Gemeente Bergen op Zoom

Raadsfractie BSD
De heren Van der Kallen en Mulder
Nieuwstraat 4
4611 RS Bergen op Zoom

30 JAN. 2020

Uw kenmerk	20004, 20005 en 20007	Ons kenmerk	U20-000837	Datum	27 januari 2020
Uw brief	17, 18 en 19 januari 2020	Beh. door	J.L.G.M. Baaten, CISO	Doorkiesnr.	0164 - 277850
Onderwerp:	Kwetsbaarheden in Citrix	Afdeling	BD, Control & Audits	Bijlage(n)	

Geachte heren Van der Kallen en Mulder,

Naar aanleiding van uw brieven beantwoord ik graag uw vragen rondom de kwetsbaarheden van bepaalde producten / versies van Citrix. De brieven zijn beantwoord met de kennis van nu (27 januari).

Uw brief met kenmerk 200004 dd 17 januari 2020

1. Bent u op de hoogte van de gevaren op alle versies van het Citrix ADC en de Citrix Gateway servers?
   Ja, daarvan zijn wij op de hoogte.

2. Heeft uw college hier eenduidige coördinatie rondom opgezet?
   Ja, de coördinatie van security incidenten is structureel belegd bij onze Chief Information Security Officer (CISO). Hij heeft direct toegang tot het College en de directie.

3. Gebruikt de gemeente Bergen op Zoom, of gebruiken samenwerkende instanties rondom de gemeente dit systeem?
   Ja, wij passen Citrix software onder meer toe om op een veilige wijze applicaties en gegevens vanuit ons datacenter beschikbaar te stellen aan medewerkers die buiten het stadskantoor werken. Andere gemeenten, samenwerkend met en middels ICTWBW gebruiken ook producten van Citrix. Het beheer van deze omgeving is belegd bij ICTWBW.

4. Zo ja, zijn deze instanties ingelicht en op de hoogte van dit kritieke lek?
   Ja, ook zij zijn op de hoogte van de kwetsbaarheden.

5. Wanneer zijn deze instanties ingelicht en door wie?

Op 24 december 2019 zijn zowel de gemeenten als ICTWBW ingelicht door de Informatiebeveiligingsdienst (IBD, onderdeel VNG). Daarnaast staan de CISO's van de aangesloten gemeenten en ICTWBW dagelijks en direct met elkaar in contact.

6. Zo ja, is het gebruik van dit systeem opgeschort?

Op zaterdag 18 januari is Citrix 'uitgezet' en vervolgens op maandag 20 januari om 6:00u weer 'aangezet'. Vooralsnog wordt Citrix 's nachts (23:00u - 6:00u) uitgezet.

7. Zo niet, waarom niet?

nvt

8. Mocht er gebruik gemaakt worden en zijn van dit systeem, is er controle gedaan naar eventueel misbruik van dit lek?

De activiteit van de firewall wordt middels actieve analyse bewaakt.

9. Is hierbij data gestolen?

Daar zijn geen aanwijzingen van.

10. Is er getracht in te breken?

Uit de analyses van het inkomend internetverkeer blijkt dat er diverse pogingen zijn gedaan om onze systemen binnen te dringen. Deze pogingen zijn niet geslaagd.

11. Wie coördineert dit?

De coördinatie van security incidenten is structureel belegd bij onze Chief Information Security Officer. Hij heeft direct toegang tot het College en de directie en staat in directe verbinding met ICTWBW. De coördinatie van de technische uitvoering is belegd bij ICTWBW.

Uw brief met kenmerk 200005 dd 18 januari 2020

1. Heeft u wetenschap van dit AIVD ambtsbericht?

   nee

2. Op welke manier en via welke kanalen heeft u dit bericht ontvangen.

   Gemeenten worden primair door VNG Realisatie / Informatiebeveiligingsdienst geïnformeerd waarbij verwezen kan worden naar openbare informatie van NCSC.

3. Mocht de gemeente Bergen op Zoom intern, of extern, in partnerschap of out-source gegevens op hebben geslagen die van gevoelige aard zijn:

   - Is dit in kaart gebracht en zo ja, wanneer?

   Ja, wij houden continu zicht op eigen landschap van systemen, processen en informatie. En wanneer de gegevens door externen worden verwerkt, hebben we tenminste vanaf 2018 een aparte registratie in het kader van de AVG

   - Is hier over gecoördineerd en is dit genotuleerd?

   Ja, de enterprise architect coördineert dit voor de gehele organisatie en de Functionaris Gegevensbescherming waakt onder meer over het Register van Verwerkingen
   Daarbij kan geen sprake van notulering zijn. Wij beschikken ingevolge AVG over een Register van Verwerkingen en onderliggende Verwerkingsovereenkomsten.

