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

Detectie & schadebeperking ransomware

Inleiding

Ransomware-aanvallen 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 aanbevelingen voor detectie & schadebeperking bij ransomwareaanvallen.

Om ransomware aanvallen en datadiefstal zo veel als mogelijk is te voorkomen of te beperken kijken we naar het NIST Cybersecurity Framework (CSF v1.1). Dat is een raamwerk voor het beheer van cyberbeveiliging. Het is ontwikkeld door het National Institute of Standards and Technology (NIST) in de Verenigde Staten Het NIST-raamwerk bevat 5 aanbevolen basisfuncties van de cybersecurity cyclus die organisaties in de publieke en private sector kunnen volgen om hun cyberbeveiligingsprofiel te versterken. Dat betreft: identificeren, beschermen, detecteren, reageren en herstellen. (Er is ook een NIST-CSF V2.0 met meer stappen) In deze nota geven we aanbevelingen voor detectie en reageren met schadebeperking.

Bij detectie is het doel om bedreigingen en beveiligingsincidenten zo snel mogelijk te detecteren. Dit omvat het gebruik van monitoringssystemen, logboekanalyse en andere technologieën om ongeautoriseerde activiteiten op te sporen.
We reageren wanneer een beveiligingsincident wordt gedetecteerd en dan is het essentieel om snel te handelen om verdere schade te beperken. We gebruiken in deze fase de vooraf ontwikkelde reactieplannen, het in gang zetten van schadebeperkende maatregelen en het coördineren van de respons van de organisatie.

Dit document wordt beheerd en er wordt tweejaarlijks bekeken welke veranderingen aanpassing van dit memo vereisen. Aanvallers verzinnen immers telkens nieuwe methoden en ook kunnen er steeds weer meer zaken gedetecteerd worden: zo ontstaan mogelijk weer nieuwe inzichten.

Doel

Dit document heeft tot doel het management aan te moedigen om in de 'koude fase' (dus voordat je bent gehackt) al te starten met het verbeteren van detectie en na te denken over een passende reactie in geval van een succesvolle ransomwareaanval. Het vooraf bepalen van reacties is van essentieel belang om ransomwareaanvallen zo vroeg mogelijk te detecteren en eventuele gevolgschade te minimaliseren.

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.

Advies

Organisaties kunnen de volgende detectie- en reactie-verhogende stappen ondernemen om beter voorbereid te zijn op een eventuele ransomwareaanval:

- Richt detectie in op basis van anti-ransomware-use-cases aan de hand van de meest voorkomende Indicatoren-of-Compromise.
- Maak een incident responseplan gericht op ransomware en neem hierin de schadebeperkende acties in mee.
  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.
- Oefen de maatregelen in tabletop-oefeningen en managementgames.
- Neem uitkomsten van oefeningen mee in het actualiseren van de operatie, draaiboeken en incidentresponsplannen.: het is essentieel om regelmatig crisisoefeningen te houden waaronder een crisisoefening op dit thema inclusief betrokkenheid van de operationele laag.

Bespreek de te nemen maatregelen met het management en leg keuzes vast in beleid. Doe als eerste stap een volwassenheidscheck van de cyberweerbaarheid van jouw organisatie. Hierdoor krijg je een beter beeld van de capaciteiten binnen de organisatie met betrekking tot het identificeren van Indicators of compromise (IoC). Gebruik hiervoor de readiness-checklist van Versterken Soc Stelsel Rijk (VSSR) en/of het NOREA Ransomware Framework.

Detectie

Hieronder presenteren we een lijst (niet uitputtend) van zogenaamde Indicators of Compromise (IoC) als aanwijzingen dat je mogelijk (bijna) slachtoffer bent van ransomware en/of datadiefstal:

- Meldingen bij de servicedesk over plotselinge versleuteling van bestanden en onbereikbaarheid van verschillende diensten.
- Een indicatie van zogenaamde laterale beweging (lateral movement) door een kwaadwillende actor:
  - Anti-virusmeldingen of talrijke meldingen van systemen waarin de antivirussoftware is uitgeschakeld,
  - Een opvallende toename in het aantal onsuccesvolle inlogpogingen,

