Rapportage zonder veiligheidsgevoelige informatie

Incident Response & Digitaal forensisch onderzoek

Klantnaam: Gemeente Hof van Twente

Datum: 08/03/2021

Versie: 1.0

Projectnaam: 20107 – Orly

Vertrouwelijk

Dit document is geclassificeerd als vertrouwelijk. De informatie in dit document en de bijbehorende bijlagen zijn alleen bedoeld voor Gemeente Hof van Twente. Het gebruik van dit document door een andere partij dan hiervoor genoemd is niet toegestaan, tenzij deze partij uitdrukkelijk is geautoriseerd door Gemeente Hof van Twente. De informatie in dit document is als vertrouwelijk gemarkeerd en valt onder de bepalingen van een geheimhoudingsovereenkomst.

Als u het gepresenteerde document onbedoeld ontvangt en/of u hebt geen toestemming om het document in uw bezit te hebben, verzoekt NFIR B.V. u om het document onmiddellijk te sluiten en terug te sturen naar NFIR B.V.

Elk misbruik van dit document of de informatie in dit document is niet toegestaan. NFIR B.V. aanvaardt geen aansprakelijkheid voor enig ongeoorloofd gebruik of misbruik van het gepresenteerde document door een derde partij of voor schade veroorzaakt door de inhoud van dit document.

Copyright © 2021 NFIR BV

Handelsnamen

NFIR en het NFIR-logo zijn handelsmerken van NFIR B.V. Alle andere handelsmerken in dit document zijn eigendom van de vermelde partijen.

Over NFIR

NFIR is een specialist in cyberbeveiliging. Bij NFIR zijn cyber-engineers in dienst: Hackers die weten wat ze doen, testers die de werking van ICT-infrastructuren en software begrijpen, privédetectives die, indien nodig, onderzoeken kunnen uitvoeren en adviseurs/consultants die u het juiste advies kunnen geven of die u kunnen ondersteunen bij een incident.

POB-vergunning

Het ministerie van Justitie en Veiligheid heeft NFIR een vergunning afgegeven, waardoor NFIR haar werkzaamheden mag uitvoeren. Deze vergunning betreft de POB-vergunning. De POB-vergunning dekt het verwerken van strafrechtelijke gegevens, waarmee NFIR in aanraking kan komen bij het uitvoeren van haar diensten.

Het POB-vergunningnummer van NFIR is: 1672.

Managementsamenvatting

Inleiding

Gemeente Hof van Twente (hierna: gemeente) heeft op 4 december 2020 NFIR B.V. (hierna: NFIR), naar aanleiding van een beveiligingsincident, verzocht incident response en digitaal forensisch onderzoek te verrichten.

Aanleiding van het verzoek van de gemeente is ontstaan op 1 december 2020. De ICT-infrastructuur bij de gemeente is getroffen door een ransomware-aanval, waardoor kritieke systemen en de bijbehorende data voor de bedrijfsvoering niet meer toegankelijk waren. NFIR heeft de gemeente ondersteund met een korte triage fase. Hierbij is vastgesteld dat een nieuwe server infrastructuur noodzakelijk was, gezien de wens van de gemeente om zo spoedig mogelijk weer met dienstverlening te kunnen starten. Tegelijkertijd was op de 'oude' infrastructuur het digitaal forensisch onderzoek gestart. NFIR heeft geadviseerd omtrent een veilige opbouw van de infrastructuur.

Situatie bij aanvang incident

Abstract gezien bestaat het netwerk van de gemeente deels uit servers op locatie van het gemeentehuis en uit een back-up-oplossing in een datacenter van de externe IT - dienstleverancier.

Uitgaande van de aanwezige documentatie, zouden er 124 fysieke en virtuele servers aanwezig moeten zijn. Omdat het netwerk niet meer functioneerde toen NFIR op locatie aankwam, kon er geen uitspraak worden gedaan over de juistheid van de beschikbare documentatie.

NFIR heeft vastgesteld dat er 89 virtuele servers niet meer aanwezig waren in het netwerk van de gemeente. Uit onderzoek is gebleken dat deze 89 virtuele servers verwijderd waren.

Dertien servers waren nog wel aanwezig in verschillende staten:

- Vijf servers waren versleuteld. Bestanden op versleutelde systemen konden niet meer worden geopend. Eén van de versleutelde servers betrof een back-upserver.
- De overige acht servers waren niet versleuteld. Het systeem kon worden opgestart en aanwezige bestanden konden worden gelezen. Deze servers bevatten informatie om het netwerk in technische zin te laten werken.

Gedurende het onderzoek heeft NFIR een sleutel ontvangen voor vier van de vijf versleutelde systemen. Van het vijfde systeem, de back-upserver, is geen sleutel ontvangen.

In totaal konden daarmee twaalf servers diepgaand worden onderzocht. Daarnaast waren logboeken beschikbaar van de firewall, fysieke servers en het opslagmedium.

Met deze beschikbare informatie zijn door NFIR onderstaande onderzoeksvragen beantwoord.

Conclusie

1. *Op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk, dan wel netwerk?*

Op basis van onderzoek aan de niet verwijderde servers en de firewall, is bevonden dat de aanvallers toegang hebben verkregen tot het netwerk van de gemeente via het Remote Desktop Protocol (RDP)[1]. Vanuit de configuratie in de firewall is vastgesteld dat een File Transfer Protocol (FTP)-server sinds 29 oktober 2019 via het internet toegankelijk is geworden. In de logboeken zijn miljoenen inlogpogingen waargenomen op de FTP-server: ook wel bekend als brute-force aanvallen. Bij een brute-force aanval worden combinaties van gebruikersnamen en wachtwoorden geprobeerd, tot een succesvolle inlogactie plaatsvindt. In de praktijk wordt regelmatig gebruik gemaakt van woordenboeken met daarin veelvoorkomende combinaties.

Het eerste moment van ongeautoriseerde toegang heeft plaatsgevonden met het account “testadmin”. Het wachtwoord van het “testadmin”-account was op 15 oktober 2020 gewijzigd naar “Welkom2020”.

Gezien de waargenomen brute-force aanvallen van buitenaf, is het waarschijnlijk dat het wachtwoord is geraden. Het “testadmin”-account had de hoogste rechten binnen het netwerk van de gemeente. Mede hierdoor konden de aanvallers zich direct vrij over het netwerk bewegen en malicieuze handelingen uitvoeren.

a. *Tot welke systemen is ongeautoriseerd toegang verkregen?*

Uit onderzoek aan de twaalf servers en logboeken uit de firewall, is gebleken dat ongeautoriseerde toegang heeft plaatsgevonden tot tenminste negen systemen. Op de overige drie servers zijn geen sporen aangetroffen van ongeautoriseerde toegang.

b. *Wanneer is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk?*

NFIR heeft door middel van forensisch onderzoek vastgesteld dat de aanvallers initieel toegang hebben gekregen tot het netwerk van de gemeente op 9 november 2020. Op dat moment werd voor het eerst ingelogd met het account “testadmin” op de FTP-server.

Vanaf 29 november 2020 werd via de FTP-server op diverse servers ingelogd binnen het netwerk “Hof-van-Twente”. De aanwezigheid van de aanvallers werd voor het laatst waargenomen op 1 december 2020.

