Ministerie van Binnenlandse Zaken en Koninkrijksrelaties

DGOO:
CIO Rijk

Datum:
7 mei 2024

Versie: 1.0

Redactie:
cisorijk@minbzk.nl

Contact:
cisorijk@minbzk.nl

memo

Bescherming Ransomware en datadiefstal - Bestuurlijke Dilemma's

Inleiding

Ransomwareaanvallen vormen een dreiging voor Nederlandse organisaties. Niet alleen kan er financiële impact zijn, ook kan er door het versleutelen van systemen en/of data impact zijn op het operationele proces van een organisatie. Indien er datadiefstal wordt gepleegd, kan er imagoschade dan wel restschade optreden. Het bieden van bescherming tegen ransomware en datadiefstal is onderdeel van de routekaart Digitale Weerbaarheid. Hiervoor is een werkgroep ingericht die bezig is met diverse kennisproducten.
Eén van die producten is dit memo met een aantal bestuurlijke dilemma's. Tijdens een ransomwareaanval, vaak in combinatie met datadiefstal, worden bestuurders regelmatig geconfronteerd met ingewikkelde besluiten.
Geen van de te nemen besluiten komt zonder aanzienlijke risico's. Dit heeft bijvoorbeeld betrekking op het betalen van het losgeld.
De dilemma's kunnen in crisisplannen en managementgames voor ransomware worden meegenomen. Dit moet leiden tot een hogere weerbaarheid tegen aanvallen met ransomware.
Dit document wordt beheerd en er wordt tweejaarlijks bekeken welke veranderingen aanpassing van dit memo vereisen. Aanvallers verzinnen immers telkens nieuwe methoden en zo ontstaan mogelijk weer nieuwe inzichten en dilemma's.

Doel

Dit document is bedoeld om management aan te sporen in de koude fase al na te denken over bestuurlijke dilemma's die tijdens een ransomwareaanval kunnen voorkomen.

Voorbereiding in de koude fase (voordat je bent gehackt)

Organisaties kunnen de volgende stappen ondernemen om voorbereid te zijn op een eventuele ransomwareaanval:

- Bespreek genoemde dilemma's met het management en leg keuzes vast in beleid. Leg hierin ook een relatie met de eigen crisisorganisatie: een ransomwareuitbraak is al snel een 'crisis' en dan moet de eigen crisisorganisatie geactiveerd worden. Bij een rijksbrede uitbraak heeft dit ook een relatie met het Nationaal Crisisplan Digitaal[1].
- Neem uitkomsten mee in draaiboeken en herstelplannen: het is essentieel om regelmatig crisisoefeningen te houden waaronder een

[1] Nationaal Crisisplan Digitaal | Rapport | Rijksoverheid.nl

crisisoefening op dit thema inclusief betrokkenheid van de operationele laag.
- Werk een onderhandelingsstrategie en een woordvoeringslijn uit: deze kan je al grotendeels uitwerken in de koude fase en dan ben je goed voorbereid op een eventuele crisis.
- Oefen de dilemma's in tabletop-oefeningen en managementgames. Er komt in 2024 een managementgame beschikbaar om spelers meer bewust te maken van de dilemma's.
- Het NCSC heeft een incident responsplan [i] geschreven specifiek op ransomware. Maak een eigen versie in de koude fase, zodat je e.e.a. hebt liggen mocht jouw organisatie geraakt worden door ransomware.

Scope
Toepassingsgebied is in eerste instantie de Rijksoverheid. De doelgroep van functies die dit memo vooral ter harte zouden moeten nemen betreft: CISO, CIO, CDO, CTO, Bestuurder, Directeur, IT-Manager, IT-Architect, Business Continuity Manager en Security Adviseur. Echter, een bredere doelgroep kan mogelijk ook gebruik maken van dit memo.

