Notitie
Onderzoek netwerkinbraak Senzer afgerond

Datum: 9 april 2021
Van: Marion van Limpt, algemeen directeur Senzer
Aan: Leden Dagelijks Bestuur Senzer
Kopie: CMT Netwerkinbraak

In de ochtend van 9 maart is bij een reguliere check van het Senzer-netwerk ontdekt dat er een inbraak gaande was. Senzer heeft meteen het interne digitale netwerk uitgeschakeld en losgekoppeld van internet en van andere netwerken zoals die van de gemeenten.
Er is voor melding en advies contact opgenomen met de Informatiebeveiligingsdienst (IBD) van de VNG. De voorzitter van Senzer is geïnformeerd evenals de Ondernemingsraad. Ook is er op 9 maart een formele melding gemaakt bij de Autoriteit Persoonsgegevens. Aan het einde van de dag is de pers geïnformeerd.

Ondertussen is er in de ochtend van 9 maart direct een crisisteam gevormd met alle leden van het managementteam (inclusief Chief Information Officer - CIO), manager en teamleider ICT en de Chief Information Security Officer (CISO). Het crisisteam is ondersteund door externe experts van de IBD en het gecertificeerde ICT-security-bedrijf Northwave. Het bedrijfscontinuïteitsplan van Senzer heeft als basis gediend om alle kritische processen van Senzer te monitoren. Het crisisteam is in de eerste weken twee keer per dag bij elkaar geweest.

Beheersing en herstel via drie lijnen

Er is vanaf 9 maart langs drie lijnen gewerkt aan het oplossen van de problemen:

1. Continuïteit van de dienstverlening en bedrijfsvoering.
2. Communicatie met uitkeringsgerechtigden, medewerkers, gemeenten, relaties, pers en andere stakeholders.
3. Vaststellen oorzaak en mogelijke schade.

Hieronder wordt langs deze drie lijnen een toelichting gegeven.

1. Continuïteit van de dienstverlening en bedrijfsvoering

De allereerste prioriteit lag bij het betalen van 3600 Tozo- en Participatiewet-uitkeringen die gepland stonden voor 10 maart. Tweede prioriteit was het weer operationeel krijgen van het Senzer-netwerk. Gezien het grote belang voor de uitkeringsgerechtigden is alles-op-alles gezet om de geplande uitkeringen op tijd betaald te krijgen. Dat is gelukt, zonder noemenswaardige vraagstukken.

Het Senzer-netwerk is een aantal dagen niet toegankelijk geweest. Wel hadden de medewerkers toegang tot de Office 365-applicaties, die niet op het eigen netwerk 'draaien' maar in de *cloud*, zoals mail en Word. De toegang voor een uitkeringsaanvraag (de zogenaamde Snelbalie) en ook de website zijn bereikbaar gebleven.
Alle servers zijn 'schoongemaakt' en vrij van schadelijke bestanden. Ook zijn er extra maatregelen genomen om virussen te herkennen en zijn de wachtwoorden van alle accounts vervangen. De ICT-security-experts hebben op 17 maart het netwerk schoon en veilig verklaard. Dat was het groene licht om het netwerk vrij te geven en de opnieuw geïnstalleerde desktops en laptops uit te reiken. Daarmee was de dienstverlening weer zoveel mogelijk *business as usual*. De ontstane werkachterstanden zijn vervolgens direct opgepakt.

2. Communicatie met uitkeringsgerechtigden, medewerkers, relaties, pers en andere stakeholders

In de communicatie was en is het uitgangspunt: snel en volledig openheid van zaken geven. Er is direct en via diverse kanalen gecommuniceerd op basis van een communicatieplan dat dagelijks werd geactualiseerd. Er heeft direct en meerdere malen formele communicatie met het Dagelijks bestuur van Senzer plaatsgevonden. Er is intensief contact geweest met de diverse relevante functionarissen van de zeven gemeenten. Ook zijn de zeven colleges van B&W geïnformeerd. Er is een crisissite www.senzer.nl/netwerkinbraak online gezet en er zijn updates gegeven via de socialmediakanalen van Senzer. Ook zijn de cliëntenraad en de samenwerkingspartners regelmatig geïnformeerd. Met het Eindhovens Dagblad zijn drie gesprekken gevoerd. Werkgevers en leveranciers zijn geïnformeerd en waar nodig is maatwerk geleverd om de reguliere activiteiten door te laten gaan. Er is intensief individueel klantcontact geweest via - een voor dit doel ingesteld - belteam van uitkeringsspecialisten. Uiteraard bleef het voor klanten ook mogelijk om onze locatie fysiek - coronaproof - te bezoeken voor afspraken.