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

De aanvallers hebben op verschillende momenten (in de periode van 9 tot en met 19 november 2020) software op de FTP-server geïnstalleerd met als doel om spam te versturen. Uit onderzoek aan de firewall is gebleken dat het versturen van spam door de firewall werd geblokkeerd.

Daarnaast hebben de aanvallers op 18 en 19 november 2020 vanaf vier verschillende servers verbindingen opgezet met een Command & Control server[2]. Deze verbindingen werden de nieuwe toegangsweg voor de aanvallers. Vervolgens hebben de aanvallers de initiële toegangsweg ontoegankelijk gemaakt.

[1] RDP staat voor Remote Desktop Protocol, in het Nederlands vaak "Extern bureaublad" genoemd. Dit protocol wordt gebruikt bij het overnemen van een pc op afstand.
[2] Command & Control server: Een centraal systeem die een aanvaller gebruikt om commando’s te sturen naar de systemen waarin door de aanvaller is ingebroken.

Op 30 november 2020 rond 22:00 uur zijn de aanvallers begonnen met de ransomware-aanval door het versleutelen van systemen en het verwijderen van 89 virtuele servers. De aanvallers lieten meerdere geprinte 'ransom notes'[3] achter op de printers en als bericht op versleutelde systemen, met als doel om de gemeente contact te laten zoeken met de aanvallers.

NFIR heeft vastgesteld dat een beperkte hoeveelheid gegevens zijn verzameld en weggesluisd door de aanvallers.

Uit analyse van de loggegevens van de firewall was niet vast te stellen welke informatie naar de aanvallers werd verzonden. De totale hoeveelheid aan verzonden- en ontvangen bytes betrof ongeveer 375MB tussen de servers en de aanvallers.

2. *Wie is verantwoordelijk voor het verkrijgen van ongeautoriseerde toegang, dan wel inzien, extraheren of kopiëren van gegevens?*

Het onderzoek heeft geen natuurlijke persoon aan kunnen wijzen als verantwoordelijke. Wel zijn er diverse aanknopingspunten gevonden die tot de verantwoordelijke zouden kunnen leiden. Deze aanknopingspunten zijn met de politie gedeeld.

3. *Had ongeautoriseerde toegang voorkomen kunnen worden?*

Ja, ongeautoriseerde toegang had voorkomen kunnen worden. Meerdere factoren hebben bijgedragen aan het ontstaan van het incident. Het gaat om de volgende technische- en beleidsfactoren:

- De FTP-server was toegankelijk vanaf het internet middels een open poort (RDP) – een aanvullende verificatie om in te kunnen loggen (tweefactor authenticatie) was niet ingericht.
    - Indien niet noodzakelijk is om dergelijke poorten via het internet beschikbaar te stellen, had ongeautoriseerde toegang voorkomen kunnen worden door periodiek controles uit te voeren op de firewall configuratie;
    - Indien dergelijke poorten wel bereikbaar dienden te zijn vanaf het internet, hadden aanvullende maatregelen (zoals tweefactor authenticatie) op beleidsmatig en technisch niveau moeten worden afgedwongen.
- Het wachtwoord "Welkom2020" voldeed aan het destijds door de gemeente gestelde wachtwoordbeleid (minimaal 8 karakters). Echter gaat het hier niet om individuele karakters, maar om een samenstelling van een veelgebruikt woord en een jaartal. Deze combinatie is niet geschikt om als wachtwoord te gebruiken.
    - Er had een specifieker wachtwoordbeleid opgesteld kunnen worden (waarin het gebruik van bepaalde generieke woorden verboden zijn) en dit beleid had dan zowel op technisch als beleidsniveau moeten worden afgedwongen.
- Het "testadmin" account had een dermate verhoogd rechtenprofiel (Domain Administrator-rechten), waardoor de aanvallers na het inloggen op dit account in staat waren om direct het volledige beheer van het netwerk over te kunnen nemen.
    - Een duidelijke organisatorische rechtenstructuur, beheer en toezicht op de Domain Administrators en het gebruik van een gelaagd rollenrechten-systeem – Role Based Access Control (RBAC) hadden kunnen voorkomen dat een onbevoegde beschikking kon krijgen over deze verhoogde rechten.

[3] Ransom note: een brief waarin gevraagd wordt om het betalen van losgeld.

- Door onvoldoende netwerksegmentatie (scheiding van communicatie tussen servers), was het mogelijk om verbinding te maken met andere servers binnen het netwerk van de gemeente vanaf de FTP-server.
    - Deze situatie had voorkomen kunnen worden door de servers op netwerkniveau van elkaar te scheiden (microsegmentatie) en enkel onderlinge communicatie toe te staan waar noodzakelijk.
- Een op verzoek van de gemeente uitgevoerde penetratietest heeft de kwetsbaarheden die hebben geleid tot het incident niet gedetecteerd.
    - Deze situatie had voorkomen kunnen worden door middel van een toetsbare penetratietest, waarin standaarden worden toegepast.
- Het actief en centraal monitoren van beveiligingsmeldingen (Security Operations Center (SOC)-dienstverlening) zou activiteiten, zoals de brute-force aanval op de FTP-server, tijdig aan het licht hebben gebracht;
    - Deze situatie had voorkomen kunnen worden door SOC-dienstverlening te introduceren die monitoring op beveiligingsniveau toepast.
- Doordat de aanvallers controle hadden over de systemen waarop de back-ups waren ingesteld, bleken zij in staat om back-ups te verwijderen.
    - Deze situatie had voorkomen door daadwerkelijk een back-up buiten het netwerk te bewaren, waardoor verlies van data te voorkomen was geweest. (Hierbij is het van belang dat beide back-ups geen onderlinge verbinding hebben met elkaar).

4. *In hoeverre kan een soortgelijke gebeurtenis in de toekomst voorkomen worden?*

Een soortgelijke gebeurtenis kan in de toekomst voorkomen worden door beleid, procedures en technisch passende maatregelen met elkaar in lijn te brengen – De gemeente krijgt hiermee meer grip op het creëren van een controleerbare IT-omgeving.

Daarnaast is het van belang om een regiefunctie in te richten met betrekking tot de externe IT-dienstleverancier door audits uit te voeren. Ook dienen duidelijke afspraken te worden gemaakt met leveranciers op adequate servicelevels.

Voor het voorkomen van incidenten in de toekomst is het van belang dat er een aantal basismaatregelen op het gebied van architectuur, beheer, detectie, preventie en respons worden toegepast. Door NFIR is in het hoofdstuk Aanbevelingen een uitgebreid advies gegeven over technisch passende maatregelen met betrekking tot deze onderwerpen. Hiermee kunnen risico's worden verkleind, IT-beveiligingsincidenten sterk worden beperkt en/of kan in het vervolg sneller worden ingegrepen.

Samenvattende rapportage

Dit samenvattend verslag is gebaseerd op de uitgebreide forensische rapportage, die NFIR heeft gemaakt. Een dergelijk verslag is naar zijn aard bedoeld om gebruikt te kunnen worden voor gerechtelijke procedures. Ze bevatten bijvoorbeeld daderkennis, maar ook mitigerende maatregelen en configuratieinformatie van systemen. Het naar buiten brengen van die gegevens kan zeer schadelijk zijn voor de gemeente en daarnaast zou – mocht er ooit toch een dader in beeld komen – een zaak kunnen frustreren. Waar het mogelijk is, is de informatie uit het bronrapport in deze samenvattende rapportage opgenomen.

