

Rapportage weerbaarheid van *de sector Financiën* tegen ernstige elektriciteit- en telecommunicatie-uitval

In opdracht van de ministeries van Binnenlandse Zaken en Koninkrijksrelaties/DG Veiligheid en Economische Zaken/DG Energie en Telecom

Rapportage weerbaarheid van *de sector Financiën* tegen ernstige elektriciteit- en telecommunicatie-uitval

**Nationaal Adviescentrum Vitale Infrastructuur (NAVI)
Nationale Infrastructuur ter bestrijding van CyberCrime (NICC)**

Plaats: Den Haag

Datum: 11 maart 2010

Versie: 1.0

© 2010 NAVI en NICC. De informatie in dit document mag noch geheel noch gedeeltelijk op enigerlei wijze worden aangepast, gewijzigd of verveelvoudigd zonder voorafgaande toestemming van NAVI en NICC.

Inhoud

| | |
|---|----|
| 0. Management samenvatting | 4 |
| 1. Toelichting onderzoek | 6 |
| 2. Kritische processen vitale infrastructuur financiën | 9 |
| 2.1 Vitale diensten | 9 |
| 2.2 Knooppunten | 10 |
| 3. Bevindingen: algemeen | 13 |
| 3.1 Bevindingen: weerbaarheid tegen elektriciteituitval | 15 |
| Inhoudelijke bevindingen | 15 |
| Procesmatige bevindingen | 17 |
| 3.2 Bevindingen: weerbaarheid tegen uitval telecommunicatie | 18 |
| Inhoudelijke bevindingen | 18 |
| Procesmatige bevindingen | 19 |
| 4. Conclusies | 20 |
| 5. Voorgestelde maatregelen | 21 |
| Bijlage B: Wet- en regelgeving | 25 |

0. Management samenvatting

De financiële sector behoort tot de vitale sectoren en het leveren van financiële diensten behoort tot de vitale producten en diensten. De Nederlandse samenleving is sterk afhankelijk van een ongestoorde financiële dienstverlening. Dienstverlening, leveringszekerheid en imago zijn belangrijke waarden voor de financiële sector.

Samen met de sector financiën is zijn de kritische kernprocessen en de afhankelijkheden van elektriciteit en telecommunicatie in kaart gebracht en is de mate van de huidige en gewenste zelfvoorzienendheid en/of zelfredzaamheid met de sector besproken.

De vitale processen binnen de financiële sector zijn het betaling- en effectenverkeer. Hieronder vallen de vitale diensten: toonbankbetalingsverkeer, massaal giraal betalingsverkeer, hoogwaardig betalingsverkeer en effectenverkeer. In eerder onderzoek¹ is nagegaan in hoeverre genoemde vitale diensten vitaal zijn en wat de gevolgen zijn bij uitval. Tevens zijn in dit onderzoek de knooppunten van de financiële sector benoemd waar verschillende producten of diensten samenkomen die in hoge mate of totaal afhankelijk van elkaar zijn.

De knooppunten worden ondersteund door dataverkeer (internet, vaste telecommunicatie, mobiele telecommunicatie, post- en koeriersdiensten), elektriciteit, personeel, fysieke infrastructuur en databestanden. Indien deze onderliggende infrastructuur uitvalt of storingen vertoont, raakt het vitale proces verstoord met mogelijke maatschappelijke ontwrichting als gevolg. Alle processen in de financiële sector zijn in grote mate afhankelijk van elektriciteit en van telecom.

De financiële sector is zich bewust van de afhankelijkheid van elektriciteit en telecommunicatie en heeft algemene maatregelen ter bescherming genomen die zich richten op drie categorieën:

1. Maatregelen om de kans op een gebeurtenis te verminderen
2. Maatregelen om de impact van een gebeurtenis te verminderen
3. Maatregelen om de respons op een gebeurtenis zo goed mogelijk te laten zijn

De kern van de maatregelen tegen elektriciteitsuitval zijn de volgende:

- De belangrijke locaties zijn allemaal voorzien van noodstroomvoorzieningen. De generatoren kunnen worden ingezet gedurende enkele dagen tot een week. Bij uitval van langere duur dienen de noodgeneratoren te worden bijgevoerd.
- Voor de vitale processen en systemen zijn uitwijkcentra beschikbaar.
- Elke financiële instelling heeft een eigen business continuity strategie en –plan, dat regelmatig wordt getest. Hierin wordt ook specifiek gerefereerd aan het treffen van maatregelen voor het geval elektriciteit uitvalt.
- Binnen de sector is een crisiscoördinatie structuur in het leven geroepen onder leiding van de DNB.
- De sector is aangesloten op het alerteringsstelsel van de NCTb.

Telecommunicatiediensten zijn niet in het beheer van financiële instellingen. Omdat de bedrijfscontinuïteit er vaak wel sterk van afhankelijk is, hebben de meeste financiële instellingen voor zowel vaste als mobiele telecommunicatie meerdere providers per kritische omgeving gecontracteerd. In deze contracten hebben de individuele financiële instellingen het door hen gewenste niveau van dienstverlening afgesloten.

¹ Rapportage Bescherming van de vitale infrastructuur in de financiële sector, 2005

Binnen de financiële sector is sprake van een hoog risicobewustzijn. De sector maakt serieus werk van continuïteitsbeleid. De diverse onderzoeken van de afgelopen jaren bevestigen dit beeld. Momenteel worden binnen het Platform Business Continuity Vitale Infrastructuur Financiële sector (BCVIF) initiatieven ontplooid om een update van het rapport 'Bescherming van de vitale infrastructuur in de financiële sector' (2005) te maken.

In nauwe samenspraak en afstemming met de financiële sector stelt de projectgroep op basis van de inhoudelijk en procesmatige bevindingen de volgende maatregelen voor, die in samenspraak tussen de sector en het vakdepartement verder uitgewerkt en opgepakt moeten worden. Het uitvoeren van deze maatregelen dient ervoor te zorgen dat de weerbaarheid van de financiële sector op het hoge niveau blijft waar het zich nu bevindt:

- Zet het initiatief door om met verschillende partijen in de sector een update te maken van bestaande rapportages, zoals het rapport 'Bescherming van de vitale infrastructuur in de financiële sector'. Betrek hierbij de relevante sectoren waar de financiële sector sterk van afhankelijk is (zoals elektriciteit en telecommunicatie) en daarnaast de relevante overheidspartijen. De overheid kan hierbij als facilitator optreden.
- Zorg voor structurele communicatie tussen de financiële sector en de sectoren energie (waarbinnen elektriciteit) en telecommunicatie, zowel in 'vredestijd' als ook in 'oorlogstijd'. Neem de communicatie met de sectoren telecommunicatie en elektriciteit mee in de structuur van crisiscommunicatie.
- Zorg voor structurele communicatie tussen de financiële instellingen en de veiligheidsregio's waarbinnen de sleutellocaties (A-locaties) zijn gesitueerd.
- Scherp indien nodig het 'Toetsingskader Business Continuity Planning Financiële Kerninfrastructuur' aan op de bovenstaande punten.
- Laat de telecomsector de financiële sector op de hoogte houden van de ontwikkelingen in het telecommunicatie domein.
- Analyseer als individuele financiële instelling de eigen service level agreements met de provider(s) van telecommunicatie en elektriciteit voor wat betreft de continuïteitsaspecten.
- Vraag als financiële sector de sectoren telecommunicatie en elektriciteit concrete suggesties/adviezen om de weerbaarheid tegen ernstige uitval van elektriciteit en telecommunicatie te vergroten.

