Gemeente
Amsterdam

Rapportage ICT Storing van 18 februari 2019

Vo.4 -

Opsteller: directie ICT
Kopie naar: waarnemend CIO, stedelijk directeuren D&I en ID

Inleiding

Op maandag 18 februari 2019 ontstond een storing in het Amsterdamse ICT-netwerk met omvangrijke gevolgen voor de dienstverlening naar ambtenaren en burgers gedurende die dag. Dit document geeft achtereenvolgens een beknopte weergave van de aanleiding, het feitenrelaas, de foutanalyse en de maatregelen die zijn c.q. worden ingezet naar aanleiding van de storing. Tevens wordt naar aanleiding van deze storing aangeven welke maatregelen worden genomen ten aanzien van het aspect communicatie.

Aanleiding en oorzaak van de storing

Een relatief kleine menselijke fout om 10:47 uur op maandag 18 februari 2019, resulteerde door technisch falen van apparatuur in een omvangrijke blokkade van het netwerkverkeer op het Amsterdamse ICT-netwerk. Hierdoor vielen ICT-voorzieningen uit waardoor de medewerkers van de gemeente Amsterdam hun werk niet konden doen en de dienstverlening naar de burgers via o.a. de Stadsloketten werd verstoord. Uiteindelijk was de storing om 22:37 uur diezelfde avond verholpen.

Feitenrelaas op hoofdpunten

1. Op maandagochtend 10.47 uur werd een routinematige aanpassing op [redacted] van de ICT-infrastructuur doorgevoerd. Deze [redacted] is een cruciaal onderdeel voor de beveiliging van de Amsterdamse ICT. Er zijn voortdurend aanpassingen nodig om bijv. nieuwe applicaties op de juiste manier toegang te verlenen. Dit soort aanpassingen vindt meermaals op een werkdag plaats.
   Voor deze werkzaamheden zijn bij de Directie ICT zes specialisten in dienst. Op de betreffende dag waren vier van de zes specialisten afwezig, één gepland en drie ongepland. In tegenstellig tot de geldende procedure is bij genoemde wijziging het vier-ogen principe niet toegepast.

2. De routinematige aanpassing had tot gevolg dat grote delen van het datacenternetwerk niet meer functioneerden waardoor business applicaties en aanverwante voorzieningen niet meer toegankelijk waren; wifi en internet niet functioneerden en ook mobiele apparaten niet meer toegang hadden tot het netwerk.

3. Conform de standaardprocedure is direct na het ontstaan van de fout een "rollback" uitgevoerd, met als doel terug te keren naar de oorspronkelijke situatie.

4. Na uitvoering van een succesvolle rollback om 10.50 uur van de [redacted] bleek desondanks een groot deel van het datacenternetwerk niet meer operationeel. Ook de beheeromgeving, waar de ICT-beheerders hun taken uitvoeren, was niet meer bereikbaar waardoor herstel van het probleem in hoge mate is bemoeilijkt.

5. Snel nadat de storing zich manifesteerde werd vastgesteld dat het hoogste calamiteiten-niveau van toepassing was. Om 11:10 uur werd het Operationele Team (OT) binnen ICT bijeengeroepen, dat om 11:20 de eerste van een reeks bijeenkomsten had. De laatste OT was om 22:30 dezelde avond.

6. Voor de communicatie is de gebruikelijke procedure, waarbij periodiek een status-update naar de IV-demandmanagers wordt gestuurd, toegepast. Daarnaast werd een bandje met een melding over de storing bij het Servicepunt ingesproken. Doordat Intranet niet toegankelijk was kon hier geen gebruik van worden gemaakt, wel is een melding op [redacted] verschenen. Ook email was niet te gebruiken.

7. Via de Directeur ICT zijn vanaf 12:13 uur de directeuren, wethouders en GS middels Whatsapp geïnformeerd over voortgang en status.
   Burgers werden vanaf 12:22 geïnformeerd over de storing via een bericht op het gemeentelijke twitteradres en de website van de gemeente.

8. Mede met inzet van de vaste leveranciers van ICT (in eerste instantie [redacted] en in tweede instantie is [redacted] bijgeschakeld), is door ICT gewerkt aan analyse en herstel van de situatie en is om 22:37 uur de storing verholpen.

