelers proberen alles aan te bieden in een geconsolideerd platform. In het verleden gingen de meeste investeringen naar oplossingen die ter plaatse geïnstalleerd moeten worden (on premise). In 2024 zal er voor het eerst bijna evenveel geïnvesteerd worden in cloudoplossingen als in on premise oplossingen. Vanaf 2025 zullen de cloudoplossingen duidelijk de overhand halen. Deze oplossingen kunnen immers eenvoudig en snel vanop afstand geïnstalleerd en beheerd worden.

De cybersecurity sector wordt gedomineerd door enkele grote spelers zoals Microsoft waarbij cybersecurity slechts een beperkt deel van de omzet uitmaakt. Bovendien wenst Microsoft enkel eigen producten te beveiligen zoals Windowstoestellen en Azure Cloud. De omzet die Microsoft haalt uit cybersecurity is even groot als de omzet gegenereerd door alle pure cybersecurityspelers samen. De pure spelers hebben echter het voordeel dat ze niet gebonden zijn aan een platform. Hun beveiligingstools werken zowel voor Windows als Mac, Azure, Amazon AWS, Google Cloud, Android toestellen, et cetera. Daarom zijn bedrijven steeds meer geneigd om te kiezen voor de pure, onafhankelijke spelers. Als ze ooit zouden besluiten om hun infrastructuur te wijzigen, zullen ze niet langer verplicht zijn om ook hun volledige cybersecurity omgeving om te gooien.

Bedrijven investeren in cybersecurity om elke vorm van onzekerheid maximaal af te dekken. Ze richten zich daarom eerder op kwaliteit dan op de prijs.

Volgens het Global Threat Report van CrowdStrike Holdings gebruikten bedrijven in 2022 gemiddeld 45 verschillende cybersecurity tools, afkomstig van 15 verschillende leveranciers. Dit maakt het voor hen zeer moeilijk om het overzicht te behouden. Enkele grote pure spelers zoals Palo Alto Networks, Fortinet, CrowdStrike Holdings en Zscaler proberen hierop in te spelen door één of enkele geïntegreerde platformen aan te bieden. Met deze platformen kunnen bedrijven gemakkelijk een groot deel van de beveiligingsrisico's afdekken en behouden ze ook nog eens het overzicht. Daarenboven kan men via deze platformen op eenvoudige wijze nieuwe tools toevoegen. Bij CrowdStrike en Zscaler is het slechts een kwestie van minuten vooraleer nieuwe toepassingen beschikbaar zijn voor de klanten wanneer zij dit wensen.

Sterke moat

Dankzij de trend naar meer cloudoplossingen evolueert de sector snel naar een Software-as-a-Service (SaaS) model waarbij klanten een abonnement afsluiten voor enkele jaren en maandelijks een abonnementskost betalen. Dit zorgt voor een sterke visibiliteit van de inkomsten voor de cybersecurity leveranciers. De kwaliteit van de cybersecurityoplossingen is van het hoogste belang. Bedrijven investeren in cybersecurity om elke vorm van onzekerheid maximaal af te dekken. Ze richten zich daarom eerder op kwaliteit dan op de prijs. De kost van een inbreuk is vele malen groter dan de maandelijkse abonnementskost. Bovendien zijn ze ook nog eens geneigd om deze abonnementen telkens te verlengen. Als bedrijven van cybersecurity leveranciers zouden veranderen dan gaat dit namelijk gepaard met een periode van verhoogde onzekerheid. Het duurt immers een tijdje vooraleer nieuwe tools volledig geïntegreerd zijn en niets garandeert dat de nieuwe tool exact dezelfde risico's afdekt als de bestaande tool. Bedrijven wensen deze periode van verhoogd risico te vermijden en kiezen daarom gemakkelijkheidshalve voor een verlenging van bestaande abonnementen, tenzij de kwaliteit van concurrentiële oplossingen aanzienlijk beter is. De sterkste spelers in de sector zullen er bijgevolg in slagen om de klanten naar zich toe te trekken en voor zeer lange tijd te behouden. Omdat cybersecurity cruciaal is voor bedrijven zijn de uitgaven ook absoluut niet gevoelig aan economische cycli.

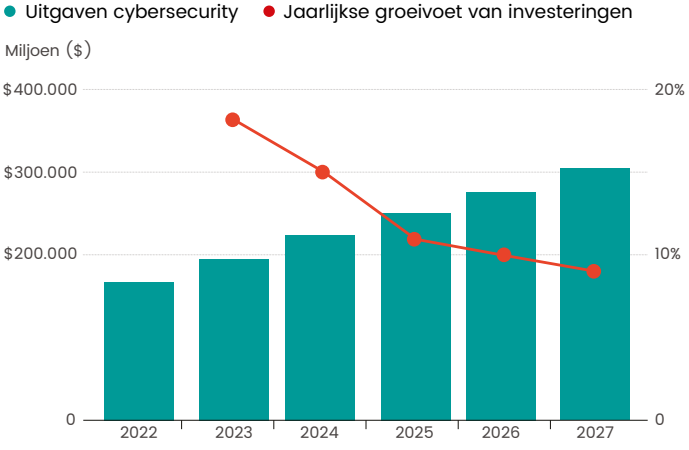
Dankzij de sterke prijszettingsmacht en voorspelbare inkomsten genereren de cybersecurity bedrijven zeer stevige kasstromen. Deze kasstromen worden gebruikt om te blijven investeren in onderzoek en ontwikkeling. De cybersecurity omgeving blijft immers zeer snel veranderen en de leveranciers moeten proberen bij te blijven met de nieuwste trends. Nieuwere niches zoals endpointbeveiling, cloudbeveiliging en identiteitsbeveiliging ontwikkelen zich dan ook veel sneller dan de traditionele netwerkbeveiliging.

