Een wereld vol Hansjes Brinker

Wie om zich heen kijkt, ziet dat beveiligen eigenlijk een aparte wereld is geworden. Behoorden systeembeheerders in de beginjaren van de IT tot de beter betaalde superdeskundige beroepen, een aantal jaren daarna leek het beheerdersdomein erg op de markt van Beverwijk, maar anno 2004 is veilig beheren een vak. Ut moet ut doen: de wens van de gemiddelde technologie-eindgebruiker is snel, simpel, standaard, stabiel en vooral safe. Dat laatste is een taak op zich die verder reikt dan het in huis slepen van firewalls en rekken vol AAA-hardware. Alle frequent wijzigende softwareversies en de dagelijks stroom aan virus-patronen en patches maken security tot een levenstaak. Net als politieagenten herken je ook onder de IT-garde de doorwinterde terreinbewakers. Het uniform met opgenaaide V ontbreekt nog, maar het zal niet lang duren of ook op dit terrein ontstaat outsourcing. Immers, wat is het verschil tussen het bewaken van de PC en het bewaken van de informatie op die PC? Het is schier onmogelijk dat controlewerk nog allemaal *erbij* te doen. Nieuwe technische ontwikkelingen gaan in de richting van *selforganising* en *remote-monitoring*. Mooie woorden voor doe het zelf op locatie en houdt toezicht op afstand.

Het doet mij denken aan het bewaken van een kostbaar museumstuk; je kunt allerlei beveiliging installeren, maar als de nachtwakers intussen naar de voetbalwedstrijd kijken, wordt geen flitslicht gezien of alarm gehoord. Ian Pearson, de futuroloog van BT, voorspelt al enkele jaren dat rond 2006 de wereld zal worden opgeschrikt door een razendsnel verspreidende virusaanval vanuit de computernetwerken zelf, een soort zelfontwikkelende IT-aids. De onderbouwing van die voorspelling klinkt onprettig realistisch. Hij baseert zich op een aantal kruisende lijnen van ontwikkeling in viruskenmerken, zelforganiserende netwerken, zelfhelende systemen en zelfregelende beheerssystemen. Zijn boodschap is dat we eerst moeten kunnen beheren, voor we het kunnen beheersen. Tot nu toe steken we net als Hansje Brinker telkens weer een vinger in een lekkend gaatje tot de dijk gerepareerd is. De klok tikt. Nog twee jaar de tijd om het beheer aan te pakken en de IT te beheersen. Of leeft u in de veronderstelling dat na U de zondvloed komt? Beheren of beheersen. Het scheelt twee lettertjes maar is een wereld van verschil. Juist dát maakt dat vele managers mislukken in hun bedoeling op de winkel te passen en uiteindelijk eindigen met een gevulde voorraadkast en boter op het hoofd. Die staken met veel poeha hun vinger in een gaatje, maar hielden hun andere hand op voor de voorbijgangers. Het typerende slag jongetjes dat thuis de boodschappen deed en het wisselgeld in eigen zak liet zitten. Onder het motto; *beheren is zorgen en beheersen maakt zorgen*, groeit de IT-security tot een nieuw terrein van spraakmakende nitwits en zakkenvullende verkopers. Overal voordeeltjes van alles-in-één-pakketten. Het doet mij denken aan het naderen van de warme zomerdagen. Als uit het niets stromen dan de aanbiedingen voor airconditioning apparaten via post, fax en e-mail binnen. Allemaal zelfstandig functionerende toestellen die beloven uw kantoor koel te houden. Hoe koel staat niet in de specificaties. Je mag ook niet zeuren voor de 999 euro voordelige aanbieding. In cyber wanen we ons een Gallisch dorp dat met de toverdrank van onze druïde die informatietechnologie beheerst. Wat zou het gemakkelijk zijn als we als een middeleeuwse vorst de informatietechnologie in onze macht zouden hebben. Maar helaas, macht bestaat bij gratie van het toelaten van die macht, en de technologie laat alleen maar toe wat we hebben geprogrammeerd. Dat maakt ook het hele wereldje wat ongrijpbaar. Bussen die op hol slaan, bruggen die open blijven staan, verkeerslichten die ineens op rood gaan, verbindingen die spontaan verbreken, software die automatisch in *reboot* gaat, bijna dagelijks lees je wel ergens een technologiefantoom. Je leest ook de toenemende twijfels over de macht en kracht van al deze kunstmatige intelligentie. Hebben wij als mensheid een gewrocht gebaard? Zijn we te ver gegaan in onze scheppingsdrang? Waren we niet wat te haastig met het in de markt duwen van al die elektronica? Kunnen we het nog wel in de hand houden? Beveiliging staat en valt met procedures en zorgvuldigheid. Met codes, passwords en tokens. Wie in de agenda van de gemiddelde IT-gebruiker bladert, ziet slecht verborgen reeksen van wachtwoorden en toegangscodes. Kennelijk is het moeilijk al die wisselende combinaties van letters en tekens te onthouden. We worden dus allemaal kandidaat voor de zwakste schakel. ■

Jacob van Kokswijk

Rond 2006 zal de wereld worden opgeschrikt door een razendsnel verspreidende virusaanval.

Jacob van Kokswijk *is parttime ICT-consultant bij CapGemini, veelgevraagd spreker bij telecomcongressen, lid van de stuurgroep Next Generation Networks initiative van de EU (jacob.van@kokswijk.nl, www.kokswijk.nl).*