Brief aan de raad

ICT storing **2020-16207**
21 juli 2020

Aan de leden van de raad,

Donderdag 9 juli 2020 in de loop van de middag heeft er een regionale netwerkverstoring plaatsgevonden binnen de Drechtsteden. Deze verstoring heeft tot uitval van de ICT-voorzieningen geleid. Rond 22 uur in de avond is de ICT-dienstverlening volledig hersteld.

Naar aanleiding van deze gebeurtenis zijn de volgende vragen gesteld.
1. Wat is er precies gebeurd?
2. Hoe heeft dit kunnen gebeuren?
3. Waarom hebben de back-up systemen het niet overgenomen?
4. Hoe gaan ICT-storingen voorkomen worden?

Oorzaak verstoring
Binnen onze netwerkomgeving zijn beveiligingsmaatregelen genomen om hackers en cybercriminelen buiten te houden. Naast bijvoorbeeld de virusscanner op de PC wordt er ook gescand op het netwerk zelf naar mogelijk malafide netwerkverkeer (Bijvoorbeeld: Het bezoeken van malafide websites, het wegsluizen van bestanden, etc.).

Door een foutieve update van een fabrikant heeft de netwerkscanner valide verkeer als mogelijk malafide verkeer aangemerkt. Hierdoor ging deze scanner netwerkactiviteit abusievelijk blokkeren. Omdat er een grote hoeveelheid netwerkverkeer abusievelijk werd geblokkeerd raakte het systeem overbelast. Dit zorgde voor een grotere verstoring. Nadat het systeem door ICT in samenwerking met de leverancier hersteld was naar de oorspronkelijke configuratie, werkte het netwerk weer naar behoren.

Onderzoek
Op het moment van de verstoring is per direct een onderzoek gestart. Verschillende beheerteams hebben zowel op locatie als op afstand onderzoek gedaan. Nadat was vastgesteld dat het probleem zich in de netwerkomgeving bevond, is direct de betreffende dienstenleverancier van dit netwerkcomponent bijgeschakeld. Ook is het crisisteam van ICT direct bij elkaar gekomen. Deze hebben de communicatie naar de verschillende gremia verzorgd en alle eindgebruikers via SMS geïnformeerd.

portefeuillehouder: Jansen, T.
informatie: Ronald Hagenaars
telefoon: 078 770 37 23
e-mail: rejl.hagenaars@zwijndrecht.nl

bijlagen:
ter inzage:

De impact van deze gebeurtenis is groot geweest. Na een dergelijk incident wordt altijd zo spoedig mogelijk een evaluatie opgestart. Enkele leerpunten die op korte termijn hieruit naar voren komen zijn:

- Zowel op strategisch (Directie) als operationeel niveau wordt deze storing geëvalueerd. Het doel is om maatregelen zowel op proces als op technisch niveau te nemen om de kans op een verstoring met dezelfde oorzaak te minimaliseren.
- Samen met de leverancier bepalen welke maatregelen nodig zijn om het update proces beter te beveiligen;
- Verhoogde dijkbewaking / waakzaamheid de komende dagen rondom het verstoorde netwerkcomponent;
- Het evalueren van het communicatieplan.

Het is echter ook fijn om te zien dat ondanks de extra communicatieve uitdagingen rondom de COVID-19 crisis, het ICT crisisteam en medewerkers snel fysiek en digitaal bij elkaar zijn gekomen om gezamenlijk deze verstoring te verhelpen.

Na de uitgebreide evaluatie zullen wij deze aan u terugkoppelen.

Hoogachtend,

De gemeentesecretaris, De burgemeester,