Naast dit verslag is door de heer Brenno de Winter op basis van zijn expertise een duidingsrapportage geschreven. Deze omvat naast de kennis van het forensisch onderzoek ook informatie over de context van de aanval. Samen met deze rapportage wordt een waarheidsgetrouw beeld geschetst van de situatie ten tijde van het ransomware-incident bij de Hof van Twente in december 2020.

Inhoudsopgave

1 Inleiding

Gemeente Hof van Twente (hierna: gemeente) heeft op 4 december 2020 NFIR verzocht digitaal forensisch onderzoek en incident response te verrichten. De aanleiding voor dit verzoek was een aantal meldingen van medewerkers in de ochtend van dinsdag 1 december 2020. Om 8:45 uur deze ochtend is op basis van deze meldingen de conclusie getrokken dat er een serieus probleem was en vervolgens is om 9:00 het bedrijfscontinuïteitsplan in werking gezet. In overeenstemming met dit bedrijfscontinuïteitsplan is vervolgens een crisisteam geformeerd.

De interne ICT-beheerders van de gemeente zijn samen met de externe IT-dienstleverancier aan de slag gegaan, om te achterhalen wat de oorzaak was van het incident en in hoeverre gegevens te herstellen waren. Aan het einde van de dag werd duidelijk dat er externe hulp nodig was. Daarom heeft er communicatie plaatsgevonden richting het Nationaal Cyber Security Centrum (NCSC) en de Informatiebeveiligingsdienst (IBD) van de Vereniging Nederlandse Gemeenten (VNG). Op woensdag 2 december 2020 is, daaropvolgend, een melding gedaan bij de Autoriteit Persoonsgegevens.

De externe IT-dienstleverancier heeft opdracht gegeven aan een datarecovery bedrijf om versleutelde bestanden te herstellen. De lokale back-up bleek versleuteld en de externe back-up bleek verwijderd te zijn. De externe back-up oplossing (gedeelde omgeving waarop zich meerdere klanten bevonden) bevond zich in het datacenter van de externe IT-dienstverlener – waarbij er een verbinding opgebouwd werd met de omgeving van de gemeente.

Het Team Digitale Opsporing (TDO) van Politie Oost Nederland heeft de gemeente in de eerste dagen ondersteund bij het nemen van de mitigerende maatregelen en onderzoek. In deze rol was de politie aanwezig bij het intakegesprek met NFIR. Hierbij is afgesproken dat zodra malafide uitvoerbare bestanden werden aangetroffen, deze door NFIR ter beschikking zouden worden gesteld aan het TDO.

Na de intake is er een gesprek georganiseerd met de gemeente, de externe IT-dienstleverancier en het onderzoeksteam van NFIR, waarin er gezamenlijk is afgesproken met de betrokken partijen dat herstelwerkzaamheden (tijdelijk) gepauzeerd werden. Dit werd besloten om te voorkomen dat forensische sporen die onderzoek naar de toedracht mogelijk maakten, als gevolg van de herstelwerkzaamheden verloren zouden raken.

Omdat de exacte toedracht, wijze van intrede en geraakte systemen nog onderwerp van onderzoek was en de veiligheid van de systemen niet langer gegarandeerd kon worden, is ook afgesproken dat NFIR allereerst de toedracht onderzocht, waarna een advies zou worden uitgebracht over de resterende herstelwerkzaamheden en de condities waaronder dit kon gebeuren. De medewerking van de externe IT-dienstverlener in het verlenen van toegang tot de omgeving(en) en het uitvoeren van de eerste werkzaamheden was cruciaal, omdat deze over specifieke kennis en toegang beschikt over het netwerk. De nadruk lag op samenwerking, waarbij de advies-regierol in handen was van NFIR.

1.1 Doel

De doelstelling was tweeledig: enerzijds is een initiële triage uitgevoerd en zijn mitigerende maatregelen genomen (incident response; zie paragraaf 1.1.1), anderzijds is digitaal forensisch onderzoek uitgevoerd (zie paragraaf 1.1.2).

1.1.1 Incident Response

Primair is verzocht dat NFIR de gemeente adviseert over de wederopbouw van het IT-netwerk en daarnaast controleert of de stappen correct zijn uitgevoerd. Dit omvatte het toetsen van de voorgestelde aanpak van de externe IT-dienstleverancier op technische werkbaarheid en het adviseren over keuzes die bij de herinrichting van het netwerk gemaakt moesten worden. Het doel was om zo snel als mogelijk naar een werkbare situatie te komen.

Tot slot is door de gemeente gevraagd te onderzoeken waarom en hoe het incident plaats heeft kunnen vinden.

1.1.2 Digitaal forensisch onderzoek

Het doel van het forensisch onderzoek was om vast te kunnen stellen op welke wijze ongeautoriseerde toegang is verkregen tot het geautomatiseerde netwerk. Dit omvatte eveneens de momenten waarop de toegang heeft plaatsgevonden en de uitgevoerde malafide handelingen. Daarnaast had het onderzoek tot doel om vast te stellen in hoeverre gegevens door ongeautoriseerde personen zijn ingezien, gekopieerd, dan wel geëxtraheerd.

1.2 Onderzoeksvragen

Op basis van de intake zijn in overleg met de gemeente de volgende onderzoeksvragen opgesteld:

1. Op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk, dan wel netwerk?
    a. Tot welke systemen is ongeautoriseerd toegang verkregen?
    b. Wanneer is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk?
    c. Welke handelingen zijn uitgevoerd in het tijdsbestek waarin ongeautoriseerd toegang is verkregen?
2. Wie is verantwoordelijk voor het verkrijgen van ongeautoriseerde toegang, dan wel inzien, extraheren of kopiëren van gegevens?
3. Had ongeautoriseerde toegang voorkomen kunnen worden?
4. In hoeverre kan een soortgelijke gebeurtenis in de toekomst voorkomen worden?

1.3 Scope

Tijdens het incident zelf is door de externe IT-dienstleverancier en de interne ICT-beheerders van de gemeente is informatie aangeleverd over de aanwezige netwerkinrichting. Uit de documentatie bleek dat er twee verschillende technische omgevingen aanwezig waren, welke zijn onder te verdelen in twee verschillende onderdelen:

- Lokale netwerkinfrastructuur in het Gemeentehuis te Goor;
- Office365 omgeving.

De aangeleverde documentatie is door NFIR gebruikt om de reikwijdte van zowel de triage als het onderzoek vast te stellen. Aan de hand van de gestelde onderzoeksvragen is in dit hoofdstuk de gehanteerde scope beschreven.

1.3.1 Incident Response

De scope van het Incident Response traject omvatte de interne IT-infrastructuur, zowel intern als extern bereikbaar. Door de externe IT-dienstleverancier en de interne ICT-beheerders van de gemeente is informatie verstrekt aan NFIR over de (voorheen) aanwezige infrastructuur en koppelingen. Er is documentatie over de inrichting van het netwerk met NFIR gedeeld.