Richting ministeries zijn er de volgende adviezen:

- Stel een prioriteringsplan op dat alle vitale sectoren omvat, waarin aangegeven wordt welke partijen na uitval weer als eerste over telecom/ICT verbindingen (en indien mogelijk elektriciteit) beschikken en communiceer dit met de financiële sector en de andere vitale sectoren.
- Stel een strategisch logistiek plan op voor de distributie van dieselolie in calamiteuze situatie. Dit advies is eerder ook al aangegeven in het rapport 'Bescherming Vitale Infrastructuur' van 2005, maar is tot nu toe nog niet uitgewerkt.
- Onderzoek of het mogelijk is om voor de telecomsector een minimum niveau vast te stellen voor de continuïteit van de dienstverlening.
- Zorg voor een intersectorale aanpak binnen de crisisbeheersing, waarbinnen de sectoren en de departementen elkaar snel weten te vinden. Aanbevolen wordt om een onderzoek te doen naar het oprichten van een Nationale Respons Board (als uitbreiding op de ideeën voor een ICT Respons Board) met daarin sterke input vanuit de verschillende vitale sectoren. Deze Nationale Respons Board moet daarbij een rol spelen bij 'All Hazards'. Afhankelijk van de soort dreiging of het type incident kunnen er verschillende expertises nodig zijn.

1. Toelichting onderzoek

1.1 Inleiding en achtergrond

Dit rapport is een verslag van de eerste stap in een proces om waar nodig de weerbaarheid van de vitale sectoren ten aanzien van de uitval van elektriciteit en telecommunicatie uitval te vergroten. Fase 1 van dit project omvat de vitale sectoren elektriciteit, telecommunicatie, financiën en gas. In fase 2 komen de resterende vitale sectoren aan de orde.

Tijdens het verloop van het project werd duidelijk dat het vergroten van de weerbaarheid van vitale sectoren niet zozeer een project is met een duidelijk eindpunt, maar veel meer een proces. Het is een proces dat bestaat uit het in kaart brengen van de huidige situatie om op basis daarvan samen te bespreken wat de gewenste situatie is en hoe daar te komen. Al met al een proces dat nauw luistert en waarbij er veel partijen nodig zijn zoals vakdepartementen, bedrijven en brancheorganisaties.

Dit betekent onder andere geen uitgebreide rapportages en het vermijden van termen als eindrapportage en eindconclusie. In plaats daarvan is dit rapport een weergave van de eerste fase van dit proces, waarbij de weerbaarheid van de sector financiën tegen uitval van elektriciteit en telecommunicatie in kaart is gebracht. Het document kan gebruikt worden als start bij de discussie die plaats zal vinden tussen alle relevante partijen.

1.2 Doel- en vraagstelling

Het doel van dit project is de weerbaarheid van de vitale sectoren ten aanzien van de uitval van elektriciteit en telecommunicatie te vergroten. Voor de financiële sector houdt dit in dat er een antwoord gegeven moet worden op de weerbaarheidsvraag: is de financiële sector voldoende weerbaar tegen uitval van elektriciteit en telecommunicatie en op welke punten zou de weerbaarheid beter kunnen?

Hierbij zijn de volgende resultaten geformuleerd:

- Er is een plan van aanpak opgesteld in nauwe samenwerking met de (partijen binnen de) sector en de vakdepartementen. Dit plan van aanpak is heel nadrukkelijk een co-productie van private en publieke partijen.
- De kritische kernprocessen en de afhankelijkheden van elektriciteit telecommunicatie per kritisch proces zijn in kaart gebracht.
- Er is een inschatting gemaakt van de mate van zelfvoorzienendheid of zelfredzaamheid. Hierbij wordt gekeken naar de kwantiteit/kwaliteit/beheersbaarheid van de dienstverlening binnen deze sector. Ook wordt gekeken naar de tijdsduur waarover deze dienstverlening operationeel kan blijven (inclusief de daarbij behorende voorwaarden).
- Per sector is tijdens het project intersectoraal overleg geïnitieerd om informatie-uitwisseling tussen de sectoren tot stand te brengen en om wederzijds begrip te bevorderen. Dit levert een bijdrage aan het vergroten van de weerbaarheid ten aanzien van uitval van elektriciteit en telecommunicatie.

Het project is uitgevoerd in samenwerking met de sector financiën en het ministerie van Financiën als verantwoordelijk vakdepartement.

1.3 Uitgangspunten

Bij de uitvoering van dit project zijn de volgende uitgangspunten gehanteerd:

- **Maatwerk per sector:** Niet elke sector is op dezelfde manier georganiseerd en niet elke sector is op dezelfde manier met business continuïteit bezig. Daarom is binnen dit project gekozen voor maatwerk per sector. Maatwerk betekent in de praktijk vooral: het vinden van de juiste aanspreekpunten en sleutelpersonen binnen een sector en het afstemmen van de relevantie van de onderzoeksvragen met deze sleutelpersonen.
- **Aansluiting bij bestaande structuren:** Voor het verkrijgen van draagvlak binnen de sectoren en het beperken van de belasting voor de sectoren is er in dit project voor gekozen zoveel mogelijk gebruik te maken van bestaande (overleg)structuren.
- **Betrokkenheid bronsectoren telecommunicatie en elektriciteit:** Belangrijk voor dit traject is de betrokkenheid van de elektriciteit en telecommunicatie sector. De kennis van deze sectoren helpt bij het verkrijgen van inzicht in de weerbaarheid van vitale sectoren tegen elektriciteit en/ of telecommunicatie uitval.
- **Intersectorale aanpak:** Dit project is er nadrukkelijk op gericht sectoren met elkaar in contact te brengen en informatie-uitwisseling te stimuleren met als doel de weerbaarheid ten aanzien van uitval te vergoten. Veel kennis over weerbaarheid is aanwezig binnen een sector maar ook de bronsectoren kunnen een rol spelen bij het vergroten van het inzicht in afhankelijkheden en de mogelijkheden voor het vergroten van de weerbaarheid. Vooral de bronsectoren elektriciteit en telecommunicatie spelen hierbij een belangrijke rol.
- **Sector-sector benadering:** Er is gekozen voor een sector-sector benadering. Dat betekent dat het contact tussen sectoren wordt gestimuleerd. De overheid treedt hierbij op als facilitator. Specifieke klant-leverancier gesprekken vallen hierbuiten. De consequentie van een sector-sector benadering is dat niet altijd de benodigde diepgang kan worden bereikt. Daarom is er daarnaast ruimte om overleg tussen klanten en leveranciers verder te faciliteren als wordt geconstateerd dat meer diepgang is vereist. Het faciliteren van deze vormen van overleg is dus mogelijk, maar valt wel buiten de scope van dit project.

1.4 Afbakening

Het Platform Business Continuity Vitale Infrastructuur Financiën (BCVIF) is het aanspreekpunt voor het project. Samen met het ministerie van Financiën en BCVIF is afgesproken het onderzoek te beperken tot betalings- en effectenverkeer binnen de financiële sector.

1.5 Vertrouwelijkheid (Groen)

Dit document is gerubriceerd als GROEN (besloten) gebruik. De gepubliceerde informatie in dit document en bijbehorende bijlagen, is alleen bedoeld voor betrokken personen. Het gebruik van het document door een andere partij dan de geadresseerde(n) is toegestaan, mits deze partij hiertoe geautoriseerd is door een geadresseerde.

Verdere gedragsregels t.a.v. groene informatie

- Informatie wordt alleen gedeeld met een bepaalde groep van personen.
- Informatie mag selectief worden gedeeld met andere organisaties.
- Informatie mag worden gebruikt buiten een (beveiligde) kantooromgeving, bijvoorbeeld telewerken.
- Informatie is voorzien van het rubriceringniveau.
- Documenten zijn voorzien van doorlopende paginanummers, het totale aantal pagina's, datum en versienummer.

Schriftelijke informatie en gegevensdragers worden opgeborgen in de daarvoor bestemde afsluitbare kast.



1.6 Leeswijzer

Hoofdstuk 2 geeft de kritische processen van het betalings- en effectenverkeer van de financiële sector weer. In hoofdstuk 3 zijn de bevindingen ten aanzien van de weerbaarheid van de sector financiën tegen elektriciteits- en telecommunicatieuitval uiteengezet. Hierbij is onderscheid gemaakt in inhoudelijke en procesmatige bevindingen. Hoofdstukken 4 en 5 bevatten conclusies en voorgestelde maatregelen ten aanzien van de weerbaarheid van de financiële sector.

