Feeling voor beveiliging

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

ICT-security

Het kan vreemd lopen. Nu de vakantieperiode is begonnen raak ook ik steeds meer in een vakantiestemming, en in dat verband herinnerde ik mij een incident dat zich een paar jaar geleden voordeed tijdens mijn vakantie.

Wij waren tijdens die bewuste vakantie in de Verenigde Staten, in de buurt van Palm Springs. Een mooie omgeving, vooral als je van woestijnen houdt. Dat doe ik, en dat betekent ook dat je een groot deel van de tijd 'uit de beschaving' bent. Maar vroeg of laat moet je weer even terug naar de beschaving voor het doen van inkopen: 'Groceries and Gas'.

Goed, we rijden een dorpje binnen en stoppen voor het plaatselijke supermarktje. Geen grote gigamarkt, maar zo'n klein dorpswinkeltje, midden in het dorp, met een paar parkeerplaatsen ervoor. Wij naar binnen voor onze boodschappen. Korte tijd later komen we weer buiten en wat doe je dan: je opent de deur van je (huur)auto om de boodschappen in te pakken en je vakantie vervolgens zorgeloos voort te zetten.

Terwijl we daarmee bezig zijn valt 't me op dat er een kabaal van je welste om me heen hoorbaar is. Ik zeg nog tegen Esther, mijn vrouw: "wat een klere herrie, laten we snel weggaan". Maar op dat moment realiseer ik me dat het *onze* auto is die zo'n kabaal maakt. Niet alleen maakt-ie geluid, maar alle lampen gaan onophoudelijk aan en uit. Nou had ik nog niet getankt, maar ik vond dit protest van de auto toch wel wat overdreven....

Daar sta je dan. Midden in een dorp bij een auto die niet van jezelf is en die je (dus) niet goed kent: de auto heeft kennelijk een alarminstallatie die afgaat om een reden die je niet begrijpt, maar die dat doet omdat jij zelf iets onduidelijks verkeerd hebt gedaan. Geloof me: je bent dan weliswaar geen autodief of -inbreker, maar je voelt je uitermate ongemakkelijk. Het excuus aan de omstanders: "I'm sorry, this is a rental car, and I have *no* idea what happened" maakt in ieder geval op jezelf een uitermate lamme indruk.

Ik heb een dergelijke situatie in een latere vakantie nog eens meegemaakt. Inmiddels weet ik wat je ertegen moet doen: gewoon de deur van de bestuurder ontsluiten met het sleuteltje (je weet maar nooit wie van de lezers nog eens iets aan deze tip heeft). Ik weet nog steeds niet wat het alarm heeft doen afgaan, maar dat is misschien ook minder relevant dan de vraag wat je vervolgens moet doen.

Een aardig beveiligingsincident, dat allerlei parallellen heeft met ICT-beveiliging, het onderwerp van deze Pictogram-column.

Opmerkelijk is het gedrag van de omstanders. Die doen eigenlijk niks. Hooguit een vage reactie zoals "hè, daar gaat (weer eens) een alarminstallatie af". Het zal de omstanders worst zijn. Ik weet niet wat de plaatselijke *police officer* zou hebben gedaan wanneer hij/zij in de buurt zou zijn geweest, maar van de omstanders heb je als *bad guy* kennelijk weinig te vrezen.

De alarminstallatie bereikt in ieder geval wel een belangrijk doel: de activiteiten van de inbreker worden vertraagd. De gedachte achter veel beveiligingsinitiatieven is niet eens zozeer om het de inbreker onmogelijk te maken zijn doel te bereiken, maar om het de inbreker zo moeilijk te maken dat-ie stopt of omkijkt naar een ander doel.

Persoonlijk vind ik de belangrijkste les van mijn vakantie-incident nog wel dat je als beheerder van een systeem (of dat nou de huurauto is of een computer) voldoende *feeling* met het systeem moet hebben om de reacties van het systeem te kunnen waarne-

men en er adequaat op te kunnen reageren. Je staat natuurlijk niet alleen voor aap wanneer je alarminstallatie afgaat door eigen toedoen, maar als je dan ook nog niet eens weet wat je ertegen moet ondernemen, dan is het wel erg droevig gesteld met je eigen kennis over 't systeem: een brevet van onvermogen, als het ware.

