

Bruce Schneier over privacy en meer

Auteur: Lex Borger > Lex Borger is een principal consultant bij Domus Technica. Hij is te bereiken via e-mail: lex.borger@domustechnica.com.

Bruce Schneier is 'the closest the security industry has to a rock star', volgens The Register. Dit staat vermeld op de omslag van 'Schneier on Security', niet eens meer het laatste boek van Bruce. Hij heeft verschillende boeken geschreven over security, zowel technisch diepgaand als over de sociale aspecten van security. Niet veel auteurs kunnen dat claimen. Voeg daarbij dat Bruce heel actief blogt en een elektronische nieuwsbrief publiceert, dan kom je tot de conclusie dat als je de kans krijgt om hem te interviewen, je dat met beide handen beetpakt. Ik heb een aantal jaren geleden in dit blad al geschreven dat 'Secrets and Lies' het beste security boek was wat ik tot die tijd gelezen had, en het staat nog steeds dik in mijn top tien. Bruce, die in het dagelijks leven Chief Security Technology Officer van BT is, was 27 mei in Nederland voor twee presentaties. Ik woonde zijn presentatie 'De psychologie van security' bij.

De presentatie van Bruce had als titel 'de psychologie van security'. Het uitgangspunt van Bruce hierbij is dat er een essentieel verschil is tussen je veilig voelen en veilig zijn. Hij stelt: "Je kunt je veilig voelen, ook als je dat niet bent en je kunt veilig zijn, zonder dat je dat zo voelt. In onze taal is er niet echt een verschil tussen deze twee begrippen."

"Economisch gezien is security altijd een afweging. Je geeft iets op om iets aan security te winnen. In een kogelvrij vest ben je veilig. Maar je geeft een stuk bewegingsvrijheid op en waarschijnlijk ook een stuk modebewustzijn. Dus de beslissing om er een te dragen is een persoonlijke afweging. Het is dus niet belangrijk om je af te vragen of een beveiligingsmaatregel werkt. Je hoort je af te vragen of een maatregel de moeite waard is. Daarom dragen mensen in Amsterdam over het algemeen geen kogelvrij vest."

"Deze afwegingen worden echter gemaakt op basis van een gevoel van veiligheid. Ik kan je een veilig gevoel geven, door je te beveiligen en te hopen dat je dat ook zo voelt. Of door je onterecht veilig te doen voelen en hopen dat je dat niet merkt. Beide methodes werken. Vroeger, toen we nog in het wild leefden, lagen gevoel en werkelijkheid dicht bij elkaar. Tegenwoordig kan daar een groot verschil in zitten." Een groot deel van zijn presentatie gebruikt Bruce om uit te leggen waar dat verschil dan in zit.

Privacy en anonimiteit

Op het internet trekken we privacy en anonimiteit vaak gelijk. Het internet wordt steeds minder anoniem. Ik vraag Bruce naar zijn mening en hij is wat genuanceerder: "Sociale netwerken maken het internet zeker minder anoniem. Echter, anonimiteit op het internet bestaat nog steeds. Dit lijkt een paradox, maar het is echt waar. Als je dat wilt, kun je volledig anoniem zijn op het web. Kwaadwil-

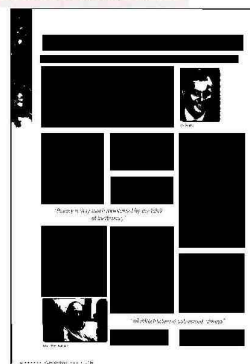
lende gebruikers passen dit toe, maar ook diegenen die verborgen willen blijven voor kwaadaardige entiteiten."

