

Reactie gevraagd



Het thema voor **Business in Risk** is deze keer brandveiligheid. In april dit jaar schreef ik in mijn commentaar al over computers en brand, nadat het rekencentrum van een Nederlandse universiteit in vlammen opging. Toen richtte ik me vooral op het maken en controleren van back-ups. Deze keer onderzoek ik de parallellen tussen de dreiging van een brand en die van een computerinbraak.

Tien jaar geleden, op 1 oktober 1993, werd de eerste firewall software uitgegeven, de Firewall Toolkit (FWTK) van de firma TIS. De makers ervan hadden toen al tien jaar ervaring met firewalls. Ik wil graag de parallel tussen brand- en inbraakdreiging trekken aan de hand van firewalls.

Firewalls

Een firewall is een systeem (meestal een server en een paar routers) dat twee netwerken met elkaar verbindt. Meestal gaat het om een bedrijfsnetwerk en het internet, maar binnen een bedrijfsnetwerk kan een firewall ook geplaatst worden, bijvoorbeeld om de R&D afdeling af te schermen van de andere afdelingen. De firewall regelt welk internetverkeer is toegestaan van het ene naar het andere netwerk en vice versa. De naam 'firewall' is in het Nederlands het beste te vertalen als 'brandwerende muur'. Een brandwerende muur is een muur die ervoor zorgt dat een brand aan de ene kant van de muur niet eenvoudig doorslaat naar de andere kant van de muur. Een brandwerende muur heeft dus een vertragende functie.

Zo heeft een firewall ook als (beveiligings)functie dat deze het inbrekers moeilijker maakt in te breken op de systemen aan de andere kant van de fire-

wall. Nota bene: ik heb het bewust over het moeilijker maken van een inbraak, niet over het onmogelijk maken van een inbraak. Een firewall is slechts een enkele laag van (hopelijk) een heel pakket aan beveiligingsmaatregelen. Vandaar ook dat ik firewall niet vertaal met 'brandmuur'; dat is een muur die brand tegenhoudt (de brand zal doven door gebrek aan zuurstof of brandstof, voordat de brandmuur het begeeft). Zoals je in de echte wereld niet alleen een brandwerende muur plaatst maar ook gebruik maakt van minder brandbare materialen en sprinklers installeert, zo behoort je in je computernetwerk ook meer maatregelen te nemen dan alleen de installatie van een firewall. Deze aanpak heet ook wel 'layered defense': de defensie bestaat uit meerdere lagen, waardoor het uitvallen van een enkele laag nog niet zorgt dat er geheel geen beveiliging meer over is.

Detectie

Het plaatsen van een firewall is een preventieve maatregel. Met een firewall kun je het aantal inbraken terugbrengen, en vaak ook de gevolgen van een inbraak verminderen. Omdat een firewall nooit honderd procent veiligheid biedt is het noodzakelijk, en dat wordt nog wel eens vergeten, er voor te zorgen dat er voldoende aan detectie en reactie wordt

gedaan. Een brandwerende muur kan brand enige tijd tegenhouden, maar zonder detectie en reactie zal de brand toch overslaan. Voor de detectie van inbraken bestaan speciale Intrusion Detection Systems (IDS) die het netwerkverkeer napluizen om te zien of er ongewenste zaken gebeuren. Hoe zo'n systeem bepaalt of iets ongewenst is, is niet eenvoudig. Een grote teleurstelling bij het in gebruik nemen van een IDS is dan ook vaak de hoeveelheid werk die gaat zitten in het goed inregelen van het systeem, d.w.z. goed aan te geven welk netwerkverkeer ongewenst is. Een simpelere methode is ook voorhanden: logging-informatie van de firewall en andere systemen bekijken om te zien of er ongewenste dingen gebeuren. Het nadeel van deze methode is dat het veel tijd kost als er veel logging informatie te bekijken is, en dat het geen uitdagend werk is.

Loos alarm

Wordt er iets ongewoons gevonden dan is het ook nog de vraag of het echt om een inbraak gaat. Een onterechte waarschuwing heet in jargon een 'false positive' (een 'false negative' is een onopgemerkte inbraak). Het minimaliseren van false positives en false negatives blijkt erg moeilijk te zijn. In feite is dat niet anders dan bij de detectie van brand. Uit