

# Beschikbaarheid van ICT is óók beveiliging

Beveiliging gaat volgens Van Dale over het 'onttrekken aan geweld, bedreiging, gevaar of schade'. Bij informatiebeveiliging denken veel mensen dan vooral aan het aspect 'vertrouwelijkheid' - voorkomen dat vertrouwelijke informatie uitlekt. En in het verlengde daarvan denken velen bij ICT-beveiliging vooral aan 'hackers'. De vraag is dan: welke informatie binnen uw organisatie is zodanig van aard dat ongewenst uitlekken serieuze schade oplevert? Als dat wel meevalt, is informatiebeveiliging dan automatisch geen issue meer? Nou... [JEROEN VAN DONGEN](#) \*

**V**ertrouwelijkheid is maar één aspect van informatiebeveiliging. Een ander aspect wordt nog wel eens vergeten en is doorgaans van veel groter belang: de *beschikbaarheid* van informatie en informatiesystemen. Immers informatie die niet beschikbaar is, is net zo nutteloos voor de procesgang van een organisatie als informatie die niet betrouwbaar is, en kan net zoveel of nog meer schade opleveren als het uitlekken van vertrouwelijke informatie. Niet-beschikbaarheid van informatie en informatiesystemen is een sluipend gevaar - vaak is het moeilijk om de kosten van een incident boven water te krijgen en veelal neemt men die moeite niet. Temeer daar ieder incident op zich vaak geen heel duidelijke impact lijkt te hebben. Met als gevolg dat de werkelijke omvang van de totale kosten verborgen blijft.

## Uitval = schade

Ook het onttrekken van een organisatie aan de schade die ontstaat als informatie en informatiesystemen niet beschikbaar zijn, is beveiliging. Uitval = schade! In een aantal gevallen is de schade erg duidelijk. Als een webwinkel een bepaalde tijd niet beschikbaar is, zal zich dat vertalen in een percentage gemiste omzet. Tenzij men een

werkelijk uniek product verkoopt, dan komen de klanten de andere dag wel terug.

Lastiger is het om de kosten te bepalen van een uurtje uitval van de bestandsopslag of de mailomgeving. Neem het volgende voorbeeld. We hebben een fictief bedrijf met 1.000 medewerkers, voornamelijk beeldschermwerkers. Tijdens een stroomstoring in het datacentrum blijkt dat de dieselgenerator niet wil starten en als na een tiental minuten de accu's van de UPS uitgeput zijn vallen de servers en netwerkapparatuur uit. Alles bij elkaar is een groot deel van de ICT-infrastructuur ongeveer vier uur uit de lucht. Laten we aannemen dat 50 procent van de medewerkers geen echte vervangende werkzaamheden kan vinden. Resultaat: 2.000 uren verloren. Als we uitgaan van een kostprijs van 40 euro/uur, dan is het directe verlies ten minste 80.000 euro. Het werkelijke verlies ligt hoger als het goed is, immers de inzet van die uren zou ook voor een of andere vorm van winst hebben gezorgd.

'Maar dat halen ze toch weer in?' Ja, als overuren waarschijnlijk... En als er tussendoor tijd genoeg is om zomaar 2.000 uren in te halen, moet wellicht eens goed gekeken worden naar

de *efficiency* van het bedrijfsproces. Hoe dan ook: de organisatie heeft 80.000 euro betaald, voor uren waar niets nuttigs mee is gedaan. Het Nederlandse woord daarvoor is *schade*. Overigens - het incident uit het voorbeeld is werkelijk gebeurd. De onderliggende oorzaak was een lege dieseltank. Bij de laatste onderhoudsbeurt was de diesel afgetapt en men had verzuimd de generator na het onderhoud weer af te tanken.

## Beschikbaarheid

Door de toenemende afhankelijkheid van geautomatiseerde informatiesystemen neemt de kans op serieuze schade bij uitval hand over hand toe. Daarom is juist in de geautomatiseerde informatievoorziening beschikbaarheid een cruciaal punt. Beschikbaarheid van informatie vereist doorgaans de beschikbaarheid, goede prestaties, toegankelijkheid en in algemene zin de juiste werking van het ICT-systeem waarin deze informatie vervat is. Jammer genoeg komt het maar al te vaak voor dat organisaties geen serieuze afspraken hebben gemaakt met hun ICT-afdeling omtrent de beschikbaarheid, en dat de ICT-afdeling zich ook nog eens strak aan deze afspraken houdt. Veelal zijn de gestelde eisen niet erg hoog en

wordt er al helemaal geen vinger aan de pols gehouden.

Maar waar gaat het dan doorgaans mis? Waar liggen de risico's? En hoe kan een organisatie daar zo goed mogelijk mee omgaan? Het is duidelijk: *business continuity* raakt aan veel aspecten van ICT-ontwikkeling en beheer. Er zijn uiteraard legio oorzaken als het gaat om uitval van ICT-voorzieningen, maar op afstand de belangrijkste is wel menselijk handelen. En incidenten op basis van menselijke fouten zijn vaak gemakkelijk te voorkomen.

### Uitval door menselijk handelen

Fouten als gevolg van onzorgvuldig handelen door mensen: dat is de belangrijkste oorzaak van uitval. Voorbeelden uit de praktijk zijn er te over.