2. Kritische processen vitale infrastructuur financiën

Wanneer de financiële sector geheel of gedeeltelijk uitvalt, heeft dit maatschappelijke en financieel-economische gevolgen. Vanwege de hoge bedragen en de grote hoeveelheden transacties die in de financiële sector plaatsvinden, kunnen de financieel-economische gevolgen en het maatschappelijke ongemak bij uitval al vrij snel zeer hoog oplopen. De vitale processen die in dit rapport worden behandeld, zijn de processen die noodzakelijk zijn in het betalings- en effectenverkeer. De financiële sector heeft een groot aantal maatregelen genomen om discontinuïteit te voorkomen. In deze paragraaf zijn de vitale diensten en knooppunten van het betalings- en effectenverkeer uiteengezet.

2.1 Vitale diensten

In eerder onderzoek² zijn de vitale diensten binnen het betalings- en effectenverkeer vastgesteld:

- **Toonbankbetalingsverkeer:** betalingen met bankbiljetten en munten en elektronische betalingen (pinpas, creditcard en chipknip), ook via internet.
- **Massaal giraal betalingsverkeer:** overschrijvingen, acceptgiro's, incasso's en salarisbetalingen (dus incl. internetbankieren). Hier worden ook het toonbankbetalingsverkeer en de handelingen bij geldautomaten verwerkt
- **Hoogwaardig betalingsverkeer tussen banken:** het betalingsverkeer tussen banken en andere kapitaal en geldmarktbetalingen
- **Effectenverkeer:** effecten- en derivatentransacties van Euronext door organisaties als LCH.Clearent SA (clearing) en Euroclear Nederland (effectensettlement). Voorts valt hieronder de buitenbeurshandel (Over-The-Counter-handel) die zich vooral in het Wholesale segment afspeelt.

In dit eerdere onderzoek is nagegaan in hoeverre een financiële dienst vitaal is. Door de sector is aangegeven dat dit overzicht nog steeds actueel is. Per vitale dienst is nagegaan welke gevolgen zich zouden voordoen als de desbetreffende dienst zou uitvallen. Zie hieronder de overzichtstabel.

| Gevolgen van uitval van vitale diensten in de financiële sector | | |
|---|---|---|
| Vitale dienst | Gevolgen van uitval | |
| | Op korte termijn | Op lange termijn |
| Toonbetalingsverkeer | <ul style="list-style-type: none"> • Lichte ontregeling maatschappelijk leven • Financieel-economische schade • Keteneffecten op beperkte schaal | <ul style="list-style-type: none"> • Ontregeling maatschappelijk leven • Aanzienlijk financieel-economische schade • Keteneffecten op beperkte schaal |
| Massaal giraal betalingsverkeer | <ul style="list-style-type: none"> • Beperkte financieel-economische schade | <ul style="list-style-type: none"> • Ontregeling maatschappelijk leven • Financieel-economische schade • Verlies maatschappelijk vertrouwen in financiële sector |
| Hoogwaardig betalingsverkeer tussen | <ul style="list-style-type: none"> • Financieel-economische schade | <ul style="list-style-type: none"> • Aanzienlijk financieel-economische schade |

² SOVI, 9 oktober 2007 en Rapportage Bescherming van de vitale infrastructuur in de financiële sector, 2005

| | | |
|--|---|---|
| banken | | |
| Effectenhandel, -clearing en -settlement | <ul style="list-style-type: none"> Financieel-economische schade | <ul style="list-style-type: none"> Aanzienlijk financieel-economische schade |

2.2 Knooppunten

In de genoemde onderzoeken³ zijn tevens de knooppunten binnen de financiële sector benoemd. Knooppunten zijn onderdelen van een netwerk van bedrijfs- en beleidsprocessen waar verschillende vitale producten of diensten samenkomen die hoog of totaal afhankelijk van elkaar zijn. In het onderzoek uit 2005 zijn de volgende knooppunten geïdentificeerd binnen de financiële sector in Nederland⁴:

| Knooppunt in financiële sector | Beschrijving |
|---|---|
| De Nederlandsche Bank B.V. | Gevestigd te Amsterdam, voor de distributie van bankbiljetten (1 locatie) en voor het aanbieden van een interbancair betaalsysteem (2 locaties). DNB handelt ook de settlement van het totale betalingsverkeer af. |
| Equens (voorheen Interpay Nederland B.V.) | Gevestigd te Utrecht, voor het aanbieden van clearingsysteem voor verwerking en uitwisseling van het interbancaire betalingsverkeer (2 locaties) en voor het aanbieden van een systeem voor PIN-betalingen (5 locaties) |
| SWIFT SCRL | Gevestigd te La Hulpe (België), voor het aanbieden van een wereldwijd netwerk voor berichtenuitwisseling tussen financiële instellingen (1 locatie) |
| LCH. Clearnet SA | Gevestigd te Parijs (Frankrijk), voor het aanbieden van een clearingsysteem voor verwerking van het effectenverkeer (2 locaties) |
| Euroclear Nederland, bedrijfsonderdeel van Euroclear Bank SA/N.V. | Gevestigd te Brussel (België) en Amsterdam, voor het aanbieden van een effectensettlementsysteem (? Locaties) |
| Euronext N.V. / Euronext Amsterdam N.V. (hierna Euronext) | Is houder van een erkenning als effectenbeurs in Nederland. Euronext draagt zorg voor de verhandeling van beursgenoteerde effecten (zowel cashproducten als derivaten) in Nederland (? Locaties) |

³ SOVI, 9 oktober 2007 en Rapportage Bescherming van de vitale infrastructuur in de financiële sector, 2005

⁴Voor een uitgebreidere beschrijving zie rapportage Bescherming van de vitale in de financiële sector, 2005

| | |
|--|--|
| Centrale verwerkingseenheden van grootbanken | De grootbanken hebben elk een aantal verwerkingseenheden waarin transacties worden verwerkt en posities worden bijgehouden. Elke bank heeft zijn eigen link met zowel het interbancaire betalingsverkeer als effectenverkeer |
|--|--|

De geografische spreiding van de fysieke infrastructuur in de financiële sector is redelijk. De gemeente Amsterdam vormt wel een geografisch knooppunt. In het navolgende overzicht is aangegeven welke processen in de financiële sector afhankelijk zijn van de vitale diensten en welke knooppunten daarbij zijn betrokken.

| Gevolgen van uitval van vitale diensten in de financiële sector | | |
|--|---|--|
| Vitale dienst | Processen | Knooppunten |
| Toonbetalingsverkeer | -Betalen aan de toonbank <ul style="list-style-type: none"> • Met bankbiljetten of munten • Via pin • Via chipknip • Via creditcard • Via internet -Geld opnemen <ul style="list-style-type: none"> • Bij geldautomaten • Bij bankbalie | -Equens (voorheen Interpay Nederland B.V.) -DNB -Banken (centrale verwerkingseenheden) |
| Massaal giraal betalingsverkeer | -Overschrijven <ul style="list-style-type: none"> • Via acceptgiro's en overschrijvingsformulieren • Via incasso's • Via elektronisch bankieren • Via internetbankieren • Van mobiel bankieren -Verwerking van periodieke betalingen (salarissen, uitkeringen, pensioenen) | -Equens (voorheen Interpay Nederland B.V.) -DNB -Banken (centrale verwerkingseenheden) |
| Hoogwaardig betalingsverkeer tussen banken | -Betalingsverkeer tussen banken -Treasuryverkeer tussen grote bedrijven -Afwikkeling van valutatransacties | -Banken (centrale verwerkingseenheden) -DNB -Swift SCRL |
| Effectenhandel, -clearing en – settlement | -Beurshandel -Clearing en settlement | -Euronext -LCH. Clearnet SA -Euroclear Nederland -DNB |



De financiële sector is in grote mate afhankelijk van andere vitale infrastructuren, zoals de telecommunicatiesector en de elektriciteitssector. De knooppunten worden ondersteund door dataverkeer (internet, vaste telecom, mobiele telefonie, post- en koeriersdiensten), elektriciteit, personeel, fysieke infrastructuur en databestanden. Indien deze onderliggende infrastructuur uitvalt of storingen vertoont, raakt het vitale proces verstoord met mogelijke maatschappelijke ontwrichting als gevolg.

