COT | Instituut voor Veiligheids- en Crisismanagement
an Aon company

Digicrisis: Leren van Dorifel

Aanpak Virusuitbraak Gemeente Weert Augustus 2012

Expert Opinion | Rapportage van bevindingen | Januari 2013

Ontwikkeld in samenwerking met:	Gemeente Weert
Contactgegevens opdrachtgever	De heer Marc Knaapen, gemeentesecretaris
Datum	15 januari 2013
Versie	Definitief
Projectleider	Dennis de Hoog, senior onderzoeker – adviseur
E-mailadres	d.dehoog@cot.nl
Telefoonnummer	070-3122020

Inhoudsopgave

1 Inleiding

1.1 Aanleiding

In augustus 2012 wordt een groot aantal Nederlandse organisaties getroffen door het Dorifel (XDocCrypt) virus. Aanvankelijk lijken vooral gemeenten slachtoffer. Al snel wordt duidelijk dat een diversiteit aan organisaties – waaronder universiteiten, banken en netbeheerders – te lijden hebben onder de gevolgen van het virus. Het virus infecteert via de besturingssoftware van Microsoft in hoog tempo bestanden. Oorspronkelijke bestanden worden onder invloed van het virus beschadigd, verwijderd en vervangen door een geïnfecteerd bestand dat vele malen groter is dan het bronbestand.[1]

De gemeente Weert bevond zich onder de getroffen organisaties. 'Dorifel' besmette in de nacht van dinsdag 7 op woensdag 8 augustus zeer veel bestanden. Om verdere besmetting tegen te gaan besloot de gemeente kort na detectie van het virus om de ICT af te schakelen. Dit om verdere verspreiding te beperken en om systematisch naar een oplossing toe te kunnen werken. Als gevolg van het virus en de bestrijding van de uitbraak, was de kantoorautomatisering niet langer bruikbaar. Dagen werk ging verloren en reguliere werkzaamheden konden niet langer uitgevoerd worden. Daarnaast was de gemeente niet meer in staat om de burgers van Weert het reguliere dienstverleningsniveau te bieden.

De gemeente besloot transparant naar buiten te treden over het incident en de gevolgen. Met name om zo de burgers van Weert te behoeden voor het virus en te informeren over het verwachte herstel van de dienstverlening. De gemeente wilde door naar buiten te treden ook de maatschappelijke alertheid bevorderen en schade voor andere organisaties te beperken. Weert groeide in die zomerdagen uit tot symbool van de virusuitbraak.

Tegen deze achtergrond benaderde het COT de gemeente Weert om gezamenlijk lering te trekken uit het incident. De gemeente is geïnteresseerd in een deskundigheidsoordeel (*Expert Opinion*) over de bestrijding van het incident. Ook wil de gemeente van opgedane ervaringen leren. Mede om zo de gemeenteraad nader te kunnen informeren over de opgedane ervaring en onderkende verbetermogelijkheden.

1.2 Achtergrond

De virusuitbraak biedt een unieke gelegenheid om de landelijke kennis over cyberrisico's en –crises te verrijken. Dit mede omdat de crisisstructuren niet zijn geënt op digitale risico's en de traditionele crisispartners zoals de veiligheidsregio en de hulpverleners, niet op deze nieuwe risico's zijn toegerust. Dat betekent dat het incident een unieke kans biedt om beschikbare kennis over dit specifieke risico en de respons op dergelijke incidenten te verrijken.

In de volgende subparagrafen schetsen we het perspectief waaruit wij cyberrisico's benaderen. We doen dat aan de hand van het COT/Aon White Paper *Cyberrisico's onder controle. Risicomanagement in het digitale tijdperk (2012).* Achtereenvolgens komen aan bod:

1. zes kenmerken van cyberrisico's;
2. drie oorzaken van cyberrisico's; en
3. negen mogelijke gevolgen van cyberrisico's.

[1] Zie voor meer informatie over het Dorifel-virus, bijvoorbeeld: http://blog.fox-it.com/2012/08/09/xdoccryptdorifel-document-encrypting-and-network-spreading-virus/ of https://www.ncsc.nl/actueel/nieuwsberichten/virus-dorifel-beschadigt-microsoft-office-documenten.html

1.2.1 Zes kenmerken

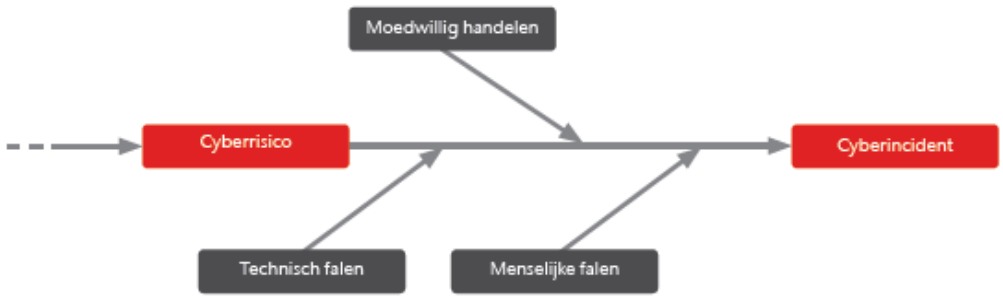
Cyberincidenten laten zich in vele gedaanten zien, maar er bestaan ook opvallende overeenkomsten. We spreken in dit verband over de zes ‘O’s’:

1. **Onzichtbaar** Een cyberincident blijft vaak (lang) onzichtbaar, in tegenstelling tot bijvoorbeeld een bedrijfsongeval. Hierdoor wordt de urgentie ervan, onterecht, minder snel gevoeld.
2. **Omvangrijk** De ervaring leert dat de effecten van een cyberincident omvangrijk zijn en de haarvezels van een organisatie raken. Juist door de aanzienlijke afhankelijkheid van ICT en data, zijn de gevolgen snel op grote schaal merkbaar. Voor de financiële sector geldt dit zeker, gezien de grote verwevenheid van digitale systemen en primaire processen.
3. **Onduidelijk** Een cyberincident heeft doorgaans een ‘modern technologisch karakter’ met een geheel eigen vakjargon. In de praktijk blijkt het dan ook lastig om grip te krijgen op een dergelijk incident en implicaties, interventies en tijdsduur te kunnen overzien.
4. **Opzettelijk** Moedwillig handelen door criminelen is bij een cyberincident nooit uit te sluiten. Bovendien kent menig incident een internationale, vaak slecht traceerbare bron.
5. **Onbegrensd** Cyberincidenten zijn per definitie grensoverschrijdend. De impact van een probleem, fout of opzettelijke handeling is schaalbaar. De effecten blijven vrijwel nooit beperkt tot één afdeling, één organisatie of zelfs één land. De onbegrensde crisis dus. Wat als een lokaal issue begint, heeft al snel internationale gevolgen.
6. **Onzeker** Elke crisissituatie kenmerkt zich door onzekerheid. De eerste vijf ‘O’s’ maken dit nog het beste duidelijk. Daar voegen we aan toe de wetenschap dat er nog weinig referentiemateriaal is waar we op terug kunnen grijpen.

1.2.2 Oorzaken

Wij zien drie belangrijke oorzaken van cyberrisico’s:

1. **Moedwillig handelen:** risico’s die te maken hebben met cybercriminaliteit. Denk aan het verspreiden van kwaadaardige software, identiteitsfraude en hacking.
2. **Technisch falen:** risico’s als gevolg van falende systemen zoals ICT-storingen of uitval.
3. **Menselijk falen:** onder deze categorie vallen risico’s door het niet goed beheren of beveiligen van de ICT-infrastructuur. Denk aan het kwijtraken of onbetrouwbaar raken van informatie of het te laat of niet adequaat updaten van software of systemen.



1.2.3 Gevolgen

Bij de Dorifel-uitbraak is sprake van moedwillig handelen. De schade van een dergelijk digitaal incident beperkt zich meestal niet tot één discipline en één (onderdeel van een) organisatie. Hoewel De impact van een digitale crisis werkt dan ook door in:

1. **Reputatie:** een zorgvuldig opgebouwde en gekoesterde reputatie kan in één klap op losse schroeven komen te staan.
2. **Continuïteit:** er treedt verstoring op van kernprocessen waardoor de operatie vertraging oploopt of zelfs volledig stagneert.
3. **Veiligheid:** de veiligheid van systemen en informatie valt niet langer te garanderen.
4. **Betrouwbaarheid:** onder invloed van één casus is de kans aanzienlijk dat de ervaren betrouwbaarheid van de gehele informatievoorziening en dienstverlening van een organisatie in het geding komt.
5. **Kwaliteit:** processen, systemen en dienstverlening leiden potentieel kwaliteitsverlies.
6. **P**rivacy: de privacy van medewerkers, klanten of leveranciers wordt mogelijk bedreigd.
7. **Financiële positie:** directe kosten die voortvloeien uit een cyberincident en/of indirecte kosten verbonden met herstel en preventieve maatregelen kunnen de financiële positie van een organisatie negatief beïnvloeden.
8. **Stakeholders:** belanghebbenden ervaren de gevolgen van cyberrisico's.
9. **Compliance**: normen, standaarden, regel- en wetgeving worden mogelijk geschonden.

Bij het optreden van een grootschalig cyberincident kunnen we zelfs het optreden van een institutionele crisis niet uitsluiten. Bovendien zal de maatschappelijke impact te allen tijde groot zijn.

1.3 Opdrachtformulering

In opdracht van de gemeente Weert heeft COT Instituut voor Veiligheids- & Crisismanagement (verder: COT) een *expertopinie* opgesteld, in aanvulling op een door betrokkenen vanuit de gemeente zelf uitgevoerde evaluatie van het incident ('Evaluatie aanpak virusbesmetting augustus 2012'). De interne evaluatie bevat een reconstructie van de feiten. De nadruk lag hierbij op het vaststellen wat er precies is gebeurd, welke besluiten zijn genomen en wat daarvan het effect is geweest.

De nadruk in de COT-rapportage ligt op de analyse en beschouwing van deze crisis in de context van onze expertise op het vlak van crisismanagement en continuïteitsmanagement in het algemeen – en digicrises in het bijzonder. Deze expertopinie – vanuit een specifiek crisismanagementperspectief – vormt daarmee een verdere verdieping op de bestaande evaluatie.

Het COT voerde hiertoe de volgende activiteiten uit:

- Een analyse van door de gemeente verstrekte documenten
- Een analyse van openbaar toegankelijke informatie
- Het voeren van dieptegesprekken met een geselecteerd aantal sleutelfiguren
- Het begeleiden van een validatiebijeenkomst met sleutelfiguren
- Het opstellen van een hoofdlijnenrapportage.

Deze rapportage bevat achtereenvolgens de bevindingen, aanbevelingen en algemene lessen van het COT.

2 Bevindingen

Hieronder beschrijven wij onze bevindingen ten aanzien van de gemeentelijke aanpak van de virusuitbraak. Met deze bevindingen plegen wij een verdiepende analyse op de door de gemeente uitgevoerde interne evaluatie ('Evaluatie aanpak virusbesmetting augustus 2012'). Voor specifieke achtergronden, gebeurtenissen en details verwijzen wij naar de betreffende evaluatie. Voor een beeld van het verloop van het incident – op hoofdlijnen – verwijzen wij naar de bijlage. Hier hebben wij op basis van de gemeentelijke evaluatie het verloop van het incident beknopt gereconstrueerd.

1. Er was sprake van een landelijke virusuitbraak, vele organisaties ondervonden hinder

De virusuitbraak bleef niet beperkt tot de gemeente Weert. Er was sprake van een landelijk cyberincident. Een scala aan organisaties (gemeenten, universiteiten, banken en netbeheerders) worden in die periode door het virus getroffen. Het aantal organisaties dat hierover actief naar buiten trad, was gering.

2. De uitbraak was niet te voorkomen, de oorzaak lag buiten de gemeente

Het Dorifel-virus is met opzet ontwikkeld en verspreid. De oorzaak van de verstoring kwam 'van buiten'. Het blijft onduidelijk of de gemeente specifiek doelwit was. De gemeente heeft vanwege het moedwillige karakter van het incident aangifte gedaan.

