



Raadsmemo

Citrix crisis

aan: de raad van de gemeente Hillegom
datum: 20 januari
zaaknummer:
portefeuillehouder: Anne de Jong
behandelend ambtenaar: Alma Weitenberg

Citrix lek geen gevaar voor HLTsamen

De kwetsbaarheid in bepaalde systemen van Citrix hebben geen gevolgen gehad voor de gemeenten Hillegom, Lisse en Teylingen. De Citrix servers waar HLTsamen mee werkt zijn goed beveiligd. Omdat de berichtgeving sinds vrijdag tegenstrijdig was of op de versie van HLTsamen de voorgestelde maatregelen van Citrix afdoende waren, heeft HLTsamen besloten om landelijk advies te volgen en geen enkel risico te nemen door deze specifieke server uit te schakelen. Maandagochtend kreeg HLTsamen groen licht vanuit het Nationaal Cyber Security Centrum (NCSC) om veilig te kunnen starten. De werkorganisatie HLTsamen blijkt al de juiste beveiliging te hebben. Hierop is besloten de Citrix server weer aan te zetten zodat onze klanten volledig gebruik kunnen maken van de dienstverlening.

Wat was er aan de hand?

Door een kwetsbaarheid in bepaalde systemen van Citrix kunnen hackers toegang krijgen tot zo'n server. Vanuit het Nationaal Cyber Security Centrum (NCSC) is het advies gekomen om deze specifieke Citrix-servers uit te schakelen. Dit advies hebben de gemeenten Hillegom, Lisse en Teylingen opgevolgd. Net zoals de Tweede Kamer, een aantal provincies en Hogescholen.

Veiligheid voor alles

Zodra de kwetsbaarheid door Citrix bekend werd gemaakt, zijn de voorgestelde maatregelen door de werkorganisatie HLTsamen uitgevoerd. Op 16 januari kwam er een bericht dat de maatregelen niet op alle versies van Citrix zouden werken. De berichtgeving was op vrijdag nog zo tegenstrijdig of de versie van HLTsamen de voorgestelde maatregelen van Citrix afdoende zijn. Door deze ontwikkelingen in combinatie met de blijvende onzekerheid heeft HLTsamen besloten om geen enkel risico te nemen en deze specifieke server uit te schakelen.

Grote gevolgen

Het uitzetten van de Citrix server heeft grote gevolgen. In eerste instantie direct gevolgen voor de interne organisatie. Vanaf een andere locatie inloggen op het netwerk was niet meer mogelijk. HLTsamen heeft een flexfactor van 30%. Dat betekent dat er voor meer dan 100 mensen een werkplek beschikbaar moest zijn. Door het uitvallen van de server was het voor inwoners niet mogelijk om via de website een afspraak te maken. Op vrijdagmiddag om 17:30 uur kwam een bericht van Centric (de leverancier van onder andere de burgerzakenapplicatie) dat ook zij de server gingen uitzetten. Dat betekende dat er geen dienstverlening aan de publieksbalie kon plaatsvinden voor de inwoners van de drie gemeenten.

Geen toegang

De hackers van een Citrix server staan erom bekend dat zij geen sporen achter laten op de server. HLTsamen maakt gebruik van een SIEM-oplossing. Met deze oplossing kunnen ook uitgewiste sporen gezien worden. Met de informatie die we op dit moment hebben kunnen wij zien dat er geen ongeoorloofde toegang is geweest. Wij blijven de berichtgeving vanuit de landelijke instanties nauwlettend volgen.

Kernteam

In het weekend van donderdagavond 16 januari tot en met maandag 20 januari is er door een kernteam hard gewerkt om de gevolgen van het uitzetten van de Citrixserver zo goed mogelijk op te vangen voor inwoners en medewerkers.

Zondagavond kwam er groen licht van NSCS en maandagochtend van Centric zodat de server weer aangezet kon worden en alles volledig werkt.

Op zaterdag zijn de afspraken met klanten voor maandag afgezegd. Toen op maandagochtend bleek dat de Citrix server weer gestart kon worden, is er met de klanten gebeld dat zij alsnog langs konden komen.