De financiële sector is het meest afhankelijk van elektriciteit en telecom. De dienst ‘massaal giraal betalingsverkeer’ is het meest gevoelig voor uitval van deze onderliggende infrastructuren. Ook het toonbank betalingsverkeer is in grote mate afhankelijk van andere vitale infrastructuren. Het hoogwaardig betalingsverkeer tussen banken en het effectenverkeer kent minder afhankelijkheden, doordat noodmaatregelen zijn getroffen. Deze diensten zijn voor de continuïteit van dienstverlening vooral afhankelijk van vaste telecom. Dit geldt ook voor de knooppunten. Banken maken gebruik van verschillende telecomproviders om het risico van uitval te minimaliseren.⁵

⁵ Voor een uitgebreidere beschrijving zie rapportage Bescherming van de vitale in de financiële sector, 2005

3. Bevindingen: algemeen

De maatregelen ter bescherming van de vitale infrastructuur in de financiële sector richten zich op drie categorieën⁶:

1. **Maatregelen om de kans op een gebeurtenis te verminderen:** Voorbeelden zijn beveiligingsmaatregelen, toegangspoortjes, screening en surveillance. In de financiële sector wordt door individuele instellingen een groot aantal maatregelen genomen, die er op zijn gericht om de kans op gebeurtenissen te verminderen: screeningsmaatregelen, bewakingsregime, toegangspoortjes etc. Een relevante nieuwe ontwikkeling in dit kader is het alerteringsstelsel van de NCTb. Tevens wisselen de financiële instellingen (en sinds 2006 ook de overheid) vertrouwelijke informatie over dreigingen, kwetsbaarheden, incidenten en good practices op het gebied van ICT-security uit binnen de Financial Institutions-Information Sharing and Analysis Center (FI-ISAC), dat sinds 2006 wordt gefaciliteerd door het NICC.
2. **Maatregelen om de impact van een gebeurtenis te verminderen:** Voorbeelden zijn uitwijkmogelijkheden, beschikbaarheid van alternatieven, noodvoorraden, extra capaciteit, buffers, back-ups, dubbele uitvoering en verzekeringen. Per vitale dienst (toonbankbetalingsverkeer, betalen op afstand, hoogwaardig betalingsverkeer tussen banken en effectenverkeer) zijn noodmaatregelen opgesteld zoals uitwijklocaties.⁷ De beslissing voor uitwijk wordt genomen, indien de storing langere tijd duurt. Bij sommige banken draaien computercentrum en uitwijkcentrum continu parallel, zodat bij uitval van de ene de andere zijn overcapaciteit plotseling moet gaan gebruiken.
3. **Maatregelen om de respons op een gebeurtenis zo goed mogelijk te laten zijn:** Voorbeelden zijn calamiteitenplannen, afspraken over crisiscommunicatie en noodbevoegdheden.

Aanvullend heeft elke financiële instelling een eigen business continuity strategie en –plan, dat regelmatig wordt getest. Sinds 1 januari 2007 is de Wet Financieel Toezicht en lagere regelgeving van kracht (zie Bijlage A voor een nadere toelichting op geldende wet- en regelgeving). Hierin wordt expliciet aandacht besteed aan de continuïteit van de bedrijfsvoering van financiële instellingen.⁸ Overigens werd ook in de voorgangers van Wft en lagere regelgeving (Wtk en Regeling Organisatie en Beheersing) ook al expliciet aandacht besteed aan business continuity. De eisen, die aan het business continuity beleid worden gesteld, zijn naar aanleiding van de aanslagen op 11 september 2001 aangescherpt. In overleg met de sector heeft DNB een toetsingskader opgesteld om de robuustheid van het betalings- en effectenverkeer te verstevigen (Toetsingskader Business Continuity Planning (BCP) Financiële Kerninfrastructuur). Hierin is vastgelegd dat:

- Elke instelling een analyse dient te hebben in welke mate men afhankelijk is van basisvoorzieningen (elektriciteit, telecom etc.) en externe providers en op welke wijze de uitwijk hiervoor is georganiseerd. Single points of failure dienen te worden geïdentificeerd
- De essentiële bedrijfsprocessen en systemen zo vlug mogelijk dienen te worden hervat. Hierbij kan voor de deelnemers buiten de kerninfrastructuur een langere hersteltijd gelden
- Elke instelling met zijn essentiële systemen dient te kunnen uitwijken naar een ander centrum, dat afhankelijk van het risicoprofiel, op voldoende afstand ligt van de hoofdsite. Hierbij dient een tijdshorizon voor de verwachte uitval- of hersteltijd te worden toegepast. Voorts dient een risicoafweging beschikbaar te zijn, waarin is aangegeven welke risico's bij uitwijken worden gelopen en onder welke omstandigheden de risico's kunnen worden beperkt door het systeem op de hoofdsite te herstellen en opnieuw op te starten.

⁶ SOVI, 9 oktober 2007

⁷ Voor een uitgebreidere beschrijving zie rapportage Bescherming van de vitale in de financiële sector, 2005

⁸ SOVI, 9 oktober 2007

- Uitwijk van systemen en continuity- en contingencyprocedures regelmatig dient te worden getest. Het gaat hierbij om het testen van zowel ICT-systemen als medewerkers (b.v. uitwijk van de business). Afhankelijk van het belang van het systeem en de business dient dit minimaal eenmaal per jaar te gebeuren. Desgewenst kan worden afgesproken om end-to-end voor de gehele keten te organiseren (intern en extern). Voorts kunnen testen van primary site naar secondary site worden gehouden (dit vereist wel een brede afstemming binnen de kerninfrastructuur).

Daarnaast zijn op sectorniveau maatregelen genomen in het geval zich crisissomstandigheden voordoen. Binnen de sector is een crisiscoördinatiestructuur (de Escalatiecommissie Betalings- en Effectenverkeer) in het leven geroepen onder leiding van DNB. Deze commissie heeft de taak en het mandaat om beslissingen te nemen om de voortzetting van het betalings- en effectenverkeer veilig te stellen. Hierbij krijgt ook de crisiscommunicatie aandacht. Met name in het geval van uitval van het toonbankbetalingsverkeer is communicatie richting het publiek van groot belang. Op het gebied van crisismanagement vindt binnen de sector steeds vaker Europese afstemming plaats. Tevens beschikt de sector over een aantal interbancaire noodscenario's.

De banken hebben de continuïteit van de bedrijfsprocessen gewaarborgd door een combinatie van continuïteitsbeleid, het inrichten van continuïteitsmanagement, het opnemen van continuïteitseisen in Service Level Agreements en het toetsen van de naleving hiervan en tot slot het nemen van specifieke continuïteitsmaatregelen waaronder het beschikken over een uitwijkvoorziening en calamiteitenplannen

Het stelsel van maatregelen wordt door de banken periodiek getest, waarbij aandacht is voor de calamiteitenorganisatie, de continuïteit van de geautomatiseerde dienstverlening en de mate, waarin de relevante documenten actueel en hanteerbaar blijken te zijn (onder andere calamiteitplannen en uitwijkdraaiboeken). Om de situatie van een calamiteit zoveel als mogelijk na te bootsen vindt een dergelijke test vaak plaats aan de hand van een vooraf uitgedacht scenario, waarbij veelal sprake is van een combinatie van meerdere calamiteiten.

3.1 Bevindingen: weerbaarheid tegen elektriciteitsuitval

Inhoudelijke bevindingen

Het effect van elektriciteitsuitval verschilt voor de vitale diensten binnen het betalings- en effectenverkeer.⁹

Voor het *toonbankbetalingsverkeer* geldt dat de uitval van elektriciteit voor problemen zal zorgen voor winkels en instellingen, die niet beschikken over noodstroomvoorzieningen en dus ook voor de consumenten. Zonder een dergelijke noodstroomvoorziening vallen betaal-, gelduitgifte- en chipknip-automaten uit bij die winkels en instellingen. De problemen bij het toonbankbetalingsverkeer kunnen bij een elektriciteitsstoring van korte duur worden opgevangen door gebruik van andere betaalmiddelen. Bij uitval van langere duur kan er maatschappelijke onrust ontstaan door problemen in het betalingsverkeer. Daarnaast treedt er financieel-economische schade op door omzetting van bedrijven en kan er immateriële schade ontstaan in de vorm van vermindering of verlies van vertrouwen in (onderdelen van) de financiële sector.