Bestuurlijke dilemma's:
In onderstaande tabel geven we een samenvatting van 4 dilemma's:

Items	Bestuurlijke dilemma's	
1	Betaal je losgeld?	• Het dringende advies vanuit het Kabinet is dat de overheid geen losgeld betaalt: losgeld betalen houdt het criminele verdienmodel in stand. Daarnaast is er geen garantie dat de actoren achter de aanval de decryptiesleutel daadwerkelijk overleggen. • Zijn alle opties voor herstel getoetst, zoals genoemd op de site https://www.nomoreransom.org/? • Zijn vitale functies in het geding? • Is er risico voor publicatie (datadiefstal) van persoonsgegevens en/of gevoelige interne (bedrijfs)informatie? • Indien toch betalen van losgeld overwogen wordt, is dit met de bestuurder besproken? • Werk een onderhandelingsstrategie en een woordvoeringslijn uit en ruim hier tijd voor in, in je response.
2	Houd je de verbinding naar buiten open?	• Best practice is om besmette servers of systemen zoveel mogelijk direct te isoleren. Laat de servers wel aanstaan. • Snijdt echter niet direct de gehele digitale connectie door. Hierdoor kan de versleuteling onomkeerbaar worden. • Hou deze periode zo kort mogelijk: meer gegevens kunnen vergrendeld raken of worden gestolen. • Verifieer de status van de back-up en zorg ervoor dat de back-up veilig is, • Verwijder backdoors en andere vormen van persistente toegang door de aanvallers.

3	Openbaar maken en hulp zoeken?	• Het intern melden van een datalek is verplicht, bij de AP is dat afhankelijk van de situatie • Hulp van inhoudelijk specialisten wordt aanbevolen, • Openbaarheid en transparantie versus de dreiging van permanente versleuteling, • Informeren ketenpartners en betrokkenen, • Aangifte doen.
4	Hoe ga je om met belasting personeel?	• Oplossen kost veel inspanning: goed werkgeverschap = acceptabele werkbelasting, • Bepaal maatregelen om overbelasting te voorkomen: bv inhuur extra capaciteit e.d.,

Toelichting dilemma's:

Dilemma 1 – Betalen van losgeld.
Door de aanval zijn er vitale functies in het geding, dit heeft impact op de continuïteit van de dienstverlening en potentieel een effect op de nationale veiligheid. Het gaat dagen duren voor de back-ups (indien aanwezig) teruggerold kunnen worden. Het betalen van losgeld lijkt een quick fix te zijn. De lijn vanuit de overheid is echter om geen losgeld bij ransomware te betalen. Dit omdat hiermee het criminele verdienmodel in stand wordt gehouden. Bovendien biedt het betalen van losgeld geen garanties tot oplossen van de problemen. Huidig inzicht is dat het niet strafbaar is (ii) om losgeld te betalen. Hoe ga je hier als bestuurder mee om?

Cybercriminelen kunnen ook dreigen met het verkopen en/of openbaar maken van (persoons)gegevens en/of gevoelige interne (bedrijfs)informatie tenzij je betaalt. Steeds vaker hanteren deze criminelen "double extortion" technieken: betalen voor het ontsleutelen van de data en/of betalen voor het terugkrijgen van de gestolen data (of ze verkopen het en/of benaderen jouw zakenrelaties). Onderhandelen over de betaling van losgeld kan eventueel tijd en ruimte creëren voor je response.

Kortom, als ze eenmaal toegang hebben tot jouw gegevens, moet je er rekening mee houden dat je mogelijk voor het blok wordt gezet en dat het betalen van losgeld geen garantie biedt dat je gegevens niet worden verkocht of gepubliceerd.

Uit politiegegevens blijkt dat slachtoffers soms toch bereid zijn te betalen, omdat de gestolen data bijvoorbeeld gevoelige (persoons-)gegevens van werknemers en/of klanten kan bevatten. Dit brengt een risico met zich mee voor betrokkenen, reputatieschade en verlies van gegevens. Zo kunnen er situaties ontstaan waarin het lijkt dat losgeld betalen noodzakelijk is:

- Bijvoorbeeld, als gevolg van ontoereikende back-ups ben je niet in staat om herstel uit te voeren met acceptabel dataverlies, of de back-ups zijn mogelijk ook besmet.
- Het betreft tijdkritische processen en het herstel duurt te lang, wat maatschappelijke ontwrichting tot gevolg kan hebben.

- Als gedreigd wordt om de gegevens openbaar te maken of te verkopen, kan dat soms heel verstrekkende gevolgen hebben;
- Het herstel van dienstverlening kan dagen duren, en soms lijkt het aantrekkelijk om het gevraagde losgeld toch te betalen als snelle oplossing.