De anti-virussoftware van de gemeente was op het moment van de uitbraak up-to-date. Producten van leveranciers van software en anti-virussoftware – in het geval van Weert Microsoft en Symantec – bleken echter nog niet toegerust op het Dorifel-virus. Derhalve mag geconcludeerd worden dat de gemeente Weert ten aanzien van softwarebeveiliging en het voorkomen van de virusuitbraak heeft gedaan wat redelijkerwijs van haar verwacht mag worden.

3. Het virus had sneller gedetecteerd kunnen worden, de aanpak was in dat geval vergelijkbaar geweest

Achteraf bezien had de verspreiding beperkt kunnen worden. Hoewel het een onbekend virus betrof dat nog niet door de meest actuele virusscanners werd gedetecteerd, zijn de eerste signalen op 7 augustus aanvankelijk zuiver technisch geïnterpreteerd – niet vanuit een cybersecurity-perspectief.[2] Hierdoor raakte ook de *back-up* voorziening van de gemeente van dinsdag op woensdag geïnfecteerd. Wanneer het virus eerder was herkend, had de gemeente alsnog een vergelijkbare aanpak moeten volgen, om het veilig en ongehinderd functioneren van systemen te kunnen garanderen. De impact zou in dat geval niet veel minder zijn geweest. Hoogstens had de herstelperiode kunnen worden bekort.

4. Het bewustzijn van cyberrisico's was beperkt, van risicobeheersing nog geen sprake

Terugkijkend kan worden geconcludeerd dat het bewustzijn van digitale dreigingen beperkt was. Van gericht cyberrisicomanagement door de gemeente was voor augustus 2012 nog geen sprake. Zo wordt bijvoorbeeld nog niet optimaal voldaan aan het basisniveau aan (technische) ICT-beveiligingsvoorzieningen. Ook beschikte de gemeente niet over eventuele aanvullende maatregelen, om bijvoorbeeld vroegtijdige(r) herkenning mogelijk maken. Bovendien was de algehele aandacht voor cyberrisico's tot voor kort gering. Cybersecurity was een zaak voor specialisten, geen ambtelijk-bestuurlijk vraagstuk. Dit is overigens in lijn met het landelijk beeld. Het algehele bewustzijn van digitale risico's is ook landelijk immers nog gering.[3] Datzelfde geldt voor de bestuurlijke aandacht voor digitale risico's.[4]

---

[2] Een cybersecurity-perspectief beoordeelt digitale risico's vanuit een breed en integraal perspectief, waarin de oorzaak van virussen niet wordt bezien vanuit technisch falen alleen, maar ook moedwillig handelen of menselijk falen.
[3] Zie bijvoorbeeld het eerste en de tweede *Cybersecuritybeeld Nederland* (Nationaal Cyber Security Centrum)
[4] Zie de evaluatie van het Diginotar-incident door de Onderzoeksraad voor de Veiligheid (*'Waarom digitale veiligheid de bestuurstafel te weinig bereikt'*)

5. De systeemarchitectuur is complex, kwetsbaar en een totaaloverzicht ontbreekt

Net als voor veel andere organisaties geldt, is de totale systeemarchitectuur van de gemeente historisch gegroeid en gelaagd. Hierdoor is de complexiteit en de mensafhankelijkheid van het systeem groot. Met de complexiteit van het systeem, is ook de kwetsbaarheid toegenomen. Met name ook omdat een totaaloverzicht op de architectuur ontbreekt. Dit uitte zich onder andere op vrijdag 10 augustus toen het terugplaatsen van de *back up* de situatie wegens het ontbreken van een totaaloverzicht feitelijk verergerde en er een aanvullend probleem ontstond. Als gevolg hiervan moest er in het weekend aan de oplossing van twee problemen worden gewerkt.

6. De gemeente was niet voorbereid op een omvangrijke continuïteitsverstoring

De gemeente was enerzijds niet voorbereid op dit specifieke digitale risico, anderzijds bleek de gemeente niet voorbereid op een continuïteitsverstoring van deze omvang. De gemeente is vanuit de regionale crisisbeheersing voorbereid op externe crises zoals calamiteiten op het terrein van de openbare orde en veiligheid of de maatschappelijke gezondheid. Maar deze voorbereiding is van beperkte meerwaarde voor het beheersen van een interne 'crisis'. De gemeente beschikt daarnaast niet over een continuïteitsplan voor bijvoorbeeld ICT-uitval.[5] Ook was er geen vooraf bedachte organisatiestructuur waar de gemeente op terug zou kunnen vallen bij continuïteitsverstoringen. Hierdoor was de verdeling van verantwoordelijkheden tussen de ambtelijke organisatie en leden van het College van B&W niet helder genoeg.

7. De gemeentelijke organisatie heeft de verstoring snel, slagvaardig en succesvol aangepakt

De organisatie toonde zich veerkrachtig en in staat om de gevolgen van de verstoring goed en snel te beperken. Hieronder volgt een opsomming van factoren die aan dit succes hebben bijgedragen:

- Er is direct een aantal goede crisisbesluiten genomen: de ICT-infrastructuur van de gemeente is om verdere verspreiding te voorkomen per direct uitgeschakeld, er is besloten om transparant te communiceren over (de gevolgen van) de virusuitbraak. Bovendien is er meteen een interne, ambtelijke crisisstructuur ingericht bestaande uit het directieteam, een ICT-specialist, een communicatieadviseur en secretariële ondersteuning.
- Er is goed nagedacht over de uitgangspunten van de aanpak en deze zijn consequent gevolgd. Het herstel van de dienstverlening aan de burger stond hierbij centraal;
- De gemeente heeft goed oog gehouden voor de omgeving:
  - Er is actief en via verschillende kanalen gecommuniceerd (daarover verderop meer).
  - Er is actief gezocht naar samenwerking met externe partners (daarover eveneens verderop meer).
- Er is een 'verbindingsofficier' als lid van het kernteam aangewezen c.q. opgestaan. Deze wist het technische probleem goed te vertalen naar de betekenis voor organisatie en samenleving en vice versa.
- ICT-specialisten en andere medewerkers van de gemeente zijn teruggekomen van vakantie om de crisisorganisatie bij te staan.
- Specialisten hebben samen met enkele externen 24/7 doorgewerkt om de storing te verhelpen.
- Alle medewerkers van de gemeente toonden zich flexibel. Zij probeerden een bijdrage te leveren aan de oplossing of zochten ander nuttig werk.
- Besluiten tot het maken van kosten zijn goed afgewogen. Zo is er pas besloten tot (steviger) inzet van externen toen bleek dat de verstoring complexer en langduriger zou zijn.
- De raad is twee dagen nadat de storing geheel verholpen was (15 augustus) uitgebreid per brief geïnformeerd (op 17 augustus).