Het *massaal giraal betalingsverkeer, het hoogwaardig betalingsverkeer tussen banken en het effectenverkeer* zijn ook in sterke mate afhankelijk van elektriciteit op grond van het feit, dat ICT deze processen ondersteunt en ICT volledig afhankelijk is van elektriciteit. Hiervoor zijn echter maatregelen getroffen binnen de financiële instellingen:

- De belangrijke locaties zijn allemaal voorzien van noodstroomvoorzieningen, zoals no-break-installaties, die een vooraf bepaald deel van de installatie zonder onderbreking van stroom kan voorzien. De generatoren kunnen worden ingezet gedurende enkele dagen tot een week. Bij uitval van langere duur dienen de noodgeneratoren te worden bijgevoerd.
- Voor de vitale processen en systemen zijn uitwijkcentra beschikbaar. De beslissingen voor uitwijk wordt genomen, indien de storing langere tijd duurt. Bij sommige banken draaien computercentra en uitwijkcentrum continu parallel. Bij uitval van de ene moet de andere zijn overcapaciteit plotseling gaan gebruiken.
- Elke financiële instelling heeft een eigen business continuity strategie en –plan, dat regelmatig wordt getest. Hierin wordt ook specifiek gerefereerd aan het treffen van maatregelen voor het geval elektriciteit uitvalt.

Uitval van elektriciteit zal daarom vooral impact hebben voor consumenten en bedrijven. De rekencentra zullen hierdoor wel te maken hebben met uitgestelde aanlevering van transacties. Wanneer de elektriciteitsvoorziening weer hersteld wordt kunnen de elektronische systemen weer snel werkzaam zijn. Wel zal er sprake zijn van achterstanden in de verwerking van gegevens, die dienen te worden ingehaald.

De workshop van enkele bedrijven binnen de financiële sector met de elektriciteitsbedrijven op 16 december 2009 bleek al snel een zinvolle eerste stap te zijn om een algemeen beeld te krijgen van (de weerbaarheid van) de elektriciteitssector zelf. De uitkomsten hiervan kunnen de individuele financiële instellingen gebruiken om hun bestaande dienstverleningsovereenkomsten te beoordelen en te bespreken met hun eigen leveranciers van elektriciteit en telecommunicatie. Hierin kan worden beoordeeld of de bestaande overeenkomsten voldoen aan de continuïteitseisen, die aan de financiële instellingen worden gesteld, dan wel dat er aanvullende maatregelen moeten worden getroffen.

⁹ Afhangelijkheidsonderzoek elektriciteit TNO onderzoek 2007, SOVI, 2007

In de discussie passeerden enkele van de maatregelen, die de financiële instellingen nemen ter bescherming van hun primaire dienstverlening de revue. Bij enkele werden aandachtspunten benoemd door de vertegenwoordigers uit de sector Elektriciteit. In onderstaande tabel is hiervan een opsomming gemaakt:

| Maatregel | Aandachtspunt |
|---|--|
| Uitwijkmogelijkheden | <ul style="list-style-type: none"> • Incidenten uit het verleden hebben geleerd dat uitwijkcentra voldoende ver uit elkaar moeten liggen om de kans kleiner te maken dat het uitwijkcentrum niet hetzelfde effect ondervindt van uitval van elektriciteit (en ook andersoortige incidenten). |
| Noodstroomvoorziening | <ul style="list-style-type: none"> • De belangrijkste locaties binnen de financiële infrastructuur zijn voorzien van noodstroomvoorziening (accu's en/of noodstroomaggregaten). Soms wordt gebruik gemaakt van extra mobiele noodstroomaggregaten om accu's weer op te laden of locaties te voorzien van noodstroom. In veel gevallen zijn daarnaast waakvlamcontracten afgesloten voor het huren van extra aggregaten als dat nodig is. Waarschijnlijk zijn deze waakvlamcontracten afgesloten door meer (vitale) partijen uit de financiële sector (en ook andere sectoren) bij dezelfde leveranciers. In crisistijd zal dus niet elke financiële instelling of ander vitaal bedrijf aan de 'ingeplande' noodstroomaggregaten kunnen komen. • Zorg dat de capaciteit van de noodstroomaggregaten voldoende is om in crisissituaties de gewenste operatieën te kunnen laten draaien. Regelmatig wordt gezien dat de capaciteit van de aggregaten niet wordt verhoogd, terwijl de omvang van het operationele proces in de loop der jaren groeit. Bij groei van de organisatie, dient dus ook de capaciteit van de noodvoorzieningen mee te groeien. • Er bestaat een mogelijkheid dat in noodsituaties de noodstroomaggregaten kunnen worden gevorderd door de overheid. |
| Noodvoorraden (bijv. van diesel voor de aggregaten) | <ul style="list-style-type: none"> • Voor noodstroomaggregaten is een beperkte hoeveelheid dieselolie aanwezig op de sleutellocaties van de financiële instellingen. Bij langdurige uitval van elektriciteit is het nodig om de locaties waar deze noodstroomaggregaten draaien van dieselolie te voorzien. Deze levering van diesel kan een knelpunt worden aangezien deze afhankelijk is van: <ul style="list-style-type: none"> ○ de bereikbaarheid van de sleutellocaties, waaraan geleverd moet worden ○ de beschikbaarheid van tankauto's ○ de diesel(tussen)opslag op strategische locaties in het land ○ de werking van pompen aldaar (die ook vaak afhankelijk zijn van elektriciteit) en de mogelijkheid van politiebegeleiding/-bescherming voor de transporten te krijgen. |
| Dubbele uitvoering van de elektriciteitsvoorziening | <ul style="list-style-type: none"> • Belangrijk is om te toetsen of de dubbele aansluiting is gerealiseerd op verschillende middenspanningsringen. Daarmee neemt de leveringszekerheid toe, omdat bij uitval van de ene ring, de andere ring (als die nog wel werkt) zorgt voor continuïteit van levering. • Alleen een dubbele aansluiting op verschillende middenspanningsringen geeft nog steeds geen 100% zekerheid. Deze maatregel zal dus altijd samen moeten blijven gaan met het beschikbaar hebben van noodstroomaggregaten. • De afweging om een dergelijke investering te doen is er één, die de financiële instelling zelf moet maken op basis van een risico-inschatting en uiteindelijk ook een financiële afweging. |

| Maatregel | Aandachtspunt |
|--|---|
| Aansluiting op ringstructuur elektriciteitsnet | <ul style="list-style-type: none"> • Belangrijk is om met de A-locaties in ieder geval aangesloten te zijn op een ringstructuur in het elektriciteitsnetwerk en niet op een enkelvoudig uitgevoerde 'uitloper' hiervan. In dit laatste geval is de leveringszekerheid duidelijk lager en zijn ook de hersteltijden langer. |

Historische gegevens over de effecten van elektriciteitsuitval op de financiële sector als geheel geven aan dat de maatregelen tegen elektriciteitsuitval over het algemeen goed functioneren en dat de vitale dienstverlening niet langdurig in gevaar komt. Nationaal zijn er enkele incidenten geweest. Zo heeft een stroomstoring eind 2006 gezorgd voor een landelijke storing van pinautomaten en geldautomaten van een aantal banken. De stroomstoring in Haaksbergen in november 2005 laat zien dat het toonbankbetalingsverkeer bij stroomstoringen inderdaad uitvalt, maar dat dit in een betrekkelijk klein gebied niet tot ernstige problemen hoeft te leiden. Ook internationaal zijn enkele incidenten bekend met effecten voor de financiële sector. In 2003 waren ernstige verstoringen in de elektriciteitsvoorziening in grote delen van Canada, de Verenigde Staten, het Verenigd Koninkrijk en Italië. Hierbij moesten ook betalingssystemen overschakelen op noodstroom. Nationaal en internationaal worden incidenten binnen de sector geanalyseerd en worden verbeterpunten geïdentificeerd en verspreid.

