Wereldwijde ervaringen met **ICT-uitval en -verstoringen**

ir. Eric Luiijf,
principal consultant Information Assurance en Bescherming vitale infrastructuur, TNO Defensie en Veiligheid (eric.luiijf@tno.nl)

Grootschalige ICT-uitval of -verstoring met effecten op een regio, Nederland of wereldwijd, kan ernstige gevolgen hebben voor de veiligheid en het welbevinden van burgers en kan leiden grote economische schade. Op basis van de TNO database waarin vitale infrastructuurverstoringen en de domino-effecten daarvan worden geregistreerd gaat dit artikel nader in op dergelijke uitval en -verstoringen en de (inter)nationale voorbereidingen op ICT-rampen.

Informatiesystemen

Grootschalige uitval van informatiesystemen komt vaak voort uit de afhankelijkheid van elektriciteit. Een paradox daarbij is dat in gebieden waar de elektriciteitsvoorziening met enige regelmaat faalt minder vaak domino-effecten optreden in de telecommunicatiesector dan in gebieden waar de energieleveringszekerheid hoog is zoals in Nederland.[1] Internationaal vormt het Strategisch Overleg Vitale Infrastructuur (SOVI) een uitzondering waar de domino-effecten van elektriciteitsuitval op ICT en de mogelijke maatregelen daartegen besproken intersectoraal worden besproken.

Een andere oorzaak van grootschalige uitval van informatiesystemen vormt de razendsnelle internationale verspreiding van virussen en andere 'malware'. De laatste jaren zorgen geavanceerde detectie- en quarantaine-mechanismen in bijvoorbeeld e-mailstromen voor vroegtijdig ingrijpen. Wereldwijde besmettingen met grote verstoring van IT-systemen treden desondanks op. In het buitenland zijn al (petro)chemische fabrieken en kerncentrales uitgevallen. Ook is de controle over elektriciteitstransportinfrastructuren verloren doordat de procescontrolesystemen en -netwerken met malware besmet raakten. Dergelijke incidenten komen soms voort uit onverstandige verbindingen met het internet, Vaker komt de besmetting door besmette laptops van derden die 'onveilige gemeenschap' hebben met vitale productienetwerken. De mogelijk gevolgen kunnen, mede door domino-effecten, heel ernstig zijn. In het Informatieknooppunt Cybercrime (IKC) en internationale samenwerkingsverbanden (EuroSCSIE en MPSCSIE) werken de Nederlandse vitale sectoren samen om dit risico in te dammen.

Daarnaast zijn er de IT-kwetsbaarheden die grootschalig uitgebuit worden door criminelen, bijvoorbeeld voor het opzetten van botnets of het verzamelen van persoonlijke gegevens. De betrouwbaarheid van en vertrouwen in IT-diensten komt daarbij in het geding. Internationaal werken Computer Emergency Response Teams (CERTs) en opsporingsdiensten samen om

[1] A.H. Nieuwenhuijs, H.A.M. Luiijf, M.H.A. Klaver, 'Modeling Critical Infrastructure Dependencies', in: P. Mauricio and S. Shenoi (eds.), IFIP Volume 290, Critical Infrastructure Protection II, October 2008, 205-214.

dergelijke cybercriminaliteit enigszins in te dammen en bij ernstige verstoring samen op te trekken en kennis te delen.

Internettoegang en -diensten

Internet is door zijn opzet robuust en kan als totaal systeem niet uitvallen. Wel kunnen delen uitvallen. Dat komt door single-point-of-failures (SPoFs) of door overbelaste circuits waar geen redundante capaciteit elders in het netwerk voor bestaat. Wordt dan de zeekabel (bijv. de SEA-ME-WE) doorsneden door een aardbeving of een anker, of zijn er grote (distributed) denial-of-service aanvallen, dan zijn zelfs landen elektronisch gezien niet of nauwelijks te bereiken. Ook ISP, telecom-, en CATV-operators zien SPoFs over het hoofd, wilden niet investeren in redundantie, of moesten van de gemeente alle glaskabels in één tracé neerleggen. Uitval van honderdduizenden tot enkele miljoenen klanten voor langere tijd komt voor. De kwetsbaarheid van dergelijke SPoFs kan ook uitgebuit worden voor activistische of criminele doeleinden. Voor de lokale Internettoegang geldt hetzelfde. Als men geen tweede toegang via een bewijsbaar andere route heeft geregeld, kan het internet uitvallen inclusief alle diensten als e-mail, web en internettelefonie. Ook de crisisrespons-organisaties zijn vaak optimistisch en zien SPoFs over het hoofd.[2]