Dus anonimiteit is niet gelijk te stellen aan privacy. Wat is privacy dan wel? Bruce: "Privacy is een sociaal gegeven. Het gaat over relaties en vertrouwen. In het dagelijks leven is privacy in overvloed aanwezig. Het delen van informatie is binnen de fysieke context inefficiënt. Zelfs als je informatie deelt in een publieke setting, dan is de gedeelde informatie niet meteen publiek bekend. We zijn sociale wezens en hebben continu sociale interacties met elkaar, in verschillende contexten. Je kunt leraar zijn, vader, 's avonds uitgaan. Elke keer is de context anders en het is heel eenvoudig dat gescheiden te houden." "Op het internet is dat net andersom. Publiekelijk delen van informatie is eenvoudig. Je hoeft maar een blog te beginnen of lid te worden van Facebook of Twitter en je gedeelde informatie is publiek bekend. Het is eenvoudig geworden om bekend of zelfs beroemd te worden op het internet. En alle context is weg. Je kunt niet langer informatie delen in de juiste context. Als je je hier niet van bewust bent, kun je van een koude kermis thuiskomen. Privacy is op het internet heel moeilijk te krijgen."

Ik haalde Ashton Kutcher aan, die zelf zegt zijn privacy te waarborgen door juist veel informatie over hemzelf en zijn vrouw Demi Moore publiekelijk te delen. Bruce vindt dit geen privacy. "Hij heeft zichzelf oninteressant gemaakt."

Maar wie is dan verantwoordelijk voor de afscherming van jouw informatie? Bruce: "Dat gaat over techniek, die taak kan niet bij jezelf liggen, het is de verantwoordelijkheid van het bedrijf wat jouw informatie verwerkt. Zo werkt het in de gewone wereld ook. Je sluit je hotelkamer af, en verwacht dat daardoor jouw spullen veilig zijn. Je controleert de kwaliteit

van hun elektronische sleutelsystemen niet, daar heb je geen verstand van. Blijkt dat ontoereikend zijn, kijk je het hotel erop aan. Bij de meeste instanties heb je geen keuze om hen jouw informatie te verstrekken, zoals overheden, banken en verzekeraars. Je hoopt maar dat ze het goed beschermen. Bij sociale netwerken heb je wel de keuze. Naast te vertrouwen op hun technische verantwoordelijkheid hoor je zelf ook sociaal bewust te zijn over wat je deelt. Bedenk dat je eigen privacy-instellingen van Facebook niet te begrijpen zijn. Je wordt misleid. Jij bent ook niet de klant van Facebook, dat zijn de adverteerders. Facebook wil graag dat je informatie deelt en probeert delen aanlokkelijk te maken." Bruce trekt een vergelijking: "Jouw portemonnee bevat doorgaans informatie die te misbruiken is. Als ik jou kan verleiden tot het aan mij tonen van de inhoud van je portemonnee, is er nog niets aan de hand. Ik haal jou over dat te doen met een verhaal dat ik onderzoek doe, of ik kan je overtuigen dat iedereen het doet. Ik heb je alleen maar gemanipuleerd tot dat moment. Als ik die informatie daarna publiceer, heb ik jouw vertrouwen gebroken, maar nog steeds is jouw informatie niet misbruikt. Dat gebeurt pas als iemand die de informatie tot zich neemt er iets kwaads mee doet." Deze vergelijking illustreert mijns inziens ook het verschil in privacybeleving tussen de VS en Europa. In Europa zien we de manipulatie



al als misbruik.

Ik begon over de generatie 'Y'-jongeren, de generatie die opgegroeid is met internet en sociale netwerken. Als iemand sociaal bewust kan zijn, zijn zij het wel. Delen zij hun informatie bewust? Bruce: "Nee, er is veel onderzoek naar gedaan en jongeren begrijpen niet hoe hun informatie gebruikt wordt." Na het

doorprikken van dit ballonnetje verlaat ik dit onderwerp maar.

Outsourcing

Het sourcen van IT-beveiligingsdiensten is een discussiepunt in menig boardroom en managementteam van de IT-afdeling. Men vraagt zich

af: wel/niet doen, en onder welke voorwaarden? Bruce heeft hier desgevraagd een duidelijke mening over.

