Raad van de gemeente Beverwijk / Gemeenteraad
Postbus 450
1940 AL  BEVERWIJK

| | | |
|---|---|---|
| **documentnummer**<br>UIT-21-74187 / Z-21-78414 | **team**<br>Concern Control | **Beverwijk**<br>21 december 2021 |
| **uw kenmerk/uw brief van** | **behandeld door**<br>C.J.E. Stronkhorst | **verzonden**<br>22 december 2021 |

**onderwerp**
Vervolg hack IJmond Werkt!

Geachte raadsleden,

Eerder informeerden wij u via een raadsmemo op 28 september en 12 oktober over de hack bij IJmond Werkt!. Wij informeerden u onder andere over de hoofdlijnen en aanbevelingen van het rapport van Fox-IT, het bedrijf dat onderzoek deed naar de hack. Verder ging het memo over de heropbouw van de ICT-infrastructuur, het informeren van betrokkenen en de rol van de gemeenten in het vervolg. In dit raadsmemo geven wij u een nieuwe stand van zaken.

**Nog even in het kort**
De computersystemen van IJmond Werkt! zijn op 30 augustus 2021 getroffen door een aanval met gijzelsoftware. De hackers hebben bestanden versleuteld en gestolen. Na de hack heeft IJmond Werkt! het bedrijf Fox-IT in de arm genomen. Dit bedrijf ontdekte dat de hackers via een bestand op de server gevraagd hebben om contact met ze op te nemen, kennelijk met het doel om losgeld te eisen voor het ontsleutelen van de data. Dit contact heeft niet plaatsgevonden. Vervolgens hebben de hackers drie bestanden met gegevens van de fileserver van IJmond Werkt! op het darkweb gezet.

Fox-IT heeft onderzoek gedaan naar de hack. Het rapport is niet openbaar om te voorkomen dat derden inzicht krijgen in de netwerkstructuren van IJmond Werkt!. Raadsleden kunnen vanwege hun controlerende rol het onderzoek wel inzien bij IJmond Werkt!. Daarvoor maakt u een afspraak via info@ijmondwerkt.com. In de bijlage vindt u een publiekssamenvatting van het rapport van Fox-IT.

Fox-IT vermoedt dat de hackers naar binnen zijn gekomen door een combinatie van het ontbreken van een zogeheten tweefactorauthenticatie en zwakke wachtwoorden. Het clientvolgsysteem, dat niet gehackt is, heeft zo'n twee-factorauthenticatie wel.

Na het ontdekken van de hack zijn de experts van Fox-IT, de Informatiebeveiligingsdienst van de VNG, de Veiligheidsregio Kennemerland (VRK) en een kernteam van IJmond Werkt! en gemeenten aan de slag gegaan om de gevolgen van de hack zo klein mogelijk te houden, betrokkenen zo goed mogelijk te informeren en de ICT-omgeving weer op te bouwen. IJmond Werkt! heeft direct informatie op de website en via de media gedeeld. (Oud-) cliënten en (oud-)medewerkers hebben zo snel mogelijk een brief over de hack ontvangen en ook is er een callcenter actief.

**Aanpak heropbouw ICT-omgeving**
Aan de hand van de aanbevelingen van Fox-IT heeft de ICT-leverancier van IJmond Werkt! de nodige aanvullende beveiligingsmaatregelen genomen. Het gaat bijvoorbeeld om het verscherpen van het wachtwoordbeleid,
een meer uitgebreide logging op de systemen (bijhouden van gebeurtenissen) en het afsluiten van poorten voor toegang vanaf het internet. Deze maatregelen zijn getoetst door de CISO's (chief information security officer) van de gemeenten uit de gemeenschappelijke regeling. De maatregelen zijn akkoord bevonden voor de korte termijn. IJmond Werkt! kijkt ook nog naar aanvullende maatregelen zoals een geavanceerde tool op de server waarmee verdachte netwerkactiviteiten getraceerd kunnen worden.

Daarnaast wordt gewerkt aan een formeel vastgesteld informatiebeveiligingsbeleid. IJmond Werkt! koopt de ICT-beheerfunctie al jaren in bij een gespecialiseerd bedrijf. In samenspraak met dit bedrijf zijn de informatiebeveiligingsmaatregelen tot stand gekomen. Het uitvoeren van updates, het draaien van antivirussoftware en het maken van onsite- en offsite back-ups waren hier onderdeel van. De informatiebeveiligingsmaatregelen worden regelmatig gecontroleerd en waar nodig werd dit bijgesteld en bovendien voerde de controlerende accountant jaarlijks een audit uit. Dat was alleen nog niet vastgelegd in een informatiebeveiligingsbeleid en daar werkt IJmond Werkt! nu in afstemming met gemeenten hard aan.