[5] Organisaties in de publieke sector – waaronder gemeenten – zijn in 2010 door de Minister van Veiligheid & Justitie verzocht om continuïteitsplan voor de risico's uitval van ICT en elektriciteit op te stellen.

8. De interne en externe communicatie was toereikend en sterk

Er was vanuit het crisisteam veel aandacht voor de omgeving. Juist ook in het licht van uitgevallen communicatiemiddelen. De gemeente beschikte nog wel over de website als *online* communicatiekanaal en kon tevens Social Media inzetten (Twitter). Zo kwamen kernboodschappen, persberichten en updates alsnog naar buiten. De betrachte openheid genereerde veel aandacht van lokale, als ook nationale en internationale pers. Weert werd het symbool van de virusuitbraak. De gemeente besteedde in de berichtgeving specifiek aandacht aan het richten en bijstellen van verwachtingen van burgers. Ook gaf de gemeente burgers aandachtspunten en tips om een virusaanval te voorkomen of te beperken. De toon van de berichtgeving was feitelijk. Op één moment is voorgesorteerd op de verwachte uitkomst, te weten het herstel van de dienstverlening aan het begin van de nieuwe werkweek. Dit is op zondag 12 augustus aan pers en publiek gecommuniceerd. Helaas bleek vervolgens op die ochtend dat de dienstverlening niet geheel was hersteld.

Het crisisteam onderkende het belang van interne communicatie. Het team besloot al snel tot de inrichting van een alternatieve communicatiestructuur. Rekening houdende met de vaste vergadertijdstippen van het crisisteam werd de informatie in cascade de organisatie in gebracht. Dit verliep als volgt. Na afloop van de vergadering van het crisisteam werden de afdelingshoofden geïnformeerd, zij verzorgden vervolgens de communicatie naar de eigen mensen. Aanvullend was op elke sector een centraal informatiepunt ingericht, bemand door secretariaatsmedewerkers. Van hieruit werd informatie verspreid maar werden tevens vragen en ontwikkelingen gemeld. Daarnaast werden er papieren informatieberichten verspreid en was er een actuele lijst met veel gestelde vragen (FAQ's) beschikbaar.

9. Weert heeft zich omwille van het maatschappelijke belang kwetsbaar opgesteld

Naast het informeren van burgers en het bieden van handelingsinformatie, trad de gemeente actief naar buiten vanuit het bredere maatschappelijke belang. Ten eerste, wilde de gemeente Weert hiermee voorkomen dat burgers slachtoffer werden van de virusuitbraak. Vandaar dat de burgemeester burgers opriep om alert te zijn en er via de website informatie beschikbaar was over wat burgers hier zelf tegen konden doen. Ten tweede, wilde de gemeente andere organisaties behoeden voor het virus en samenwerking binnen de publieke sector bevorderen. Met deze aanpak heeft Weert zich onderscheiden. Het is verre van gebruikelijk dat er rond cyberincidenten actief naar buiten getreden wordt, terwijl de algehele maatschappelijke alertheid en weerbaarheid hier wel bij gebaat zijn.

10. De gemeente heeft de verstoring grotendeels op eigen kracht verholpen

Weert heeft gedurende de virusuitbraak actief gezocht naar samenwerking en uitwisseling met netwerkpartners. In de eerste plaats enkele bestaande ICT-leveranciers van de gemeente. Deze leveranciers konden echter weinig voor de gemeente betekenen, voornamelijk doordat de afgesloten contracten hier niet op toegerust bleken. Klaarblijkelijk werden er door de leveranciers buiten de contractuele verplichtingen om geen mogelijkheden gezien tot ondersteuning van de gemeente.[6]

Weert heeft actief gezocht naar contacten voor de uitwisseling van ervaring en kennis. Zo is er onder meer contact gelegd met andere gemeenten die met hetzelfde virus geconfronteerd werden. Vanwege grote verschillen in onder andere systeemarchitectuur bleek het lastig om technische vraagstukken of lessen te delen. Vanwege de aard van de crisis is niet samengewerkt met gebruikelijke crisispartners waaronder de Hulpdiensten, het openbaar ministerie of de Veiligheidsregio Limburg Noord. De inschatting was dat deze partners –gespecialiseerd in de bestrijding van traditionele crises en calamiteiten- weinig toegevoegde waarde hadden in de aanpak van dit nieuwe type crisis.

[6] Overigens gold dit niet voor Cliënt ICT Groep, Ictivity & Telindus-ISIT. Deze leverancier heeft de noodzakelijke ondersteuning en expertise wél kunnen bieden, ook buiten kantooruren ('s avonds en 's nachts, ook in het weekend). Ook de leverancier van antivirus software – Symantec – heeft de gemeente zo snel mogelijk geholpen met nieuwe virusdefinities.

Hoewel er actief is gezocht naar samenwerking met – specialistische – landelijke partners, leidde dit niet tot het gewenste resultaat. De precieze rol en functie van het Nationaal Cyber Security Centrum (NCSC – onderdeel van het Ministerie van Veiligheid & Justitie) bleef voor de gemeente onduidelijk. De algemene adviezen van het NCSC hadden geen toegevoegde waarde voor de gemeente. De aanpak van de gemeente is op hoofdlijnen met het NCSC getoetst. De gemeente kreeg in reactie bevestigd dat aanpak er één zou zijn die het NCSC ook zou adviseren. Wel is goed samengewerkt met de VNG en KING. Zo trad KING effectief op als verbindingsofficier tussen gemeenten. Dit bespaarde gemeenten werk, terwijl zij wel profiteerden van de informatiepositie van KING.