De ontvangen documentatie is in de eerste fase gebruikt ten behoeve van het beantwoorden van de onderzoeksvragen, alsmede het nemen van mitigerende maatregelen. Indien uit de triage zou blijken dat het onderzoek verder strekt dan de interne infrastructuur van de gemeente, zouden deze gegevens verdiepend worden onderzocht als onderdeel van het digitaal forensisch onderzoek.

Het Incident Response traject vond plaats op locatie bij de opdrachtgever, in een actieve samenwerking met alle betrokken partijen.

1.3.2 Digitaal forensisch onderzoek

De scope van het digitaal forensisch onderzoek richtte zich allereerst op de besmette omgevingen. Omgevingen zijn door NFIR geïdentificeerd als zijnde besmet op het moment dat sprake is van versleuteling, dan wel het onverklaarbaar ontbreken (verwijderen) van gegevens. Vervolgens is vastgesteld in hoeverre laterale beweging mogelijk was naar andere delen van het netwerk.

De clouddiensten (te denken aan de Office365 omgeving in gebruik bij de gemeente) vielen buiten scope van het digitaal forensisch onderzoek, omdat de Office365 omgeving in de periode voor het incident niet of zeer gering werd gebruikt voor het opslaan van informatie. Doordat niet meer veilig kon worden gewerkt op de lokale netwerkinfrastructuur van de gemeente naar aanleiding van het incident, is de Office 365 omgeving in gebruik genomen zodat de gemeente haar mail-functionaliteiten kon hervatten. Op de verschillende Office365 accounts werd op het moment van het incident geen multi-factor authenticatie (ook wel MFA, tweefactor authenticatie of 2FA) afgedwongen. NFIR heeft geadviseerd in het nemen van mitigerende maatregelen, zoals het afdwingen van multi-factor authenticatie, voor deze omgeving om ervoor te zorgen dat op een veilige manier kon worden doorgewerkt.

Verdiepend onderzoek richtte zich op accounts en servers, waarop malafide inlogacties hebben plaatsgevonden. Hetzelfde gold voor de infrastructuur waarop mogelijk laterale beweging heeft plaatsgevonden. De gegevens die zijn onderzocht, omvatten met name logboeken en gebruikersprofielen van gecompromitteerde (gehackte) gebruikers.

Om de onderzoeksvragen te kunnen beantwoorden heeft NFIR-onderzoek verricht op basis van technische sporen. Dit onderzoek was niet gericht op onderlinge afspraken, relaties en verantwoordelijkheden van partijen die waren betrokken bij de inrichting en beheer van het netwerk van de gemeente. Indien er aanwijzingen zouden zijn die mogelijk kunnen leiden tot een verdachte van een misdrijf, zouden deze worden gerapporteerd ten behoeve van het strafrechtelijke onderzoek.

1.4 Methodiek

1.4.1 Werkwijze incident response

Een Incident Response traject is gericht op het identificeren van een incident en vervolgens het beperken van daaruit voortvloeiende schade. De gemeente had concrete aanwijzingen dat onbevoegden toegang hebben gehad tot het netwerk. Middels triage is door NFIR vastgesteld op welke manier onbevoegden in het netwerk zijn gekomen, is advies gegeven over op welke manier de toegang kon worden ontzegd en is vervolgens geverifieerd of de genomen maatregelen toereikend waren.

NFIR heeft eerste indicatieve bevindingen gedeeld met de gemeente. In kader van incident response heeft NFIR deelgenomen aan crisis overleggen op locatie. Deze overleggen hebben plaatsgevonden in de periode 6 december 2020 tot en met 11 december 2020.

1.4.2 Procedure digitaal forensisch onderzoek

Op basis van de onderzoeksvragen zijn de volgende vier fasen gedefinieerd om deze vragen te beantwoorden:

- Fase 1: Gegevens veiligstellen
- Fase 2: Transport naar forensisch laboratorium
- Fase 3: Forensisch onderzoek
- Fase 4: Rapportage

Deze fasen worden hieronder beschreven en geven een helder kader over de uitvoering van het forensisch onderzoek. Het digitaal forensisch onderzoek heeft plaatsgevonden in de periode 5 januari 2021 tot en met de oplevering van het conceptrapport (15 februari 2021).

1.4.2.1 Fase 1: Gegevens veiligstellen

In een digitaal forensisch onderzoek is het essentieel om alle gegevens veilig te stellen, inclusief verwijderde gegevens. NFIR volgt internationale forensische richtlijnen door alle beschikbare gegevens volledig en ongewijzigd veilig te stellen met behulp van transparante en verifieerbare processen. Op deze manier kan NFIR de integriteit van de gegevens garanderen en kunnen de gegevens worden gebruikt als toelaatbaar bewijsmateriaal voor de rechtbank, mocht dit nodig zijn.

1.4.2.2 Fase 2: Transport naar forensisch laboratorium

Om gegevens effectief en efficiënt te kunnen onderzoeken, wordt gebruik gemaakt van een forensisch laboratorium. Dit laboratorium bevat ICT-infrastructuur die is ingericht om (grote hoeveelheden aan) gegevens inzichtelijk te kunnen maken.

Hierdoor dienen deze gegevens getransporteerd te worden naar het laboratorium. Vanwege het bijhouden van een zogenaamde ‘Chain of Custody’ en een ‘Chain of Evidence’ is in forensische rapportage opgenomen op welke wijze deze gegevens zijn getransporteerd, door wie en wanneer.

1.4.2.3 Fase 3: Forensisch onderzoek

NFIR maakt gebruik van apparaten en software die internationaal worden geaccepteerd voor gebruik bij digitaal onderzoek en die hun effectiviteit en efficiëntie hebben bewezen.

1.4.2.4 Fase 4: Rapportage

Alle bevindingen zullen worden samengebracht in een compleet en helder uitgewerkt rapport. Dit rapport bevat een beschrijving van de bevindingen, de conclusies op basis van de bevindingen en aanbevelingen. Het rapport wordt allereerst in concept gedistribueerd volgens de distributielijst, waarna de ontvangers een mogelijkheid krijgen tot het geven van een reactie.

2 Conclusie

Op basis van het onderzoek zijn de volgende onderzoeksvragen beantwoord:

1. *Op welke wijze is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk, dan wel netwerk?*

De aanvallers hebben toegang verkregen tot het netwerk van de gemeente via het Remote Desktop Protocol (RDP). Via RDP kan een server op afstand, via het internet, beheerd worden. De server FTP-server was voor iedereen op het internet via RDP benaderbaar. Het eerste moment van ongeautoriseerde toegang heeft plaatsgevonden met het account “testadmin”. Het wachtwoord van het “testadmin”-account was op 15 oktober 2020 gewijzigd naar “Welkom2020”.

Het is aannemelijk dat dit wachtwoord voorkomt op wachtwoordlijsten, omdat dit wachtwoord bestaat uit het veel gebruikte woord “Welkom” in combinatie met het jaartal van dat moment “2020”. Gezien de waargenomen brute force-aanvallen van buitenaf, is het waarschijnlijk dat het wachtwoord is geraden. Het “testadmin”-account had de hoogste rechten binnen het netwerk van de gemeente. Hierdoor hadden de aanvallers direct volledige controle over het gehele Windows domein “hof-van-twente”.

a. *Tot welke systemen is ongeautoriseerd toegang verkregen?*

Forensisch onderzoek heeft uitgewezen dat ongeautoriseerd toegang is verkregen tot tenminste negen systemen.