**De bestanden op het darkweb**
In het vorige raadsmemo informeerden wij u dat de hackersgroep drie bestanden gepubliceerd had op het darkweb en dat het Fox-IT nog niet gelukt was om die bestanden te downloaden. Inmiddels zijn alle bestanden gedownload. Eenmaal uitgepakt gaat het om ruim 100 Gigabytes aan data. IJmond Werkt! is nog bezig met een analyse van deze bestanden. Eerst heeft IJmond Werkt! een inventarisatie gedaan naar de meest gevoelige data. Dan gaat het om paspoorten en identiteitsbewijzen. Naar aanleiding van deze doorzoeking zijn zestien mensen geïnformeerd dat er een kopie van hun identiteitsbewijs tussen de gepubliceerde data staat.

Het onderzoek richt zich nu vooral op de aanwezigheid van client- en medewerkersgegevens die in bestandslijsten zijn opgenomen. Denk daarbij aan naam, adres, BSN, contactgegevens, loonstroken en relatie met IJmond Werkt!. Hierna zal nog een analyse plaatsvinden om mensen te informeren van wie naast de bovengenoemde persoonsgegevens nog andere gegevens gepubliceerd zijn.

Alle betrokkenen worden geïnformeerd als uit de analyse naar voren komt dat gegevens van ze online staan. IJmond Werkt! houdt ook zelf de vinger aan de pols of er vreemde activiteiten plaatsvinden. Vooralsnog zijn er geen signalen van zulk soort activiteiten.

**Hack in de media**
De media hebben een aantal keer bericht over de hack bij IJmond Werkt. In een krantenartikel in het Noordhollands Dagblad van 6 november[1] ging het over een cliënt van IJmond Werkt!. Drie weken nadat zijn gegevens online stonden is hij via de telefoon afgeperst. Volgens de ouders heeft IJmond Werkt! onvoldoende rekening gehouden met de kwetsbaarheid van deze cliënt.
Naar aanleiding van het krantenartikel heeft IJmond Werkt een gesprek gehad met de ouders van deze medewerker. In dat gesprek was wederzijds begrip voor de situatie. De inschatting is dat het onwaarschijnlijk is dat het incident verband hield met de hack. Er zijn bijvoorbeeld geen andere signalen bekend van afpersing van personen waarvan ook gegevens zijn gelekt uit hetzelfde bestand als waar de betreffende cliënt in stond.
In het krantenartikel staat verder dat er meerdere meldingen en aangiften bij de politie zijn gedaan maar ook dat het niet duidelijk is welke te relateren zijn aan de hack van IJmond Werkt!. De politie heeft deze meldingen bij navraag door IJmond Werkt! niet aangetroffen.

**Evaluatie en onze rol in het vervolg**
We willen leren van deze hack en onze aanpak. Daarbij gaat het ons niet alleen om onze reactie na deze hack. Het gaat ons er bijvoorbeeld ook om hoe we ervoor zorgen dat de beveiligingsmaatregelen ook in de toekomst blijven voldoen en of we hier aanvullende afspraken over moeten maken met onze gemeenschappelijke regelingen. Zowel de VRK als de VNG voeren een evaluatie uit over de hack en onze aanpak. Als de resultaten van de evaluatie bekend zijn zullen wij u hierover informeren. Wij verwachten hier begin 2022 bij u op terug te komen. In het proces van evalueren nemen we ook de financiële afwikkeling van de hack en de nasleep mee. Wij rapporteren hier zo nodig ook over in de P&C-cyclus.

We streven ernaar dat alle betrokkenen zo goed mogelijk over de voortgang van de hack geïnformeerd blijven. Binnenkort gaat bijvoorbeeld nog een brief uit naar inwoners uit Beverwijk en Heemskerk die een Tozo-regeling hebben ontvangen en die ooit door IJmond Werkt! over een service geïnformeerd zijn. Daarnaast streven we ernaar dat IJmond Werkt! de nodige ondersteuning krijgt. Vanwege deze redenen is er een afstemmingsplatform tussen IJmond Werkt!, functionarissen gegevensbescherming en privacy officers van de gemeenten opgericht. Dit afstemmingsplatform vervangt het na de hack ingestelde crisisteam. Het afstemmingsoverleg blijft in ieder geval bestaan tot alle betrokkenen geïnformeerd zijn en tot alle openstaande acties afgerond worden, zoals de eerdergenoemde evaluatie.

