Datalek

- Bij een datalek gaat het om ongeoorloofde of onbedoelde toegang tot persoonsgegevens, bijvoorbeeld een hacker die data steelt of een bedrijf dat een laptop met klantgegevens laat slingeren.
- Datalekken bevatten veelal gevoelige gegevens, zoals woonadressen, 06-nummers of wachtwoorden. Veel mensen worden gehackt omdat hun wachtwoord in een datalek te vinden is.
- Er worden in Nederland maandelijks duizenden datalekken gemeld bij de Autoriteit Persoonsgegevens. Een deel daarvan wordt verhandeld door criminelen.

In de zomer van 2015 had ik mijn eerste dag bij *RTL Nieuws*. Ik schudde honderden handjes, leerde iedereen kennen, kreeg een bureau en werd aan het werk gezet: verhalen maken, jij! Die eerste week leerde ik meteen wat voor impact een datalek kan hebben. In die week werd namelijk bekend dat Ashley Madison was gehackt.

Ashley Madison is een website voor vreemdgangers. Het richt zich op met name mannen die een relatie hebben en bieden hen vrouwen aan die wel in zijn voor een avontuurtje. Mannen moeten betalen om met anderen te praten, voor vrouwen is de website gratis. Of je nu even buiten de deur wilt seksen of 'gewoon'

een romantisch of opwindend gesprek wilt hebben met iemand anders dan je partner, het kan allemaal bij Ashley Madison. Hun slogan is veelzeggend: *Life is short, have an affair*.

Achter Ashley Madison zit het Canadese Avid Life Media. Dat is niet zo'n fris bedrijf. Zo kun je altijd een account aanmaken, maar als je de buitenechtelijke avontuurtjes zat bent, kun je alleen maar je profiel op 'verborgen' zetten. Als je hem wilt verwijderen moet je 19 dollar betalen – via je creditcard. Avid Life Media weet dat veel mensen uit nieuwsgierigheid op Ashley Madison kijken, maar zich snel weer bedenken en hun account willen verwijderen. En wat te denken van mensen die voor de grap het e-mailadres van een ander invoeren bij het registratieformulier? Zelfs dan moet je betalen om je account weg te laten halen. *Ka-ching*: ze verdienen daar miljoenen mee.

De hackers die inbraken bij Ashley Madison hadden meer dan 60GB aan data gestolen, van namen en e-mailadressen van de gebruikers tot hoe vaak ze van de site gebruikmaken en hun seksuele voorkeuren. Hun doel was duidelijk: deze vreemdgangerssite moest stoppen. Ze stuurden de baas een e-mail met daarin een lijst namen van gebruikers. Als Avid Life Media niet per direct zou stoppen met Ashley Madison, dan zouden ze alle gestolen data online publiceren.

Avid Life Media weigerde en de hackersgroep The Impact Team – zo noemden ze zichzelf – plaatste de data online. Iedereen kon het downloaden, het stond

zelfs op de bekende torrentwebsite Pirate Bay. Ik downloadde de data om te kijken of ook Nederlanders de website gebruikten. Heel veel mensen hebben een anoniem e-mailadres ingevoerd en gebruiken een anonieme gebruikersnaam. Ik dacht nog: de schade valt mee. Tot ik naast al die rijen data opeens een andere rij met gegevens zag staan: creditcardinformatie.

Want om als man Ashley Madison te gebruiken moet je zoals gezegd betalen. Deze creditcards zijn wél gekoppeld aan privégegevens. En dan wordt een anonieme gebruikersnaam als Johnny77 opeens John [redacted], wonend te [redacted] in het Brabantse dorpje [redacted]. Ik filterde al die creditcards op Nederland en kwam zo bij 594 Nederlandse mannen die op Ashley Madison zaten. Ik zag ook precies hoeveel ze uitgaven, waarmee je kunt inschatten hoeveel iemand van de website gebruikmaakte. Een man uit Sittard had in één jaar tijd maar liefst 17.779 dollar aan de vreemdgangerssite uitgegeven.

Sommige Nederlanders hadden hun profiel verwijderd. Dat staat dan netjes aangegeven in de data. Maar ja, wat heb je daar eigenlijk aan? Je wilt natuurlijk je data verwijderen zodat je nooit meer met Ashley Madison in verband kunt worden gebracht, om je te behoeden voor zo'n datalek. Daar gaat je 19 dollar, uitgegeven aan de schijnveiligheid dat je data daadwerkelijk van de servers zouden zijn verwijderd.