Op andere servers kon geen forensisch onderzoek worden verricht, omdat deze servers versleuteld en/of verwijderd zijn door de aanvallers.

b. *Wanneer is ongeautoriseerd toegang verkregen tot het geautomatiseerd werk?*

NFIR heeft door middel van forensisch onderzoek vastgesteld dat de aanvallers initieel toegang hebben gekregen tot het netwerk van de gemeente op 9 november 2020. Op dat moment werd voor het eerst ingelogd met het account “testadmin” op de FTP-server.

Vanaf 29 november 2020 werd via de FTP-server op diverse servers ingelogd binnen het netwerk van de gemeente. De aanwezigheid van de aanvallers werd voor het laatst waargenomen op 1 december 2020.

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

De aanvallers installeerden in de eerste periode van 9 tot en met 19 november 2020 verschillende software tools op de FTP- server. De tools die zijn geïnstalleerd hadden als doel om spam te versturen, blijkt uit onderzoek aan de bestanden. Echter, uit onderzoek aan de firewall is gebleken dat het versturen van spam door firewall is geblokkeerd.

Op 18 en 19 november 2020 zijn verbindingen opgezet met een Command & Control server vanaf vier verschillende servers. Eén van deze servers bleek ontoegankelijk gemaakt te zijn. Hierdoor konden zowel de beheerders als andere mogelijke aanvallers geen gebruik maken van het gecompromitteerde account: “testadmin”.

Op 21 november 2020 is de gebruiker “admin.mmc” aangemaakt en vervolgens gebruikt voor het verdere verloop van de aanval. Het “testadmin” account is eveneens aangepast door de aanvallers, zodat deze niet meer kon inloggen van buitenaf en de logs zijn verwijderd van de FTP-server.

De handelingen die hierna volgden waren doelgericht: *het verkennen van het netwerk ter voorbereiding van een ransomware aanval.* Op 30 november 2020 rond 22:00 uur zijn enkele malafide bestanden en scripts uitgevoerd. Door onder andere gebruik te maken van de malafide bestanden en scripts, zijn netwerkscans uitgevoerd, back-ups uit het datacenter verwijderd, vijf systemen inclusief het lokale back-upsysteem versleuteld, 89 virtuele machines verwijderd en is een ransom note uitgeprint op de printers. Op een netwerk opslagsysteem (NAS) is de hostnaam aangepast naar [deze naam komt overeen met een naam die elders in het onderzoek is aangetroffen].

Eén van de laatste handelingen van de aanvallers was het verwijderen van de eigen geplaatste tools, die waren geïnstalleerd op de FTP-server, met een programma dat herstel van verwijderde bestanden nagenoeg onmogelijk maakt.

2. ***Wie is verantwoordelijk voor het verkrijgen van ongeautoriseerde toegang, dan wel inzien, extraheren of kopiëren van gegevens?***

Het onderzoek heeft geen natuurlijke persoon aan kunnen wijzen als verantwoordelijke. Wel zijn er diverse aanknopingspunten gevonden die tot een verantwoordelijke zouden kunnen leiden. De belangrijkste aanknopingspunten zijn in de volledige rapportage benoemd. Deze aanknopingspunten zijn met de politie gedeeld.

3. ***Had ongeautoriseerde toegang voorkomen kunnen worden?***

Toegangsbeheer

De inrichting van de infrastructuur van de gemeente heeft bijgedragen aan ongeautoriseerde toegang door de aanvallers. De firewall, tussen de FTP-server en het internet, was onvoldoende beveiligd waardoor toegang tot verschillende diensten mogelijk was, waaronder het Remote Desktop Protocol. Dit was toegankelijk voor alle IP-adressen van het internet. Het account “testadmin” is gebruikt voor ongeautoriseerde toegang. Naar alle waarschijnlijkheid was dit mogelijk doordat een eenvoudig te raden wachtwoord was ingesteld en geen multi-factor authenticatie is toegepast. Daarnaast had het “testadmin” account de hoogste vorm van rechten binnen het netwerk van de gemeente (namelijk: Domein Admin rechten). De combinatie van de bovengenoemde factoren heeft geleid tot de initiële ongeautoriseerde toegang.

Segmentatie

Het netwerk was plat ingericht, wat inhoudt dat vrijwel alle systemen toegang tot elkaar hadden. Doordat de FTP-server vanaf het internet bereikbaar was, kon deze server eenvoudig als springplank gebruikt worden om alle andere servers binnen het netwerk te benaderen.

Er zijn verschillende best-practices om netwerksegmentatie in te richten, onder andere van Carnegie Mellon University(CMU)[4], het Center for Internet Security(CIS)[5] en KPN[6]. Aanvullend kan een zero-trust architectuur [7] de operationele impact van succesvolle aanvallen minimaliseren.

[4] Carnegie Mellon University Network Segmentation Practics, https://insights.sei.cmu.edu/sei_blog/2020/10/network-segmentation-concepts-and-practices.html
[5] CIS Controls, https://www.cisecurity.org/controls/controlled-access-based-on-the-need-to-know/
[6] KPN Security Zoning, https://ciso-ksp.kpnnet.org/document/detail?id=KSP-RE-287&filters=&offset=0&query=network+zoning

[7] Palo Alto Networks – Zero trust Architecture, https://www.paloaltonetworks.com/cyberpedia/what-is-a-zero-trust-architecture

Penetratietesten/Security Audits

Door een extern bedrijf is in de periode van juni 2020 een penetratietest uitgevoerd, deze penetratietest vond plaats in de periode dat de FTP-server bereikbaar was vanaf het internet. n de scope is ook het IP-adres opgenomen vanaf waar de FTP-server bereikbaar was via het internet. De bovengenoemde problemen (namelijk een server bereikbaar via RDP vanaf internet) zijn echter niet aan het licht gebracht. Deze informatie is mogelijk niet gezien of niet goed gerapporteerd. Er is geen informatie verstrekt aan NFIR over wat er met de resultaten van de penetratietesten is gedaan.

Het periodiek uitvoeren van penetratietesten dienen problemen en mogelijke dreigingen aan het licht te brengen. De gemaakt afspraken en scoping is daarbij van groot belang.

Daarbij is het van belang dat als er een penetratietest uitgevoerd wordt dat deze dan voldoet aan open en verifieerbare standaarden.

Het is bijvoorbeeld gangbaar dat de Penetration Testing Execution Standard – PTES ingezet wordt voor het testen infrastructuur, de Open Web Application Security Project – OWASP voor webapplicaties en de Common Vulnerability Scoring System - CVSS om de kwetsbaareden op risico-niveau te classificeren).

Het vastleggen van de resultaten van het onderzoek dient te worden gedaan in de rapportage (toetsend in de rapportage aan de checklists van de open standaarden).

Monitoring

Het netwerk werd onvoldoende gemonitord. Dit heeft betrekking op de hoeveelheid en intensiteit van de monitoring. Gedurende de aanval zijn er verschillende signalen geweest zowel op systeem- als netwerklaag. Eén daarvan is bijvoorbeeld de aanwezige brute force-aanvallen op de server, antivirus- en netwerklogs, alsmede het uitvoeren van scans van het interne netwerk. Wanneer actief zou worden gemonitord, had dit mogelijk geresulteerd in het eerder ontzeggen van toegang voor de onbevoegde en mogelijk zelfs de uitvoer van de ransomware voorkomen.

