Frank Brokken / f.b.brokken@rug.nl

Verzekeringen

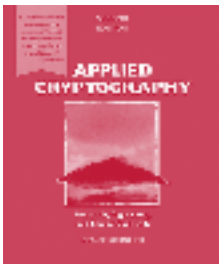
Als security manager heeft CIT-medewerker Frank Brokken de taak het 'security bewustzijn' bij de gebruikers van de universitaire ICT-voorzieningen te bevorderen. In zijn column doet Frank verslag van de stand van zaken met betrekking tot zijn missie.

Albuquerque

Soms heb je van die momenten dat je denkt: 'zie je wel, dat heb ik altijd al gedacht'. Zoiets overkwam mij afgelopen zomer in de buurt van Albuquerque. Door de omstandigheden daartoe gedwongen (geen vervelende, wees niet bezorgd) moest ik daar een week wachten op het vervolg van mijn zomerse activiteiten. Wat doe je dan nadat je 's morgens uit je slaaphol bent gekropen, hebt ontbeten en klaar bent voor de volgende dag waarin je geen verplichtingen hebt? Ik heb de neiging om dan naar een boekhandel te gaan.

Julius Caesar

Het mooie van de Amerikaanse boekhandels vind ik dat ze uitnodigen om er te zijn: overal zijn zitjes waar je eens lekker door een boek heen kunt bladeren voordat je besluit om het al dan niet aan te schaffen; bij vrijwel elke boekhandel is in de winkel zelf een plek waar je heerlijke koffie kunt bestellen en ook daarbij zijn dan weer comfortabele fauteuils waarin je opnieuw in alle rust onder het genot van een Frappuccino of zo een boek eens goed aan een inspectie kunt onderwerpen.



Zo bevond ik mij al snel in een van de boekhandels van Albuquerque waar ik in de schappen over computers een boek aantrof van Bruce Schneier. Schneier is binnen de informatiebeveiligingswereld geen onbekende. Rond 1996 verscheen zijn boek 'Applied Cryptography' waarin hij een overzicht geeft van algoritmen en toepassingen op het gebied van cryptografie.

Nou is cryptografie een integraal onderdeel van beveiliging, en het aardige - of bijzondere - is dat er erg veel manieren zijn om informatie te versleutelen. Julius Caesar maakte er al gebruik van om informatie door te geven aan de commandanten te velde met de naar hem genoemde Caesar-encryptie (een eenvoudige 3-letter-shift in het alfabet, dus 'aap noot mies' wordt 'dds qrrw plhv').

Ondanks het feit dat we zo'n encryptie tegenwoordig maar simpel vinden, heeft het zo'n jaar of duizend geduurd voordat men ontdekte hoe je zo'n encryptie eenvoudig kon 'kraken' (de Arabier Al-Kindi ontdekte het principe van letterfrequenties. Zo komt in het Nederlands de letter 'e' het vaakst voor, dus in een klassieke

Caesar-encryptie wordt dat de letter 'h'; een overzicht van letterfrequenties helpt je dan bij de rest van de ontcijfering).

Enigma-machine

Secrets and Lies

Pizzakoeriers

Zo zijn er allerlei andere anekdotes over hoe fameuze versleutelingsmethoden werken. De Duitse Wehrmacht had al voor het uitbreken van de Tweede Wereldoorlog de beschikking over de Enigma-machine. Deze wel heel bijzondere versleutelaar geeft de gebruiker de mogelijkheid om een uitermate veilige encryptie te gebruiken, die absoluut niet vatbaar is voor Al-Kindi's frequentieanalyse.

Een van de anekdotes rond de Enigma is dat de geallieerden maar niet in staat waren om de Enigma-encryptie te kraken totdat men een tekst onderschepte van zo'n 300 letters waarin geen enkele 'w' voorkwam. Nou dat is wel heel erg gek, omdat je in zo'n tekst toch met aan zekerheid grenzende waarschijnlijkheid ook een paar keer een 'w' zou moeten aantreffen. Geen 'w' kan eigenlijk alleen maar als iemand een tekst verstuurt die geheel bestaat uit de letter 'w'. Maar waarom zou men dat doen?

