GEMEENTE WEERT

De raad van de gemeente Weert

Weert, 17 augustus 2012

Onderwerp : Aanpak virus computernetwerk gemeente Weert

Beste raadsleden,

Op dinsdag 7 augustus 2012 is de gemeente Weert getroffen door een virus op het computernetwerk. Dat heeft een enorme impact gehad op onze gemeentelijke dienstverlening. Graag informeren wij u via deze brief over de gevolgde aanpak. We hopen zo mogelijke eerste vragen al te kunnen beantwoorden. Intussen werken wij aan een uitgebreide evaluatie van (de gevolgen van) de virusuitbraak. U als gemeenteraad besluit over die evaluatie en de mogelijke consequenties.

Crisisstructuur
Op dinsdagmiddag 7 augustus merkten onze medewerkers wat technische haperingen in enkele systemen. Niet iets om ongerust over te zijn, een technische storing komt immers vaker voor. Woensdagochtend 8 augustus bleek dat het verhelpen van de storingen meer tijd kostte. Daardoor konden bepaalde producten van de gemeente Weert niet verwerkt en geleverd worden. De balies Burgerzaken en Sociale Zaken bleven daarom gesloten. Over die maatregel is direct intern en extern gecommuniceerd. Er is meteen een externe specialist opgeroepen om ons te ondersteunen bij de storing.

Rond het middaguur werd duidelijk dat de situatie ernstiger was dan gedacht. De storing blijkt een virus in het computernetwerk. Het virus verspreidt zich bij elke handeling die medewerkers via de computer doen. Daarop is direct de maatregel genomen om het hele netwerk af te sluiten. Alleen op die manier kon verdere verspreiding worden voorkomen en het virus worden 'uitgeroeid'.

Organisatorisch zijn we gaan werken met een 'crisisteam' bestaande uit het directieteam, een ICT specialist, een communicatieadviseur en secretariële ondersteuning. De loco-secretaris was voorzitter van dit overleg. De ICT specialist was de verbindingsofficier naar het team mensen dat inhoudelijk met het probleem bezig was. Er is een nauwkeurig logboek bijgehouden met de dagelijkse stand van zaken, acties en besluiten. We verwerken deze gegevens in het evaluatierapport dat u later ontvangt, zodat u een goed beeld krijgt van de afgelopen week.

Het crisisteam is elke dag meermaals bij elkaar gekomen om de stand van zaken en acties af te stemmen. Dagelijks zijn in groter verband alle leidinggevenden bijgepraat (vaak twee keer per dag), waarna deze de medewerkers konden inlichten.

Beekstraat 54
Correspondentieadres: Postbus 950, 6000 AZ Weert
Telefoon: (0495) 575 000 - Telefax: (0495) 541 554 - E-mail: gemeente@weert.nl
Website: www.weert.nl

De loco-secretaris informeerde dagelijks burgemeester Heijmans, die de woordvoering over de situatie deed in de media. Wethouder Litjens werd als portefeuillehouder (ICT) sinds zondag ook aan dit klein comité toegevoegd (wegens vakantie kon dit niet eerder).

Het uitgangspunt was dat medewerkers zoveel als mogelijk hun eigen werk bleven doen. Als dat niet kon, werd in overleg met de leidinggevende bekeken of ander werk mogelijk was. Het was een geluk dat het vakantieperiode was, daardoor waren minder medewerkers dan normaal aanwezig.

De prioriteit in de hele aanpak focuste zich op drie zaken:
- De problemen met het computernetwerk zo snel mogelijk oplossen
- De dienstverlening richting inwoners zo veel mogelijk overeind houden en noodoplossingen/maatwerk verzorgen
- Heldere interne en externe communicatie

Over het virus
Het virus is een Trojaans Paard, met de naam 'Dorifel' of 'XDocCrypt' (in eerste instantie werd gedacht aan het virus Sasfis, dit is later bijgesteld). Het virus kopieert het bestand waarin je werkt en verwijdert het oorspronkelijke. Ook wordt het bestand veel groter in omvang (kb) waardoor de server heel traag wordt. Verder verspreidt het virus zich naar andere bestanden. Het is een virus gericht op Microsoft producten zoals Word en Excel.

De problemen troffen het hele netwerk, dat betekent het stadhuis, de Milieustraat/Werf en de dependance Stramproy. Daardoor moesten alle medewerkers hun computer uitzetten en mochten tot nader order niet meer inloggen (ook niet thuis via de webmail).