Firewall

Een tijdige en volledige security audit op de firewall regels had kunnen onderkennen dat de FTP-server via het RDP-protocol gekoppeld was aan het internet, zodat ook hier maatregelen tegen genomen hadden kunnen worden.

Back-ups

Gedurende het onderzoek bleken twee back-ups aanwezig in de periode voor de aanval: lokaal en off-site. Doordat de aanvallers controle hadden over de systemen waarop de back-ups zijn ingesteld, bleken zij in staat om opdracht te geven om off-site back-ups te verwijderen. De lokale back-ups waren versleuteld. Doordat er geen andere kopieën (zoals bijvoorbeeld offline-kopieën) werden bewaard van de back-ups, was herstel niet mogelijk.

Door het implementeren van authenticatie met bijvoorbeeld multi-factor Authenticatie en/of geen autorisaties toekennen van lokale systemen voor het uitvoeren gevoelige opdrachten, had voorkomen kunnen worden dat lokaal een opdracht kon worden gegeven om off-site back-ups te verwijderen.

4. *In hoeverre kan een soortgelijke gebeurtenis in de toekomst voorkomen worden?*

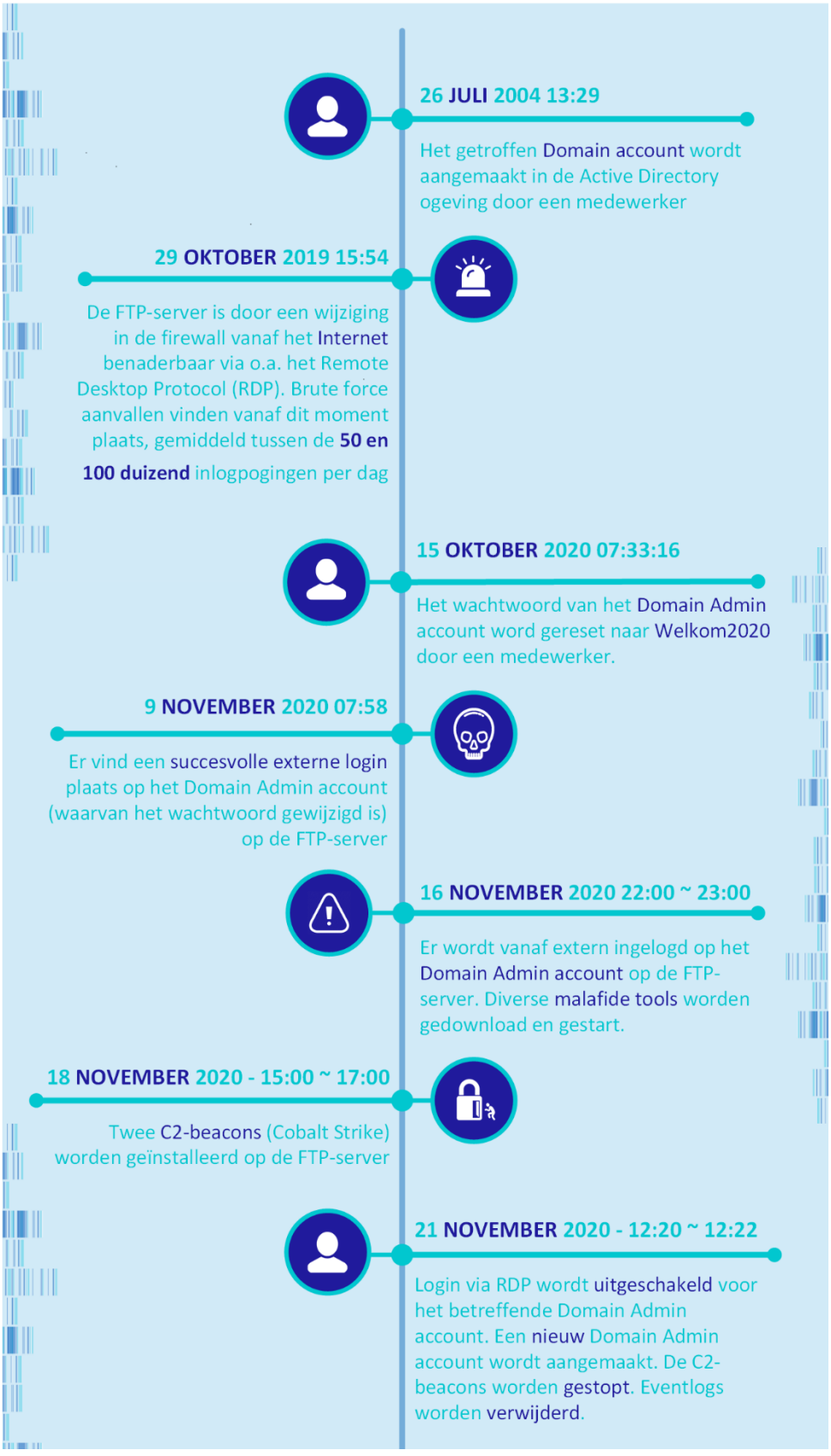
Een soortgelijke gebeurtenis kan in de toekomst voorkomen worden door beleid, procedures en technisch passende maatregelen met elkaar in lijn te brengen – De gemeente krijgt hiermee meer grip op het creëren van een controleerbare IT-omgeving.