Ook bij ICT-beveiliging kunnen zich min of meer spectaculaire incidenten voordoen, waarvan je je afvraagt hoe ze in hemelsnaam hebben kunnen optreden, en die het gevolg kunnen zijn van een gebrekkige *feeling* met het systeem, of met impliciete veronderstellingen.

Een opmerkelijk voorval had te maken met de ondergang van de H.M.S. Sheffield op 4 mei 1982: het schip werd getroffen door een Exocet-raket tijdens de Falkland-oorlog. Dat de raket door de verdediging van het schip kon breken, had te maken met het feit dat de Exocet van Franse makelij is. Frankrijk en Engeland zijn beide lid van de NAVO, en dus (*sic*!) wordt er geen Exocet-raket op een Engels schip afgevuurd, zo meende de software van de computers van de Sheffield. Tja....

Maar ook in ons oude vertrouwde RC gebeuren soms onverwachte zaken. Binnen het RC staan computers opgesteld die bij het RC in onderhoud zijn. Het *gebruik* wordt overgelaten aan 'derden'. 'Onderhoud' betekent in dit geval niet meer dan 'het aan de praat houden van het besturingssysteem en het uitvoeren van *patches* die door de softwareleverancier worden aangeboden'. Da's niet echt een goed recept voor '*feeling* houden met het systeem', maar zo zijn de afspraken nou eenmaal.

Wanneer vervolgens de gebruiker van het systeem een database-server installeert, waarop het standaard, door de leverancier van de database-software ingestelde wachtwoord (twee letters (!!)) in gebruikt blijft, dan moet je niet vreemd opkijken dat zo'n database-server wordt *gehacked*. De inbreker die daarmee merkwaardig genoeg ook toegang kreeg tot het systeem zelf, installeerde meteen ook maar een web- en ftp-server.

Het duurde enige tijd voordat de inbraak (door de gebruiker, niet door de RC-beheerders) was geconstateerd. De schade viel achteraf gelukkig mee, maar wat ik hiervan leer is:

- softwareleveranciers installeren soms onverwachte, en naar de huidige inzichten onverstandige *defaults*: weet wat er op je computer is geïnstalleerd en zorg ervoor dat onnodige software is afgesloten of verwijderd.
- het zou goed zijn wanneer onderhoudsafspraken er niet alleen op gericht zijn een computer 'aan de praat' te houden. Het systeembeheer moet eigenlijk ook in de gelegenheid worden gesteld *feeling* met het systeem te ontwikkelen, waardoor het systeem aan de beheerder duidelijk kan maken *dat* er onregelmatigheden plaatsvinden.
- gebruikers hebben een eigen verantwoordelijkheid wanneer het gaat om zaken als het kiezen van wachtwoorden. Het blijven gebruiken van een *default*, door de software-leverancier ingesteld wachtwoord, is niet verstandig. Enige tips: kies een wachtwoord van minstens zes tekens, niet alleen letters, maar gebruik ook cijfers en speciale tekens.
- beveiliging is niet een zaak van alles of niets, maar voornamelijk een kwestie van mentaliteit. Wie de medewerking heeft van de betrokkenen (softwareleveranciers, systeembeheerders, gebruikers) kan jarenlang met plezier gebruik maken van ICT-systemen. De *hacker* zal een redelijk beveiligd systeem al snel overslaan, om op zoek te gaan naar een eenvoudiger slachtoffer.

Het opzetten van beveiliging is zoiets als het afsluiten van verzekeringen: het helpt je de ellende te minimaliseren, maar kan niet meer garanties bieden dan dat. Net zoals een brandverzekering niet betekent dat je vervolgens maar een vuurtje kunt stoken in de huiskamer, betekent ICT-security niet dat je 'de beveiliging' als gebruiker maar helemaal over moet laten aan 'de beheerder'. Maak er *teamwork* van, om zo te bereiken dat ICT-systemen langdurig veilig kunnen worden gebruikt.