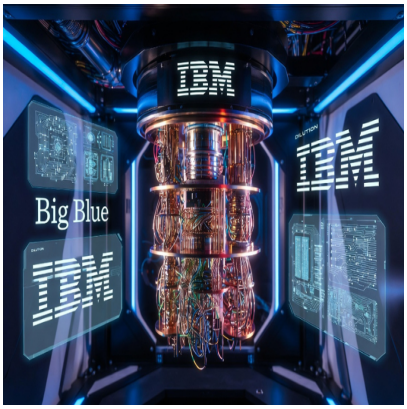

Cybersecurity wordt kwantumsecurity

Beschrijving

De ruil van LVMH naar IBM in portefeuille oogt op het eerste gezicht vreemd, maar achter deze transactie schuilt een van de grootste verschuivingen die de digitale wereld te wachten staat: de opkomst van de kwantumcomputer en de gevolgen daarvan voor onze beveiliging.

IBM is de facto de leider in kwantumcomputing

Onder de bedrijven die de race naar een bruikbare kwantumcomputer aanvoeren, neemt IBM een bijzondere plaats in. Het beheert al jaren een wereldwijd toegankelijke vloot kwantummachines in de cloud, heeft consequent gekozen voor supergeleidende qubits en haalt zijn eigen mijlpalen keer op keer. De routekaart is helder en openbaar. Het middelpunt van die strategie is Quantum Starling, gepland voor 2029: de eerste grootschalige, foutbestendige kwantumcomputer ter wereld. Daarna volgt rond 2033 een nog krachtiger systeem. Het bedrijf investeert de komende vijf jaar meer dan tien miljard dollar in dit thema en bouwt samen met de Amerikaanse overheid de eerste speciale kwantumfabriek van het land. IBM isop dit moment de meest complete en geloofwaardige speler is.

Kwantum in een stroomversnelling

Lange tijd was kwantumcomputing iets voor de zeer lange termijn: fascinerend, maar ver weg. Dat beeld is aan het kantelen. De doorbraak met de Willow-processor eind 2024 liet zien dat foutcorrectie daadwerkelijk werkt en bracht de hele sector in een stroomversnelling. Beleggers reageerden uitbundig. In november en december 2024 stegen sommige zuivere kwantumaandelen met honderden procenten, terwijl die bedrijven nog nauwelijks of geen winst maken. Dat is het klassieke patroon van een thema dat plotseling in de mode raakt: de verwachting rent ver vooruit op de werkelijkheid. Inmiddels worden de eerste commercieel bruikbare machines rond 2030 verwacht. De horizon is dus niet langer vaag, maar concreet genoeg om er als belegger rekening mee te houden.

Van cybersecurity naar kwantumsecurity

De meest ingrijpende gevolgen liggen niet in de geneeskunde of de logistiek, maar in de beveiliging van onze digitale wereld. Vrijwel alle versleuteling die vandaag het internet, het betalingsverkeer en staatsgeheimen beschermt, rust op wiskundige problemen die voor gewone computers praktisch onoplosbaar zijn. Een voldoende krachtige kwantumcomputer kan die problemen wÃ©l kraken. Daarmee verandert alles wat we weten over encryptie en authenticatie in Ã©Ã©n klap fundamenteel.

Hoe concreet die dreiging is, laat bitcoin zien. De beveiliging van de bekendste cryptomunt rust op precies zulke wiskundige problemen. Recent onderzoek toont aan dat een kwantumcomputer met minder dan een half miljoen fysieke qubits een bitcoinsleutel in ongeveer negen minuten zou kunnen kraken, een raming die twintig keer lager ligt dan wat een paar jaar geleden nog voor onmogelijk werd gehouden. En die negen minuten zijn veelzeggend, want het bitcoinnetwerk heeft gemiddeld tien minuten nodig om een transactie te bevestigen. Een aanvaller zou een transactie dus kunnen onderscheppen op het moment dat de publieke sleutel zichtbaar wordt, daaruit de private sleutel afleiden en er met het geld vandoor gaan nog voordat de oorspronkelijke betaling rond is. Wat vandaag als onkraakbaar geldt, kan zo binnen een paar jaar in minuten worden opengebroken.

