Business kritisch of missiekritisch,

is er nog wel verschil?

Organisaties zijn steeds meer afhankelijk van ICT. Als de voorzieningen uitvallen, is de impact op processen groot en vaak niet meer acceptabel. Een IT-manager van een crematorium vertelde dat de communicatievoorzieningen daar in feite missiekritisch zijn geworden: het is natuurlijk niet mogelijk om een herdenkingsdienst over te doen of een livestream te laten falen. Maar de afhankelijkheid gaat veel verder. Volgend jaar treed ook de Wet weerbaarheid kritieke entiteiten (Wwke) in werking. In dit artikel kijken we naar hoe diverse organisaties omgaan met missiekritische voorzieningen, om de basis te bespreken. In het volgende artikel gaan we in op de wet en voor wie dit belangrijk is.

ICT-voorzieningen kennen we al een lange tijd. In de jaren 80 van de vorige eeuw, begon ICT en mobiele communicatie voorzichtig een rol te spelen in de zakelijke wereld. Deze noviteiten werden gezien als leuk voor erbij of ook 'nice to have'. Dit veranderde langzaam in noodzakelijk of 'need to have'. Op heel veel plekken is ICT noodzakelijk voor de aansturing van processen, zonder communicatie valt het openbaar vervoer stil, kan er niet worden geopereerd of moeten winkels sluiten. Dit wordt vaak business kritisch genoemd: als het er niet is, heeft dat grote zakelijke impact. Het hoogste niveau wordt missiekritisch genoemd: als er geen voorzieningen zijn of geen communicatie mogelijk is, kan dat direct gevaar opleveren voor mensenlevens en persoonlijke veiligheid.

Nadenken

In de operationele drukte van alledag is het regelmatig lastig om aandacht te besteden aan de gevolgen van ICT verstoringen. Vanwege het toenemend belang is het toch goed om daarover na te denken. In het Engels is daar een mooie uitspraak over: 'if you fail to plan, you plan to fail'. Een stroomstoring, kapotte internetverbinding of storing op het mobiele netwerken kunnen paniek geven in de operatie en geld kosten. Voor steeds meer organisaties zijn de ICT voorzieningen zó belangrijk geworden, dat business kritisch en missiekritisch eigenlijk samenvallen. Een collega heeft daar een mooie uitspraak over: je moet er niet alleen over na-denken, maar over voor-denken.

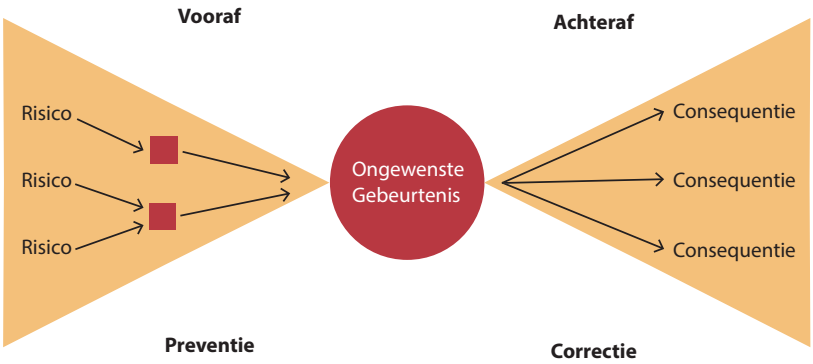
Consequenties

Daar waar voorzieningen cruciaal zijn, is het goed om na te denken over 'wat als'. Wat zijn de alternatieven, als een systeem niet beschikbaar is. Eigenlijk zit daar een paar vragen voor: welk doel heeft de organisatie en wat is noodzakelijk om dat doel te bereiken. Dit is een strategisch vraagstuk waar uiteindelijk het management over beslist. Als de impact van een storing niet zo belangrijk is of als de gevolgen als beperkt worden gezien, waarom zou je dan investeren in alternatieven en redundante oplossingen. Sommige organisaties gaan hier heel gestructureerd mee om, bijvoorbeeld met het 'bowtie' methode. Aanleidingen en gevolgen kunnen daarmee gestructureerd inzichtelijk worden gemaakt (zie de afbeelding in de vorm van een strik). Het is een vorm van risicomanagement, waarbij niet alleen directe maar ook indirecte gevolgen (zoals imagoschade) kunnen worden meegenomen. Soms wordt dit ook gekwantificeerd: wat zijn de kosten voor de redundante oplossing versus wat is de gevolgschade. Dat maakt het wel heel rationeel, maar als er mensenlevens mee gemoeid zijn is dat niet eenvoudig te berekenen.

