

DE TIEN GROOTSTE NASDAQ-BEDRIJVEN; TOEN EN NU

► TOEN: 31 DECEMBER 1999

► NU: 25 FEBRUARI 2015

AANDEEL	MARKT WAARDE*	AANDEEL	MARKT WAARDE*
Microsoft	606	Apple	755
Cisco	360	Microsoft	363
Qualcomm	332	Google	340
Intel	277	Amazon	178
WorldCom	228	Facebook	177
Oracle	151	Intel	164
Dell	132	Gilead Sciences	158
Sun Microsystems	117	Cisco	151
Yahoo	103	Comcast	128
JDS Uniphase	75	Amgen	120

*in miljarden dollars. Bron: NasdaqOMX

nomen gezien als een prelude voor het ontstaan van de kredietcrisis uit 2008. Wie zijn geschiedenis niet kent, is gedoemd deze te herhalen, maar daarmee is niet gezegd dat de torenhoge koersen nu weer het begin van veel narigheid zijn. Daarvoor zijn de verschillen met de situatie van vijftien jaar geleden te groot.

1 ECHE WINST

Om te beginnen met het meest voor de hand liggende verschil: veel technologiebedrijven die nu aan de Nasdaq zijn genoteerd, maken 'echte' winst en die winst helpt hen om reserves op te bouwen.

In 2000 was dat anders, toen was een goed idee en een beetje omzet voor een bedrijf al genoeg om mateloos populair te worden op de beurs. De kans dat de top-techbedrijven van nu over een paar jaar niet meer bestaan, is dan ook een stuk kleiner dan anderhalf decennium geleden.

2 MINDER PURE TECHNOLOGIE

Toegegeven, de Nasdaq blijft een beurs voor technologie-aandelen, maar het aandeel van echte IT-bedrijven binnen de Nasdaq Composite-index is een stuk kleiner dan vijftien jaar geleden. Biotechbedrijven, kabelondernemingen en farmaceuten hebben aan gewicht gewonnen.

De veranderingen in de technologiewereld worden duidelijk

zichtbaar bij vergelijking van de tien grootste bedrijven op de Nasdaq, nu en vijftien jaar geleden (zie tabel). Alleen Cisco, Intel en Microsoft komen in beide ranglijsten voor, hoewel de beurswaarde van deze techgiganten behoorlijk is gekrompen.

3 WAARDERING VEEL LAGER

Goedkoop zijn – vooral Amerikaanse – aandelenbeurzen al lang niet meer. Maar de idiote waarderingen uit het jaar 2000 zijn nog maar sporadisch te vinden.

In 1999 bedroeg de gemiddelde koers-winstverhouding van de Nasdaq Composite-index meer dan 150. Dergelijke waarderingen zijn nu uitzondering, bijvoorbeeld bij de populaire maar weinig winstgevende online retailer Amazon. Tegenwoordig betalen beleggers gemiddeld ongeveer 27 keer de winst voor een technologie-aandeel.

EN EEN OVEREENKOMST

Alle verschillen ten spijt is er een ding hetzelfde als vijftien jaar geleden. Analisten waren destijds zeer optimistisch over techaandelen. Totdat het fout ging. En ook nu zien analisten nog steeds ruimte voor stijgende koersen. Zij geven voor een groot deel van de grote Nasdaq-aandelen een koopadvies. Maar de argumenten die ze gebruiken om hun optimisme te rechtvaardigen ogen een stuk realistischer dan destijds.



CYBERCRIME & DE BELEGGER

door Paul Koster

Het was een harde strijd die bedrijven als General Electric, Philips en Siemens begin twintigste eeuw uitvochten bij de ontwikkeling van steeds betere gloeilampen. In 1911 leek General Electric een voorsprong te nemen op zijn Nederlandse concurrent met een nieuwe techniek die voor een sterkere gloeidraad in de peertjes moest zorgen. Anton Philips hoorde van de plannen en betaalde een ingenieur van het Amerikaanse bedrijf om het procedé in Eindhoven uit te komen leggen. Uiteindelijk wist Philips de nieuwe generatie gloeilampen ongeveer even snel als de concurrentie op de markt te brengen.

Honderd jaar geleden was technologie vaak alleen het doelwit van bedrijfs-spionage, tegenwoordig is het doelwit én middel. Cybercrime is verworpen tot een grote en nog steeds onderschatte bedreiging voor consumenten, bedrijven en daardoor ook beleggers. Wereldwijd worden de kosten van digitale diefstal geschat op zo'n 350 miljard euro per jaar, en het is de snelst groeiende vorm van criminaliteit. In Nederland loopt de schade jaarlijks op tot tien miljard euro.

En het zijn niet de minste bedrijven die getroffen worden door digitale aanvallen van buiten. Zo werden hoogtechnologische ondernemingen als Gemalto en ASML onlangs gehackt. Beide bedrijven haastten zich om te verklaren dat bij de inbraken geen gevoelige informatie is buitgemaakt, maar dat dit bij een volgend slachtoffer wel het geval kan zijn, lijkt geen twijfel.

De kwetsbaarheid voor hackers heeft allereerst te maken met de toenemende interactiviteit tussen systemen en producten. Alle communicatie maakt kwetsbaar voor meeluisteren van buitenaf, met alle mogelijke gevolgen van dien. Zo ontdekten beveiligingsexperts twee jaar geleden lekken in medische röntgen-apparaten waardoor hackers deze op afstand over konden nemen en toegang hadden tot medische gegevens. Daarnaast kan de technologische infrastructuur bij grote ondernemingen zo complex zijn dat maar weinigen deze kunnen overzien. Zorgelijk zijn berichten uit de financiële wereld waar fusies en overnames hebben gezorgd voor een lappendeken van computersystemen die in elkaar zijn geschoven. Dat klinkt als een kwetsbare werkelijkheid.

Een onderneming honderd procent beveiligen tegen cybercriminaliteit is onmogelijk, zo vertellen de experts. Toch is het zonneklaar dat ondernemingen afdoende maatregelen moeten nemen om strategische informatie zeker te stellen. Des te schrijnender is het dat uit recent onderzoek van KPMG blijkt dat beveiligingsinspanningen van bedrijven in geen verhouding staan tot de risico's die ze lopen. Voor bestuur en commissarissen is een belangrijke rol weggelegd om deze zaken op de juiste waarde te schatten. Wij zullen ze daar namens beleggers vragen over stellen tijdens de komende cyclus van aandeelhoudersvergaderingen.