dialogic
innovatie • interactie

Radically Open Security

Verkenning risicofactoren ransomware-aanvallen

Managementsamenvatting (NL)

ir. ing. Reg Brennenraedts MBA, ir. Tommy van der Vorst, Jessica Kats MSc, dr. Melanie Rieback, Anouk Vos MSc, ir. Nick Jelicic, Roos Jansen MSc, Tessel Blom MSc, Nino van Sambeek

Opdrachtgever:
WODC

Publicatienummer:
2021.148-2222-MSNL

Datum:
Utrecht, 5 augustus 2022

Managementsamenvatting

Introductie

In opdracht van het Wetenschappelijk Onderzoek- en Documentatiecentrum (hierna: WODC) heeft Dialogic een verkennend onderzoek naar risicofactoren voor ransomware-aanvallen uitgevoerd. Dit onderzoek heeft als doel het in kaart brengen en kwantificeren van factoren die ransomware-aanvallen beïnvloeden. Een tweede doelstelling is het bieden van inzicht in de mogelijkheden tot bewustwording onder bestuurders van middelgrote en kleine organisaties, zowel in de publieke als private sector. Het onderzoek beantwoordt de volgende onderzoeksvragen:

1. Welke risico's brengen ransomware-aanvallen met zich mee?
2. Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?
3. Welke soorten partijen zijn bij deze aanvallen betrokken?
4. Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie?
5. In hoeverre zijn deze factoren kwantificeerbaar?
6. Met welk instrument kunnen beleidsmakers in middelgrote en kleine organisaties bewust worden gemaakt maken van de risico's van ransomware?
7. Wat zijn belangrijke factoren voor bedrijven en organisaties om met het instrument aan de slag te gaan?

Voor de uitvoering van dit onderzoek is gebruik gemaakt van verschillende methoden: literatuuronderzoek, verkenning van bestaande risicotaxatiemodellen, verkenning van cybersecurityverzekeringen, interviews, casestudies van getroffen organisaties in Nederland en validatiesessies. In dit onderzoek wordt getracht de meest actuele situatie te schetsen van de vraagstukken die hier spelen.

Impact van ransomware-aanvallen

De eerste onderzoeksvraag luidt: *Welke risico's brengen ransomware-aanvallen met zich mee?*

Het risico op een cyberaanval is groot en groeiend. Ransomware is een specifieke cyberaanval. Hierbij richten criminelen zich meestal op het versleutelen van data van het slachtoffer en in mindere mate het voorkomen dat het slachtoffer toegang krijgt tot zijn eigen systemen. De kern van ransomware is dat het slachtoffer door de dader (typisch: vanwege de versleuteling van data) onder druk wordt gezet om iets tegen zijn of haar zin te doen. Meestal is dit het betalen van losgeld (*ransom*). Er zijn vier vormen van aanvallen. Bij *single extortion* worden bestanden versleuteld en worden slachtoffers gechanteerd door de dreiging toegang tot deze bestanden te verliezen. Bij *double extortion* worden naast versleuteling de gegevens gestolen en wordt gedreigd deze openbaar te maken. Bij *triple extortion* worden bovendien andere cyberaanvallen, zoals DDoS-aanvallen, op systemen van het slachtoffer uitgevoerd om het herstelproces complexer te maken. Tenslotte worden bij *quadruple extortion* ook de relaties van het slachtoffer gechanteerd met het openbaar maken van hun gegevens.

De impact die dergelijke aanvallen kunnen hebben op organisaties bestaat uit de volgende aspecten:

1. Additionele kosten voor de inhuur van capaciteit om op de aanval te reageren;

2. Kosten door verlies van data;
3. Kosten door openbaarmaking van data die bestaan uit (a) kosten door reputatieschade, (b) boetes, bijvoorbeeld als gevolg van de AVG en (c) schadevergoedingen;
4. Betaling van losgeld;
5. Kosten door verstoring bedrijfscontinuïteit;
6. Herstelkosten voor systemen.

De gemiddelde losgeldbetaling is lastig exact te bepalen, maar ligt waarschijnlijk tussen de $ 50.000 en $ 500.000. Het inschatten van de kosten van de verstoring van de continuïteit van ondernemingen is nog lastiger, maar lijkt een vaak veelvoud te zijn van de losgeldbetalingen. Van de andere posten is het lastig om dit kwantitatief te duiden en verschillen ook sterk per casus.