Toen de dienstverlening leek te zijn hersteld, waren er nog opstartproblemen. Allereerst, omdat er geen verbinding was met de Gemeentelijke Basis Administratie (GBA) wegens het – onbewust – losgekoppeld laten van betreffende computers van het netwerk. Ten tweede, omdat de verbinding met de leverancier van reisdocumenten (SDU) door deze leverancier was dichtgezet. Deze verbinding kon pas na een inspectie door de leverancier weer worden gebruikt. En ten derde, waren er nog tot en met woensdag 15 augustus problemen met de externe mail van de gemeente. Dit bleek het gevolg van het afsluiten van de mogelijkheid tot extern mailverkeer door KPN. De acties door SDU en KPN zijn vooraf niet afgestemd met de gemeente en hebben ertoe geleid dat de dienstverlening – vanuit het perspectief van de gemeente – niet optimaal kon worden hersteld. Naar nu wordt aangenomen, is Weert na melding van het virus aan virussoftware leverancier Symantec op een lijst met risico-organisaties geplaatst. Het wekte bij de gemeente bevreemding dat zij hierover niet in kennis is gesteld.

11. De situatie werd intern als crisis ervaren, maar was voor de buitenwereld een verstoring

De virusuitbraak werd door de gemeentelijke organisatie als crisis ervaren en aangepakt. Een aantal factoren was hierbij doorslaggevend. Ten eerste het gevoel van urgentie dat bij betrokkenen ontstond door het stagneren van de publieke dienstverlening en het verlies van productiviteit van de ambtelijke organisatie. Ten tweede de ervaren politiek-bestuurlijke druk. Betrokken bestuurders wensten ook een zo snel mogelijk herstel van de dienstverlening. Ambtelijk betrokkenen gingen er tevens vanuit dat dit ook voor de gemeenteraad het geval zou zijn. Ten derde vanwege de druk die op de organisatie ontstond toen Weert actief naar buiten trad over de virusuitbraak en impact hiervan.

Voor de buitenwereld was er echter geen sprake van een crisis maar een storing in de gemeentelijke dienstverlening. Er was geen sprake van een fysieke crisis met gevolgen voor de publieke gezondheid of openbare orde. Ook bleven negatieve gevolgen voor de burgers van Weert beperkt, afgezien van een tijdelijk niet- of disfunctioneren van de gemeentelijke dienstverlening. Vanwege de vakantieperiode, was het aantal burgers dat aanspraak maakte op de gemeentelijke dienstverlening lager dan normaal. Tevens was de Gemeente in staat om 'noodgevallen' in behandeling te nemen en daarmee een beperkte dienstverlening te garanderen. Bovendien is de verstoring uiteindelijk snel opgelost: de dienstverlening werd binnen vier werkdagen grotendeels hersteld. De reactie van burgers was op een enkele uitzondering na begripvol.

12. De gemeente heeft door het incident productiviteitsverlies en financiële schade geleden

Door effectief op te treden heeft de gemeente de impact van de virusuitbraak kunnen beperken. De gevolgen voor de maatschappelijke dienstverlening zijn beperkt gebleven. Datzelfde geldt voor eventuele imago-effecten. Ook is door kordaat optreden de impact van de virusuitbraak voor de systemen en bestanden van de gemeente geminimaliseerd. De effecten van het incident voor de gemeente zijn direct en indirect van aard. Direct, in de zin dat er werk verdwenen is en er productiviteitsverlies geleden is. Indirect vanwege de kosten die nodig waren om een zo snel mogelijk herstel te realiseren. Zowel voor de inzet van externe deskundigen als voor hardware die nodig was om het herstel te bespoedigen. Aangezien deze schade niet gedekt wordt onder de huidige verzekeringen van de gemeente, komen de kosten op conto van de gemeente. In totaal worden de directe en indirecte kosten op circa EU 50.000,- geschat.

13. Er is sinds de verstoring meer aandacht voor digitale risico's, echter nog niet structureel

Tegen de achtergrond van de virusuitbraak is het bewustzijn van de digitale kwetsbaarheid van de gemeente sterk toegenomen. ICT en digitalisering hebben meer dan voorheen de aandacht van het Directieteam. Verder zijn er op verschillende plekken binnen de organisatie initiatieven om digitale kwetsbaarheden in de toekomst te verminderen. Mede in afwachting van de evaluatie van de virusuitbraak en de mogelijk daaropvolgende discussie is nog geen systematische actie ondernomen om kwetsbaarheden te bepreken. In dat verlengde is er nog geen sprake van centrale regievoering of -aansturing van een verbetertraject.

3 Aanbevelingen

Uitgaande van onze observaties doen wij de Gemeente Weert hieronder enkele aanbevelingen ter verdere versterking van de beheersing van digitale risico's en voorbereiding op de gevolgen van digicrises.

1. *Beschouw digitalisering en de hiermee verbonden risico's als expliciete vraagstukken voor directie en bestuur.* ICT behoort tot de kern van de gemeentelijke organisatie en is een cruciaal middel voor het uitoefenen van de maatschappelijke functie. Zij is daarmee niet langer alleen een ondersteunende dienst. Het ligt bovendien voor de hand dat de afhankelijkheid van ICT in de nabije toekomst steeds verder toe zal nemen. ICT is daarmee een strategisch vraagstuk geworden. En strategische vraagstukken, die de kern van de organisatie raken, vereisen per definitie directe betrokkenheid van directie en bestuur.[7] Strategische vraagstukken kunnen niet overgelaten worden aan specialisten of portefeuillehouders. Dit dient weerspiegelt te zijn in de verantwoordelijkheidsstructuur van de gemeente: in termen van verantwoordelijkheden, taken en doelen. Datzelfde geldt voor de beheersing van risico's verbonden met voortschrijdende digitalisering. Overigens ligt hier ook een controlerende taak voor de Weerter gemeenteraad.