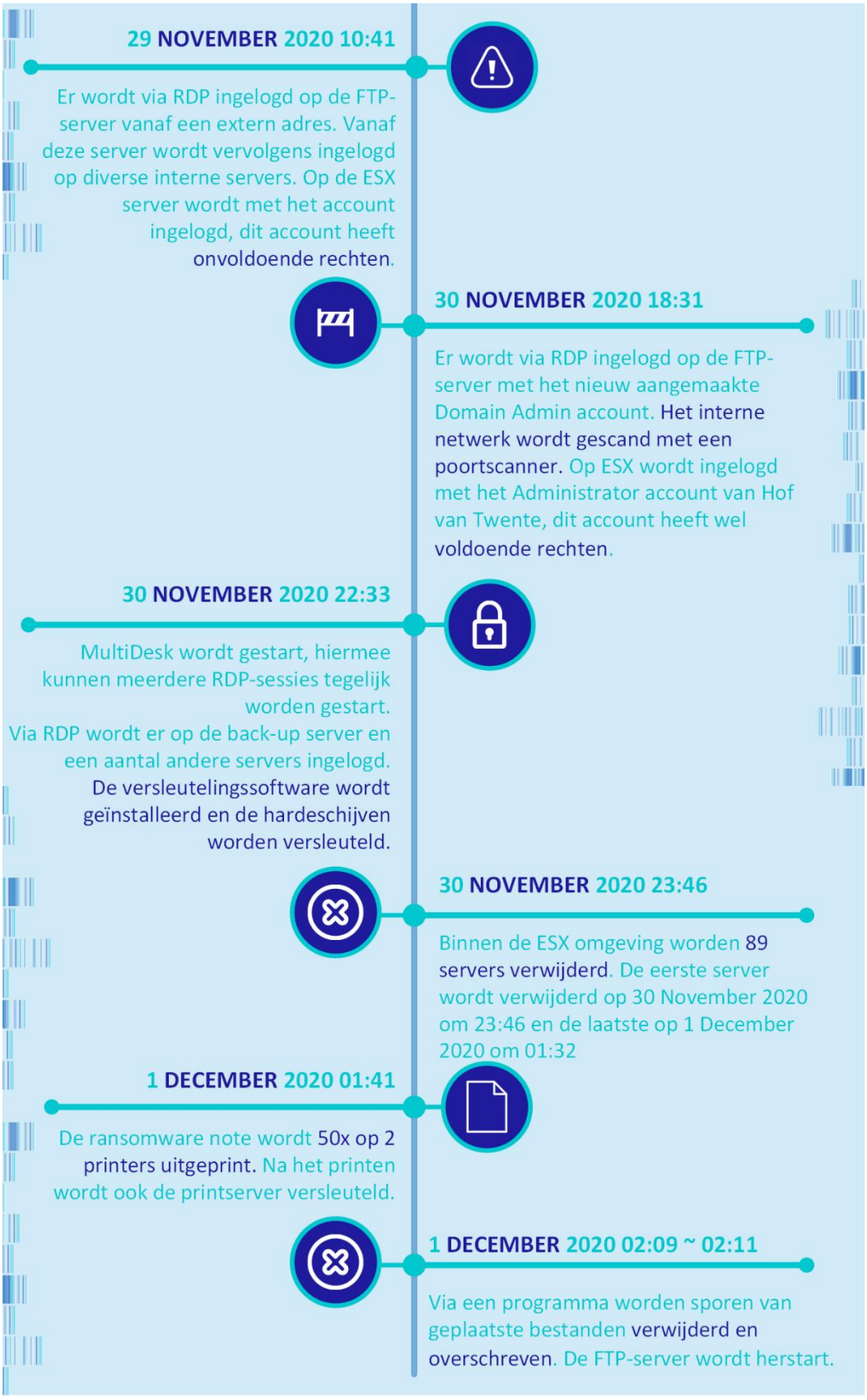
Daarnaast is het van belang om een regiefunctie in te richten met betrekking tot de externe IT-dienstleverancier door audits uit te voeren. Ook dienen duidelijke afspraken te worden gemaakt met leveranciers op adequate servicelevels.

Voor het voorkomen van incidenten in de toekomst is het van belang dat er een aantal basismaatregelen op het gebied van architectuur, beheer, detectie, preventie en respons worden toegepast. Door NFIR is in het hoofdstuk Aanbevelingen een uitgebreid advies gegeven over technisch passende maatregelen met betrekking tot deze onderwerpen. Hiermee kunnen risico's worden verkleind, IT-beveiligingsincidenten sterk worden beperkt en/of kan in het vervolg sneller worden ingegrepen.

2.1 Tijdslijn

In Figuur 1 worden de belangrijkste gebeurtenissen in een tijdslijn weergegeven:





Figuur 1 – Tijdslijn van bevindingen uit het rapport

3 Aanbevelingen

In dit hoofdstuk worden aanbevelingen gegeven gebaseerd op het onderzoek en de getroffen mitigerende maatregelen. Deze aanbevelingen zijn van belang om toekomstige incidenten tijdig te ondervangen en voorkomen. NFIR adviseert om die reden onderstaande maatregelen. Dit hoofdstuk is onderverdeeld in drie categorieën: preventie, detectie en response.

3.1 Preventie

In deze paragraaf worden preventieve maatregelen besproken ter voorkoming van incidenten.

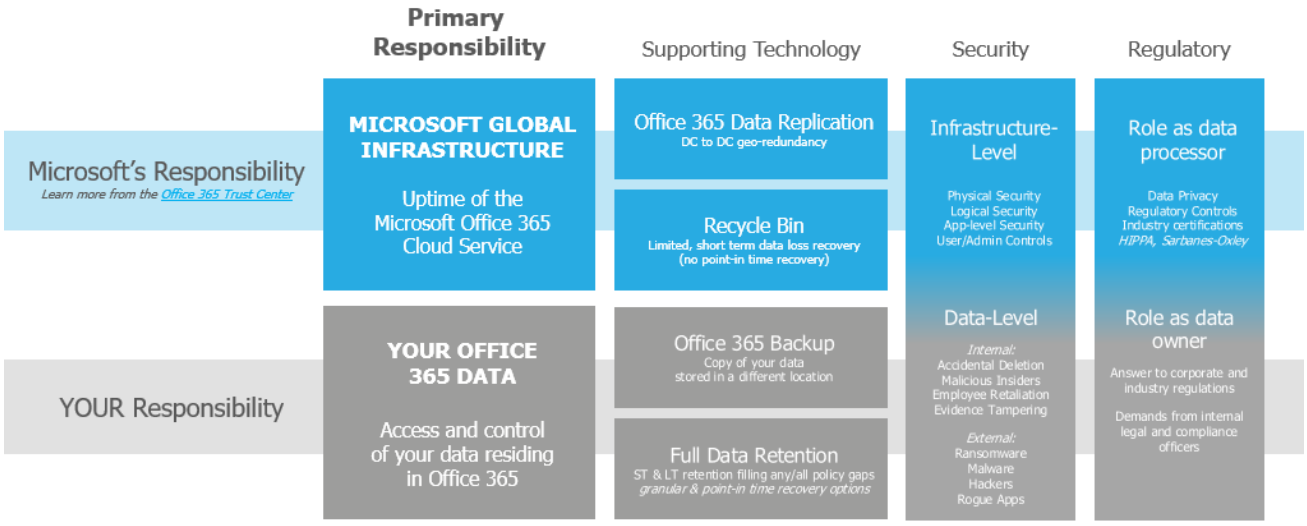
3.1.1 3-2-1 principe

NFIR adviseert het toepassen van een 3-2-1 back-up principe staat voor 3 kopieën van de data, waarbij 2 kopieën op verschillende data dragers staan en 1 kopie op een andere locatie wordt bewaard. Wanneer dit principe goed geïmplementeerd is kan een men bij een ransomware aanval altijd eenvoudig terugschakelen naar de oude situatie met een beperkt verlies van data. Hierbij dienen de juiste authenticatie en autorisaties te zijn ingericht. Een nuttige handreiking is recentelijk door de IBD geboden voor het inrichten volgens het 3-2-1- principe.[8]

Met een werkende off-site backup had de door deze aanval verloren data grotendeels kunnen worden hersteld.

Wat betreft de back-ups van de Office 365 omgeving, is op basis van de gesprekken met de beheerders vastgesteld dat er geen back-up oplossing is ingericht. Volgens de documentatie van Microsoft, welke door VEEAM is gepubliceerd op haar website[9], is het de verantwoordelijkheid van de organisatie om een dergelijke back-up oplossing te implementeren. NFIR adviseert daarom om te verifiëren of er een back-up oplossing is voor Office365. Indien dit niet mogelijk is, zal geadviseerd worden om deze zo snel mogelijk te implementeren om eventuele risico's op dataverlies te minimaliseren.