3. Vaststellen van de oorzaak en mogelijke schade: Onderzoek Northwave

Op 9 maart is op advies van het IBD contact gelegd met een aantal CERT-gecertificeerde ICT-security- bedrijven voor het uitvoeren van het forensische onderzoek naar oorzaak en schade. Vanuit deze selectie is de opdracht verstrekt aan Northwave. Het onderzoek is direct gestart en heeft zich gericht op de volgende vier onderzoeksvragen:

I. Hoe kreeg de aanvaller toegang tot het netwerk van Senzer?

De aanvallers zijn rond 27 februari binnengedrongen via Citrix, de applicatie waarmee medewerkers op afstand op het eigen netwerk konden. Deze applicatie vormde de zwakke schakel in de ICT-infrastructuur van Senzer. Ze was verouderd en stond op de nominatie om vervangen te worden. Na het incident is Citrix versneld vervangen. Op de Citrix-applicatie was geen Multi Factor Authenticatie (MFA) aangebracht, waardoor alleen een wachtwoord voldoende was voor toegang.
Toelichting: In juni 2019 is door een gespecialiseerd bedrijf een penetratietest uitgevoerd op het Senzer-netwerk. Daarbij werd een 'laag risico' gedetecteerd op het gebruik van de Citrix-applicatie. Het ontbreken van MFA werd bij dat onderzoek niet aangegeven als een kwetsbaarheid. Vanuit een risicomanagement-afweging is destijds besloten om er geen prioriteit aan te geven. In 2020 nam thuiswerken door corona een vlucht. Landelijk nam het aantal hacks

op (thuis)systemen daarmee ook toe. Een van de maatregelen die toen genomen zijn, is het versneld invoeren van MFA op Microsoft365. Invoeren van MFA op de Citrix-applicatie is niet doorgezet, omdat dit technisch complex was en mogelijk negatieve gevolgen had voor thuiswerken en de dienstverlening van Senzer. Er is op dat moment gekozen om in plaats hiervan Windows Virtual Desktop (WVD) zo snel mogelijk te implementeren als vervanger van Citrix. Na de netwerkinbraak is Citrix niet meer geactiveerd, maar is versneld WVD geïnstalleerd. Inmiddels hebben alle Senzer-medewerkers extern toegang tot het netwerk via WVD.

II. Welke stappen heeft de aanvaller genomen nadat deze toegang had?
De aanvaller heeft een zogeheten achterdeur geïnstalleerd waardoor later gemakkelijk en ongemerkt opnieuw het netwerk van Senzer kon worden binnengedrongen. Daarna heeft de aanvaller losgeld-software geplaatst op het netwerk, die op 9 maart is geactiveerd en het netwerk heeft platgelegd. Tevens heeft de aanvaller een deel van de back-ups verwijderd, maar niet de snapshots (een soort kopie van alle data in het netwerk).
Toelichting: Senzer heeft geen contact gelegd met de aanvallers en heeft dus geen losgeld betaald. Dit heeft twee redenen. De eerste heeft te maken met het feit dat Senzer beschikt over goede en beveiligde snapshots waar de aanvaller niet bij kon. Daardoor was het mogelijk om zelf snel het netwerk te herstellen. Ook de hoeveelheid versleutelde en onbruikbare informatie was hierdoor relatief gering. De tweede is principieel van aard; het uitgangspunt bij publieke organisaties is om niet in onderhandeling te gaan met cybercriminelen.

III. Heeft de aanvaller persoonsgegevens of andere vertrouwelijke informatie gestolen?
Northwave heeft hier grondig technisch onderzoek naar verricht en komt tot de conclusie dat het hoogst onwaarschijnlijk is dat er persoonsgegevens of andere vertrouwelijke informatie is gedownload en gestolen. Daarbij geeft Northwave aan dat de aanvallers niet bekend staan om het downloaden en stelen van gegevens, maar zich vooral richten op het verkrijgen van losgeld.