FMEA

Een andere methode die ook wordt toegepast is FMEA: Failure Mode & Effect Analysis. Hierbij

Overtreffende trap van redundantie bij Defensie: PACE
Voor verbindingen bij militaire eenheden, wordt uitgegaan van het PACE principe, waarbij de afkorting staat voor Primary, Alternative, Contingency en Emergency. De verbindingen zijn hier letterlijk missiekritisch en mensenlevens kunnen zeker in gevaar zijn. Redundantie wordt daarom heel serieus opgepakt en gaat veel verder dan alleen een back-up. Het begin is een primaire verbinding plus een alternatief, maar vervolgens wordt er ook nagedacht over een oplossing als de eerste twee niet beschikbaar zijn. Tot slot is er ook nog een oplossing voor noodsituaties. Natuurlijk is de dreiging voor militairen veel groter en heeft men soms te maken met radio jamming en actieve verstoring, maar grote calamiteiten kunnen ook in Nederland voorkomen. Organisaties doen er goed aan om verder te kijken dan alleen redundantie.



wordt gekeken naar alle mogelijk manieren waarop iets kan gebeuren, iets stuk kan gaan en wat daar de effecten van zijn. Het is ook een methode om door middel van gestructureerde analyse de gevolgen zoveel mogelijk te mitigeren. Bij een technisch communicatiesysteem is het mogelijk om tientallen potentiële oorzaken van storingen te verzinnen. En met de overgang naar moderne 4G/5G gebaseerde communicatie, zijn meestal diverse (cloud)diensten betrokken voor authenticatie, datacommunicatie, berichtafhandeling en meldkamer applicaties, waarmee de mogelijke oorzaken alleen maar toenemen.

Risicobepaling
Als een organisatie het belangrijk vindt, dan wordt nagedacht over de risico's, de gevolgen en de mogelijke oplossingen bij verstoringen. Bij de politie is het C2000 portofonie netwerk een missiekritisch netwerk: het moet altijd mogelijk zijn om met collega's en de meldkamer te communiceren. Als dit netwerk uitvalt, hebben politiemensen de mogelijkheid om met een push-to-talk app op hun beveiligde smartphone ook portofonie diensten te kunnen gebruiken. Het is wel vaker dat de alternatieve oplossing niet helemaal hetzelfde werkt, maar de belangrijkste communicatie blijft mogelijk. In veel ziekenhuizen worden bijvoorbeeld portofoons uitgerold naar de afdelingen als de telefooncentrale uitvalt, zodat men kan blijven communiceren bij medische calamiteiten. Natuurlijk verliest men functionaliteit, maar normaal duurt een verstoring slechts kort, zodat het ongemak beperkt blijft.

Streven naar eenvoud
Niet alleen in Nederland, maar ook elders zien organisaties dat communicatie missiekritisch is geworden. Daarbij wil men liever niet meer afhankelijk zijn van externe systemen en netwerken. De dienstverlening van publieke netwerken is gebaseerd op tientallen systemen die samenwerken. Streven naar eenvoud vermindert in ieder geval het aantal mogelijke oorzaken. Daarnaast worden in publieke netwerken dagelijks upgrades, updates en wijzigingen uitgevoerd, die allemaal een verstoring kunnen veroorzaken.
Een leerzame anekdote van lang geleden over ons nationale telefonienetwerk: bij een analyse van verstoringen en klantklachten werd duidelijk dat het overgrote deel tussen 08:00 en 17:00 ontstond. Dat werd de aanleiding om toegang tot de technische ruimtes sterk te reguleren en gedegen change management te implementeren. Niemand werd nog toegelaten, tenzij je van te voren had aangekondigd wat je wilde doen en daarvoor ook toestemming had gekregen. Het aantal verstoringen liep erna terug…

Private oplossingen
Het streven naar eenvoud en controle over de systemen, zorgt er mede voor dat veel organisaties wereldwijd kiezen voor private 5G oplossingen. De radiotechnologie is zeer robuust en flexibel en het ecosysteem groeit enorm. Persoonlijk denk ik dat niet alle oplossingen even geschikt zijn voor missiekritisch gebruik, maar er is volop keuze in leveranciers. En waar publieke netwerken het nog heel moeilijk vinden om een overstap te maken naar echt 5G met stand alone netwerken, is dat bij private netwerken standaard. Hierdoor is het mogelijk om verschillende gebruikersgroepen andere prioriteiten in het netwerk te geven.

Het blijft techniek
Bij een organisatie met missiekritische behoeften is het hele communicatiesysteem redundant uitgevoerd, op twee verschillende locaties in het gebouw. Daarnaast is er een complete noodstroomvoorziening. Toch is er vaak voor gekozen om een portofoniesysteem als noodoplossing aan te houden, dat met een basisstation met accu minimaal 4 uur altijd kan blijven functioneren. Want het blijft allemaal techniek, en techniek kan nu eenmaal storingen hebben. Maar ook steeds meer organisaties zien hun communicatie als minstens business kritisch en kiezen voor bijvoorbeeld satelliet-communicatie als back-up voor hun communicatie.

In het volgende artikel gaan we onderzoeken voor welke organisaties de Wet weerbaarheid kritieke entiteiten (Wwke) relevant is en wat men naast een risicobepaling geacht wordt te doen.

Over de auteur
Eildert van Dijken is Principal Consultant bij Strict en is al vele jaren bezig met mobiele communicatie. Hij is vooral betrokken bij connectiviteitsvraagstukken, voert regelmatig onderzoek uit en publiceert over nieuwe technologieën.