In de Verenigde Staten is na 11 september 2001 gebleken, dat de persoonlijke contacten tussen centrale bankiers, toezichthouders en particuliere banken van grote waarde waren, waardoor flexibel kon worden gereageerd. Een les uit de Verenigde Staten is bovendien, dat er voldoende afstand moet zijn tussen de vitale knooppunten en de locatie van uitwijkcentra, zodat de kans kleiner is, dat ze door dezelfde crisis worden getroffen.

Procesmatige bevindingen

Uit de workshops met een vertegenwoordiging van de elektriciteitssector en later met een vertegenwoordiging van de sector telecommunicatie is gebleken dat de financiële instellingen in hun business continuïteitsplannen al rekening houden met de gevolgen van uitval van elektriciteit en telecommunicatie, maar dat tot nu toe niet of nauwelijks inzicht bestond in de wijze waarop deze sectoren hun dienstverleningsniveau kunnen waarmaken. De onderlinge uitwisseling van informatie in de bijeenkomsten heeft een veel duidelijker beeld verschaft van de weerbaarheid van deze 'bronsectoren', als ook van de mogelijk te nemen (extra) maatregelen binnen de eigen sector. Op dit moment bestaat nog geen periodiek intersectoraal overleg.

3.2 Bevindingen: weerbaarheid tegen uitval telecommunicatie

Inhoudelijke bevindingen

Uitval van telecommunicatie kan grote gevolgen hebben voor de financiële sector. Het is niet wenselijk dat die uitval zich grootschalig en langdurig zal voordoen. Telecommunicatiediensten zijn niet in eigen beheer bij de financiële instellingen. Omdat de bedrijfscontinuïteit er vaak wel sterk van afhankelijk is, hebben de meeste financiële instellingen voor zowel vaste als mobiele telecommunicatie in principe meerdere providers van diensten per kritische omgeving gecontracteerd. In deze contracten hebben de individuele financiële instellingen een door hen gewenst niveau van dienstverlening afgesloten.

Bij deze telecommunicatiediensten dient nog het onderscheid te worden gemaakt in algemene telecommunicatiediensten en de meer specifieke diensten. Tot de algemene telecommunicatiediensten behoren de vaste- en mobiele telefoonnetwerken en het internet. Hiervan zijn het toonbankbetalingsverkeer en deels het massaal giraal betaalverkeer afhankelijk. Specifieke diensten zijn de dedicated netwerken. Deze worden vooral in het hoogwaardige betalingsverkeer, het effectenverkeer en deels in het massaal giraal betalingsverkeer gebruikt.

De weerbaarheid tegen uitval van de telecommunicatieverbindingen is verder worden uitgewerkt in de workshop, die samen met vertegenwoordigers van de sector Telecommunicatie is uitgevoerd. Enkele aandachtspunten die hieruit naar voren zijn gekomen zijn:

- Net als uit de onderzoeken van andere sectoren blijkt is de uitval van telecommunicatie voor een groot deel afhankelijk van de voorziening bij de klant (in dit geval dus de financiële instelling) zelf. Bij elektriciteitsuitval valt de actieve apparatuur (als telefooncentrale, handsets, VOIP-apparatuur) van de ontvangende partij (abonnee) ook uit tenzij de klant zijn eigen continuïteitsvoorzieningen heeft getroffen. Het kan dus voorkomen dat het telecommunicatienetwerk operationeel is terwijl de financiële instelling geen diensten meer heeft omdat de eigen communicatievoorzieningen niet meer werken. De enige uitzondering hierop is het POTS¹⁰/ISDN¹¹ netwerk, dat (nog) fantoomspanning vanuit de eind- of wijkcentrale levert aan huisaansluitingen zodat de ouderwetse KPN-toestellen (zonder elektriciteitsstekker) en ISDN-toestellen (beperkte functionaliteit van één speciaal geschakeld toestel) nog werken. Het is dus zaak dat de interne telefonie binnen de financiële instellingen is aangesloten op de noodstroomvoorziening.
- De telecomsector heeft aangegeven dat wanneer een (vitaal) bedrijf een dedicated verbinding heeft, deze verbinding bij uitval van elektriciteit niet direct zal uitvallen. Een dedicated verbinding houdt in dat de actieve componenten van de verbinding worden gevoed vanuit de eindpunt- of wijkcentrale. De telecomsector heeft daarbij aangegeven dat hiervoor contractuele continuïteitseisen kunnen worden afgesproken.
- De financiële instellingen zijn zelf verantwoordelijk voor het inzichtelijk maken van de afhankelijkheid van telecom (en eventueel ICT) en de impact bij uitval hiervan (bijv. door uitval van elektriciteit). De telecommunicatiebedrijven kunnen hier waar gewenst bij ondersteunen. Alle bedrijven met een vitaal belang dienen met hun leverancier van telecommunicatie af te stemmen welke continuïteitseisen zij stellen en wat er in dit kader aangeboden kan worden door de leverancier van telecommunicatiediensten. Hierover dienen dan passende (contractuele) afspraken te worden gemaakt. Dit iets wat tussen de afnemer en de leverancier moet worden afgestemd. De financiële vergoeding, die gekoppeld is aan het te leveren dienstverleningsniveau is in eerste instantie een commerciële aangelegenheid. Daar waar de maatregelen het

¹⁰ Plain Old Telephony System

¹¹ Integrated Services Digital Network

niveau van de individuele organisatie ontstijgt, is een rol weggelegd voor de overheid als facilitator en wellicht zelfs als regelgever.

- De telecomsector en ook de elektriciteitssector hebben aangegeven dat de zelfredzaamheid (bijv. ook door het treffen van maatregelen in de eigen organisatie) van de financiële instellingen van groot belang is. Zij dienen zoveel mogelijk zelf de continuïteit en zelfredzaamheid te organiseren bij uitval van elektriciteit (met als gevolg uitval van telecommunicatie) dan wel telecommunicatie. Dit kan in de vorm van noodstroomvoorzieningen en dubbel uitgevoerde verbindingen, die ook werkelijk fysiek gescheiden zijn. Dit laatste geldt voor zowel de telecommunicatie als de elektriciteit. De financiële instelling dient hierin zelf stappen te ondernemen en om de tafel te gaan met de leveranciers van telecommunicatie en elektriciteit. De telecomsector heeft daarbij aangegeven dat in ieder geval de volgende onderwerpen dienen te worden besproken:
 - Stroomstoring telt soms mee in overeengekomen beschikbaarheid. Het is daarbij niet altijd mogelijk om speciale afspraken te maken, omdat telecommunicatie ook deels afhankelijk is van derden.
 - Het maken van additionele afspraken om de continuïteit van de dienstverlening te verhogen. Daarbij kan worden gedacht aan (extra) noodstroomvoorziening in het netwerk van de leverancier van telecommunicatie, redundantie (bijv. door twee aansluitingen op verschillende locaties) etc. Deze extra dienstverlening kan de aanbieder van telecommunicatie als maatwerk voor de klant leveren.
 - Het vragen om inzicht in de infrastructuur van de leverancier van telecommunicatie om als financiële instelling zelf een goede inschatting te kunnen maken of de geboden redundantie ook daadwerkelijk redundantie betekent. Gelet moet worden op het feit dat gezien de grote mate van interconnectiviteit en verwevenheid van de infrastructuur het zo kan zijn dat het dubbel uitvoeren van verbindingen uiteindelijk geen effect resulteert, omdat mogelijk alle communicatie ergens in het netwerk van de provider of twee verschillende providers over dezelfde lijn of hetzelfde kabeltracé gaat.
- De telecommunicatieleveranciers geven aan dat de mogelijkheid bestaat om door middel van het afsluiten van een hoger dienstverleningsniveau meer prioriteit bij herstel verkregen te krijgen. Hierbij moet wel rekening worden gehouden dat bij uitval van elektriciteit de telecommunicatiebedrijven hiervoor ook afhankelijk zijn van de volgorde van opschakeling, die door de elektriciteitsbedrijven wordt gehanteerd.

