Cybercrisis, back to basics

In het domein van de cybercrisis gaat de aandacht vooral uit naar preventie. Maar hoe slim we ook worden in het voorkomen van een cybercrisis, er zijn altijd mensen die nog slimmer zijn in het veroorzaken ervan. Het is daarom verstandig om meer aandacht te besteden aan crisismanagement.

tekst Arthur Zanders

Een koude nacht in Milaan, Pierre Manzano wil naar huis. Dan vallen de verkeerslichten uit. Manzano wordt uit zijn Alfa geslingerd als auto's op elkaar botsen in heel Europa. Operators kijken vol ongeloof toe terwijl het elektriciteitsnet bezwijkt. Mensen worden plotseling in kou en duisternis gestort. Het dodental loopt snel op.

Dit is de teaser van een spannende thriller van de Oostenrijkse schrijver Marc Elsberg. Het boek kwam in 2012 uit en zou verplichte literatuur moeten zijn voor securitymanagers, ICT'ers, crisismanagers en eigenlijk alle burgers. Niet om te leren hoe problemen worden opgelost, maar wel om ons ervan bewust te maken wat de problemen kunnen zijn. Het boek is fictie maar eigenlijk ook niet. Het beschreven scenario, een stroomuitval door een cyberaanval, heeft zich al herhaaldelijk in werkelijkheid voorgedaan. Elsberg beschrijft echter ook het vervolg. De paniek, de chaos en de ontreddering die en dergelijke ramp teweeg kan brengen.

PREVENTIE

Waren de kwetsbaarheden van computersystemen en het gebruik van internet vroeger nog het domein van doemdenkende computernerds, inmiddels is iedereen hier wel van doordrongen. Hoewel, het lijkt toch nog alsof we ons hier onvoldoende zorgen over maken. Natuurlijk zal niemand het belang van goede beveiliging, goede wachtwoorden, firewalls en virusscanners nog ontkennen maar de vraag is toch of we voldoende voorbereid zijn op mogelijke consequenties. Het hebben van een sprinklerinstallatie, brandblussers en bhv'ers verkleint de kans op een catastrofale brand maar grote branden komen toch regelmatig voor.

In het domein van de cybercrisis gaat telkens de aandacht vooral uit naar preventie. Terecht natuurlijk, maar er zijn twee grote problemen. Ten eerste is de omgeving zeer complex en onoverzichtelijk en ten tweede worden de meeste cybercrises opzettelijk veroorzaakt, vaak met politieke motieven. Hoe slim we ook worden in het voorkomen van een cybercrisis, er zijn altijd mensen die nog slimmer zijn in het veroorzaken ervan. Het is daarom verstandig om ook meer aandacht te besteden aan het omgaan met cybercrises, aan crisismanagement dus.

PROBLEMEN

Laten we eerst eens kijken naar de verschillende categorieën van problemen waarmee we te maken kunnen krijgen:

Voorzieningen niet betrouwbaar

Door een cyberaanval of -storing ontstaan problemen met allerlei computer- en netwerkvoorzieningen. Hierdoor kunnen bedrijven, burgers en overheden geen gebruik meer maken van voorzieningen. Ze werken niet of zijn niet betrouwbaar.
Een voorbeeld hiervan zagen we in 2011 toen het bedrijf DigiNotar, dat zorgde voor de beveiliging van overheidswebsites in Nederland, werd gehackt. Hierdoor ontstonden twijfels over de veiligheid van websites en werd geadviseerd DigiD en de website van de belastingdienst niet te gebruiken. Het leidde tot crisisberaad op het hoogste niveau.

Crisis in fysieke wereld

Een volgend probleem ontstaat wanneer een computerprobleem leidt tot crisis in de fysieke wereld. Omdat we tegenwoordig vrijwel alles aan netwerken koppelen, zien we dat we al snel in deze categorie terecht komen.
In mei 2017 werden meer dan 200.000 computers in 150 landen geïnfecteerd met het WannaCry-virus. In Nederland werd Q-park getroffen, maar in het Verenigd Koninkrijk moesten operaties in ziekenhuizen worden geannuleerd.
Begin dit jaar heeft een cyberaanval plaatsgevonden op een petrochemisch bedrijf in Saoedi-Arabië die als doel had een explosie met veel slachtoffers te veroorzaken. Het mislukte door een fout in de computercode van de aanvallers. Overigens wordt het in dit bedrijf aangevallen veiligheidssysteem wereldwijd gebruikt voor olieraffinaderijen, chemische fabrieken en kerncentrales. In dit soort gevallen kan een cybercrisis dus tot doden en gewonden leiden. Ook het

HET IS VERSTANDIGER OM MEER OVER WEERBAARHEID NA TE DENKEN

HOE DEDEN WE DAT IN DE JAREN VIJFTIG?

voorbeeld waar dit artikel mee begon, het uitvallen van vitale infrastructuur, kan direct of indirect tot fysieke slachtoffers leiden.