IV. Is de ICT-omgeving van Senzer weer veilig?
De ICT-omgeving van Senzer is weer veilig en betrouwbaar verdedigd tegen soortgelijke aanvallen. Hiervoor zijn de nodige technische maatregelen genomen ter voorkoming en is de monitoring verder uitgebreid. Alle externe toegang gebeurt nu met MFA. Senzer heeft daarbij snel kunnen reageren omdat de voorbereidingen voor een nieuwe externe toegang (WVD, als vervanging van Citrix) reeds in gang waren gezet vóór de aanval. Ook het adequaat reageren en terug kunnen zetten van snapshots heeft bijgedragen aan een snel herstel. Het rapport en de observaties van Northwave over de aanval, het informatieveiligheidsbeleid en de beheersingsaanpak van Senzer zijn gedeeld met de IBD. In bijlage het gehele rapport (n.b. vanwege de internationale werkwijze van Northwave is het gehele rapport in het Engels, met een managementsamenvatting in het Nederlands).

Vervolgacties: aanpak schade en optimalisatie van processen

Nu de oorzaak is vastgesteld, het netwerk weer schoon en veilig is en de dienstverlening weer op reguliere wijze verloopt, richt de aandacht van Senzer zich op de nazorg, schade-oplossing en het uitvoeren van de aanbevelingen uit het rapport. De gevolgen van de netwerkinbraak zijn relatief beperkt gebleven voor zowel de externe relaties als de interne organisatie. De meest acute vraag, het betalen van uitkeringen, is op tijd gelukt, het netwerk en de applicaties waren relatief snel weer in de

lucht, de dienstverlening snel weer op gang en de medewerkers kunnen weer op kantoor en vanuit huis op het netwerk werken.

Het is hoogst onwaarschijnlijk dat er belangrijke informatie ontvreemd is. Wat wel verloren is gegaan zijn bepaalde back-ups met daarin mogelijk historische gegevens die niet meer in gebruik waren en een deel van de klantcontactgegevens van afnemers/ondernemers. Daarnaast moeten naast de productieomgeving ook weer testomgevingen en dergelijke worden opgebouwd.

Aanbevelingen rapport geïntegreerd in bestaande informatieveiligheidsbeleid
Het verdere herstel van de ICT-omgevingen én de aanbevelingen uit het rapport zijn belegd bij een projectgroep die vanuit het managementteam wordt aangestuurd. Alle aanbevelingen worden ingepast in de reeds vanuit Senzer uitgevoerde en al lopende acties voor het versterken van de informatiebeveiliging.

De volgende acties - naar aanleiding van de aanbevelingen - zijn inmiddels uitgevoerd:

- Toepassen van MFA op alle externe toegangen op het Senzer-netwerk.
- 24/7 veiligheidsmonitoring van de logging van de netwerktoegang en opvolging.
- Doorvoeren van afgedwongen verplichting tot versterkte wachtwoorden.

De volgende acties - naar aanleiding van de aanbevelingen - staan op de korte termijn ingepland:

- Actualiseren en verscherpen van het *‘incident respons plan’* specifiek voor IT-incidenten.
- Interne campagne gericht op belang van informatieveiligheid, bewustwording van risico’s en de benodigde gedragingen.
- Segmentering van het netwerk, waarbij elk segment zal worden voorzien van een ander versterkt wachtwoord.
- Aanscherpen van het patch- en updateproces, waardoor alle systemen tijdig worden voorzien van de benodigde updates.
- Herijken en verbeteren van het realiseren van back-ups.
- Herijking van de bestaande toegangsrechten op alle gebruikte informatiesystemen op basis van minimale privileges. Een useraccount krijgt hierbij uitsluitend die rechten die essentieel zijn voor de beoogde functie.
- Structureel inbedden van 24/7 veiligheidsmonitoring van de logging van het interne netwerk en de toegang tot het netwerk.

Kosten
De netwerkinbraak heeft geleid tot extra kosten vanwege de inzet van de crisisdiensten van Northwave en het tijdelijk extra monitoren van de ICT-omgeving. Verder zijn de directe kosten beperkt gebleven en is er geen sprake geweest van het betalen van losgeld.

Flinke impact, maar ook positieve effecten

De gevolgen van het incident voor de dienstverlening zijn relatief klein gebleven, maar de netwerkinbraak en de nasleep hebben een grote impact gehad op de Senzer-medewerkers. De positieve uitkomst is dat de Senzer-organisatie heeft laten zien te beschikken over een gezonde dosis veerkracht en probleemoplossend vermogen. In het Northwaverapport staat dat ‘Senzer goed voorbereid was op cyber-gerelateerde incidenten en perfect gehandeld heeft aan de hand van incident response-plannen die Senzer al paraat had'. Met als nevenopbrengst dat de relevante werkprocessen en veiligheidssystemen versneld een upgrade hebben gehad, zodat we in de toekomst beter gewapend zijn tegen mensen die digitaal kwaad in de zin hebben.