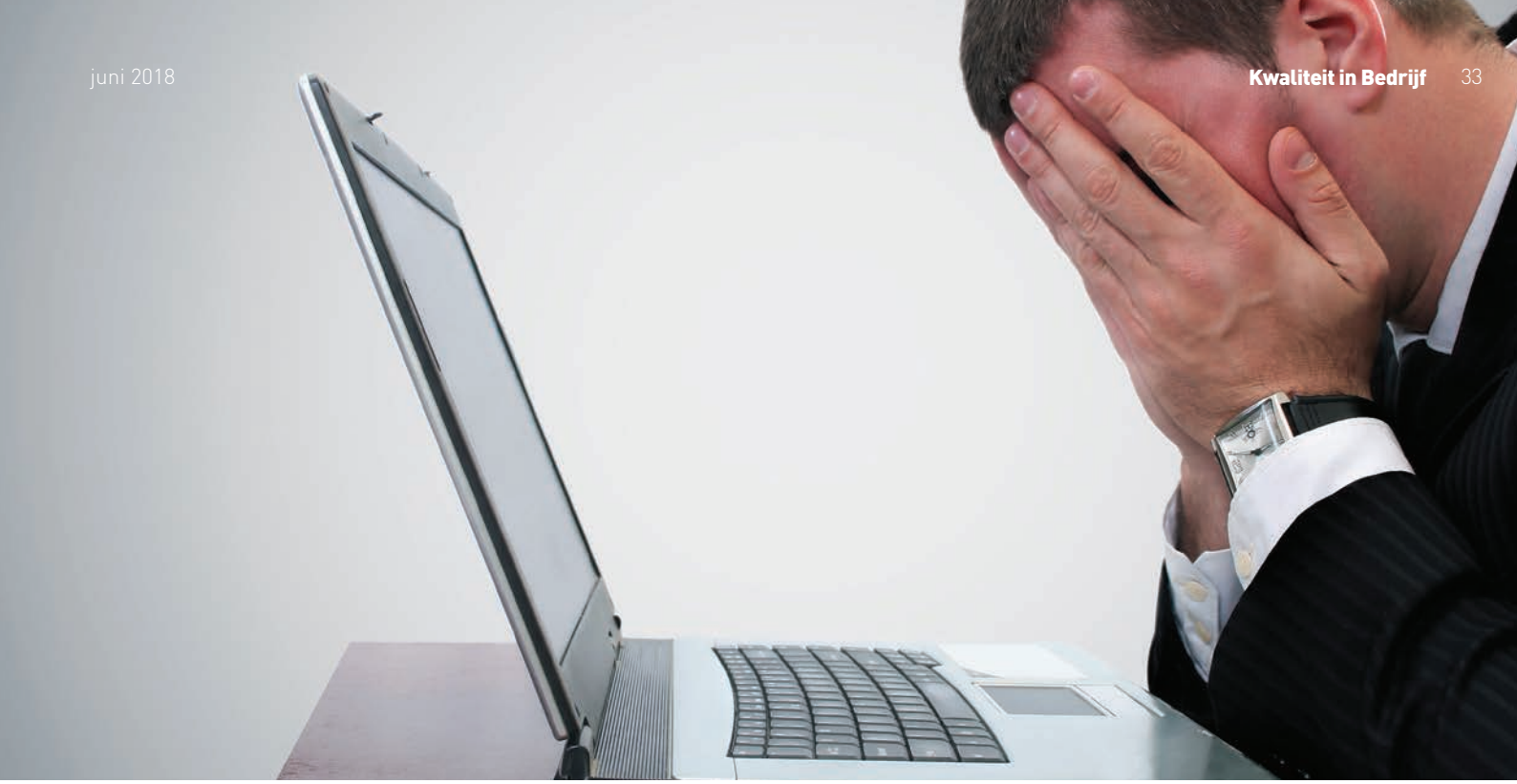

Ga op zoek naar de IT-afhankelijkheden in uw organisatie

IS ONZE AFHANKELIJKHEID VAN IT NOG ACCEPTABEL?

Er is bijna geen organisatie meer die niet een zekere mate van afhankelijkheid kent van IT. Ik durf zelfs te stellen dat de meerderheid ongelofelijk afhankelijk is en enkele zelfs, zeggen ze zelf, volledig. Hardware is een commodity geworden, dus daarover maakt men zich niet al te veel zorgen. Extra voorraad van het een en ander, naar een winkel op de hoek rennen voor een notebook of printertje of goede afspraken met de huisleveranciers van de IT-werkplekken en randapparatuur, dat lijkt wel een redelijke oplossing. Maar de afhankelijkheid van de softe kant, de applicaties, (veilige) toegang tot data en vooral de onderlinge samenhang is ongelofelijk groot. Wat nou als we 'ongelofelijk' vervangen door 'onacceptabel', sla ik dan de plank volledig mis, of ...?

Door Gert Kogenhop, bcm+

Het is duidelijk dat de afhankelijkheid van IT enorm is en alleen nog maar verder gaat toenemen. IT Continuity – of zoals dat in die kringen ook vaak wordt genoemd Disaster Recovery – wordt steeds belangrijker. Er wordt dan ook veel tijd, geld en energie gestoken in redundancy, in de vorm van meerdere datacenters en allerlei oplossingen om te voorkomen dat IT uitvalt. Allemaal prima vanzelfsprekend, echter, de complexiteit van de 'aan elkaar geknoopte systemen', volledig geïntegreerde oplossingen, centrale databases (lees: één dus) en andere synergie verhogende oplossingen maken organisaties enorm afhankelijk en kwetsbaar. Dagelijks merk ik dat gebruikers de *Recovery Time Objective* en *Recovery Point Objective* van alles wat zij toch écht nodig hebben om te kunnen functioneren niet kennen, om over alternatieven maar te zwijgen. Zonder IT zijn héél véél organisaties 'Het Haasje!'.

EEN RISICOBEOORDELING

Eén van de belangrijkste elementen tijdens het implementeren van een *Business Continuity Management Systeem* (BCMS) is het uitvoeren van een risicobeoordeling. Krijgen de afhankelijkheid van IT en de actuele bedreigingen rond dit thema – denk aan cybercrime – de juiste aandacht en het benodigde gewicht? Zijn we nog in de ontkenningsfase, steekt de struisvogel z'n kop in het zand of is men realistisch en worden de kwetsbaarheden, de verschillende bedreigingen en dus het risico voldoende onderkend? Goed om in beeld te hebben welke kritische processen afhankelijk zijn van bepaalde applicaties of data, bijvoorbeeld, en om de juiste herstelstrategie paraat te hebben. Wat is een acceptabele impact wanneer applicaties uitvallen of data niet beschikbaar is?

Ga op zoek naar de IT-afhankelijkheden in uw organisatie en laat u niet verrassen door deze vaak te verhelpen bedreiging. 'Voorbereiding is 90% van het resultaat' is een oude en misschien wel afgezaagde tegeltjeswijsheid, maar in dit geval een goed advies.