Digitale beveiliging van Weert
De anti-virussoftware van de gemeente was helemaal up-to-date. Echter, omdat dit een nieuw virus is dat nog niet herkend werd door anti-virussoftware, heeft het virus het netwerk van de gemeente Weert (en vele andere organisaties) kunnen binnendringen.

De gevolgen voor Weert waren groot. De problemen met betrekking tot de dienstverlening duurden zes dagen. Weert is kortom 'hard' getroffen. Dit had verschillende redenen:
1. Weert is één van de eerste organisaties die alarm heeft geslagen. Door naar buiten te treden, hebben we andere organisaties kunnen behoeden voor dit virus of in ieder geval de gevolgen kunnen beperken. Zij hebben maatregelen kunnen treffen, Weert niet.
2. Het virus is 'begonnen' bij een afdeling met veel klantcontacten. Waarschijnlijk is via een bijlage bij een mail daar het virus binnengedrongen. Deze afdeling is gericht op contacten met inwoners, werkt nauw samen met andere collega's en is zeer actief qua gebruik van programma's en bestanden. Door die specifieke kenmerken van de afdeling waar het begon, verspreidde het virus zich heel snel.

We zijn aan het onderzoeken of de inrichting van ons netwerk, de server(s) en de netwerkschijven, invloed heeft gehad op de verspreiding van het virus. Dit is een zeer complex en technisch verhaal. Zo is het maar de vraag, of een andere inrichting van onze ICT omgeving, effect zou hebben gehad op de (mate van) verspreiding. Dit is een punt dat we meenemen in de evaluatie naar uw raad.

Wat meteen duidelijk was, is dat onze Gemeentelijke Basis Administratie (GBA, het systeem waarmee Burgerzaken alle officiële persoonlijke gegevens van mensen registreert) op een ander systeem zit en daarmee veilig is gesteld.

Aanpak dienstverlening
Zoals gezegd had de dienstverlening richting inwoners prioriteit. Ondanks dat we voor veel werkzaamheden de computer of digitale toepassingen nodig hebben, hebben we ingezet op maatwerk en het bieden van noodoplossingen.

- Zo bleef de receptie bemenst om inwoners die vragen hadden, te woord te kunnen staan.
- Ook de telefonie bleef bereikbaar en werd extra bemenst. Voor die medewerkers zijn 'stand alone PC's' geregeld zodat informatie opzoeken via de website (die wel normaal toegankelijk bleef) toch mogelijk was. Echter, veel was ook niet mogelijk. Deze klanten vroegen we de gemeentelijke berichtgeving in de gaten te houden. Mensen konden zelf op een later moment terugbellen, of de gemeente maakte een terugbelnotitie.
- Inwoners die met spoed een dienst of product van de gemeente nodig hadden, adviseerden we de gemeente te bellen. In overleg boden we maatwerk. In principe konden alle producten en diensten van Burgerzaken, behalve rijbewijzen, worden geleverd via noodprocedures. Mensen die bijvoorbeeld een paspoort met spoed nodig hadden konden zo toch worden geholpen, evenals het doen van aangifte van overlijden of geboorte.
- Het uitbetalen van de uitkeringen van Sociale Zaken is niet in gevaar geweest. Via 'omwegen' is die handeling verricht.
- De website was wel normaal toegankelijk, dat betekent dat inwoners daar wel informatie konden opzoeken.
- E-mailverkeer was niet mogelijk evenals het sturen van digitale formulieren via de website. In de communicatie is mensen aangeraden telefonisch contact op te nemen met de gemeente of de mail/formulier opnieuw te sturen zodra we digitaal weer op de been zouden zijn.
- We hebben veel aandacht besteed aan onze communicatie zodat inwoners 'niet voor niks' naar het stadhuis toe kwamen (zie hieronder de alinea Communicatie).

Aanpak ICT
Zoals gezegd leken de problemen eerst op een technische storing, pas later bleek dat we te maken hadden met een virus dat zich razendsnel verspreidde. Niet alleen in ons systeem, maar ook bij andere organisaties. Zo werd het probleem van Weert, ineens een probleem van velen. Daarmee is niet gezegd dat de gemeente Weert de eerste was bij wie het virus uitbrak, wel waren we de eerste die transparant hierover communiceerden.