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

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

Bijlage(n): Samenvatting Fox-IT rapport.

---

[1] https://www.noordhollandsdagblad.nl/cnt/dmf20211105_54996192?utm_source=google&utm_medium=organic

**Samenvatting rapport NCC/FOX-IT IJmond Werkt!**

**Inleiding:**
IJmond Werkt! heeft NCC/FOX-IT het Ransomware-incident dd. 6-9-2021 laten onderzoeken. Hieronder een korte samenvatting van het rapport van 28-9-2021. Deze samenvatting is tot stand gekomen in samenwerking met het IBD, de Infomatie Beveiligings Dienst van de Vereniging Nederlandse Gemeenten (VNG).

Het rapport is niet openbaar, om verschillende redenen. Enerzijds staan er aanbevelingen qua beveiliging in die IJmond Werkt! op dit moment nog aan het implementeren is. Anderzijds staat er bedrijfsgevoelige informatie in. Bovendien kan met het volledig vrijgeven IJmond Werkt! onbedoelde schade toegebracht worden omdat mogelijke technische kwetsbaarheden openbaar worden. Het is daarom zaak duiding te geven aan het rapport. Ook voor andere organisaties, zodat zij ook weten waar ze op moeten letten.

Het forensisch onderzoek kon slechts summier en zonder harde conclusies blijven door het ontbreken van voldoende logging, het onbruikbaar maken van backups en de versleuteling van bewijsmateriaal. Er staan daarom veel aannames in het rapport met waarschijnlijke oorzaken, waardoor een incident als dit zou kunnen zijn ontstaan. De aanvallers kregen **waarschijnlijk** toegang via een gebruikersaccount (niet voorzien van tweevoudige factorauthenticatie), die op dat moment open stond en waarschijnlijk beveiligd was met een makkelijk te raden wachtwoord. Via deze toegang zijn de nodige technische hacker-trucs gebruikt om uiteindelijk de beheerrechten te verkrijgen.

**Aanval**
De aanvaller maakte gebruik van Ransomware-as-a-service CONTI. Hiervoor is hoogstwaarschijnlijk gebruik gemaakt van de RDS infrastructuur (remote desktop services, voor beheer op afstand). Dit strookt met de bekende werkwijze van ransomware-criminelen. Hoewel er twee eerder verdachte activiteiten in het jaar 2020 zijn geconstateerd, dateren de vroegste indicatoren van dit misbruik leidend tot de geplaatste hack van 30-8-2021, waarop volgend op 5-9-2021 de ransomware is geactiveerd. Overigens is vastgesteld dat de twee verdachte activiteiten in het jaar 2020 niet tot vervolgacties hebben geleid.

**Data buitgemaakt**
Er is bewijs gevonden dat er op 30-8-2021 een upload tool is aangetroffen die waarschijnlijk is gebruikt voor het daadwerkelijk wegsluizen van de gestolen data. Deze tool betreft een soort dropbox clouddienst, genaamd “MEGA-upload”. Door de criminele organisatie is een dataset van ca. 85GB met de titel IJmondwerkt op een openbare downloadsite geplaatst. Daarbij geven ze aan dat het gaat om 100% van de buitgemaakte data.

**Data versleuteld**
Nadat de data is buitgemaakt zijn de bestanden versleuteld en de backups verwijderd. Wederom geven de onderzoekers weinig details door het ontbreken van logging en het feit dat met de bestanden ook het eventuele bewijsmateriaal is versleuteld.
Tijdens het onderzoek is gebleken dat er een Cobalt Strike toolkit is gebruikt om toegang te krijgen via een aantal Command and controlservers, te weten:

- lh1.lhsrvrs[.]net IP Address Cobalt Strike
- lh2.lhsrvrs[.]net IP Address Cobalt Strike
- lh3.lhsrvrs[.]net IP Address Cobalt Strike

**Acties en maatregelen**
In het hoofdstuk inperking, sanering en geleerde lessen staan korte termijn acties en maatregelen, alsmede aanbevelingen voor de langere termijn.