AI: vloek of zegen?

Een ander belangrijk aspect dat bedrijven richting de grootste en beste spelers duwt, is het belang van data. Het aantal aanvallen stijgt zeer snel en de aanvallen worden steeds meer divers. Naarmate een leverancier meer klanten heeft, kan het meer data verzamelen over alle mogelijke aanvallen die deze ooit al gezien heeft en kan het bijgevolg ook de andere klanten beter beschermen. Het is een understatement om te zeggen dat Artificiële Intelligentie (AI) tegenwoordig een hot topic is. AI begint ook steeds meer zijn intrede te doen in de cybersecurity sector. Dankzij de overvloed aan verzamelde data kunnen AI-modellen ontwikkeld worden die moeten helpen bij de beveiliging tegen aanvallen. CrowdStrike is één van de voorlopers in de ontwikkeling en het gebruik van AI binnen de sector.

Anderzijds zal AI ook leiden tot een explosie van het aantal aanvallen. Via generatieve AI zal het veel gemakkelijker worden om op grote schaal aanvallen uit te voeren. Bovendien zal dit ook de drempel tot het uitvoeren van aanvallen sterk verminderen. Nu worden aanvallen voornamelijk uitgevoerd door IT-specialisten met de nodige expertise. Door de ontwikkeling van generatieve AI-modellen zullen ook mensen zonder gespecialiseerde kennis aanvallen kunnen uitvoeren omdat het AI-model het moeilijke werk zal doen. Een goede bescherming zal dus uitermate cruciaal blijven. Morningstar verwacht dan ook dat de cybersecurity markt tot 2027 gemiddeld met minstens 13% per jaar zal blijven groeien (grafiek 3).

Grafiek 3: Evolutie van uitgaven voor cybersecurity en de jaarlijkse groeivoet
Bron: Morningstar



Disclaimer

Dit is een publicatie van Leo Stevens & Cie, een beursvennootschap vergund door de NBB (Nationale Bank van België).

Deze publicatie mag niet beschouwd worden als 'onderzoek op beleggingsgebied' zoals bedoeld in het koninklijk besluit van 3 juni 2007. Het is een publicitaire mededeling. De wettelijke voorschriften ter bevordering van de onafhankelijkheid van onderzoek op beleggingsgebieden zijn hierop niet van toepassing. Eventuele aanbevelingen zijn niet onderworpen aan een verbod om al voor de verspreiding van onderzoek op beleggingsgebied te onderhandelen.

Deze publicatie mag niet als persoonlijk beleggingsadvies beschouwd worden. Leo Stevens & Cie kan niet garanderen dat de in de publicatie behandelde financiële instrumenten voor u geschikt zijn. Mocht u op basis van deze publicatie overgaan tot een financiële transactie, dan draagt u hier zelf de volledige verantwoordelijkheid voor. Beleggen in financiële instrumenten (zoals aandelen) kan grote risico's inhouden. Alvorens tot een transactie over te gaan, moet een belegger beschikken over de nodige ervaring en kennis om de eventuele risico's die gepaard gaan met de transactie ten volle in te schatten, in staat zijn om deze risico's te dragen waarbij beseft moet worden dat het belegde kapitaal geheel of gedeeltelijk verloren kan gaan.

Medewerkers van Leo Stevens & Cie kunnen vóór de verspreiding van deze aanbevelingen handelen in het financieel instrument.

Eventuele rendementen die in deze publicatie vermeld werden, zijn gerealiseerd geworden in het verleden. Er is geen garantie dat zij ook in de toekomst behaald zullen worden. Men kan evenmin zeker zijn dat de beschreven scenario's, verwachtingen en risico's zullen uitkomen in de realiteit. Zij dienen als indicatief beschouwd te worden. De gegevens die in de publicatie vermeld worden, zijn louter informatief en kunnen aan veranderingen onderhevig zijn. Wisselkoersschommelingen kunnen vooropgestelde resultaten en rendementen beïnvloeden.

De publicatie geeft de analyse weer van de auteur op de vermelde datum. Hoewel de analyse gebaseerd is op volgens de auteur betrouwbare bronnen, kan de correctheid, volledigheid en actualiteit van de gebruikte informatie niet gegarandeerd worden.

Leo Stevens

PUUR & PERSOONLIJK VERMOGENSBEHEER

Leo Stevens
Vermogensbeheer met een pure & persoonlijke missie

Leo Stevens begeleidt u in het beheer van uw vermogen als geen andere financiële instelling in België: puur en persoonlijk.

Schildersstraat 33
2000 Antwerpen
T +32 3 242 03 70

info@leostevens.com
www.leostevens.com