[8] https://www.informatiebeveiligingsdienst.nl/product/back-up-en-recovery-gemeente/
[9] https://www.veeam.com/blog/office365-shared-responsibility-model.html



Figuur 2 – Office 365 Verantwoordelijkheden

3.1.2 Toegangsbeleid

Een strak toegangsbeleid zorgt ervoor dat bepaalde rechten niet zomaar een diverse accounts worden toegekend. Wanneer multi-factor authenticatie wordt gebruikt, zijn gelekte of geraden wachtwoorden geen probleem, omdat de aanvallers niet over de multi-factor beschikten. Tevens wordt aangeraden om een wachtwoordbeleid af te dwingen dat gebruik van eenvoudig te raden wachtwoorden weet te voorkomen.

3.1.3 IT-security beleid

Een duidelijk IT-security beleid zorgt ervoor dat er weloverwogen keuzes worden gemaakt bij de inrichting van het netwerk en het gebruik van het netwerk. Wanneer hier duidelijk over wordt gecommuniceerd met medewerkers zal dit voor een algeheel verhoogd veiligheidsniveau zorgen.

3.1.4 Segmentatie

Het is belangrijk om een netwerk gesegmenteerd in te richten zodat niet alle servers en alle data in één keer getroffen worden bij een aanval. Segmentatie moet zorgdragen dat bij een aanval slechts één of enkele servers worden getroffen en niet de gehele infrastructuur.

3.1.5 Security awareness trainingen

Training kan ervoor zorgen dat het algehele securityniveau van de organisatie omhooggaat en medewerkers beter beschermd zijn tegen phishing en getraind worden in het gebruik van goede wachtwoorden.

3.1.6 Security audits/penetratietesten

NFIR adviseert om periodiek security audits/penetratietesten uit te voeren. Door middel van security audits/penetratietesten kunnen dreigingsrisico's vroegtijdig aan het licht komen en worden aangepakt. Het periodiek uitvoeren van security audits is van belang vanwege het dreigingslandschap dat continue veranderd.

3.2 Detectie

In deze paragraaf worden detectie maatregelen besproken, voor het tijdig herkennen van IT-beveiligingsincident.

3.2.1 Actieve monitoring netwerk

NFIR adviseert het monitoren van netwerkverkeer op kwaadaardige activiteit op basis van bekende en niet bekende dreigingen. Door een combinatie van monitoring op bekende indicatoren en monitoring op afwijkend gedrag in het netwerkverkeer kunnen vroegtijdig risico's worden geïdentificeerd.

Er is tijdens het incident vastgesteld dat er op een hoofdlocatie van de gemeente een zogenoemde Intrusion Detection System (IDS) oplossing geplaatst diende te worden. Een IDS monitort en analyseert het netwerkverkeer. Bij detectie van een mogelijke dreiging worden er waarschuwingen verzonden. Het advies van NFIR is dan ook om een permanente IDS oplossing te introduceren.

Daarnaast adviseert NFIR om een vorm van Security Operations Center (SOC) dienstverlening te introduceren, waarmee actief meegekeken wordt naar dreigingen op het netwerk om zo vroegtijdig te kunnen acteren in het geval van een geslaagde aanval.

3.2.2 Actieve monitoring systemen

SentinalOne is door de gemeente gekozen als Endpoint oplossing voor het monitoren van systemen. Het wordt geadviseerd om dit op alle systemen te installeren en gebruik te maken van de volgende technieken welke dreigingen vroegtijdig kunnen herkennen en ingrijpen:

- Ondersteuning van op bestand gebaseerde analyse (file hashing);
- Ondersteuning van externe toegang tot doelsystemen om in te kunnen grijpen;
- Cloud-gebaseerd (om in het geval van compromittatie controle te kunnen herpakken);
- Ondersteuning voor multi-factor authenticatie (MFA) voor het beheerdersplatform van de Endpoint oplossing.

3.2.3 Actieve monitoring logbestanden

NFIR adviseert om logbestanden actief te monitoren op afwijkend gedrag. Hierdoor kan een vroegtijdig signaal ontstaan van afwijkend gedrag of pogingen van kwaadaardige activiteit, ook van binnenuit de organisatie. Het advies van NFIR is dan ook om in kaart te brengen welke omgevingen er aanwezig zijn en daarop een vorm van logverzameling te introduceren (door middel van bijvoorbeeld een log-server of vergelijkbare oplossing).

Deze logoplossing kan in het geval van een incident gebruikt worden om de toedracht van een incident en de omvang van een eventuele te onderzoeken scope sneller en accurater vast te kunnen stellen.

Hier is hierbij van belang dat tenminste de volgende systemen hier onderdeel van zijn, waarbij de opslagretentie van de logbestanden een periode van tenminste een jaar betreft:

- Firewalls
- Switches
- Servers (virtueel)
- Servers (fysiek)
- Citrix omgeving

Actieve monitoring van logbestanden had het incident kunnen voorkomen dan wel beperken.

3.2.4 Monitoring SOC

Het monitoren op- en het afhandelen van beveiligingsincidenten is een andere specialisatie, waar andere expertise voor benodigd is. Bij een "Security Operations Center" wordt (continue) gecontroleerd of binnen de gehele ICT-Infrastructuur sprake is van beveiligingsproblemen. Dit kan variëren van meldingen onderzoeken van gecompromitteerde gebruikersaccounts tot aanwijzingen onderzoeken dat een grote hoeveelheid aan gegevens wordt gedownload. Indien er aanwijzingen zijn dat sprake is van een incident, kan de gemeente eerder ondersteuning vragen voor het uitvoeren van digitaal forensisch onderzoek en Incident Response.

3.3 Response

3.3.1 Incident Response plan

Tijdens een incident zijn er veel acties die uitgevoerd moeten worden. Door deze situaties te trainen, kan er tijdens een incident veel sneller gehandeld worden. Onderwerpen als een data recovery plan en incident response plan zijn hulpmiddelen die van grote waarde zijn tijdens een incident.

Een Incident Response Plan is bedoeld om bij incidenten snel en effectief te kunnen handelen, maar ook de juiste data weet vast te leggen voor onderzoek.

In dit plan worden scenario's beschreven met daarbij horende te nemen maatregelen. Zo kan de gemeente en de mogelijk onderzoekende partij tijd en kosten worden bespaard. Handreikingen vanuit de NIST kunnen ondersteunen bij het inrichten van een Incident Response plan. Publiek beschikbare standaarden zijn eveneens beschikbaar bij NIST en SANS[10]. Ook bij het ontwikkelen van een dergelijk plan en bijbehorende beleidsstukken is een PDCA-cyclus zeer belangrijk: komt het beleid overeen met tests uit de praktijk?

3.3.2 Oefenen van scenario's

Het oefenen van een incident zorgt ervoor dat een organisatie getraind is op het moment dat het fout gaat. De training zorgt ervoor dat betrokken entiteiten exact weten wat ze moeten doen en niet direct schrikken wanneer een dergelijke situatie ontstaat. Ook kunnen tijdens de training knelpunten naar voren komen die alvast kunnen worden opgelost.

[10] https://nvd.nist.gov/800-53/Rev4/control/IR-8; https://www.sans.org/reading-room/whitepapers/incident/paper/1791

NFIR B.V.
Verlengde Tolweg 2
2517 JV Den Haag
Telefoon: 088 - 323 02 05
info@nfir.nl
https://www.nfir.nl