2. *Garandeer structurele, organisatiebrede aandacht en doelen voor digitale risico's op basis van de opgedane ervaring en geleerde lessen.* Sinds de virusuitbraak zijn er zoals vermeld initiatieven genomen om de kwetsbaarheden van de gemeente te beperken. Wij adviseren om de ervaring, lessen en wensen trajectmatig te verankeren en uitvoering te geven. In het bijzonder bevelen wij aan om:
   a. Het bewustzijn van digitale risico's te bevorderen, rekening houdend met wat realistisch gezien van specifieke (groepen) intern betrokkenen mag worden verwacht
   b. Gericht te investeren in risicobeheersing – niet alleen op organisatorisch maar juist ook op ICT-vlak. Cyberrisicomanagement moet een integraal en vast onderdeel worden van de bedrijfsvoering.
      i. De gemeente moet kunnen beschikken over een totaaloverzicht van de bestaande ICT-infrastructuur
      ii. De gemeente moet beter inzicht hebben in de eigen digitale risico's én de impact van deze risico's voor de gemeentelijke bedrijfsvoering en dienstverlening kennen. Dit om de gemeentelijke risico's tot op een aanvaardbaar niveau terug te brengen. Evident ligt hier een belangrijke rol voor ICT
      iii. Voor aanpassing en uitbreiding van de architectuur dient de gemeente een duidelijke verantwoordelijkheidsstructuur te ontwerpen. Uitgangspunt hierbij is, dat besluiten niet op afdelingsniveau genomen worden, maar op het niveau van het Directieteam
      iv. Eén van de deelthema's welke verder aandacht verdient is contractmanagement (afspraken en eisen aan leveranciers)
      v. Ook dient de mogelijkheid tot het verbeteren van de cyberverzekeringsdekking van de gemeente expliciet te worden verkend

3. *Bevorder de gemeentelijke voorbereiding op crises – inclusief continuïteitsverstoringen*
   Wij bevelen de gemeente aan om het crisis- en continuïteitsmanagement verder te versterken. Consolideer hiertoe de werkwijze en lessen van Dorifel in een strategische crisisprocedure opdat de gemeente ook intern beschikt over een crisisstructuur. Doe dit bij voorkeur generiek om zo ook de voorbereiding op andere interne verstoringen, incidenten of crises te verbeteren. Zorg voor een glasheldere taakverdeling tussen bestuur en ambtenarij. Voorzie tevens in aansluiting op voor de gemeente bekende structuren en werkwijzen (actiecentra e.d.). Maak van de crisisdiagnose een standaardactiviteit van het crisisteam.[8] Dit om over- of onderschatting van gebeurtenissen en hun impact te voorkomen. Zorg er verder voor dat de

[7] Zie ook: British Standard Institute, PAS 200:2011, *Crisis management-Guidance and good practice*.
[8] Onderdeel van die diagnose is de vaststelling van de aard (A), betrokkenen (B) en specifieke context (C) van het probleem. Op grond van dat gedeelde beeld kan de strategie inclusief bestuurlijke uitgangspunten worden bepaald en de vereiste opschalingprocedure.

gemeente nu conform het verzoek van de Minister van Veiligheid & Justitie beschikt over een operationeel continuïteitsplan ter verbetering van de voorbereiding op uitval van ICT en elektriciteit.

4. *Ga met VNG, KING en andere gemeenten in gesprek over het verbeteren van kennis-uitwisseling en informatiestroomlijning* In het gesprek met landelijke partners moet de verbetering van de volgende onderwerpen centraal staan:
   - De uitwisseling van kennis en expertise over voor gemeenten relevante bedreigingen
   - Het stroomlijnen de informatie-uitwisseling tussen cruciale marktpartijen en getroffen organisaties. Dit om te voorkomen dat gemeenten zonder hun medeweten op een 'zwarte lijst' terecht komen op basis waarvan andere marktpartijen – ongemerkt – acties kunnen ondernemen die mogelijk nadelig uit kunnen pakken voor organisaties.

5. *Deel de lessen actief met belanghebbenden, relevante ketenpartners en andere geïnteresseerden.* Weert heeft ervaring opgedaan met een (forse) continuïteitsverstoring door uitval van ICT als gevolg van een virusuitbraak. Door de steeds verder toenemende afhankelijkheid van ICT, ligt het in de lijn der verwachtingen dat dit type incident in de toekomst steeds vaker voor zal komen. Gegeven de relatieve noviteit en de neiging van veel organisaties om incidenten af te schermen van de buitenwereld, is er nog weinig bekend over de specifieke dynamiek van de 'digicrisis'. Wij moedigen Weert aan om de ingezette transparante lijn ook te vervolgen voor wat betreft de opgedane ervaring en geleerde lessen. Dit om organisaties binnen en buiten de publieke sector de kans te geven om te leren van de lessen van Weert en de algehele maatschappelijke weerbaarheid tegen digitale incidenten te versterken.

4 Leren van Dorifel: algemene lessen

De virusuitbraak en de daaropvolgende bestrijding, levert niet alleen lessen op voor de gemeente Weert. Op basis van de transparante en goed gedocumenteerde aanpak (inclusief interne evaluatie) is het mogelijk om enkele algemene lessen te identificeren. Deze lessen kunnen door gemeenten en andere organisaties worden benut om digitale risico's te beheersen en de voorbereiding op cyberincidenten te versterken.

1. Digitale risico's zijn strategische risico's

ICT is niet langer alleen een ondersteunende dienst. ICT maakt steeds meer onderdeel uit van de kernactiviteiten van een organisatie. Digitale risico's zijn daarmee verworden tot strategische risico's. De aandacht voor digitale risico's dient zich daarom niet te beperken tot het domein van de ICT. Digitale risico's verdienen daarom structurele bestuurlijke aandacht.