   - Zo ja, kunt u daarvan een afschrift overleggen?

   Het register is openbaar en opvraagbaar bij de gemeente Bergen op Zoom conform artikel 6 van ons Privacybeleid.

   - Zo niet, waarom niet?

   Niet van toepassing

4. Zijn de systemen reeds offline gehaald en wanneer dan?

   Als u refereert aan systemen welke via Citrix Application Delivery Controller of Citrix Gateway ontsloten worden dan kan ik u melden dat de ADC en Gateway vanaf zaterdag 18 januari 2020 zijn uitgezet. Vanaf dat moment zijn deze systemen op werkdagen tussen 6:00u en 23:00u beschikbaar waarbij intensief gemonitord wordt. De achterliggende systemen zijn niet uitgeschakeld, zodat deze intern nog steeds beschikbaar zijn voor onze dienstverlening en bedrijfsvoering.

5. Zo niet, wanneer gaat dit gebeuren en kunt u laten weten of dit en wanneer dit dan ook gebeurd is uiteindelijk?

   Zie hierboven

6. Is er een mogelijkheid om de tijdslijn en geschiedenis van de ontwikkeling rondom dit voorval inzichtelijk te krijgen zodat er eventueel lessen getrokken kunnen worden voor in de toekomst?

   Major security incidents worden altijd geëvalueerd. Tijdens het incident worden de belangrijkste ontwikkelingen gedocumenteerd en na afloop van het incident wordt deze documentatie definitief gemaakt.

7. Is er contact geweest met de leverancier?

   Nee

8. Zo ja, kunt u de notulen van dit contact overleggen?

   Niet van toepassing

9. Zo niet, waarom niet?

   Gemeenten worden primair door IBD en NSCS geïnformeerd. Citrix levert éénzijdig adviezen over mitigerende maatregelen en te zijner tijd de patches.

10. Is er een mogelijkheid om als evaluatie deze casus te gebruiken om er met de politieke partijen lering uit te trekken in een vergadering waarbij ook eventueel de fractieassistenten aan deel kunnen nemen? (Ons bekend zijn er bij twee partijen fractieassistenten die meer kennis hebben van de ICT dan de duo's of Raadsleden).

    Grote (bijna-)incidenten worden immer zorgvuldig geëvalueerd, zo ook deze. Zo zullen we specifiek het besluitvormingsproces beschouwen om verbeteringen te identificeren. Natuurlijk staan wij er voor open om deze met de raad te delen.

11. Zijn de college leden beslagen met voldoende basale ICT kennis om de verantwoordelijkheid over deze ingewikkelde materie te willen, kunnen en durven dragen?

    Naar het oordeel van de CISO beschikt de portefeuille-houder over voldoende kennis om zijn verantwoordelijkheid in deze te nemen.

12. Is er iemand binnen het ambtelijk apparaat, of het college die de afweging gemaakt heeft om n.a.v. specialistische berichtgeving de systemen veiligheidshalve reeds eerder offline te halen? Zo ja, wanneer?

    Ja, op 17 januari. De CISO heeft intensief overlegd met de CISO's van ICTWBW en de andere aangesloten organisaties. Daarbij heeft ICTWBW expliciet aangegeven dat de door Citrix geadviseerde mitigerende maatregelen succesvol zijn getroffen en dat onze infrastructuur over meerdere 'lines of defence' beschikt. Daardoor heeft ICTWBW technisch het vertrouwen dat onze systemen veilig zijn. De door Citrix geadviseerde mitigerende maatregelen zijn reeds op 26 december 2019 getroffen. Eén en ander sluit naadloos aan op het advies van IBD en NCSC.

13. Zo niet, waarom niet?

    Niet van toepassing

Uw brief met kenmerk 200007 dd 19 januari 2020

1. In uw persbericht: ,, Vanaf afgelopen december zijn er diverse maatregelen genomen om aanvallen van 'buiten' te voorkomen ". Op welke maatregelen doelt u?

   Wij doelen daarmee op de mitigerende maatregelen zoals die door Citrix werden geadviseerd die ook door IBD en NCSC zijn geadviseerd.

2. In uw persbericht: ,, De verwachting is dat er maandag in de loop van de ochtend wel weer kan worden ingelogd. ". Kunt u tot in detail omschrijven hoe u tot deze conclusie komt?