**NCC benoemt de volgende "inperkingen" (containment):**

- Stel alle wachtwoorden opnieuw in en maak gebruik van strenge wachtwoordregels (zoals minimaal 15 karakters).
- Schakel twee-factor-authenticatie (2FA/MFA) in voor alle accounts die extern te gebruiken zijn.
- Stel het KRBTGT-account twee maal opnieuw in, in geval de inrichting op het oude domein plaatsheeft; echter in geval van IJmond Werkt! is er sprake van een nieuw domein en dit dus niet van toepassing.
- Trek alle bestaande sessies voor extern beschikbare diensten in en laat ze opnieuw verbinden; in geval van IJmond Werkt! is dit niet van toepassing doordat een nieuw domein is ingericht.
- Blokkeer de IP-adressen en bestanden gebruikt door Conti [1].

**NCC benoemt de volgende "saneringen" (remediation):**

- Voorzie alle computersystemen van een geüpdatete anti-virusoplossing, in combinatie met Windows Defender.
- Bouw computersystemen opnieuw op waarvan is vastgesteld dat deze getroffen zijn door de ransomware.
- Beperk diensten met toegang tot internet; alleen servers die functioneel met internet moeten communiceren.
- Installeer alle computers van eindgebruikers opnieuw; in vervolg hierop heeft IJmond Werkt! opgeschaald door nieuwe Remote Desktop Serverhosts te installeren en in te richten.
- Controleer de Office 365 omgeving op ongewenste toegang en toegang tot gevoelige informatie; in vervolg op deze aanbeveling heeft IJmond Werkt! op basis van een nadere analyse de toegang verder ingericht.

**NCC benoemt de volgende "lessons learned":**

[1] De IBD acht het te smal om precies deze adressen te blokkeren, het is beter om in het algemeen gebruik te maken van beschikbare dreigingsinformatie. Het heeft immers weinig zin om alleen deze command & control servers te blokkeren en alle andere bekende servers door te laten.

- Wachtwoordbeheer en -toezicht was onvoldoende op orde om dit incident te voorkomen.
    - Advies: Gebruik “Microsoft Local administrator password solution”, een passwordmanager voor systeembeheerders.
- Logging en toezicht hierop was onvoldoende op orde om dit incident te kunnen waarnemen:
  Adviezen:
    - Gebruik een SIEM voor het signaleren van onregelmatigheden in verzamelde logfiles.
    - Configureer Powershell logging om misbruik hiervan tijdig te kunnen signaleren.
    - Installeer Microsoft SYSMON voor extra logging mogelijkheden.
    - Zorg voor voldoende opslagcapaciteit voor Windows logging.
- Generieke accounts werden gebruikt voor systeembeheer
    - Advies: Zorg dat accounts alleen rechten hebben die absoluut noodzakelijk zijn voor de rol en scheid de accounts per rol.
- Er was geen duidelijk incident responsplan
    - Advies: stel dit plan op voor toekomstige incidenten

Overige maatregelen wederopbouw ICT en veiligheid door IJmond Werkt!

- Alle punten hiervoor benoemd bij ‘containment’ en ‘remediation’ zijn door IJmond Werkt! geheel opgepakt, waarbij de volgende maatregelen als extra zijn toegevoegd:
- Als extra ten opzichte van de voorgestelde ‘containment’ is/ zijn:
    - nieuwe domeincontrollers geïnstalleerd;
    - een nieuwe Remote Desktop (RD) Gateway server geïnstalleerd;
    - nieuwe group-policies op basis van Microsoft Baseline voor de servers en gebruikers ingericht;
    - op dit moment werken ‘thuiswerkers’ op basis van een opgegeven thuis-IP adres op het netwerk van IJmond Werkt!;
    - conditionele toegang op MS 365 office is ingericht;
    - veilig mailverkeer via Zivver als standaard optie voor mailverkeer ingeregeld.
- Als extra ten opzichte van de ‘remediation’ is/ zijn:
    - ‘Intune’ ingeregeld ten behoeve van de centrale beveiliging en centraal kunnen beheren van de in gebruik zijnde laptops;
    - een nieuwe firewall die categorieën kan blokkeren in plaats van enkel individuele IP-adressen.
- De ‘lessons learned’ zijn ofwel inmiddels meegenomen ofwel in voorbereiding genomen om toe te voegen, waarbij met name de SIEM oplossing en het incident responsplan nog volgen.