2. Overzicht en inzicht zijn randvoorwaardelijk voor een goede beheersing en bestrijding

De ICT-architectuur van organisaties is historisch gegroeid en gelaagd. Hierdoor blijkt het in de praktijk lastig om een overzicht te hebben van de ICT. Ook ontbreekt vaak inzicht in hoe ICT zich verhoudt tot de primaire processen van organisaties. Waar zitten de kritieke afhankelijkheden? Wat gebeurt er als de ICT uitvalt? Dit inzicht is noodzakelijk om een beeld te vormen bij de risico's die een organisatie loopt. Voor een goede beheersing van risico's en bestrijding van incidenten is dit overzicht en inzicht cruciaal.

3. De verbinding tussen ICT en de rest van de organisatie moet hecht zijn

Binnen organisaties bestaat er vaak een afstand tussen ICT en andere afdelingen. Deze twee werelden komen niet als vanzelf bijeen. Voor wat betreft de bestrijding van digitale incidenten is het echter cruciaal om deze vaak nog gescheiden werelden te overbruggen. De bestaande crisisstructuren worden vaak niet optimaal gebruikt bij ICT-incidenten. Er is behoefte aan een 'verbindingsofficier' die ICT en de rest van de organisatie aan elkaar smeedt. Ook moeten technische en andere oplossingen die deel uitmaken van de aanpak met elkaar in balans worden gebracht.

4. De continuïteit staat altijd op het spel

Hoewel er altijd veel aandacht wordt besteed aan de oorzaak van cyberincidenten, staat het bij de bestrijding van de crisis, het beperken van de impact centraal. Veel recente cyberincidenten maken duidelijk dat zij een voorname bedreiging vormen voor de continuïteit. In de aanpak van cyberincidenten zal het beperken van de effecten voor de continuïteit en een zo snel mogelijk herstel altijd hoge prioriteit hebben.

5. Er zijn geen vaste spelers en het speelveld is niet vastomlijnd

Cyberincidenten zijn niet plaatsgebonden. Het speelveld is daardoor niet vastomlijnd. Er zijn dan ook geen vaste spelers. Individuele organisaties kunnen te lijden hebben onder de gevolgen van een cyberincident. Maar datzelfde geldt voor netwerken en ketens van met elkaar verbonden organisaties. Organisaties zijn voor wat betreft de bestrijding in de eerste plaats zelf aan zet. Zij worden hierbij mogelijk ondersteund door leveranciers en specialistische overheden. Bij een cyberincident zal de netwerkkaart vooralsnog telkens opnieuw moeten worden uitgetekend.

6. Transparantie is in het belang van de samenleving

Geconfronteerd met een cyberincident, zullen veel organisaties worstelen met de vraag of zij wel transparant moeten zijn. Transparantie kan immers afbreuk doen aan een goed imago of kwetsbaarheden van een organisatie blootleggen. Transparantie helpt echter de alertheid bij anderen bevorderen. Hierdoor worden zij in staat gesteld om zich tegen een dreiging teweer te stellen en de impact te beperken. Transparantie over cyberincidenten, mits proportioneel en met beleid, is daarmee in het belang van de samenleving.

7. Meerdere, robuuste communicatiekanalen zijn noodzakelijk

Geconfronteerd met een cyberincident, is het cruciaal om te kunnen blijven communiceren. De kans is echter groot dat de bestaande communicatiemiddelen niet meer kunnen worden gebruikt. Communicatie moet daarom redundant zijn uitgevoerd. Een organisatie dient meerdere, onafhankelijke communicatiekanalen te kunnen gebruiken die gezamenlijk voldoende robuust zijn.

8. Technische oplossingen zijn nooit volkomen en creëren mogelijk zelfs nieuwe problemen

Bij de bestrijding van cyberincidenten ligt er vaak grote nadruk op het doorvoeren van technische oplossingen. De praktijk leert echter dat deze oplossingen vaak weerbarstig zijn. Het testen en hertesten van technische oplossingen is belangrijk. Het communiceren van een hersteltermijn is niet raadzaam. Dit niet alleen omdat het vaak langer duurt om de oplossing te realiseren, maar ook omdat de oplossing vaak nieuwe vraagstukken blootlegt waardoor vanuit het perspectief van belanghebbenden soms nog geen sprake is van een oplossing.

Bijlage Verloop van het incident op hoofdlijnen

Hieronder geven we een (niet uitputtend) overzicht van gebeurtenissen plaats in de periode 7-14 augustus 2012. Het overzicht is gebaseerd op de interne evaluatie van de gemeente Weert (Evaluatie aanpak virusbesmetting augustus 2012).

Dag 1: Eerste melding

Op dinsdag 7 augustus 2012 werd een melding gedaan door een medewerker van de gemeente Weert dat er iets vreemd aan de hand was met de pc. Er wordt een intern onderzoek gedaan door de systeembeheer van het team ICT. Het komt vaker voor dat meldingen worden gedaan dat een applicatie niet datgene doet wat het moet doen of dat er iets met het netwerk aan de hand is in verband met *perfomance* problemen. Hierdoor rijst er geen vermoeden dat van iets anders dan normaal sprake is. De betreffende bestanden worden geselecteerd en verwijderd en de originele bestanden worden teruggeplaatst. Het euvel lijkt verholpen.

Dag 2: Vermoeden van virus

Op woensdag 8 augustus 2012 wordt in de ochtend het vermoeden uitgesproken dat er sprake was van een virus. Diezelfde ochtend wordt daarvan meteen melding gedaan bij de sector bedrijfsvoering (verantwoordelijk voor ICT services). Besloten wordt de balies te sluiten en contact op te nemen met leveranciers. Na het doornemen van de constateringen de ICT dienstverlener Cliënt ICT vindt opschaling plaats naar het Directie Team (DT).

Nadat het DT is geïnformeerd over de analyse wordt besloten om zoveel mogelijk openheid van zaken te geven over de constatering van het computervirus bij de gemeente Weert. Ook wordt besloten dat medewerkers van de gemeente Weert geen werkzaamheden meer mogen verrichten middels de pc (bekend was namelijk dat het virus zich daardoor verspreidt). Kort daarna wordt het hele netwerk afgesloten. Er wordt een taak- en rolverdeling afgesproken en de burgemeester wordt geïnformeerd. In de middag meldden zich de eerste media voor interviews en reportages.