"Alle diensten kunnen worden geoutsourced. Dus ook securitydiensten. Het maakt niet uit wat het specifiek is, als het een infrastructuurele dienst is, kun je het outsourcen. Nu maakt iedereen zich hier nog druk over, maar dat zal veranderen. Outsourcing gaat aanslaan. CEO's zullen zich hier echt niet meer druk over maken, het wordt gewoon contrac-

tueel uitgevoerd. Er wordt alleen gekeken of de dienstverlener goed werk levert. De CEO gaat zich echt niet druk maken over details. Wereldwijd wordt van alles geoutsourced. Als

het fout gaat, riskeert de CEO gevangenisstraf (SOX), maar uiteindelijk zal infrastructuurele dienstverlening extern afgenomen worden."

Ik neem authenticatie als voorbeeld voor zo'n dienstverlening. In Nederland is men bezig aan een nationaal initiatief, OpenID plus. Is dit dan een handig alternatief voor de inrichting van een eigen (gesloten) authenticatiedienst? Bruce: "Dat hangt er helemaal vanaf. Wat omvat de dienst precies? Hoe wordt het toegepast? Waarvoor wordt het gebruikt? Of

authenticatie nu open of gesloten is maakt niet uit. Het belangrijkste is om je te realiseren dat om het goed uit te voeren vooral de dienst in detail goed ingevuld moet zijn."

Friday Squid Blogging

Een opvallende blogactiviteit van Bruce is 'Friday Squid Blogging'. Iedere vrijdag blogt Bruce iets gerelateerd aan de pijlknktvis. Is dit

de sociale netwerkversie van een vrijdagbeleving? Vergelijk het met de 'Follow Friday (#FF)' activiteit op Twitter. Ik vroeg Bruce over zijn squid blogging.

"De filosofie achter de squid blogentries is dat ik er elke vrijdagmiddag eentje maak. Soms sla ik een vrijdag over, soms zet ik er twee neer, wanneer ik wat meer materiaal heb." Maar ja, dit zegt nog niet waarom hij het doet. Dat geeft hij echter niet prijs, ook niet na verder aandringen. Wel wil hij nog kwijt: "Blogentries zijn geen eindige bron die geconserveerd moet worden. Als ik minder zou bloggen over pijlknktvissen maakt dat niet dat ik meer over security ga bloggen." Dit laatste is in ieder

geval goed nieuws voor de critici die deze wisseling van onderwerp niet helemaal begrijpen en bang zijn iets te moeten missen van security door de squid entries.

Links
Blog: www.schneier.com
Boeken: www.schneier.com/books.html



"Single sign-on is hard, authentication is hard"

"You cannot understand your Facebook privacy settings"

"You can feel secure, even if you are not"

"Privacy is very much maintained by the fabric of inefficiency"

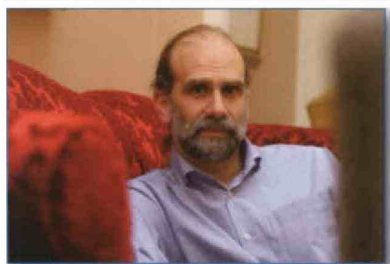


Foto: Peter Houlihan

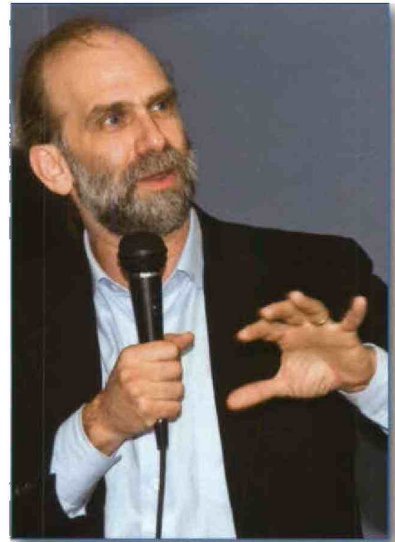


Foto: Bob Andrews



Lex Berger.