Het virus in het computernetwerk van de gemeente Weert bleek hardnekkig en lastig te bestrijden. Er waren veel systemen en bestanden geïnfecteerd. De aanpak was complex en kostte veel tijd. Daarom is de eigen bezetting van ICT specialisten meteen opgeplust (mensen die zijn teruggeroepen van vakantie). Ook is de hulp van externe deskundigen ingeroepen. Dit waren mensen van Symantec (onze leverancier van anti virus software) en Cliënt ICT Groep (consultancy bureau voor netwerk systemen).

Naast dit team specialisten in huis, had de gemeente overleg over de aanpak met het ministerie van Justitie en Veiligheid, het Nationaal Cyber Security Centrum, de Vereniging van Nederlandse Gemeenten, KING en andere getroffen organisaties.

De aanpak was zoals gezegd zeer complex, maar samen te vatten in een paar stappen:
Stap 1: het inkapselen van besmette bestanden en deze in quarantaine zetten.
Stap 2: zorgen dat er geen nieuwe besmetting kan plaatsvinden (virusscan)
Stap 3: het terugzetten van een schone back-up van vóór de virusinfectie (restore).
Stap 4: nogmaals alles scannen op virussen en fouten
Stap 5: testen van alle applicaties, systemen etc.
Stap 6: handmatig alle computers één voor één opstarten

Dit klinkt op papier heel eenvoudig, echter in de praktijk kwamen we allerlei hobbels tegen die snel herstel moeilijk maakten. Zo was de server bijvoorbeeld erg traag geworden door het virus, duurt het scannen van grote hoeveelheden data nu eenmaal lang en moesten bepaalde zaken handmatig één voor één worden getest (opstart computers, systemen en applicaties).

Een vergelijk maken met het herstel van andere organisaties is 'appels met peren vergelijken', daar kwamen we achter toen we contact zochten met andere getroffen instellingen. Oplossingen bij de één, werkten niet bij de ander en vice versa. Bovendien was Weert heel transparant in haar communicatie omdat de problemen een direct effect hadden op de dienstverlening aan inwoners. Dit was niet bij iedere andere organisatie het geval. Hoewel wellicht het beeld is ontstaan dat het bij Weert langer duurde dan elders, verzekeren wij u dat dit niet het geval is. De inhoudelijk deskundigen (bijv. VNG, KING, externe ICT specialisten die ons ondersteunden), waren positief over de Weerter aanpak.

Aanpak Communicatie
Er waren een paar gouden regels in de communicatie over het virus: Transparant, met regelmaat communiceren (ook in het weekend), gericht op feiten en niet op aannames /verwachtingen/hoop. Onze berichtgeving focuste met name op de dienstverlening, de aanpak van het virus en op waarschuwingen/tips aan mensen over hoe om te gaan met de beveiliging van hun eigen computer.

Externe communicatie
In de externe communicatie maakten we gebruik van verschillende kanalen:
- Website (speciale dossierpagina www.weert.nl/virus met daarop alle persberichten, links naar artikelen en tv-uitzendingen, links naar andere instanties)
- Twitter (voor korte mededelingen, 1750 volgers)
- Printmededelingen (posters) opgehangen in het stadhuis (zoals bekend een doorgang voor veel winkelend publiek).
- Telefonie (Klanten Contact Centrum extra bemenst, zie alinea Dienstverlening)
- Balies (Receptie extra bemenst en bij balie Burgerzaken maatwerk toegepast, zie alinea Dienstverlening)
- Via persberichten informeerden we de pers, die hier een vertaalslag van maakte richting hun lezers/kijkers.
- Voor inwoners is er in het weekend een speciaal telefoonnummer opengesteld voor dringende vragen.

Interne communicatie
De interne communicatie kon niet digitaal verlopen. Daarom richtten we ons op persoonlijke communicatie (overleggen en telefonische mededelingen via een belboom) en schriftelijke mededelingen. Via het crisisteam werden de leidinggevenden geïnformeerd over updates, waarna zij de medewerkers informeerden. Ook werden schriftelijke berichten uitgedeeld en opgehangen in het stadhuis. De griffie informeerde de gemeenteraad. De secretariaten werden ingeschakeld voor het verzamelen van vragen.

Sentiment
In zes dagen tijd, waarvan twee weekenddagen, zijn tien persberichten en tien interne mededelingen verspreid. Via twitter zijn 23 berichten verstuurd (openbare tweets, hierin zijn de Direct Messages niet meegenomen omdat dit persoonlijk contact met inwoners/bedrijven betreft). De piek van de informatievoorziening lag in de eerste twee dagen.