Zo werd recentelijk bij een organisatie een langdurige uitval van het e-mail-systeem veroorzaakt doordat een beheerder buiten de reguliere wijzigingsprocedures 'even snel' iets wilde aanpassen. Helaas had hij zijn wijziging niet zo goed doordacht waardoor de boel 'plat' ging. En er ging uiteindelijk ook nog mail verloren. Nogmaals helaas, want vervolgens bleek ook de back-up-procedure niet geheel tot de letter gevolgd te zijn waardoor het terugzetten van een back-up 'wat langer' duurde.

Of een incident als gevolg van stroomuitval, waarbij servers uitvielen die eigenlijk op de wel aanwezige UPS/generator aangesloten hadden moeten zijn. Later bleek dat ten tijde van de installatie van de servers geen stroomkabels van voldoende lengte beschikbaar waren om bij de juiste *wall-outlet* te komen en werden de servers dus maar aangesloten op *wall-outlets* die niet aan de noodstroomvoorziening waren gekoppeld. En niemand heeft deze situatie later rechtgezet.

Bij een ander incident bleek men ongeveer vijftien minuten voor het begin van de werkdag te zijn begonnen met een wijziging die in het gunstigste geval vijftien minuten in beslag zou nemen. Als je op die manier het noodlot tart, kun je er uiteraard op wachten dat het niet allemaal volgens plan gaat. En zo geschiedde, met als gevolg dat

het vervolgens uren duurde voordat de gebruikers weer toegang hadden tot het systeem.

Ook een aardige is het uitrollen van *software updates* zonder deze van tevoren te testen - iets wat al bij menig bedrijf een berg ellende heeft veroorzaakt. Je kunt natuurlijk (de fabrikant van) de software de schuld geven, maar dat is wel erg kort door de bocht.

### Voorkomen beter dan genezen

Grip krijgen op de beschikbaarheid van ICT-voorzieningen is iets wat voor veel organisaties interessant kan zijn. En daarvoor hoeft u geen ICT-insider te zijn. Enige ondersteuning van iemand met ICT-kennis kan echter geen kwaad.

Een goed begin is om alle ICT-incidenten over een periode van bijvoorbeeld een jaar eens te analyseren, na te gaan hoeveel uitval er is geweest en een schatting te maken van de kosten die hiermee gemoeid waren. Denk daarbij dan aan gederfde omzet, verloren uren en de kosten die de ICT-afdeling heeft moeten maken om de situatie weer te herstellen. Het gaat hier overigens ook niet alleen om de werkplekautomatisering, maar zeker ook om allerhande andere systemen (databases, websites etc.). Het hoeft niet precies - een ruwe schatting is goed genoeg.

Als blijkt dat ook in uw organisatie ongemerkt aanzienlijke sommen geld verloren gaan door uitval van ICT-voorzieningen, is het tijd om actie te ondernemen. Begin in dat geval eens met het stellen van serieuze eisen aan uw ICT-afdeling aangaande beschikbaarheid van voorzieningen, inclusief

een controlesysteem en sancties. Grote kans dat u veel weerstand ondervindt: men begint over hoge kosten voor het *redundant* uitvoeren van hardware, en men klaagt over de benodigde extra menskracht. Het eerste argument (kosten) is niet relevant, want de meeste winst is doorgaans te behalen door het indammen van menselijke fouten. En of het tweede argument (extra menskracht) hout snijdt, is maar zeer de vraag - stevig doorvragen kan daar wel een antwoord op geven. Menselijke fouten komen doorgaans voort uit tijdsdruk als gevolg van slecht plannen en/of de menselijke neiging om zaken te onderschatten ('dat kan wel even tussendoor'). De enige manier om dergelijke fouten in een ICT-omgeving uit te bannen is het strikt scheiden van productieomgevingen en andersoortige omgevingen en het strak hanteren van formele wijzigingsprocedures voor de productieomgeving. Geen wijzigingen in de productieomgeving anders dan via het formele wijzigingsproces. Ook hier kunt u rekenen op de gebruikelijke klaagzangen dat 'dat niet werkbaar is', 'dat dan alles nog langer gaat duren' en 'dat we zoveel mensen niet hebben', enzovoort. Echter, mits pragmatisch aangepakt, hoeft een strakkere werkwijze geen negatieve consequenties te hebben en is er geen sprake van extra kosten - wel van een verandering van werkwijze. En deze verandering roept, net als elke verandering, nu eenmaal onherroepelijk weerstand op - maar uw eerdere berekening laat zien wat het overwinnen van die weerstand waard is. «

*\*Jeroen van Dongen CISSP is directeur bij LBVD Consultancy*

### Samenvatting

- » De **beschikbaarheid** van informatie en informatiesystemen is een aspect van informatiebeveiliging dat nog wel eens wordt vergeten.
- » Door de toenemende afhankelijkheid van geautomatiseerde informatiesystemen neemt de kans op serieuze **schade** bij uitval toe. Daarom is beschikbaarheid een cruciaal punt.
- » **Fouten** als gevolg van onzorgvuldig handelen **door mensen** vormen de belangrijkste oorzaak van uitval.
- » De enige manier om dergelijke fouten in een ICT-omgeving uit te bannen is **het strikt scheiden** van productieomgevingen en andersoortige omgevingen en het strak hanteren van formele wijzigingsprocedures voor de productieomgeving.