Een RI&E? Denk vooral goed na over risico's, zegt Ben Ale

Risico-inventarisatie en -evaluatie was ooit bedoeld om ondernemers bewust te maken van de gevaren waaraan zij hun personeel blootstelden en wat ze daaraan eventueel konden doen. In 1989 werd een Europese richtlijn van kracht die de minimale bescherming regelde die werkgevers hun werknemers moesten bieden.

Die Europese richtlijn was, net als de Seveso-richtlijn die ging over de grote rampen, niet alleen bedoeld om de werknemers te beschermen. Het doel was vooral om in Europa een gelijk speelveld te creëren. Het kon niet blijvend zo zijn dat werknemers in het ene land een betere bescherming kregen dan in het andere. En de werkgevers in het ene land daaraan dus meer geld kwijt waren dan in het andere.

Van doelvoorschriften naar middelvoorschriften

Zoals in alle Europese richtlijnen, werd ook in deze bepaald dat de overheden erop moesten toezien dat die bescherming daadwerkelijk werd geboden. Dat maakte het niet alleen onvermijdelijk om deze bescherming wettelijk vast te leggen, maar ook om in de wet te regelen dat er een schriftelijk verslag zou zijn. Dat kon de overheid dan controleren en erover rapporteren aan de EU. Die schriftelijke vastlegging werd in 1994 de RI&E. Met in de geest van die tijd hoofdzakelijk doelvoorschriften. De werkplek moest zo veilig mogelijk zijn, het zoeken en vinden van eventuele middelen was aan de werkgevers en werknemers.

> *Zoals in veel andere wetten bleken doelvoorschriften ook voor de RI&E niet te werken*

Net zoals in veel andere wetten bleek dat ook voor de RI&E niet te werken. Er kwam een langzame omschakeling op gang naar middelvoorschriften in de vorm van arbeidscatalogi. Het doel echter is nog steeds hetzelfde. Het gaat daarbij niet om het papier, maar om de veiligheid op de arbeidsplaats. En belangrijker nog: dat werkgevers en werknemers zich bewust zijn van de gevaren en daarom die maatregelen nemen en zich zo gedragen dat ze niet het slachtoffer worden. Gezond weer naar huis blijft het hoofddoel.

Nieuwe bedreigingen: automatisering en geopolitiek

Bijna alles in de wereld is op de een of andere manier ‘slim’ of op een andere manier ‘automatisch’ gemaakt. Dat wil zeggen dat ook dingen die we vroeger zelf deden en waarvoor geen elektriciteit nodig was, nu ‘op stroom’ lopen. Een typemachine is een computer geworden, een fiets een e-bike en deuren gaan vanzelf open en dicht. We betalen niet meer met geld maar met een kaart, ook in de tram, de bus of de trein. En veel, heel veel daarvoor benodigde gegevens zijn opgeslagen in de grote wolk.

Als de stroom uitvalt, zijn onze gegevens onbereikbaar

Omdat het allemaal vanzelf gaat, vergeten we wel eens dat die grote wolk toch uiteindelijk bestaat uit computers, harde schijven en kilometers koperdraad en glasvezel, die om te functioneren heel veel elektriciteit nodig hebben. Als de stroom uitvalt, bij de wolk of bij de tussenstations die ons met die wolk verbinden, kunnen we ook niet meer bij de gegevens. De voorraadadministratie blijft dan niet meer up-to-date en als het geheugen van de kassa ook in de cloud zit, is ook dat onbereikbaar geworden. Als dat een uurtje duurt is dat voor de meeste ondernemingen niet al te erg, tenzij je in valuta of aandelen handelt. Dan kun je in een uurtje wel failliet gaan. Duurt het langer, dan wordt het voor steeds meer ondernemingen problematisch.

In veel apparaten zitten accu's die nog vrij lang meegaan. Een laptop of tablet blijft het wel een paar uur doen en smartphones een uurtje. Maar apparaten die veel energie gebruiken en daarom direct op het lichtnet zijn aangesloten, houden ermee op. Computers zonder accu's stoppen ermee. Ook als er een spanningsbeveiliging op zit. Meestal starten ze weer goed op als de stroom terugkomt en soms moeten ze een zetje hebben. Helaas verdwijnt er soms ook informatie, waardoor bestanden onbruikbaar worden of onvindbaar. Dat is ook vaak moeilijk te traceren.

> *Robots stoppen er dus mee, zonder dat meteen duidelijk is hoeveel energie er nog in zit*

Robots, elektrische deuren en kassa's houden ermee op

Behalve de informatiesystemen stoppen ook alle andere dingen die stroom gebruiken. Robots stoppen er dus mee, zonder dat meteen duidelijk is hoeveel energie er nog in zit. Komt de stroom weer terug dan gaan die robots misschien weer bewegen, maar wellicht niet zoals dat had gemoeten. Deuren gaan niet meer open of dicht, maar is er weer stroom dan gaan openstaande deuren misschien opeens toch dicht. Betaalautomaten werken niet meer en geldautomaten ook niet. Wie net zijn pasje in een automaat heeft gestoken of net op akkoord heeft gedrukt, moet maar afwachten of het pasje terugkomt of het geld. Zelfs als de la van de kassa nog open wil, is het de vraag of klanten nog wel contant geld hebben. Het licht gaat in ieder geval uit, de airco ook en de koelinstallaties stoppen ermee.

