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.

[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.

NCC benoemt de volgende "lessons learned":

- 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.