gemeente
beverwijk

Z0699833B54

Aan de raad
van de gemeente Beverwijk

documentnummer
UIT-20-47918

zaaknummer
Z-20-67205

Beverwijk,
31 januari 2020

afdeling
Bedrijfsvoering

team
Informatieregie

behandeld door
P.B.M. Bakker

uw kenmerk/uw brief van

verzonden
04 FEB. 2020

onderwerp
Citrix kwetsbaarheid

Geachte raadsleden,

Er is de afgelopen weken veel media-aandacht geweest voor veiligheidsproblemen bij Citrix. Onze ambtelijke organisatie maakt voor thuiswerken gebruik van de Citrix Netscaler.

Uit onderzoek is gebleken dat onbevoegden toegang hebben gehad tot die Netscaler. Deze is op 14 januari 2020 vervangen. Er heeft vervolgens forensisch onderzoek plaatsgevonden. De resultaten van dit onderzoek treft u hierbij aan (IN-20-61620).

De belangrijkste conclusie uit dit onderzoek is dat geen indicaties zijn gevonden dat persoonsgegevens bekeken, onttrokken of gekopieerd zijn. Alleen de accountnaam van de niet meer in gebruik zijnde Netscaler is mogelijk bekeken.

Alle adviezen uit het onderzoek zijn met hoge prioriteit opgepakt.

Hoogachtend,
burgemeester en wethouders van Beverwijk,
de gemeentesecretaris, de burgemeester,

drs. E.R. Loenen drs. M.E. Smit

Bijlage(n): bevindingen onderzoek NFIR (IN-20-61620)

stationsplein 48
postbus 450
1940 al beverwijk
www.beverwijk.nl
info@beverwijk.nl
telefoon
0251 256256
fax 0251 256444

IT FORENSICS & INCIDENT RESPONSE

Gemeente Beverwijk
T.a.v. Dhr. P. Bakker
Postbus 450
1940 AL Beverwijk
Dit document is opgeleverd via Nextcloud

Den Haag, 31 januari 2020

Ons kenmerk : 20007 - Osnabrück
Betref : Bevindingen onderzoek

Geachte heer Bakker, beste Paul,

Op 24 december 2019 is bij Gemeente Beverwijk (de opdrachtgever) bekend geworden dat een kritieke kwetsbaarheid aanwezig was in de Citrix apparatuur (met als identificatienummer CVE-2019-19781). Naar aanleiding van deze bekendmaking heeft de Gemeente de door Citrix gepubliceerde mitigatiestappen genomen. De opdrachtgever heeft de externe leverancier tevens opdracht gegeven om die stappen ook op de nieuwe NetScaler-omgeving toe te passen.

Aanleiding voor nader onderzoek was dat op 20 januari 2020 idoor systeembeheerders van de opdrachtgever verschillende malafide programmatuur zijn waargenomen op de reeds uitgeschakelde oude NetScaler-omgeving. NFIR is gevraagd onderzoek te doen op de veiliggestelde gegevens van de opdrachtgever.

Samenvatting

Aan de hand van het door NFIR verrichte onderzoek, zijn de onderstaande onderzoeksvragen beantwoord.

1. Heeft daadwerkelijk ongeautoriseerd toegang plaatsgevonden op een van de Netscaler appliances?

Aan de hand van de onderzochte gegevens en middels het gebruikte plan van aanpak, is door NFIR geconstateerd dat ongeautoriseerde toegang is verkregen door aanvallers.

   a. Zo ja, op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk, dan wel netwerk?

Met behulp van de CVE-2019-19781 kwetsbaarheid is toegang gekregen tot de Netscaler met de naam 'BRANDGANS'.

b. Wanneer is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk, dan wel netwerk?

De eerste ongeautoriseerde activiteit die geconstateerd is, heeft plaatsgevonden op 10 januari 2020 om 21:41:24 uur (GMT +1). De eerste sporen van daadwerkelijke intrede zijn op 11 januari 2020 om 10:18:58 uur waargenomen in de logboeken van het onderzochte goed en bijbehorende back-ups.

c. Zo ja, is ongeautoriseerd toegang geweest tot andere geautomatiseerde werken, dan wel netwerk?

Na analyse van de daartoe beschikbare databronnen heeft NFIR geen indicaties gevonden dat aanvallers ongeautoriseerde toegang hebben verkregen tot andere geautomatiseerde werken[1] binnen haar netwerk.

2. Welke handelingen zijn uitgevoerd in het tijdsbestek waarin ongeautoriseerd toegang is verkregen?

Naar alle waarschijnlijkheid zijn commando's uitgevoerd waarmee getest is of de Netscaler kwetsbaar was voor CVE-2019-19781. Daarnaast is een automatische taak aangemaakt, die ieder minuut een bestand downloadt. Tot slot heeft NFIR geconstateerd dat twee verschillende cryptocurrency miners geïnstalleerd zijn.

a. Zijn er aanpassingen gemaakt in de configuratie op de Netscaler appliances?

In de veiliggestelde gegevensdragers is onderzoek verricht aan alle configuratiebestanden. De data en tijden van modificatie, als aangetroffen kopieën, zijn hierbij geanalyseerd. Aan de hand van dit onderzoek zijn geen indicaties gevonden van ongeautoriseerde configuratie aanpassingen op de Netscaler appliances.

3. In hoeverre is er sprake van malafide programmatuur?

Aan de hand van aangetroffen code vanuit open bronnen en overeenkomende acties op het onderzochte systeem, zijn met aan zekerheid grenzende waarschijnlijkheid twee verschillende cryptocurrency miners geïnstalleerd.

[1] Geautomatiseerd werk: Onder geautomatiseerd werk wordt verstaan een apparaat of groep van onderling verbonden of samenhangende apparaten, waarvan er één of meer op basis van een programma automatisch computergegevens verwerken (art. 80sexies, Sr.).

4. In hoeverre zijn gegevens ingezien, geëxtraheerd of gekopieerd?

Mogelijk is een configuratiebestand ingezien waarbij interne servernamen, IP-adressen en wachtwoorden in de vorm van een hashwaarde staan. Deze hashwaarde moet worden gekraakt om een leesbaar wachtwoord te krijgen. Afhankelijk van de sterkte van het wachtwoord kan dit enkele seconden of jaren duren. NFIR heeft verder geen indicaties gevonden dat – buiten accountnamen van administrators – persoonsgegevens zijn ingezien, geëxtraheerd of gekopieerd.

5. Indien gewenst, welke aanvullende mitigerende maatregelen kunnen genomen worden?

Tijdens en na afloop van het onderzoek zijn de volgende adviezen uitgebracht:

- *Schakel de Netscalers uit na het veiligstellen van de gegevens, tot deze voorzien zijn van de updates;*
- *Installeer de systemen met de laatste updates om de kwetsbaarheid 'CVE-2019-19781' te verhelpen;*
- *Vervang de certificaten die zijn aangetroffen op de Netscalers;*
- *Blijf de betrokken systemen na de nieuwe installatie monitoren op misbruik van kwetsbaarheden;*
- *Zorg dat de Netscaler logbestanden op een centrale locatie worden opgeslagen, waar ze voor een langere periode kunnen worden bewaard.*
- *Wijzig preventief de wachtwoorden van alle gebruikers die in het ns.conf bestand voorkomen en de (mogelijk) bijbehorende AD account(s)*

Hoogachtend,

Namens NFIR BV
Maaike Hielkema