Er worden contacten gelegd met andere getroffen organisaties (collega-gemeenten en een woningbouwcorporatie) en er is een eerste contact met KING (Kwaliteitsinstituut Nederlandse Gemeenten) die als intermediair wil optreden tussen de gemeente en deskundigen en andere getroffenen.

Dag 3: Netwerk geïnfecteerd

Op donderdag 9 augustus 2012 wordt in de ochtend geïnventariseerd hoe groot de omvang van de infectie is. De virusinfectie bleek aanzienlijk te zijn: het gehele netwerk (waaronder de gebruikers data), enkele Windows servers en Samba Shares zijn geïnfecteerd.

Het DT komt bij elkaar om de situatie te beoordelen en besluit om alles te richten op herstel van de dienstverlening bij de afdeling Publiekszaken. De burgemeester wordt door het DT en specialisten bijgepraat. De gemeente Weert staat in de belangstelling van regionale en landelijke media.

Vanuit Symantec worden nieuwe definitiebestanden toegestuurd voor het detecteren van het virus. Het resultaat was niet zoals beoogd. Het werd getest maar de definitiebestanden werkten niet goed. Besloten wordt om de backups (eerder opgeslagen versies van bestanden en programma's) terug te zetten. Hier werd een virusscan op losgelaten om zo te achterhalen of de backup besmet was. Ook PC's worden gescand op virussen. De actie werd uitgezet om te beginnen met de 'restore', maar deze actie stagneert. De hele nacht wordt er doorgewerkt aan de restore.

Dag 4: Herstelwerkzaamheden

Op vrijdag 10 augustus 2012 stuurt Symantec nieuwe 'virus definition' bestanden. Uit de uitgevoerde scan bleek dat de schijven niet geïnfecteerd bleken te zijn. Client ICT richtte de Symantec virus console server in. Alle pc's worden opnieuw gescand. Een scan werd uitgevoerd van de windows servers, pc's en telefoontoestellen werden losgekoppeld van het netwerk. Met andere leveranciers werd contact gezocht voor kennis op het gebied van VM-Ware. Linux en OES werden hersteld. Er worden afspraken gemaakt over de weekendbezetting, over praktische zaken en het informeren/afstemmen met de burgemeester. Er wordt een speciaal telefoonnummer beschikbaar gesteld en gecommuniceerd voor mensen die in het weekend willen bellen omdat ze in de problemen dreigen te komen of zich zorgen maken.

Dag 5: Continuering herstelwerkzaamheden

Op zaterdag 11 augustus 2012 wordt gewerkt aan het voorzien in opslagcapaciteit en de inrichting van een quarantaine omgeving ingericht. Na scanning en het updaten worden de servers gecheckt in de productieomgeving. De pc's werden voor de 2e maal gescand. Een restore van de netwerkserver werd uitgesteld tot de reserve storage er zou zijn. Het duurt lang om de servers om te zetten naar de veilige omgeving en de reserve storage was erg langzaam. Er wordt besloten om de nacht door te werken.

Dag 6: Continuering herstelwerkzaamheden, voorgenomen hervatting dienstverlening

Op zondag 12 augustus 2012 worden alle virtuele servers gescand. Technisch gezien wordt er doorgewerkt aan het herstellen van de netwerkfunctionaliteit. Na een controle blijkt dat de servers schoon zijn en de gecontroleerde servers worden aangezet. Interflex (het tijdregistratiesysteem voor medewerkers) komt weer in de lucht. Ook het KCC was weer prima telefonisch bereikbaar. De virusscanner werd opgestart met als resultaat: "schoon". Langzaam maar zeker komt alles weer onder controle. Er is alles op alles gezet om na het weekend weer gewone dienstverlening te kunnen verlenen. Dat ziet er aan het eind van de zondag goed uit. Op basis daarvan is de berichtgeving op de website positief: er wordt de verwachting uitgesproken dat de dienstverlening op maandag weer normaal is.

Dag 7: Opstart en gestage hervatting dienstverlening

Op maandagochtend 13 augustus blijken er tegenvallers te zijn in de functionaliteit bij burgerzaken. Niet alle diensten konden daadwerkelijk getest worden; een aantal handelingen mag volgens rijksrichtlijnen pas uitgevoerd worden als zich daadwerkelijk een klant meldt met een verzoek. Omdat er hectiek ontstaat bij de balie van burgerzaken, worden noodmaatregelen getroffen. Er wordt een gastvrouw/-heer geregeld vanuit de organisatie om wachtende klanten goed voor te lichten over welke diensten nu adequaat geleverd kunnen worden en waarvoor ze beter terug kunnen komen.

Binnen enkele uren zijn de aanloopproblemen opgelost en loopt de dienstverlening normaal. Steeds meer pc's worden aangekoppeld. Teams en afdelingen konden langzaam aan weer opstarten en hun werk hervatten. De gehele dag stond in het teken van het aankoppelen van de pc's aan het netwerk.

Dag 8: Terug in bedrijf

Op dinsdag 14 augustus is de gemeente volledig operationeel. Externe hardware wordt getest op virussen om risico's van herhaling te voorkomen. De helpdesk wordt extra bemensd om te reageren op eventuele vragen en problemen. De crisisorganisatie wordt ontbonden. Er wordt mondeling gerapporteerd aan het college van B&W. Ook wordt aangifte gedaan op basis van artikel 350 a van het wetboek van strafrecht: computer hacking.

Over het COT

Het COT is een gespecialiseerd bureau op het gebied van veiligheids- en crisismanagement. Ons werkterrein strekt zich uit van vraagstukken over security ambities en de vormgeving van lokaal veiligheidsbeleid tot de voorbereiding op crisissituaties. Met onze kennis en kunde helpen we opdrachtgevers in complexe situaties waarbij grote risico's worden gelopen, strategische belangen op het spel staan en vaak vele stakeholders zijn betrokken. Advies, onderzoek, en training en oefening vormen de basis van onze dienstverlening. Het COT opereert vanuit Den Haag en is een volledige dochteronderneming van Aon Nederland.

Meer informatie: www.cot.nl