Procesmatige bevindingen

Ook los van dit traject worden momenteel al op meerdere plekken de banden tussen de financiële sector en de sector Telecommunicatie aangehaald. Soms in georganiseerd verband, soms ook door de individuele financiële instellingen. Hier dient uiteindelijk ook het initiatief te ontstaan. De bedrijven zijn immers zelf in eerste instantie verantwoordelijk voor hun eigen Business Continuity Planning. Wel wordt aangeraden om nauw met de leveranciers (van bijv. elektriciteit en telecommunicatie) te overleggen of het dienstverleningsniveau passend is bij het gewenste beschermingsniveau voor de financiële organisatie. Uiteindelijk wordt dan op basis van een risico-analyse, wettelijke kaders, regulering en een financiële afweging besloten of maatregelen ook daadwerkelijk geïmplementeerd.

4. Conclusies

Er bestaat een grote afhankelijkheid van de financiële sector ten aanzien van elektriciteit en telecom. De dienst ‘massaal giraal betalingsverkeer’ is het meest gevoelig voor uitval van deze onderliggende infrastructuren. Ook het toonbank betalingsverkeer is in grote mate afhankelijk van deze vitale infrastructuren. Het hoogwaardig betalingsverkeer tussen banken en het effectenverkeer kent minder afhankelijkheden, doordat noodmaatregelen zijn getroffen. Deze diensten zijn voor de continuïteit van dienstverlening vooral afhankelijk van vaste telecom. Dit geldt ook voor de knooppunten. Banken maken gebruik van verschillende telecomproviders om het risico van uitval te minimaliseren.¹²

Binnen de financiële sector is sprake van een hoog risicobewustzijn. In de afgelopen jaren is serieus werk gemaakt van continuïteitsbeleid. De diverse onderzoeken van de afgelopen bevestigden allemaal dit beeld. Zo is in 2005 een zeer waardevol rapport opgesteld met de titel ‘Bescherming van de vitale infrastructuur in de financiële sector’. Dit is gedaan onder voorzitterschap van het ministerie van Financiën. Momenteel worden binnen de BCVIF initiatieven ontplooid om een update van dit rapport te maken.

In het kader van dit onderzoek zijn de eerste stappen gezet om de banden tussen de financiële sector en de sectoren energie (waarbinnen elektriciteit) en telecommunicatie verder aan te halen. De meeste financiële instellingen hebben weliswaar contracten met een bepaald dienstverleningsniveau afgesloten met zowel leveranciers van elektriciteit en telecommunicatie. Wat echter nog ontbreekt, is inzicht in de wereld, die achter deze dienstverleningsovereenkomsten zit. Om dit inzicht te verbeteren hebben de leden van het platform BCVIF in een gezamenlijke workshop met vertegenwoordigers uit van de elektriciteitsleveranciers gezamenlijk de wereld van de levering van elektriciteit verkend. Hetzelfde is gedaan met vertegenwoordigers uit de sector telecommunicatie. Deze bijeenkomsten zijn als nuttig ervaren en dienen regelmatig worden herhaald.

¹² Voor een uitgebreidere beschrijving zie rapportage Bescherming van de vitale in de financiële sector, 2005

5. Voorgestelde maatregelen

In nauwe samenspraak en afstemming met de financiële sector stelt het projectteam op basis van de inhoudelijk en procesmatige bevindingen de volgende maatregelen voor, die in samenspraak tussen de sector en het vakdepartement verder uitgewerkt en opgepakt moeten worden. Het uitvoeren van deze maatregelen dient ervoor te zorgen dat de weerbaarheid van de financiële sector op het hoge niveau blijft waar het zich nu bevindt:

- Zet het initiatief om met de verschillende partijen in de sector een update te maken van het rapport ‘Bescherming van de vitale infrastructuur in de financiële sector’ door. Dit is een initiatief dat in de gezamenlijkheid van het ministerie van Financiën, de toezichthouders en de financiële instellingen kan worden opgepakt. Belangrijk is dat hierbij de sectoren telecommunicatie en elektriciteit, waarvan de financiële sector sterk afhankelijk is, worden betrokken. Ditzelfde geldt voor de hulpverleningsdiensten en de veiligheidsregio’s aangezien deze in crisissituatie een belangrijke rol spelen als het gaat om informatievoorziening en logistiek. Neem in deze update ook rekening met toekomstige ontwikkelingen, binnen de financiële sector en daarbuiten:
 - Dynamiek in het betalingsverkeer
 - Betalen via nieuwe media (als internet en mobiele telefonie)
 - Dynamiek in de effectenhandel
 - Fusies
 - Hervorming toezicht
 - Introductie van IP-netwerken (Telecommunicatie)
 - Introductie ‘smart grids’ (Elektriciteit)
- Zorg voor structurele communicatie tussen de financiële sector en de sectoren energie (waarbinnen elektriciteit) en Telecommunicatie. Dit kan enerzijds worden gedaan door bijvoorbeeld het platform BCVIF periodiek te verbinden aan het PIV (Platform Integrale Veiligheid (Energie) en het NCO-T (Telecom). Ook kunnen verbindingen ontstaan tussen de FI-ISAC en de Energy-ISAC en Telecom-ISAC binnen het Informatieknooppunt Cybercrime als het gaat om digitale dreigingen. De nieuw te vormen platformorganisatie voor bescherming van de nationale infrastructuur kan hierin een faciliterende rol spelen. De financiële sector heeft na de sessie met de bronsectoren zelf aangegeven dat deze samenwerking er voor dient te zorgen dat:
 - onderzocht wordt in hoeverre in hoeverre de knooppunten binnen de financiële sector een prioritering kunnen krijgen in de af- en opschakelplannen voor de elektriciteitsvoorziening, voor zover dit überhaupt mogelijk is. Hetzelfde geldt voor de prioritering bij het herstel van telecommunicatie na ernstige uitval.
 - de financiële sector in de crisissituatie zo snel mogelijk weet heeft van de duur van de uitval van elektriciteit, dan wel van telecommunicatie om de eigen responsplannen hierop af te kunnen stemmen. Hiervoor is het van belang dat er in crisissituaties direct contact is tussen de sector financiën en de sectoren elektriciteit en telecommunicatie.
 - de individuele financiële instellingen een assessment uitvoeren op bestaande contracten met de leveranciers van elektriciteit en telecommunicatie. Dit om te toetsen of deze voldoende waarborgen bieden om het gewenste beschermingsniveau te garanderen. Daarbij dient te worden gekeken naar de mogelijkheden (en ook kosten) van dubbele aansluitingen en naar de aansluiting van A-locaties op een ringstructuur binnen het elektriciteitsnet. De elektriciteitssector heeft daarbij aangegeven dat hierbij goed dient te worden gekeken naar naar de locatie waar deze A-locaties zich bevinden (bijv. niet op een uitloper van de infrastructuur van de elektriciteit) en de aansluitingen van de uitwijkcentra. Tevens

is uit sessie van andere sectoren met de telecommunicatiebedrijven gebleken dat het belangrijk is dat de interne telecommunicatievoorzieningen van de financiële instellingen zijn aangesloten op de noodstroomvoorziening.

- De financiële sector heeft zelf aangegeven dat men graag structurele communicatie wil hebben tussen de financiële instellingen en de veiligheidsregio's waarbinnen de sleutellocaties (A-locaties) zijn gesitueerd. Hierin kan het ministerie van BZK als verantwoordelijk ministerie voor de veiligheidsregio's een belangrijke rol in spelen. Deze structurele communicatie is nodig om er voor te zorgen dat:
 - in crisissituaties de verantwoordelijken binnen de veiligheidsregio's zich het belang beseffen van deze A-locaties voor het overeind houden van de financiële sector als één van de vitale infrastructuren in Nederland.
 - hiermee de financiële instellingen ook worden gefaciliteerd bij bijv. dieseltransporten en bescherming van deze locaties bij langdurige uitval, dan wel dat zeer terughoudend wordt omgegaan bij mogelijke vordering van noodstroomaggregaten.
- DNB kan indien nodig het 'Toetsingskader Business Continuity Planning (BCP) Financiële Kerninfrastructuur' aanpassen op de bovenstaande punten om hiermee de weerbaarheid op het gewenste niveau te brengen. Hierbij is het wel van belang dat het ministerie van Financiën, de toezichthouders en de financiële instellingen zelf gezamenlijk af dienen te spreken wat dit gewenste niveau van weerbaarheid dan is.

