voorstel

Zwolle

Informatienota voor het college

Datum 22 mei 2019

Openbaar

Onderwerp	Veiligheid bij gebruik Huawei apparatuur
Versienummer	V 1.0
Informant	M. Hol
Afdeling	Advies en Faciliteiten Management / AF
Telefoon	038 498 2681

Parafering datumparaaf

Afdelingshoofd

Portefeuillehouder

Raad

☐ Informatienota voor de raad

☐ n.v.t.

Bijlagen

1.Informatie Beveiligsdienst Gemeenten

Ontwerp besluit

Het college besluit kennis te nemen van:

1.De veiligheid van gebruik van HuaWei-apparatuur.

Collegebesluit d.d.:

☐ Conform

☐ Gewijzigd

☐ Aangehouden

☐ Teruggenomen

Datum 22 mei 2019

Toelichting op het voorstel

Inleiding
HuaWei is de laatste weken veel in het nieuws vanwege het mogelijke risico op spionage via door hun geleverde apparatuur. De spionage heeft vooral betrekking op apparatuur die onderdeel uitmaakt van het nog te realiseren 5G-netwerk. De AIVD waarschuwt hiertegen en dit is mogelijk een opmaat naar de stellingname van de Nederlandse overheid in de China strategie die naar verwachting medio juni verschijnt.

Kernboodschap
HuaWei is sinds de vorming van het SSC een standaard geworden en ONS ICT gebruikt in de ICT infrastructuur vooral HuaWei netwerkcomponenten. Dit zijn componenten die intern worden gebruikt en achter een firewall zijn geplaatst. Overigens is de firewall van een andere leverancier.
Dit jaar is vervanging gepland van netwerkcomponenten voor Overijssel (de zogenaamde switch access laag).
Een andere netwerk vervanging betreft (een deel van) de WiFi voorziening bij alle partners. Hiervoor is geen apparatuur van HuaWei voorzien, omdat HuaWei nog niet een voldoende volwassen product heeft.
Hiernaast is de hardware in de server-storage infrastructuur ook grotendeels van HuaWei. Op termijn zal de server-storage hardware van HuaWei worden vervangen door producten van een andere leverancier, maar dit is in dit verband niet relevant.

Toelichting

Veiligheid
De Informatiebeveiligingsdienst Gemeenten (IBD) heeft zowel de functie van kenniscentrum als sectoraal CERT en werkt voor alle Nederlandse gemeenten en hun aangesloten ICT-samenwerkingsverbanden, intergemeentelijke sociale diensten en belastingsamenwerkingen. De IBD biedt ondersteuning in geval van een incident om schade te beperken en de situatie op te lossen. En de IBD levert informatie over bedreigingen. Ook Gemeente Zwolle en ONS ICT zijn aangesloten bij de IBD. De IBD ziet geen risico bij het gebruik van Chinese apparatuur zoals van HuaWei in de context van gemeente Zwolle / SSC-ONS, namelijk LAN componenten. Wel pleit de IBD voor een aantal algemene maatregelen ter verhoging van veiligheid, zoals actueel houden van netwerk software, veiligheidsbewustzijn en monitoring.

Vervolg:
Totdat de overheidsstrategie voor China verder uitgewerkt is, volgen gemeente Zwolle en SSC-ONS ICT de lijn:

- Zonder overleg met partners kan SSC-ONS kleine vervanging gewoon uitvoeren (incidentele switch/router)
- SSC-ONS kan risicovolle vervangingen alleen uitvoeren na goedkeuring van de partners (bijvoorbeeld LAN-componenten Overijssel)
- Bij de vervanging van WiFI componenten Zwolle en Overijssel wordt geen gebruik gemaakt HuaWei apparatuur.
- Aanleg van 5G telefoonnetwerk voor gemeente Zwolle zal plaatsvinden met in acht neming van de adviezen van de AIVD en de IBD omtrent gebruik van HuaWei componenten.

Openbaarheid
Openbaar

Datum 22 mei 2019

BIJLAGE 1. Informatie Beveiligingsdienst Gemeenten

Is Chinese technologie wel veilig?
Vanuit de politiek klinkt de roep om cruciale digitale infrastructuur te beschermen tegen Chinese betrokkenheid. Onze eigen inlichtingendienst AIVD waarschuwt in het recente jaarverslag voor het risico van Chinese spionage. Het kabinet werkt met acht ministeries aan een zogeheten China-strategie. Deze strategie gaat over het voorkomen van oneerlijke concurrentie en bedrijfsspionage door China. De IBD verwacht niet dat de kabinetsstrategie zich zal uitstrekken tot consumentenelektronica of losse randapparatuur. Vanuit gemeenten krijgen we de laatste tijd vragen over Chinese technologie, en of het nog wel slim is om bijvoorbeeld Huawei telefoons of een switch van een Chinese fabrikant aan te schaffen. De IBD acht het risico dat de Chinese overheid Nederlandse gemeenten via achterdeurtjes in apparatuur van Chinese makelij bespioneert laag. Gerichte spionage door staten of criminelen (ondermijning) is niet afhankelijk van de toevalligheid of een organisatie gebruik maakt van een bepaald product. Er wordt bij spionage vrijwel altijd gebruik gemaakt van kwetsbaarheden in de combinatie van mens en techniek.

Weerbaarheid tegen spionage
De IBD adviseert gemeenten ten aanzien van spionage het volgende:

- Versterk actief het bewustzijn (onder bestuurders, managers en medewerkers) met betrekking tot de waarde van de informatie waarover zij beschikken en van de mogelijke interesse van criminelen en buitenlandse overheden.
- Werk aan een veilige cultuur. Daarbij zijn gebruikers, de inrichting van gegevensstromen en databases en de gebruikte technieken voor detectie van incidenten belangrijke aandachtspunten.
- Veel belangrijker dan ‘de China-vraag’ bij aanschaf van nieuwe ICT-apparatuur is de vraag hoe lang een product ondersteund wordt door middel van software-updates vanuit de fabrikant. Na menselijke fouten ontstaan de meeste incidenten door misbruik van ongepatchte kwetsbaarheden in soft- en hardware. Het actueel houden van soft- en hardware verkleint niet alleen het risico op incidenten maar ook het risico op spionage door staten en criminelen.

Als u werkt aan deze drie aandachtspunten dan ziet de IBD geen bezwaren in de aanschaf ICT-apparatuur vanwege de nationaliteit van de fabrikant.