Tot slot zijn er ook maatschappelijke effecten van ransomware-aanvallen . Door ketenafhankelijkheden kan de verstoring van de bedrijfscontinuïteit van één aangevallen organisatie een grote impact hebben op andere organisaties in de keten, zoals klanten en leveranciers. De overtreffende trap hiervan zijn uiteraard aanvallen op vitale sectoren waardoor grote delen van de economie indirect getroffen zullen worden. Bovendien kunnen daders, doordat er koppelingen tussen de ICT-systemen van verschillende organisaties zijn, ook overspringen tussen organisaties. Een laatste maatschappelijk effect is een mogelijk afname van vertrouwen in de democratische rechtstaat doordat criminelen niet (kunnen) worden vervolgd.

Opzet van ransomware-aanvallen

De tweede onderzoeksvraag luidt: *Hoe zien ransomware-aanvallen er tegenwoordig uit en welke instrumenten worden hierbij ingezet?*

Een ransomware-aanval bestaat uit verschillende stappen waarin per stap van verschillende instrumenten gebruik gemaakt wordt.

1. **Initial access**. De aanvaller krijgt een eerste toegang (‘foothold’) bij het slachtoffer, vaak een account van een medewerker van een organisatie binnen een specifieke applicatie of op een specifieke server. Hiertoe wordt gebruik gemaakt van instrumenten die automatisch scannen op zwakheden in systemen. Ook wordt er veel gebruik gemaakt van (spear)phishing.
2. **Consolidatie toegang en positie**. Wanneer de aanvaller eenmaal een ingang heeft, zal deze proberen de toegang tot de systemen van het slachtoffer uit te breiden. Zo zal de aanvaller zoeken naar systemen met waardevolle informatie en toegang tot accounts proberen te verkrijgen met meer rechten op deze systemen. Deze stap vraagt relatief veel (niet-geautomatiseerd) handwerk en er wordt gebruik gemaakt van verschillende tools en software.
3. **Data-exfiltratie**. Bij sommige ransomware-aanvallen worden gegevens van het slachtoffer gestolen, waarna de aanvaller de dreiging van doorverkoop of publicatie van de data gebruikt als chantagemiddel. Bij exfiltratie wordt niet alleen gekeken naar bestanden die zich op de eigen server van een organisatie bevinden, maar, maar vaak gebruik gemaakt van clouddiensten (zoals Dropbox en OneDrive), webgebaseerde diensten (zoals Mega en WeTransfer) en zelfs van systemen die door het slachtoffer ingezet worden voor het maken van eigen back-ups.
4. **Ransomware deployment**. De eerste twee stappen waren generieke stappen die in veel verschillende cyberaanvallen gebruikt worden. Bij deze stap maakt de aanvaller de keuze om ransomware in te zetten om zo hun positie in systemen van slachtoffers snel te gelde te maken. De ransomware-software voert de daadwerkelijke ‘gijzeling’ van

bestanden uit. Doel van deze stap is om een grote hoeveelheid (liefst waardevolle) bestanden van een organisatie te versleutelen met een sleutel waarover alleen de aanvaller beschikt.

5. **Chantage en cash out.** In deze fase communiceert de aanvaller met het slachtoffer en maakt deze kenbaar wat het slachtoffer moet doen om de aanval te stoppen en de gegevens terug te krijgen of publicatie tegen te gaan.

Een ransomware-aanval kan zowel gericht als ongericht zijn. Bij een ongerichte aanval maakt het de aanvaller niet uit welke organisatie of persoon het slachtoffer wordt. Bij een gerichte aanval heeft een aanvaller a priori een specifieke organisatie in het vizier. Tegenwoordig is voornamelijk sprake van 'semi-gerichte' aanvallen op organisaties. Na de eerste stap (*initial access*) wordt bepaald welke toegangsgegevens interessant genoeg zijn om de volgende stap mee in te gaan. Dit proces herhaalt zich in de daaropvolgende stappen.

Betrokken actoren bij ransomware-aanvallen

De derde onderzoeksvraag is als volgt: *Welke soorten partijen zijn bij deze aanvallen betrokken?*

De eerste ransomware-aanvallen werden gepleegd door individuele criminelen, maar inmiddels is er sprake van een uitstekend functionerende supply chain van verschillende soorten actoren met een hoge mate van specialisatie. Het ransomware-ecosysteem opereert bijna alsof het een legitieme, goed ontwikkelde dienstensector is. Initiële toegang tot netwerken wordt bijvoorbeeld vaak via platformen verkocht aan de hoogste bieder. Er zijn verschillende soorten partijen die op verschillende manieren deze toegang proberen te verwerven. De kopers van de initiële toegang werken dit op hun beurt uit, consolideren deze positie en verkopen deze positie wederom aan de hoogste bieder. De daadwerkelijke ransomware-aanval komt pas in de fase erna. De partijen die ransomware-software ontwikkelen en beheren zijn niet altijd de partijen die deze software ook daadwerkelijk gebruiken. Vaak worden er affiliates ingezet die de aanval uitvoeren. Er zijn daarnaast datamanagers die gestolen data analyseren, verkopen en/of openbaar maken. In de laatste stap (chantage en cash out) zijn een breed scala aan partijen betrokken: onderhandelaars, helpdesks, witwassers, et cetera.