   Uit het oogpunt van bedrijfsveiligheid duid ik dat graag op hoofdlijnen.
   Onze infrastructuur is zodanig opgebouwd dat er meerdere "lines of defence' zijn. Citrix vormt er daar één van. Door deze uit te schakelen, blijven vele andere systemen hun werk doen, alleen zijn deze niet meer van buiten af te benaderen. Op maandagochtend is deze 'poort' weer opengezet en werden alle digitale diensten en bedrijfsvoering weer zonder problemen benaderbaar zoals tevoren.

3. Bent u zich bewust dat een eventuele patch voor dit kritieke lek uitgebreid getest dient te worden en nog niet klaar is, of zijn onderhavige systemen gemitigeerd? Zo ja, zijn deze dan getest en door wie, hoe en wanneer?

   Wij zijn door NSCS geadviseerd om de patches van Citrix te vertrouwen. Na installatie worden testen uitgevoerd die gebruikelijk zijn bij een upgrade van firmware in dergelijke netwerkcomponenten. Aanvullend wordt van bepaalde toepassingen de basisfunctionaliteit getest.

4. Bent u niet van mening dat het terug in gebruik nemen misschien wel beter gecoördineerd kan worden met het Nationaal Cyber Security Centrum van de Rijksoverheid? Bent u bereid dit te overwegen en zo niet, kunt u tot in detail motiveren waarom u denkt dat de overweging van terug in gebruik name goed te kunnen overzien?

   Gemeenten worden primair door de Informatiebeveiligingsdienst (onderdeel VNG) geïnformeerd en geadviseerd waarbij verwezen kan worden naar openbare informatie van NCSC. Gemeenten besluiten in deze zelfstandig op basis van risico-afweging. Vroegtijdig implementeren van mitigerende maatregelen en de opbouw van onze infrastructuur liggen aan de basis van het besluit om Citrix tijdens 'extended office hours' beschikbaar te stellen.

5. Zijn de basale maatregelen om te kunnen overwegen het systeem weer in gebruik te gaan nemen genomen? Denk aan: aanpassing standaard poorten, clientcertificaten, webapplicatiefirewall en white en eventueel black-listing, eventueel via de gecontracteerde internet provider van de gemeente.

   Dergelijke mitigerende technische maatregelen zijn geëvalueerd en als nodig geïmplementeerd.

6. Beseft u zich dat de punten bij vijf geen zekerheid geven op veiligheid daar de leverancier eigenlijk met de handen in het haar zit nu en de gevolgen van het lek eigenlijk niet te overzien zijn? Bent u zich bewust van het feit dat de leverancier niet eenduidig is in de communicatie en dat hoogstwaarschijnlijk de Rijksoverheid het voorzorgprincipe heeft toegepast en de waarschuwing en later ook het advies heeft uitgerold. (Vandaar ons verzoek om punt 4 goed te overwegen of op zijn minst eerst in overleg te treden om hun kennis te onderzoeken).

   Wij zijn door NSCS geadviseerd om de patches van Citrix te vertrouwen. Wij hebben geen redenen om aan te nemen dat dat advies niet zorgvuldig en met voldoende kennis van zaken is opgesteld. Hoewel wij onder meer de door Citrix geadviseerde mitigerende maatregelen vroegtijdig hebben geïmplementeerd én onze infrastructuur over meerdere 'lines of defence' beschikt, hebben wij gemeend om het advies van de IBD en NCSC over preventief afsluiten te volgen: "Better safe than sorry".

   Uw suggestie om met het NCSC in overleg te treden om hún kennis te onderzoeken zou kunnen impliceren dat wij zelf over diepgaande technische kennis van deze materie beschikken. Deze kennis is doorgaans niet bij gemeenten aanwezig en juist daarom zijn samenwerkingen als IBD en NCSC ingericht.

7. Is het niet veiliger om alle medewerkers gewoon op het kantoor te laten inloggen en voor de noodzakelijke inloggers een alternatieve login op te zetten en de Netscaler uit te laten tot nader order?

   Wij hebben onder meer de door Citrix geadviseerde mitigerende maatregelen vroegtijdig geïmplementeerd én infrastructuur beschikt over meerdere lines of defence. Monitoring door ICTWBW heeft uitgewezen dat het aantal inbraakpogingen na zaterdag 19 januari tot nul is gedaald. Dat zijn voor ons overwegingen geweest om Citrix ADC en Citrix Gateway tijdens 'extended office hours' beschikbaar te houden en daarmee de continuïteit van de dienstverlening naar klanten en de continuïteit van de bedrijfsvoering in goede balans met de andere aspecten van informatie-veiligheid te houden.

Met vriendelijke groet,

het college van burgemeester en wethouders van Bergen op Zoom,
namens het college,

Dhr. A. Harijgens