Kortom:

- Controleer of je ransomware onschadelijk kan maken. Voor sommige typen ransomware is software ontwikkeld waarmee de versleuteling van bestanden ongedaan kan worden gemaakt, zonder dat hiervoor losgeld aan de ransomware-groep hoeft te worden betaald.
- De overheid heeft een voorbeeldfunctie en betaalt geen losgeld. In de uiterste noodzaak dat dit wordt overwogen, moet dit zeer zorgvuldig worden afgewogen in relatie tot de noodzaak tot betalen. Betrek hierbij de hoogste bestuurders en woordvoering.

Dilemma 2 – houd je de verbinding naar buiten open?
Het is een best practice om geïnfecteerde systemen of servers onmiddellijk van het netwerk te isoleren om verdere verspreiding van ransomware te voorkomen en de schade te beperken. Het kan voorkomen dat in bepaalde specifieke situaties, zoals bij onderhandelingen met ransomware-operators, experts advies geven over het tijdstip en de wijze waarop een verbinding verbroken moet worden. Deze adviezen kunnen variëren afhankelijk van de omstandigheden. Het is belangrijk om de cybersecurity-richtlijnen en -procedures van uw organisatie te volgen in geval van een ransomwareaanval en, indien mogelijk, samen te werken met cybersecurity-experts en instanties voor incidentrespons om de juiste maatregelen te nemen om de aanval te beperken en te herstellen.

Ook zonder de verbinding door te snijden kan je al risico mitigerende maatregelen nemen. Belangrijk is om de gecompromitteerde systemen/servers te isoleren van het internet en van elkaar, zodat verdere schade voorkomen wordt en herstel door kan gaan. Overigens moet je dan wel zeker weten dat de malware is verwijderd in de herstelomgeving.

Het isoleren van de IT-infra van het internet heeft tevens een business impact, omdat daardoor een aantal primair proces systemen niet meer zullen werken. Indien de besmetting gelokaliseerd is en slechts impact heeft op enkele processen kan de overweging gemaakt worden om niet om niet de volledige verbinding van de interne IT-infrastructuur met het internet te onderbreken. Bijvoorbeeld om overige kritieke/vitale processen met hoge maatschappelijke waarde te laten blijven functioneren.
Wanneer je geverifieerd hebt dat de back-up actueel en voldoende volledig is en (dus) restore mogelijk is, is dat een mogelijke oplosrichting waarbij versleuteling eventueel is te voorkomen.

Als je door een ransomware-groepering bent aangevallen, moet je er rekening mee houden dat de aanvaller geavanceerde middelen heeft ingezet. Denk aan backdoors en andere manieren om toegang tot de IT-omgeving te behouden zelfs nadat back-ups zijn teruggezet.

Verbreek de verbinding zodra je zeker weet dat de meest recente back-up volledig is en de restore succesvol kan zijn & je backdoors uitgesloten en onklaar gemaakt hebt.
Ongeacht of je back-ups hebt zul je altijd een incident response-proces moeten aftrappen. Organisaties van de Rijksoverheid kunnen het NCSC te bellen voor incident response (IR), en in overleg met het NCSC een commerciële IR-partij in de hand te nemen. Die IR-partij kan vervolgens op basis van professioneel onderzoek advies geven over dit soort kwesties.
Als slachtofferorganisatie kan het lastig zijn om zelf back-ups terug te zetten, temeer omdat het vaak moeilijk is om zelf te bepalen of back-ups schoon zijn. Daarnaast verhelpt het terugplaatsen van een back-up bijvoorbeeld niet de kwetsbaarheid die is misbruikt om initieel binnen te komen.
Het NCSC wil daarnaast graag weten wanneer een organisatie binnen de Rijkoverheid door ransomware (of een ander type aanval) is getroffen, zelfs wanneer de aanval uiteindelijk meevalt.

Dilemma 3 – openbaar maken en hulp zoeken
Hoe communiceer je naar de buitenwereld over een compromittatie? Welke communicatielijnen moet je hiervoor gebruiken? Met wie moet je hierover overleggen?

Kernwaarde van de overheid is transparantie en openbaarheid van bestuur. Zoek je de openbaarheid en zo ja wanneer. Sommige cybercriminelen dreigen echter met permanente versleuteling of openbaarmaking van gevoelige gegevens als je hulp zoekt van specialisten en/of aangifte doet. Dit lijkt vooral een loos dreigement: ze zijn vooral op zoek naar geld en dat krijgen ze niet als ze de gegevens permanent ontoegankelijk maken of de publiciteit zoeken.

