Schoolvoorbeeld Yahoo toont impact van falend cybersecuritybeleid

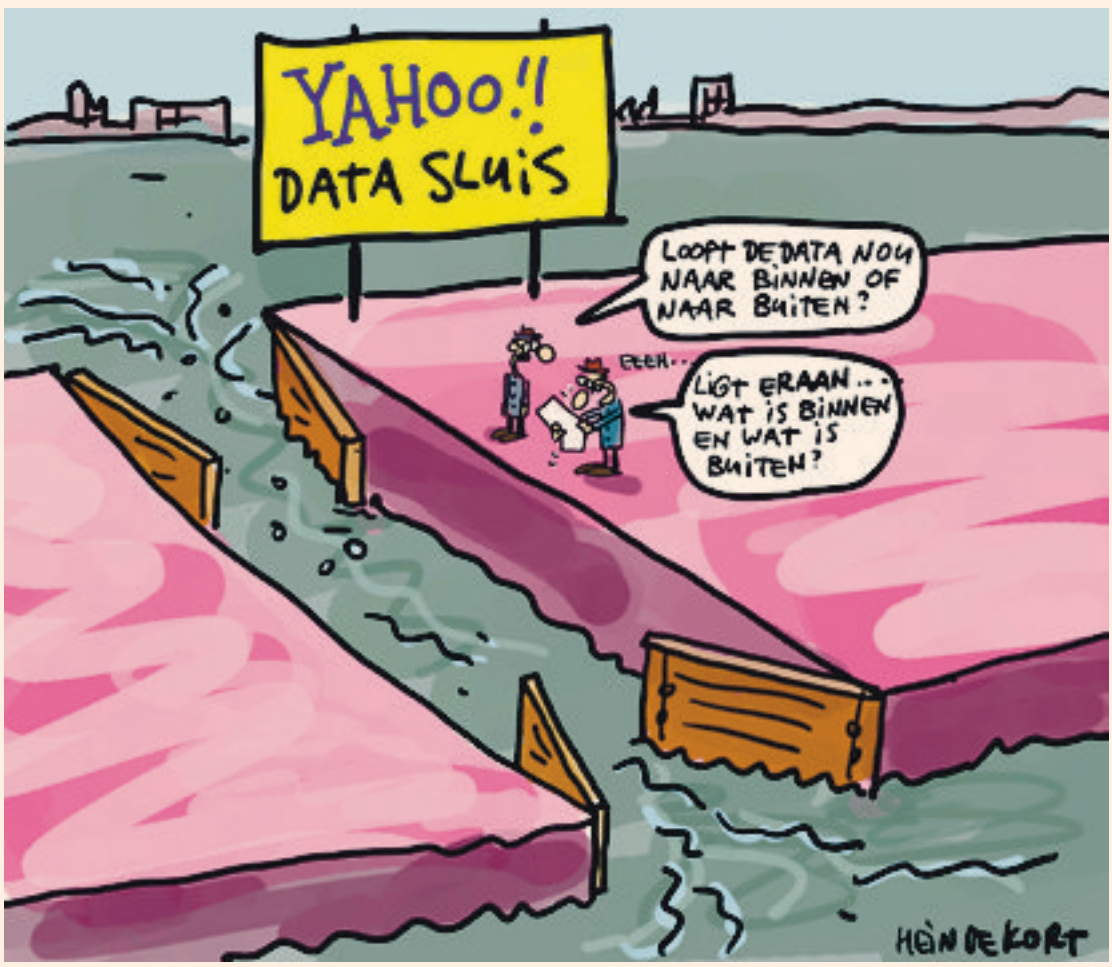
Datalekken des te ernstiger omdat Yahoo ze geheim hield ondanks meldingsplichten

Axel Arnbak

Yahoo verkeert in zwaar juridisch weer. Het internetbedrijf heeft meer dan vijftig rechtszaken aan de broek hangen. Financiële- en privacytoezichthouders in de VS en in Europa lanceren diepgaande onderzoeken naar Yahoo's cybersecuritypraktijken. En middenin de juridische puinhoop en overnamegesprekken met telecomgigant Verizon stuurde Yahoo begin maart General Counsel Ron Bell ook nog eens de laan uit.

De chaos heeft alles te maken met drie gigantische datalekken bij het bedrijf in 2012, 2013 en 2014, waarbij hackers respectievelijk 200 miljoen, 1 miljard en 500 miljoen accounts buitmaakten. Pas toen telecomgigant Verizon het zwalkende internetbedrijf medio 2016 wilde overnemen, onthulde Yahoo eerst mondjesmaat in september en daarna pas in december de astronomische omvang van de datalekken. De respons van Yahoo is een schoolvoorbeeld van hoe een bedrijf alles verkeerd kan doen vóór en vooral ná een groot datalek. Daarnaast bieden de incidenten inzicht in de financiële, juridische en bestuurlijke schade als het echt misgaat.