Wat ook opviel: de wachtwoorden die mensen gebruikten waren echt ontzettend zwak. Hierdoor kunnen criminele hackers de versleutelde wachtwoorden

makkelijk kraken en misbruiken om bij andere online accounts in te loggen, bijvoorbeeld online bankieren of sociale media. Iedereen begreep dat dat een risico vormde. Maar er was nog een ander risico waar je niet zo snel aan denkt, maar waar criminelen wel misbruik van maken: op basis van de wachtwoorden kunnen ze anonieme gebruikers identificeren.

Er waren zat leden die niet betaalden voor Ashley Madison, maar er wel een account hadden. Bij hen staan dus geen privégegevens. Deze mensen hadden in principe de juiste voorzorgsmaatregelen genomen: een willekeurige gebruikersnaam en een anoniem e-mailadres. Maar een wachtwoord gebruiken mensen vaak voor verschillende online accounts. Wat de criminelen deden: ze kraakten dat wachtwoord en keken vervolgens in andere datalekken of datzelfde wachtwoord voorkwam. Want terwijl veel mensen wel een anoniem e-mailadres gebruikten, vielen ze toch terug op datzelfde oude vertrouwde wachtwoord.

Stel: het wachtwoord van het anonieme account knappeman1989@gmail.com met de gebruikersnaam knappeman1989 is 'PSV_debeste89'. Dan zoek je op dat wachtwoord in andere datalekken en kijk je of het daar ergens voorkomt. En jawel: een zekere voornaamachternaam@gmail.com gebruikt het ook bij een website voor hondenliefhebbers. De kans is dan heel groot dat diegene ook achter het anonieme account op Ashley Madison zit. En dat was interessante informatie voor de hackers.

De identiteit van de leden van Ashley Madison was namelijk goud waard. Terwijl het gros van de criminelen mensen hackt om bankrekeningen te plunderen, hadden deze criminelen een ander idee. Voor veel gebruikers was het een groot geheim dat ze lid waren van een vreemdgangerswebsite. Ze hebben vrouw, kind, een publieke functie of belangrijke baan. Ofwel, ze zijn een gemakkelijk doelwit omdat ze buiten de deur seksten of wilden seksen. Dat wisten de criminelen ook.

> Hoi NAAM,
>
> Je bent een gebruiker van Ashley Madison sinds DATUM. Je woont op ADRES en bent geboren op DATUM. Je registreerde je met het IP-adres IP-ADRES in de buurt van LOCATIE. Je gebruikte de gebruikersnaam GEBRUIKERSNAAM met het wachtwoord WACHTWOORD. Je was op zoek naar OPSOMMING SEKSUELE VOORKEUREN. Van alle berichten die je hebt gestuurd, was het bericht op DATUM het beste, jij smeerlap!
>
> Als je niet binnen 48 uur 1000 euro in bitcoins overmaakt, dan stuur ik dit naar al je familie, vrienden en collega's zodat ze weten wat voor viezerik je bent.

Dit soort e-mails krijgen gebruikers van Ashley Madison in hun inbox. Mensen schrikken zich kapot: ze willen niet dat anderen weten dat ze op een vreemdgangerswebsite stonden, laat staan wat hun seksuele fantasieën zijn of welke berichten ze hebben gestuurd.

Dat de crimineel ook hun privéberichten heeft, is een leugen; maar dat weten de slachtoffers niet.

Het is extra eng voor degenen die gebruikmaken van een anonieme gebruikersnaam en e-mailadres. Zij krijgen deze afpersingsmail op hun échte e-mailadres binnen, met daarin hun échte naam en – als ze hadden betaald – ook het woonadres. Dan denk je bij jezelf: shit, ik ben er gloeiend bij.

Het is dan ook logisch dat heel veel mensen het losgeld betalen, vooral degenen die iets te verliezen hebben. Een hoge overheidsfunctionaris, bestuurder van een multinational, burgemeester, belangrijke generaal, bekende journalist of een priester. De criminelen hoeven alleen maar geautomatiseerd afpersingsmails te sturen en alle bitcoins te innen. In sommige e-mails plaatsen ze zelfs een QR-code waarmee je in één keer een bitcoinbetaling kunt doen – wel zo gebruiksvriendelijk. In korte tijd stromen vele tienduizenden euro's binnen. Later bleek dat de criminelen nauwelijks overgingen tot het verspreiden van die gevoelige data om slachtoffers onder druk te zetten: ze verdienden zoveel met de e-mails dat dat helemaal niet nodig was.