Er is zijn diverse soorten datalekken en die moet je soms openbaar maken. Voorbeelden van datalekken zijn het stelen van persoonsgegevens, ongeautoriseerde toegang tot persoonsgegevens en het verloren gaan van persoonsgegevens. Die moet je altijd intern melden als datalek en in sommige gevallen ook bij de Autoriteit Persoonsgegevens (binnen 72 uur).
Het kan ook zijn dat het niet gaat om persoonsgegevens maar om andere gegevens die voor de organisatie van (vitaal) belang zijn Bijvoorbeeld gevoelige informatie over de bedrijfsvoering van de organisatie of beleidsvoorstellen met maatschappelijke implicaties. Dit kan onder de meldplicht van de NIS2 vallen. Daarnaast moet je overwegen of de openbaarheid gezocht wordt als verklaring voor de (mogelijke) verstoring en in het kader en transparantie.

Melden bij de bestuurlijke lijn binnen de eigen organisatie is geen dilemma maar je moet ook het personeel van je eigen organisatie op de hoogte brengen.
Meer communicatiedilemma's zijn:

- Het kan voorkomen dat cybercriminelen eisen dat je geen contact opneemt met de Politie en andere instanties. Vraag toch het NCSC voor ondersteuning (onder voorwaarde van geheimhouding) en ook voor melding door NIS-partijen (Sectoren die onder de NIS2-richtlijn vallen, 2020)

  - Meldplicht onder de WBNI geldt nog niet voor Rijksoverheidsorganisaties maar dit gaat met de NIS2 veranderen;
  - Het is belangrijk dat rijksorganisaties het NCSC benaderen als ze slachtoffer zijn van ransomware. Ook kunnen ze een expertorganisatie in te huren;
  - Alle incidenten die bij het NCSC worden gemeld, worden door het NCSC strikt vertrouwelijk behandeld.
- Wanneer informeer je ketenpartners zodat zij maatregelen kunnen treffen om met een mogelijke impact op hun organisatie om kunnen gaan?
- Tegelijkertijd kan (te) vroeg melden ook lastig zijn omdat de informatie nog niet volledig is. Vroeg melden is nuttig omdat anderen dan eventueel ook maatregelen kunnen treffen. Soms kan je niet meer melden dan dat een incident nog in onderzoek is en er nog weinig bekend is. Daarnaast kun je je afvragen of het realistisch/wenselijk is om een volledig en 100% betrouwbaar beeld te creëren met de waarschijnlijk beperkte (financiële/personele) middelen die je als organisatie ter beschikking hebt,
- Het onnodig of onjuist melden kan leiden tot imagoschade, maar het niet melden kan mogelijk zelfs tot meer schade leiden dan het melden, zelfs als het beeld niet volledig is. In het kader van een transparante overheid en gezien het huidige maatschappelijke klimaat, wordt de impact van het niet melden hoger ingeschat dan van wel melden.

Dilemma 4 – Belasting van personeel

Hoe ga je om met de belastbaarheid van medewerkers?
Het herstel van de voorzieningen kost veel tijd en dit geeft een stevige en langdurige extra belasting. Goed werkgeverschap vereist dat je hier vooraf over nadenkt en voorkomt dat medewerkers uitvallen. Hoe lang hanteer je een crisisorganisatie? Hoe voorkom je langdurige overbelasting voor medewerkers?

Werk vooraf uit hoe je langdurige overbelasting voorkomt, bv door:

- Afschalen van crisisorganisatie naar reguliere lijnen en processen,
- Andere activiteiten tot een minimum terug te brengen of zelfs stilleggen,
- Extra inhuur van menskracht bijvoorbeeld voor het uitvoeren van routinematig werk of juist voor ontbrekende expertise,
- De werkdruk bij de IT-afdeling kan zeer hoog zijn. Zij moeten immers hun omgeving opnieuw gaan opbouwen (waarschijnlijk in samenwerking met een IR-partij). Dit kost tijd en energie, en zal voor extra belasting zorgen in een situatie waarmee zij mogelijk minder ervaring hebben,
- In dit onderzoeksrapport[iii] staat advies aan managers met betrekking tot personeelszorg voor, tijdens en na een aanval.

[i] Incidentresponsplan Ransomware | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)
[ii] Is het betalen van losgeld bij ransomware niet in strijd met de wet? - Security.NL.
[iii] Northwave-Research-After-the-crisis-comes-the-blow-The-mental-impact-of-ransomware-attacks-1.pdf (hubspotusercontent-eu1.net)