Het gevaar is bovendien niet pas iets voor over tien jaar. Kwaadwillenden verzamelen nu al versleutelde gegevens met de bedoeling die later te ontcijferen, zodra de techniek zover is. Data die vandaag wordt buitgemaakt maar jarenlang geheim moet blijven, loopt daardoor nu al risico. Cybersecurity gaat daarom niet langer alleen over firewalls en wachtwoorden, maar over kwantumsecurity. Elke bank, verzekeraar, overheid en zorginstelling zal de komende jaren zijn systemen moeten overzetten naar versleuteling die ook tegen kwantumcomputers bestand is

IBM staat aan beide kanten van de medaille

Juist hier komt de positie van IBM volledig tot uiting, want het bedrijf staat aan beide kanten van dezelfde medaille. Aan de ene kant bouwt het de machines die de huidige versleuteling ooit kunnen kraken. Aan de andere kant heeft het de verdediging mede ontworpen: twee van de drie eerste vastgestelde standaarden voor post-kwantumversleuteling komen uit zijn eigen laboratoria. Zo verandert de dreiging die IBM zelf helpt creÃ«ren, meteen in een bron van inkomsten. Het bedrijf combineert daarmee een voorsprong in de technologie van de toekomst met een concrete verdienplek in het heden. Wie exposure zoekt naar het groeiende thema beveiliging, krijgt dat er bij IBM als het ware gratis bij.

De waardering maakt het verschil

Nu zijn zuivere cybersecurityaandelen over het algemeen erg hoog gewaardeerd. De markt heeft de structurele groei van het thema al ruimschoots ingeprijsd, wat het opwaartse potentieel beperkt. Voor die kwaliteit betaal je dus een volle prijs. IBM is precies het tegenovergestelde. Het aandeel is deze

zomer hard onderuitgegaan na een winstwaarschuwing en verloor op Ã©Ã©n dag meer dan een kwart van zijn beurswaarde. Daardoor noteert het nu rond zeventien tot twintig keer de verwachte winst, ongeveer dertig procent goedkoper dan de rest van de IT-sector en zelden zo laag in zijn eigen geschiedenis. De onderliggende oorzaak was bovendien vooral een kwestie van timing: uitgestelde orders zijn niet verloren orders. Onder die zwakke omzet zit een gezond bedrijf, met miljarden aan vrije kasstroom en een dividend dat sinds 1916 zonder onderbreking wordt uitgekeerd.

Diezelfde korting geldt voor de kwantumbelofte. Omdat de opbrengsten van Starling nog een aantal jaren in de toekomst liggen, zit die kans nu nauwelijks in de koers verwerkt. Waar beleggers bij de zuivere kwantumspecialisten honderden procenten koersstijging betalen voor bedrijven zonder winst, krijg je bij IBM een leidende positie in kwantumcomputing er bijna voor niets bij, boven op een stabiel en winstgevend bedrijf.

De comfortabele weg naar de kwantumeeuw

Van de doorbraak in kwantumcomputing profiteren uiteraard ook de brede technologiereuzen als Microsoft en Alphabet. Zij bieden de meest comfortabele blootstelling: sterk genoeg om van de doorbraak te profiteren zonder dat hun voortbestaan ervan afhangt. Maar IBM voegt daar iets aan toe wat die twee niet bieden: het staat aan de spits van kwantumcomputing Ã©n van kwantumsecurity, en het is bovendien fors goedkoper geworden. Honderd jaar na de geboorte van de kwantummechanica verandert de theorie opnieuw de wereld, deze keer via de computer en de beveiliging. De ruil van LVMH naar IBM is een beweging van de volle prijs voor stilstand inruilen voor een lage prijs voor de toekomst.

Han Dieperink, Chief Investment Officer

Disclaimer

Abonneer op deze nieuwsbrief via www.aureus.eu/nieuwsbrief