De Duitsers, ook niet gek, hadden zich al vroeg gerealiseerd dat het aantal berichten van de Oberkommandantur naar de eenheden te velde vlak voor een offensief groter was dan daarbuiten, en dat dat soort informatie - *traffic-analysis* genaamd - voor de vijand nuttig is te weten: men weet niet *wat* er gebeuren zal, maar wel *dat* er iets zal gebeuren. Reden genoeg om op je hoede te zijn....

Merkwaardig is dat de Duitsers zich dat rond WO-II al wel realiseerden, maar de Amerikanen niet: het was kort voor 'Desert Storm' duidelijk dat er iets op handen was door het opmerkelijk grote aantal pizzakoeriers dat pizza's afleverde bij het Pentagon.

Kortom, encryptie is erg belangrijk in de wereld van de geheimhouding en het boek van Bruce Schneier is dan ook een juweel dat in geen boekenkast van de zichzelf respecterende beveiliger mag ontbreken. Dat vond hij zelf ook. Tot begin 2000.

Human factor

In begin 2000 (en een revisie in 2004) publiceerde Bruce een nieuw boek: 'Secrets and Lies'. Het was dat boek dat ik in Albuquerque onder ogen kreeg. Een werkelijk prachtig boek (en ik heb het dan ook gekocht) dat ik iedereen die enigszins geïnteresseerd is in IT-beveiliging ten zeerste kan aanraden. Ik ga de essentie van het boek hier niet verklappen, maar wel een paar tipjes van de sluier oplichten.

Een ervan is dat Bruce in het boek al snel tot de conclusie komt dat encryptie weliswaar een noodzakelijke voorwaarde voor beveiliging is, maar dat encryptie op zich simpelweg niet zal leiden tot betere beveiliging. De factor van betekenis, zegt Bruce, is de zogeheten 'human factor'.

Nou knikken we allemaal natuurlijk braaf ja, en we gaan verder tot de orde van de dag. Tenminste, dat was wel mijn eerste reactie toen ik dat las. Maar hij werkt de stelling verder uit en komt tot het inzicht dat - omdat het nou eenmaal erg moeilijk is om directe beloning uit te stellen voor iets waarvan je niet weet of het ergens toe leidt - pogingen om mensen warm te laten lopen voor beveiliging geen of weinig effect hebben.

Bruce vergelijkt het met de auto-industrie: het gaat daar helemaal niet om kreukelzones, airbags en veiligheidsgordels. Die zijn alleen maar lastig voor de fabrikant. Zonder die *gadgets* zijn auto's goedkoper te fabriceren en de klant heeft de neiging daarvoor te vallen. Waarom dan toch dat dure veiligheidsonderzoek?

Omdat het moet. Van wie? Van de verzekeringsmaatschappijen, die anders veel moeten uitkeren aan claims en dus hun premies gaan aanpassen aan de veiligheid van auto's. Hoe veiliger hoe lager de premie. Het is duidelijk wie hier de verantwoordelijkheid toegeschoven krijgt: de fabrikant (en natuurlijk toch ook wel de automobilist: wie roekeloos rijdt krijgt z'n schade niet vergoedt).

Zwakke plekken

Die benadering vinden we niet terug bij het gebruik van software. Of je nou open source software of gesloten software gebruikt, in de gebruiksovereenkomst staat dat je de fabrikant niet aansprakelijk kunt stellen voor problemen die voortvloeien uit het gebruik van het product.

Kortom, Bruce stelt dat technische maatregelen ter verbetering van de beveiliging en pogingen om de gebruiker zich bewust te maken van de (on)veiligheid van het gebruik weinig effect sorteren zolang de gebruikte software allerlei zwakke plekken vertoont en de fabrikant daar niet op aangesproken kan worden. Tot die tijd blijft de gebruiker primair zelf verantwoordelijk voor een veilig gebruik van de computer. Denk daar maar eens aan wanneer u Word de volgende keer opstart. Ik heb het al eens eerder geschreven: computerbeveiliging is een erg boeiend vak.

Frank B. Brokken
Weet gelukkig meer van beveiliging dan van verzekeren