De afpersingsmails zijn zo effectief dat leden van Ashley Madison zelfs jaren na de hack nog steeds dit soort mailtjes ontvangen, alleen dan een stuk gerichter. De criminelen zetten er dan de namen van hun partner, kinderen of collega's bij, die gemakkelijk te vinden zijn via sociale media, om het slachtoffer onder druk te zetten om toch te betalen. Of de criminelen beloven

om de data voor altijd te verwijderen van het internet, zodat ze niet meer worden lastiggevallen – wel tegen een prijs, natuurlijk. Maar die data staan, ook nu je dit boek leest, nog steeds overal op het internet.

Er is zelfs een bedrijf dat een zoekmachine bouwde waar je een e-mailadres invoert en kunt zien of diegene een account had op Ashley Madison. Dat wordt niet alleen misbruikt door vrouwen die het e-mailadres van hun man invullen, maar ook door vrienden, collega's en willekeurige anderen die gewoon 'voor de lol' e-mailadressen invullen van mensen van wie ze denken dat ze vreemdgaan. Het bizarre is: je kunt het bedrijf betalen om je gegevens uit de zoekmachine te laten verwijderen. Maar daarmee haal je die data maar op één plek weg. Iedereen die de gegevens heeft, kan zo'n zoekmachine beginnen – en dan kun je opnieuw dokken.

De impact van het datalek is enorm. Tientallen miljoenen mensen leefden jaren in angst dat hun partner, familie, vrienden of collega's weet zouden hebben van hun buitenechtelijke avontuurtjes of de interesse daarin. Voor sommigen was de angst en schaamte zo groot dat ze zichzelf van het leven beroofden. Een van de slachtoffers is een 56-jarige Amerikaanse dominee, die een aantal dagen na de hack een einde aan zijn leven maakte. In zijn afscheidsbrief noemt hij Ashley Madison en schrijft hij aan zijn vrouw en twee kinderen dat het hem ontzettend spijt. 'Hij bood genade, barmhartigheid en vergeving aan alle anderen, maar

hij kon zichzelf dat op de een of andere manier niet geven,' vertelde zijn vrouw tegen CNN.

De hackers van The Impact Team hebben hier nooit op gereageerd. In de paar interviews die ze via e-mail hebben gegeven, zeiden ze dat ze het gemunt hadden op bedrijven die 'honderden miljoenen verdienen aan de pijn, geheimen en leugens van anderen'. Avid Life Media is voor zover bekend het enige bedrijf dat door The Impact Team is aangevallen. Ashley Madison looft nog altijd een beloning van 500.000 dollar uit in ruil voor de identiteit van een of meerdere hackers, maar ze lijken van de aardbodem te zijn verdwenen.

De hackers van The Impact Team worden 'hacktivisten' genoemd, een combinatie van hackers en activisten. Hun motief was activistisch: een einde maken aan de praktijken van Ashley Madison. Er was ook heel wat mis met Ashley Madison: ze vroegen geld om je account te verwijderen, maar verwijderden vervolgens die data niet, zo werd duidelijk uit de gestolen websitedata die door de hackers online werden geplaatst. Ook bleek dat er vrijwel geen vrouwen op de website zaten. Ashley Madison verdoezelde dat door nepprofielen van knappe vrouwen aan te maken waarop mannen konden reageren – tegen betaling natuurlijk.

Die louche praktijken alleen zijn natuurlijk nog geen reden om een bedrijf helemaal kapot te hacken. Nee, de hackers vonden dat de website moreel niet door de beugel kon. Ze vergeleken Ashley Madison

met een dealer die drugs bleef verkopen aan verslaafden. Daarom hebben ze alle data online gepubliceerd: om de website zo veel mogelijk te schaden, in de hoop dat het aantal gebruikers zou stagneren of dalen. Dat daarvoor miljoenen mensen moesten boeten, en zelfs mensen om die reden uit het leven stapten, maakte de hackers blijkbaar niet uit. In de cybersecuritywereld wordt The Impact Team dan ook niet als hacktivisten gezien, maar gewoon als criminelen: ze hadden de louche praktijken van Ashley Madison immers ook op een manier aan het licht kunnen brengen zonder de gebruikers te schaden.

Het bizarste aan dit verhaal is misschien nog wel: de hack heeft Ashley Madison niet de kop gekost. Integendeel, ze hebben inmiddels meer dan 60 miljoen leden, het hoogste aantal gebruikers ooit.

Foutje, bedankt

In het nieuws lees je vaak over datalekken. Dan is er bijvoorbeeld een bedrijf gehackt waardoor de gegevens van klanten op straat zijn komen te liggen. Of een bedrijf heeft zijn online veiligheid niet goed op orde waardoor iemand zomaar bij gevoelige gegevens kan. Er gaat een hele wereld schuil achter een datalek, ver verborgen voor de normale internetgebruiker. De gegevens uit zo'n lek kunnen namelijk veel geld waard zijn.