De datalekken zijn in de eerste plaats ernstig, omdat Yahoo gevoelige klantinformatie jarenlang ondermaats beveiligde en talloze publieke waarschuwingen van experts in de wind sloeg. De miljard gestolen passwords waren in 2013 bijvoorbeeld beschermd met het al in 1991 uitgebrachte en allang onbetrouwbaar bevonden MD5-algoritme. Een 22 jaar oude technologie gebruiken om een miljard passwords te beveiligen is hetzelfde als een Zeppelin laten landen tijdens spitsuur op Schiphol: levensgevaarlijk. De lekken zijn nog veel ernstiger, omdat Yahoo ze geheim heeft gehouden, ondanks talloze wettelijke meldingsplichten. Het beursgenoteerde bedrijf jaagt daarmee aandeelhouders, toezichthouders, potentiële koper Verizon en een miljard gebruikers tegen zich in het harnas. Bovendien heeft Yahoo alle gebruikers doelbewust blootgesteld aan cybercrime, vooral als ze nietsvermoedend dat ene password ook voor andere online diensten gebruikten. Iedereen wil nu bloed zien en Yahoo moet op de financiële, juridische en bestuurlijke blaren zitten.



ILLUSTRATIE: HEIN DE KORT VOOR HET FINANCIEELE DAGBLAD

De hack biedt een uniek inzicht in de kosten van falende cybersecurity governance. Verizon en Yahoo hadden een koopprijs van $ 4,8 mrd afgesproken. Na alle berichtgeving heeft Verizon een korting van $ 350 mln bedongen op de aankoopprijs. Naast deze korting spraken Verizon en Yahoo af dat de twee bedrijven de kosten van de gehele juridische nasleep zullen delen. In het bedrag zijn kosten gecalculeerd als reputatieschade, juridische procedures en mogelijke boetes van toezichthouders.

De juridische kosten zullen vast veel verder oplopen dan de korting van $ 350 miljoen. Yahoo schrijft in het openbare jaarverslag van 1 maart 2017 dat

Financiële en bestuurlijke kosten na historisch datalek pijnlijk zichtbaar

consumentengroepen al 43 juridische procedures zijn begonnen vanwege de hack. Gedupeerde aandeelhouders zijn ook een procedure gestart tegen Yahoo, en vier afzonderlijke zaken tegen individuele bestuurders. Yahoo verspijkerde tussen september en december 2016 al $ 16 mln aan advocaatkosten. Dit doet denken aan de jarenlange juridische nasleep van het TJ Maxx incident uit 2007, toen bekend werd dat de Amerikaanse retailer twee jaar had verzwegen dat een cybercrimineel de creditcardgegevens van 45 miljoen klanten had buitgemaakt. De nasleep zou TJ Maxx € 800 mln hebben gekost.

In Europa hebben nationale privacywaakhonden intensieve pan-Europese samenwerking aangekondigd om de nieuwe EU dataverordening internationaal te handhaven. Eerste ontvanger van een onderzoeksbrief is Yahoo, dat mogelijk de eerste Europese boete krijgt opgelegd van 4% van de wereldwijde jaaromzet. Op ruim $ 5 mrd is dat meer dan $ 200 mln, in slechts één handhavingsonderzoek.

De top van Yahoo moet het ook persoonlijk ontgelden. Ceo Marissa Mayer ontsloeg begin maart haar topjurist Ron Bell zonder ontslagvergoeding en moet zelf haar bonussen over 2016 en 2017 van $ 14 mln inleveren. Als de kwestie blijft voortslepen, zal het daar voor Mayer vast niet bij blijven.

Cybersecurity staat al een poos op de beleidsagenda, maar pas als het goed misgaat, komen de pijnlijke financiële en bestuurlijke impact van falend cybersecuritybeleid aan het licht. Het datalek bij Yahoo zal misschien niet de geschiedenisboeken ingaan als het grootste ooit, daarvoor is het internet nog te jong. Maar het Yahoo-fiasco zullen wij wel blijven doceren als hét schoolvoorbeeld van falend cybersecuritybeleid.

Axel Arnbak is advocaat bij De Brauw Blackstone Westbroek en onderzoeker aan het Instituut voor Informatierecht van de UvA. Reacties: @axelarnbak