Richting ministeries worden de volgende maatregelen voorgesteld:

- Stel een prioriteringsplan op dat alle vitale sectoren omvat, waarin aangegeven wordt welke partijen na uitval weer als eerste over telecom/ICT verbindingen (en indien mogelijk elektriciteit) beschikken en communiceer dit met de financiële sector en de andere vitale sectoren.
- Stel een strategisch logistiek plan op voor de distributie van dieselolie in calamiteuze situatie. Dit advies is eerder ook al aangegeven in het rapport 'Bescherming Vitale Infrastructuur' van 2005, maar is tot nu toe nog niet uitgewerkt.
- Onderzoek of het mogelijk is om voor de telecomsector een minimum niveau vast te stellen voor de continuïteit van de dienstverlening.
- Zorg voor een intersectorale aanpak binnen de crisisbeheersing, waarbinnen de sectoren en de departementen elkaar snel weten te vinden. Aanbevolen wordt om een onderzoek te doen naar het oprichten van een Nationale Respons Board (als uitbreiding op de ideeën voor een ICT Respons Board) met daarin sterke input vanuit de verschillende vitale sectoren. Deze Nationale Respons Board moet daarbij een rol spelen bij 'All Hazards'. Afhankelijk van de soort dreiging of het type incident kunnen er verschillende expertises nodig zijn.

Bijlage A: Gebruikte documentatie¹³

Dunn Cavelt, M. and Suter, M., Public–Private Partnerships are no silver bullet: An expanded governance model for Critical Infrastructure Protection – International Journal of Critical Infrastructure Protection. Zurich: Center for Security Studies, 27 augustus 2009

Ernst & Young, Afhankelijkheden vitale sectoren van de beschikbaarheid en betrouwbaarheid van de vitale (Telecommunicatie en ICT) infrastructuur, Den Haag: Ernst & Young, 6 februari 2008

Luijff H.A.M., Nieuwenhuijs, A.H., Kernkamp, A.C., Jong, de K.Y., Burger, H.H., Bik, A.L., Hoogstraaten, J.M., Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten - Den Haag: TNO, 2003.

Luijff H.A.M., Critical infrastructure dependencies hurt, don't they? - Weak spot analysis - Den Haag: TNO, 2008.

Luijff H.A.M., Nieuwenhuijs, A.H., Kernkamp, A.C., Jong, de K.Y., Burger, H.H., Bik, A.L., Hoogstraaten, J.M., Bescherming Vitale Infrastructuur: Quick-scan naar vitale producten en diensten - Den Haag: TNO, 2003

[Redacted text]

Programma Nationale Veiligheid, Nationale Risicobeoordeling Leidraad Methode - Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, juni 2008

Programma Nationale Veiligheid, Nationale Risicobeoordeling Bevindingenrapportage - Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 2008

Programma Nationale Veiligheid, Robuustheid communicatiemiddelen tijdens crises – Den Haag: ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1 juli 2009

Rapport bescherming vitale infrastructuur Ministerie van Binnenlandse Zaken en Koninkrijksrelaties, 1 september 2005

Sutton, D., Critical information infrastructure protection Interdependency between Energy and Telecommunications, ENISA Quarterly Review Vol. 5, No. 3, September 2009

[Redacted text]

Overig

Bescherming van de vitale infrastructuur in de financiële sector – januari 2005

Business Continuity Oversight Expectations for systematically important payment systems (European Central Bank)

Critical Infrastructure Protection Modelling and Analysis Program (CIPMA)- Trusted Information Sharing Network (TISN) for Critical Infrastructure Protection, Banking and Finance, Energy, Communications, and Water Services Sector Tasking and Dissemination Protocols May 2009

¹³ De gebruikte documentatie die hier is opgenomen is de documentatie die geraadpleegd is voor het gehele traject *Weerbaarheid van vitale sectoren tegen ernstige elektriciteit en telecommunicatie uitval*.



Definition of a methodology for the assessment of mutual interdependencies between ICT and electricity generation / transmission infrastructures-MIA (Methodology for Interdependencies Assessment)

Evaluatie Crisisoefening Waterproef 20 maart 2009

High Level Principles for business continuity (august 2007)

Jaarrapportages NCO-T leden richting EZ, met daarin kwetsbaarheden van Telecom/ICT sector

Betrouwbaarheid van elektriciteitsnetten in Nederland in 2008 , KEMA, 20 mei 2009

Kwaliteits- en capaciteitsdocumenten Gas en Elektriciteit

Scenario langdurige elektriciteitsuitval als gevolg van een terroristische aanslag

Sectorale rapportages per vitale sector ten behoeve van de tweede beleidsbrief Bescherming Vitale Infrastructuur aan de Tweede Kamer) voor eind 2009 gepland)

Sectorale rapportages per vitale sector ten behoeve van de tweede beleidsbrief Bescherming Vitale Infrastructuur aan de Tweede Kamer)

The IRRIS European Integrated Project: www.irris.org (Integrated Risk Reduction of Information Based Infrastructure systems)

Toetsingskader Business Continuity Planning (BCP) Financiële Kerninfrastructuur (Versie: 2007)

Simulating interdependent Critical Infrastructures with SimCIPAndrij Usov Fraunhofer IAIS,

Wet en regelgeving zoals Elektriciteitswet en diverse codes

Bijlage B: Wet- en regelgeving

Sinds 1 januari 2007 is de Wet Financieel Toezicht en lagere regelgeving van kracht. Hierin wordt expliciet aandacht besteed aan de continuïteit van de bedrijfsvoering van financiële instellingen.¹⁴ De wetgeving geeft kaders voor verantwoordelijkheden en plichten van instellingen op uiteenlopende gebieden, zoals risicobeheersing, uitbesteden van bedrijfsprocessen, rechten en plichten van (potentiële) cliënten en informatietechnologie.

In het kader van het betalings- en effecten verkeer is DNB, naast prudentieel toezicht op de banken, verantwoordelijk voor systeemtoezicht op betaal- en (in samenwerking met de AFM) effectenafwikkelingsystemen. Standaarden en normen zijn vastgesteld in een aantal (internationale) normenkaders, waarin ook normen worden gesteld aan business continuity. Voorbeelden hiervan zijn de Core Principles voor Systeemrelevante betalingssystemen (CP VII: Veiligheid en operationele betrouwbaarheid) en de Aanbevelingen voor effectenafwikkelingsystemen (aanbeveling 11: Operationele betrouwbaarheid) en centrale tegenpartijen (aanbeveling 7: Operationeel risico).

Daarnaast heeft DNB, in overleg met Nederlandse marktpartijen, die met elkaar de kerninfrastructuur van het betalings- en effectenverkeer vormen, het Toetsingskader Business Continuity Planning (BCP) Financiële Kerninfrastructuur afgesproken. Met de normen uit dit kader wordt niet alleen rekening gehouden met het risico van technisch-organisatorisch falen, maar ook het opvangen van natuurrampen en calamiteiten als gevolg van bewust menselijk handelen (waaronder terrorisme). Het gaat om aanbevelingen, die instellingen, toezichthouders en overseers kunnen gebruiken. In het toetsingskader wordt expliciet stilgestaan bij de menselijke factor en het business continuity plan voor het betalings- en effectenverkeer als geheel. De instellingen van de kerninfrastructuur zijn immers van elkaar afhankelijk. DNB heeft het initiatief bij de noodplannen voor de sector en zal ook de crisiscoördinatie op zich nemen in geval van een grootschalig incident binnen het betalings- en effectenverkeer.

¹⁴ SOVI, 9 oktober 2007