Eerste analyse van de storing

- De *aanleiding* van de netwerkstoring is de beschreven menselijke fout inzake de [redacted] aanpassing. Bij het herstellen van deze fout, is volgens standaard procedure succesvol een rollback uitgevoerd. Desondanks heeft het datacenternetwerk zich hierdoor niet hersteld wat heeft geleid tot de langdurige uitval.
- Na analyse van de situatie kan dit feit vooralsnog niet anders worden verklaard dan dat de oorzaak een fout in de [redacted] apparatuur moet zijn. Een fout die onder normale omstandigheden niet voorkomt maar door een bepaalde samenloop van omstandigheden kan optreden.
  Dit type fouten in netwerksoftware is een bekend fenomeen in dergelijke complexe netwerken. De kans van optreden is minimaal, de impact kán heel groot zijn.
- Gelet op het feit dat het betreffende datacenternetwerk tenminste sinds 2016 -opbouw binnen ICT-Centraal- goed functioneert; er weinig tot geen storingen plaatsvinden en goed wordt onderhouden, met directe 2e en 3e lijns support van [redacted] respectievelijk de netwerkfabrikant [redacted] is er geen aanleiding om te veronderstellen dat sprake is van een structureel probleem.
- Ook herhaling van deze feitelijke verstoring is niet aan de orde, niet op korte termijn gelet op de verscherpte beheermaatregelen. Zie hieronder. En daarna niet door structurele oplossing via de fabrikant [redacted]
- Communicatie met de stad tijdens deze grote verstoring is onvoldoende geweest: de huidige communicatieafspraken bij dergelijke onverhoopte verstoringen voldoen niet meer aan de behoeften van de organisatie.

Maatregelen n.a.v. deze storing

Een aantal maatregelen zijn, cq. worden genomen teneinde het risico dat een dergelijke ingrijpende verstoring zich opnieuw kan voordoen te mitigeren.

1. Binnen de afdeling ICT Datacom zijn c.q. worden naar aanleiding van de bevindingen een aantal preventieve en repressieve maatregelen aangescherpt en verbeterd.
2. Specialisten van de leverancier [redacted] zijn ingeschakeld om:
   a. een onderzoek uit te voeren naar de vermeende fout in de netwerkapparatuur in de context van de configuratie van het datacenternetwerk van de Gemeente. Dit is standaard procedure bij dergelijke vermeende fouten;
   b. om te adviseren over verbeteropties en mogelijke stroomlijning of vereenvoudiging van de inrichting. Dit naar aanleiding van voorschrijdende inzichten en best practices teneinde de kwetsbaarheid in het algemeen zo mogelijk te verkleinen.
3. De draaiboeken en protocollen van het Operationeel Team (OT) dat verantwoordelijk is voor sturing bij dergelijke incidenten, worden aangescherpt. De samenstelling van het OT wordt tevens tegen het licht gehouden.

Maatregelen op het vlak van communicatie:
Geconcludeerd wordt dat de huidige communicatieafspraken niet meer voldoen aan de behoefte van de organisatie. In overleg met communicatie en IVE worden nieuwe communicatieafspraken gemaakt waarin tenminste onderstaande punten worden geborgd:

4. Beschikbaarheid van een zo optimaal mogelijk communicatiekanaal bij het niet beschikbaar zijn van de reguliere kanalen (mail en intranet), analoog naar de burgers.
5. Via de IVE identificeren van kritische bedrijfsprocessen waar aanvullende communicatie noodzakelijk is boven de generieke stedelijke communicatie.
6. Uitgewerkte communicatiematrix wie naar wie communiceert en op welke momenten wordt gecommuniceerd.

Deze maatregelen zijn in gang gezet. Coördinatie wordt momenteel ingeregeld. Rapportage vindt plaats rechtstreeks aan [redacted] De waarnemend directeur ICT rapporteert aan de waarnemend CIO en stedelijk directeur ID over de genomen maatregelen, de voortgang wordt besproken in het reguliere CIO-ICT overleg en middels de prestatiedialoog.

De doorlooptijd van de beschreven maatregelen is naar rato van prioriteit maximaal 2 maanden.