Tijdens de crisis is permanent aan mediawatching gedaan; dat wil zeggen bijhouden wat er in de media wordt gezegd over de virusuitbraak (stuk archivering) en handelen als de berichtgeving niet klopt of mensen vragen/klachten hebben.

Wat opvalt:
- Er waren weinig klachten en vragen over het virus (mensen belden met hun normale vragen naar de gemeente, niet specifiek over het virus. Dit gold ook voor de dialoog op twitter).
- Er was veel media-aandacht voor de kwestie, zowel lokaal, regionaal, nationaal en zelfs internationaal. De piek lag vooral op woensdag 8 en donderdag 9 augustus. Op woensdag 8 augustus was Weert trending topic op twitter en donderdag 9 augustus opener van het NOS journaal en RTL Nieuws. Ook zondag was er een piek vanwege het nieuws dat de gemeente aangifte ging doen bij de politie.
- In de berichtgeving zoomden de media de eerste twee dagen o.a. in op hoe de ambtenaren werkten zonder computer (met typemachines bijvoorbeeld).
- Er waren heel veel klassieke retweets van nieuwsberichten (het nieuws direct doorgeven, zonder oordeel erover).
- In de beginfase waren er veel 'lollige' berichten op de reguliere nieuwsfora (bijv. over de ambtenaren die nu niet konden werken en over het thema Trojaans paard).
- Als er inhoudelijke reacties waren, dan waren die vooral te lezen op ICT-fora.

Tijdens de hele crisis zijn we alert geweest op de beeldvorming en het imago van de gemeente als gevolg van deze virusuitbraak.

Wat opviel was dat, hoewel we door de beperkte dienstverlening niet iedereen hebben kunnen helpen, de meeste inwoners erg begripvol waren. We denken dat de transparantie en regelmatige communicatie over het onderwerp hieraan hebben bijgedragen. Daar kregen we ook complimenten over (persoonlijk bij de balie en telefonie maar ook op fora en twitter).

Schade
De gemeente Weert heeft dinsdag 14 augustus aangifte gedaan bij de politie van computer hacking (Art. 350a Wetboek van Strafrecht). De politie en het Openbaar Ministerie doen onderzoek naar het doel van de aanval en de dader(s). Daar is nu nog niets van bekend.

De virusaanval was zeer ingrijpend en we hebben veel schade geleden. Denk aan externe deskundigen die zijn ingehuurd, productietijd die verloren is gegaan, medewerkers die extra uren hebben gewerkt en bestanden en systemen die mogelijk gerepareerd of vervangen moeten worden.
Verder zijn mails en webformulieren die aan de gemeente zijn gestuurd tussen woensdagmiddag 8 augustus en dinsdagochtend 14 augustus niet aangekomen. In onze berichtgeving, roepen we mensen die ons in die periode hebben gemaild, op om de mail of het formulier opnieuw te sturen.
Ook was afgelopen woensdag en donderdagochtend niet mogelijk om te mailen naar externen. Daarnaast moeten als gevolg van het terugzetten van de back-up sommige bestanden opnieuw worden gemaakt.

Kortom, de schade is groot. Hoe groot dat bedrag precies is, onderzoeken we nu. Ook onderzoeken we hoe we verzekerd zijn bij een dergelijke kwestie. Die zaken komen aan de orde bij het evaluatierapport.

Evaluatierapport
We zijn zeer blij dat onze dienstverlening weer op peil is en de problemen voor inwoners als gevolg van het virus, zijn verholpen. Nu wordt gewerkt aan een uitgebreide evaluatie van de gevolgen van de virusuitbraak. Daarin nemen we uiteraard leerpunten mee. Ook gaan we in op de vraag of Weert haar ICT-omgeving anders moet inrichten in de toekomst. De evaluatie en het advies van de externe specialisten die ons hebben ondersteund, nemen we hierin ook mee.

De gemeenteraad zal over die evaluatie en de mogelijke consequenties moeten besluiten. Het is nu nog niet mogelijk om aan te geven wanneer het evaluatierapport klaar is, het heeft echter onze prioriteit.

Praktisch
Via de griffie heeft u richtlijnen gekregen hoe om te gaan met uw eigen computer, laptop, mobiele telefoon, tablet, USB sticks etc. Deze zijn nog steeds van toepassing. Heeft u daar vragen over, dan is de ICT helpdesk u graag van dienst (tel. 575 666).

Met vriendelijke groet,

M. Meertens,
loco-secretaris

H. Litjens,
loco-burgemeester

Bijlage(n) : geen.