

Contactpersoon: dhr. T. Quist
Afdeling/Team: Directie/Staf
E-mail: post@heerhugowaard.nl

Ons kenmerk: Bij20-028
Zaaknummer: Cbb

RAADSINFORMATIEBRIEF

Aan het Presidium van Heerhugowaard

Onderwerp: Informatiebrief Kwetsbaarheden Citrix-servers

Heerhugowaard, 23 januari 2020

Geachte leden van het Presidium van Heerhugowaard,

Kennisnemen van

Als gevolg van ontdekte kwetsbaarheden in producten van Citrix zijn beveiligingsmaatregelen genomen. Hierdoor is het tijdelijk niet mogelijk op afstand toegang te krijgen tot het gemeentelijk netwerk.

Inleiding

In ons land worden incidenten en kwetsbaarheden op nationaal niveau gemonitord door het Nationaal Cyber Security Centrum (NCSC) van het ministerie van Justitie en Veiligheid. Zij waarschuwen als risico's toenemen en actie noodzakelijk is. Deze waarschuwingen ontvangen wij veelal via de Informatiebeveiligingsdienst (IBD) van de VNG. Op 24 december 2019 zijn wij door de IBD voor het eerst gewaarschuwd voor zeer kritische kwetsbaarheden die zijn ontdekt in Citrix-producten. De door hen geadviseerde beveiligingsmaatregelen zijn direct, op kerstavond, opgevolgd. In de avond van donderdag 16 januari deelde de IBD ons mee dat de effectiviteit van deze beveiligingsmaatregelen mogelijk niet afdoende is. Geadviseerd werd, indien mogelijk, de Citrix-servers uit te zetten tenzij intensief gemonitord kan worden op mogelijk misbruik.

Kernboodschap

De gevolgen van het advies van de IBD om de Citrix-servers uit te zetten is beoordeeld, waarbij is afgewogen welke gevolgen dit zou hebben voor bv. de dienstverlening en de medewerkers van de werkorganisatie. Hierbij is meegewogen dat tests hadden aangetoond dat sinds kerstavond hackers meerdere keren, zonder succes, geprobeerd hebben binnen te dringen door gebruik te maken van de bekende kwetsbaarheid. Besloten is het advies van de IBD op te volgen en de Citrix-servers offline te halen, hetgeen diezelfde avond heeft plaatsgevonden.

Het NCSC heeft laten weten dat indien op 9 januari de beveiligingsmaatregelen (advies 24 december) niet waren genomen de organisatie er redelijkerwijs van mag uitgaan dat deze is gecompromitteerd. De organisaties die dit betreffen dienen een herstelplan op te stellen en forensisch onderzoek te laten doen op hun netwerk, waarna alsnog de beveiligingsmaatregelen en patches dienen te worden geïnstalleerd. Doordat wij tijdig, op kerstavond, de maatregelen hebben genomen zijn deze herstelacties niet nodig.

Consequenties

De maatregelen hebben vooralsnog beperkte gevolgen voor de dienstverlening gehad. Als gevolg van het offline halen van de Citrix-servers is het gemeentelijk netwerk enkel te benaderen in het gemeentehuis van Heerhugowaard, de Binding en de gemeentewerf van Heerhugowaard. Hierdoor is thuiswerken tijdelijk niet mogelijk. De GO-app en de websites van de gemeente en de raad zijn wel te benaderen van buiten de gemeentelijke locaties.

Communicatie

Het Presidium wordt via deze raadsinformatiebrief geïnformeerd. De medewerkers van de werkorganisatie worden via verschillende kanalen op de hoogte gehouden van de ontwikkelingen.

Vervolg

Citrix heeft aangekondigd vrijdag 24 januari een patch beschikbaar te stellen waardoor de kwetsbaarheid niet meer kan worden misbruikt. Zodra deze beschikbaar is wordt deze geïnstalleerd en getest, waarna de directie besluit of en wanneer de Citrix-servers weer via internet beschikbaar worden gesteld.

Bijlage(n)

Meer informatie over de kwetsbaarheden en de beveiligingsadviezen kunt u vinden op de website van het Nationaal Cyber Security Centrum; www.ncsc.nl.

Hoogachtend,

Burgemeester en wethouders van Heerhugowaard,
de secretaris, de burgemeester,



A.S. Meijer



A.B. Blase