Alleen in instellingen met een noodaggregaat blijven de basisvoorzieningen functioneren. Tenminste, als het noodaggregaat het doet. Voor al dit soort dingen zijn oplossingen, mits die zijn geïnstalleerd. Maatregelen tegen de gevaren van het vanzelf weer opstarten van robots na een stroomstoring staan in veel arbo-catalogi. Er zijn echter nog wel meer gevaren denkbaar dan het bekneld raken tussen plotseling bewegende deuren. Zoals opgesloten raken in liften, de weg niet meer kunnen vinden in donkere gangen en boze klanten die niet kunnen afrekenen en zich ook niet kunnen beheersen.

Verbonden systemen kwetsbaar voor cyberaanvallen

De afhankelijkheid van informatiesystemen en de chips in veel apparaten maken ons ook

afhankelijk van de integriteit van de informatiestromen zelf. Het is verleidelijk om alle informatie en veel van de transacties via computer en smartphone te laten afwikkelen. Vaak zijn de onderdelen van een systeem met elkaar verbonden via een intranet en dat is dan weer verbonden met het internet. Makkelijk om te kijken of een ander filiaal nog voorraad heeft. De administratie staat online en in de cloud. En ook makkelijk om op weg naar huis vast de koffiemachine op te starten. Het is makkelijk voor energiebedrijven om meters op afstand te kunnen aflezen. Wat dan in theorie ook wel weer makkelijk is voor overheden en anderen, om na te gaan wie wanneer thuis is of thuiskomt. Maar dat terzijde.

> *De verbondenheid van al die systemen maakt ze kwetsbaar voor cyberaanvallen*

De verbondenheid van al die systemen maakt ze kwetsbaar voor cyberaanvallen. Die zijn vaak niet eens tegen een bepaald bedrijf gericht, maar iedere computer die niet voldoende beschermd is is een potentieel doelwit. Zelfs met een bijgewerkte en goed functionerende firewall annex virusdetector is het een wapenwedloop tussen de provider van de bescherming en het virus, wie er sneller bij de computer is.

Welk besturingssysteem bestuurt onze computers?

Ongelukkig is dat we vaak niet kunnen weten met welk besturingssysteem de computer die onze machines bestuurt eigenlijk is uitgerust. En of dat systeem wordt ge-updatet en of dat ook kan. De besturing van een apparaat is ook maar gewoon een programma en dat moet wel compatibel zijn met het besturingssysteem. Dus misschien is de versie van het programma wel recent, maar draait de computer die het besturingswerk doet nog op windows XP of gewoon DOS. Omdat die hardware decennia kan meegaan, zijn dat er nog heel veel.

Dat is allemaal prima zolang die apparaten niet ook op het internet staan aangesloten. Aangesloten kan een virus of *ransomware* het hele systeem onbruikbaar maken. De minst beschermde ingang bepaalt de kwetsbaarheid. Naast lastig en kostbaar kan dat ook onveilig zijn, als het gaat om een robot of hijskraan bijvoorbeeld, of zelfrijdende karretjes in een magazijn.

Andere, nieuwe risico’s: terrorisme en conflicten

Een ander, relatief nieuw risico is terrorisme. Als gevolg van een pakketje kan zomaar de hele straat worden afgezet waarin de onderneming is gevestigd. Daar kun je dan niet meer bij. De politie is wel bereid de deur dicht te doen, maar zet niet het alarm aan. Evenmin regelt zij verwarmingen, pompen en andere dingen die op tijd aan- of afgezet moeten worden. Je kunt niet meer bij de administratie of de kluis. En de omzet is ook even nul.

Als er iets gebeurt waardoor de ruiten ingaan, zijn de problemen nog groter. Dan kan in principe iedereen bij de spullen in de zaak. En het kan even duren voordat de omgeving is afgezet.

Je kunt als onderneming ook betrokken raken in een conflict. Dat kan over plofkippen gaan of de herkomst van de kleding. Een actiegroep kan uw onderneming als doelwit kiezen, er binnendringen en aan knoppen, schakelaars, computers en andere dingen zitten. De als gevolg daarvan ontregelde processen leveren ook gevaren op.

> *De vraag of dat allemaal in een RI&E moet staan is eigenlijk niet zo belangrijk*

Een RI&E? Denk vooral goed na over risico’s

Of zulke risico’s voor een onderneming relevant zijn, hangt af van de inhoud van de werkzaamheden en van de installaties die daarvoor nodig zijn. En of stroomuitval of gehackt of bezet worden gevaarlijk is of alleen maar geld kost, verschilt ook van geval tot geval. In ieder geval is het verstandig erover na te denken. En niet, zoals recentelijk containerbedrijven, ziekenhuizen en in Engeland de hele gezondheidszorg, overvallen te worden door een storing en er dan achter te komen dat je al veel eerder maatregelen had moeten nemen.

De vraag of dat allemaal in een RI&E moet staan is eigenlijk niet zo belangrijk. Wel belangrijk is de vraag of ondernemers erover nadenken en er zo nodig iets tegen doen. Het voorkomen van ellende is vaak een stuk minder kostbaar dan het opruimen ervan achteraf.

Ben Ale | em. hoogleraar veiligheid en rampenbestrijding

> TIP: Ben Ale is dagvoorzitter op de Praktijkdag RI&E