    - Creatie van lokale gebruikers op verschillende clients of servers,
    - Aanzienlijke wijzigingen in Group Policy Object (Groepsbeleid),
    - Plotselinge toename in het aantal bestanden in de dagelijkse incrementele back-up; dit kan duiden op versleutelde bestanden.
- Opvallend grote gegevensstromen naar onduidelijke bestemmingen, wat kan wijzen op datadiefstal.
- Toename van intern netwerkverkeer, bijvoorbeeld door vulnerability- of poortscanning.
    - Toename van LDAP-verkeer.
    - Aanwezigheid van verdachte applicaties zoals NLTest, Bloodhound en Mimikatz-software
    - Dit kunnen indicaties zijn van cybercriminelen die betrokken zijn bij ransomware, datadiefstal of spionagepogingen.
- (Pogingen tot) verbindingen met bekende ransomware-websites en nieuwe IoCs (Indicators of Compromise) die vertrouwelijk worden gedeeld door het NDN van NCSC.
    - Zorg ervoor dat je verdachte IP-adressen matcht met je firewall- of DNS-loggingapparatuur om command-and-control-verkeer te identificeren.
    - Maak gebruik van open-source tools of commerciële tools om deze IoCs te detecteren.

Mogelijke schade-beperkende acties
Als vuistregel houden we aan dat de specifiek te nemen maatregelen afhangen van het soort malware en de mate van weerbaarheid van de organisatie. Maatregelen zouden bij voorkeur (grotendeels) gebaseerd moeten zijn op de BIO (27002 Controls).

Hieronder volgt een (niet uitputtende) lijst van specifieke schadebeperkende maatregelen die genomen kunnen worden bij een ransomware besmetting:

- Isoleer besmette servers/systemen of netwerksegmenten van internet en de rest van het netwerk om kans op besmetting van andere systemen te beperken,
    - Bij een Virtuele Desktop Infrastructuur (VDI) kan je de specifieke VDI's isoleren. Vanuit VMware kan je dan alsnog toegang krijgen tot het console van de machine,
- Beperkt de netwerk connectie met gevoelige systemen om datadiefstal in te perken,
    - Isoleer de systemen zoveel mogelijk, zet ze niet uit en zorg dat de systemen wél bereikbaar blijven,
    - Houd hierbij tevens rekening met businesscontinuïteit-vraagstukken,
- Veiligstellen forensisch materiaal (Dit is vooral bedoeld om juridische stappen te kunnen nemen en/of lering te trekken voor aanvullende preventie/detectie maatregelen) en scannen op en verwijderen van de malware: voorkomen verdere besmetting,
    - Gebruik het vooraf opgestelde plan waarbij het scenario afhankelijk kan zijn van de statelijke of criminele actor,
    - Scan je systemen om alle besmettingen te vinden,

    - Voer daarna een memory dump uit op die systemen: forensische bewijsverzameling,
    - Verwijder waar mogelijk de malware.
- Scan je systemen op backdoors en andere vormen van onwenselijke resistente toegang (onderdeel van detectie): dit voorkomt verdere besmetting én voorkomt een her-besmetting van je systemen,
    - Let op: scannen en onklaar maken volgt pas nádat de voorgaande stappen genomen zijn,
    - Maak eventuele achterdeuren (backdoors) indien mogelijk onklaar. Houd er echter rekening mee dat na het uitschakelen van achterdeuren meestal een herstel (restore) nodig is, wat vaak aanzienlijke tijd in beslag kan nemen.
    - Scan-software op basis van signatures is niet altijd up-to-date. Tools zoals Endpoint Detection and Response (EDR) en Extended Detection and Response (XDR) zijn moderne oplossingen. Deze draaien op de achtergrond mee en reageren op verdachte activiteiten. Zelfs bij een zero-day kan een EDR/XDR tool reageren.
- Optimaliseer communicatie met ketenpartners zodat zij mitigerende maatregelen kunnen nemen,
    - Werk samen met het NCSC, zij kunnen vaak nuttige informatie geven over de besmetting en de statelijke of criminele actor,
    - Voer een tabletop-oefeningen uit voor de hele cyclus,
- Isoleer de back-upvoorzieningen: dit borgt de herstelbaarheid van je systemen en voorzieningen.

[i] Incidentresponsplan Ransomware | Publicatie | Nationaal Cyber Security Centrum (ncsc.nl)