Vaste en mobiele telefonie- en datadiensten

De nieuwe cultuur van 'always anywhere on-line' brengt het risico van een lage tolerantie voor verstoringen. Bedrijven en burgers zijn geheel van slag als hun Blackberry niet minstens drie e-mailberichten per uur toont. Laat staan dat die dienst zo'n 12 uur uitvalt zoals in 2007 gebeurde. Men kan niet e-mailen en e-mail ontvangen: men bestaat niet meer!
Uitval van vaste en mobiele communicatie wordt vaak veroorzaakt door noodweer en rampen als aardbevingen of overstromingen. Naast de technische uitval van componenten ontstaat daarbij overbelasting doordat velen tegelijk willen communiceren. Als netwerken meer diensten leveren, zal een overbelasting in één dienst al gauw congestie van een andere telecommunicatiedienst veroorzaken. Als de normale beschikbaarheid 99.99% is, maakt een communicatie-inspanning over mogelijke ICT-uitval tijdens bijzondere omstandigheden geen indruk, noch in het buitenland, noch in Nederland: het zal zo'n vaart niet lopen.
Analyses van rampen laten zien dat na herstel van de infrastructuur een 30% hogere netwerkbelasting gemeten wordt dan voor de ramp. Omdat men zich ongerust maakte over familie en kennissen wordt er vaker gecommuniceerd, een effect dat zich gedurende meer dan een jaar voortzet. Een aantal landen heeft zijn ontwerpcriteria hierop aangepast.

Technische storingen en menselijke fouten brengen SPoFs in de infrastructuur aan het licht zoals kwetsbare locaties en gateways met andere operators. Systeemupgrades en onvoorziene extra netwerkbelasting omdat men de abonnees ineens hogere snelheid biedt, hebben in de afgelopen jaren geleid tot onvoorziene neveneffecten en langdurige, grootschalige ICT-uitval. Een beperkt aantal landen heeft een publiek-privaat crisisplan en -organisatie voor de hele ICT-sector, bijvoorbeeld de Special Task Force on Information Assurance (SONIA) in Zwitserland en het Nationaal Continuïteitsoverleg Telecommunicatie (NCO-T) in Nederland.
De perceptie van een hoge betrouwbaarheid van veel nieuwe communicatie- en datadiensten maakt dat wij onszelf afhankelijk van die diensten maken. We vergeten daarbij dat de dienstverlening niet betrouwbaarder kan zijn dan die van de onderliggende infrastructuur en techniek. Rampbestrijdingsorganisaties in Nederland en daarbuiten trappen wel eens in deze val en zijn afhankelijk van overbelastinggevoelige netwerken met SPoFs.

ICT-rampbestrijding

Qua preventie en preparatie analyseert het VS National Infrastructure Simulation and Analysis Center (NISAC) met simulatiemodellen onder andere de kans op ICT-uitval per regio en de mogelijke gevolgen van een volgende wervelstorm. In Europa en Nederland zijn we nog niet zover, ook al werkt TNO in het EU project DIESIS aan de contouren van een dergelijke Europese en Nederlandse faciliteit.
Qua preparatie en respons hebben veel landen CERT-organisaties die hun overheid en/of vitale sectoren helpen bij het wegnemen van ICT-kwetsbaarheden en bij de aanpak van incidenten. Een aantal landen, waaronder de VS, het VK, Estland en Zuid-Korea, ontwikkelt daarnaast beleid en een responsorganisatie voor de nationale bescherming tegen Cyberwar. Dit mede naar aanleiding van de recente Cyberaanvallen op Estland, Georgië, Kirgizië en Zuid-Korea. Ze oefenen grootschalig op oefeningen om cyberaanvallen te weerstaan (bijv. Cyberstorm in de VS). Ook Nederlandse ICT-systemen en -netwerken worden aangevallen vanuit het buitenland. Over de vele partijen die zich in meer of mindere mate samen bezig houden met de ICT-rampbestrijding in Nederland kunt u elders in dit magazine meer lezen.

[2] E. Luiijf and M. Klaver, 'Insufficient Situational Awareness about Critical Infrastructures by Emergency Management', in: *Proceedings Symposium on "C3I for crisis, emergency and consequence management, Bucharest*, May 2009, NATO RTA, Paris. RTO-MP-IST-086.