Crisisorganisatie zelf

Een andere categorie van problemen en kwetsbaarheden is die van de crisisorganisatie zelf. Datgene dat we inrichten om problemen bij crisis te managen, is vaak min of meer op dezelfde manier ingericht als het domein waar de crisis optreedt.
Zo werden door het WannaCry-virus in het Verenigd Koninkrijk ook de ambulancediensten getroffen.

Crisis blijft gevoed worden

Tot slot in deze beperkte opsomming een specifiek kenmerk bij de responsfase van een cybercrisis. Bij klassieke crisisscenario's is de bron van de crisis en het verloop van de daaruit volgende problemen veelal overzichtelijk en beperkt. Een brand of ontsnapping van gevaarlijke stoffen kan worden aangepakt en de consequenties nemen dan snel af. Overstromingen, orkanen of aardbevingen zijn lastig maar vaak relatief overzichtelijk en ook hier is het verloop vaak redelijk voorspelbaar. Dit kan bij een cybercrisis heel anders zijn. Terwijl we bezig zijn met de consequenties te managen, kan de bron nog onduidelijk zijn en aanwezig blijven zodat de crisis als het ware gevoed blijft worden.

'OLDSKOOL'

Er gebeurt veel op cybersecuritygebied. Er zijn veel verschillende organisaties en centra die zich ermee bezig houden. Zo hebben we het Nationaal Cyber Security Centrum (NCSC), onderdeel van de Nationaal Coördinator Terrorismebestrijding en Veiligheid van het ministerie van Justitie en Veiligheid waarin publieke en private partijen samenwerken. Maar ook de NIDV (de stichting Nederlandse Industrie voor Defensie en Veiligheid), verschillende universiteiten en private partijen houden zich ermee bezig. Maar toch. Los van alle uitstekende initiatieven en activiteiten om ons tegen cybercrises te beschermen, lijkt het verstandig om toch ook 'oldskool' te kijken naar onze crisisorganisaties.

WEERBAARHEID

Al in 1988 schreef Wyldavsky in zijn boek *Searching for Safety* over de strategie van weerbaarheid (*resilience*). Deze strategie zou een belangrijke leidraad moeten zijn voor het organiseren van crisisbeheersing. Vaak zien we dat dezelfde bedrijfsmatige uitgangspunten die in een normale organisatie de efficiëntie verhogen, worden gebruikt in crisisbeheersing. Crisisexpertteams die via digitale netwerken samenwerken (ICAweb), het delen van informatie tussen de verschillende lagen in de crisisorganisatie via netwerksystemen (LCMS), het alarmeren en communiceren via digitale systemen (P2000 en C2000), terminals met mobiele data in hulpverleningsvoertuigen, allemaal prachtige systemen maar uitermate kwetsbaar. Ons USAR-team dat in het buitenland wordt ingezet bij rampen is een voorbeeld van een hulpverleningsorganisatie die vrijwel zonder support van systemen kan functioneren. Die ervaring zou misschien beter gebruikt kunnen worden.

We zouden ons de vraag moeten stellen wat we binnen de crisisbeheersing nog kunnen doen als er geen GSM-netwerk en internet zijn en dus e-mailservers en VoIP-telefoons niet werken en wifi-signalen wegvallen. Hoe lang gaan politieauto's, ambulances en brandweervoertuigen nog functioneren als de tankpas bij de benzinepomp niet meer werkt? In de crisisbeheersing is het misschien verstandiger om minder over efficiëntie en meer over effectiviteit en weerbaarheid na te denken.

VIJFTIG JAAR GELEDEN

Ook in de advisering naar bedrijven en burgers is wellicht nog wel wat te verbeteren. Natuurlijk is het goed te waarschuwen voor veilig gebruik van netwerken, goede wachtwoorden en virusscanners. Maar wat als alles uitvalt? Hoe bereidt een gezin met kleine kinderen zich voor op een week zonder stroom, verwarming, drinkwater, voedsel en werkende pinpas? Wat doet een bedrijf om processen veilig te stellen als alles faalt en de parameters van de installatie niet meer uit te lezen zijn? Oplossingen zijn misschien niet eenvoudig, maar misschien soms ook wel. Hoe deden we dat vijftig jaar geleden ook alweer? ■

Arthur Zanders is directeur/consultant Zanders Consulting & Training BV: Risico en Crisismanagement, en domeincoördinator Delft Safety and Security Institute TU Delft.