Verreweg het meest voorkomende motief voor ransomware-aanvallen is financieel gewin. Activisme komt slechts sporadisch voor. Ransomware-criminelen gedragen zich deels als rationele actoren: de kosten, opbrengsten en pakkans worden geregeld zorgvuldig afgewogen. Daders lijken relatief vaak uit landen te komen die voorheen deel uitmaakten van de Sovjet-Unie. In sommige gevallen vallen daders bepaalde soorten organisaties bewust niet aan. Voorbeelden zijn organisaties uit landen in de voormalige Sovjet-Unie en de zorgsector gedurende de Coronacrisis.

Risicofactoren voor ransomware-aanvallen

De vierde en vijfde onderzoeksvraag zijn: *Welke interne en externe factoren dragen bij aan ransomware-risico's voor een organisatie? In hoeverre zijn deze factoren kwantificeerbaar?*

Bij interne factoren gaat het over aspecten waar het mogelijke slachtoffer zelf controle over heeft. Voor het onderzoeken van de interne factoren is gekeken naar literatuur, (cyber)risicotaxatietools en cybersecurityverzekeringen. Door te tellen hoe vaak factoren in deze verschillende bronnen voorkomen is gekwantificeerd hoe groot deze risicofactor is. De onderstaande tabel toont de tien interne factoren die het vaakst in deze drie bronnen benoemd worden, gerangschikt naar omvang van de risicofactor. Een generieke interne

risicofactor die de onderstaande factoren overkoepelt is het niet goed in kaart hebben welke systemen gebruikt worden. De uitkomsten zijn geverifieerd met interviews.

1. Geen goede back-up | fase: herstellen
2. Onvoldoende training medewerkers over phishing, scams, etc. | fase: voorkomen
3. Software is niet up-to-date | fase: voorkomen
4. Niet hebben van een *incident response plan* | fase: herstellen
5. Onvoldoende gebruik van (up-to-date) anti malware oplossingen| fase: voorkomen
6. Onvoldoende *privileged access strategy* | fase: beperken
7. Onvoldoende beveiligde accounts | fase: voorkomen
8. Onvoldoende continue monitoring | fase: beperken
9. Onvoldoende netwerksegmentatie | fase: beperken
10. Onvoldoende e-mailsecurity | fase: voorkomen

Naast de bovenstaande lijst is er een flinke serie met andere factoren die minder vaak benoemd worden. Dit zijn veelal technische maatregelen om te voorkomen dat infecties plaats kunnen vinden.

Bij externe factoren gaat het om de eigenschappen waar het mogelijke slachtoffer geen of beperkt controle over heeft. In lijn met de verschillende soorten impact die aanvallen op organisaties hebben komt hier naar voren dat de volgende aspecten de verwachte opbrengst voor daders (en hiermee het risico voor slachtoffers) verhogen (1) het hebben van een hogere omzet, (2) de inzet van IT-systemen waarvan uitval de bedrijfscontinuïteit kan verstoren en (3) de opslag van persoonsgegevens. Het hebben van een geschiedenis in het betalen van losgeld kan het risico voor organisaties mogelijk ook verhogen, al verschillen de meningen van experts op dit onderwerp. De volgende twee aspecten verlagen de kosten voor de dader: de lage pakkans en het niet te veel op de radar komen.

Beleidsopties om risico's te verkleinen

De zesde en zeven onderzoeksvragen luiden: *Met welk instrument kunnen bestuurders in middelgrote en kleine organisaties bewust worden gemaakt van de risico's van ransomware?* en *(Hoe) kunnen de vastgelegde factoren worden gebruikt in dit instrument?*

Uit onze analyse komt naar voren dat een bewustwordingscampagne voor bestuurders van kleine en middelgrote organisaties waarschijnlijk een doelmatig en doeltreffend instrument is om de kans op en de impact van ransomware-aanvallen te verminderen. Op dit moment worden zowel het risico als de impact van deze aanvallen onderschat door bestuurders van organisaties. De ICT'ers zijn zich veel beter bewust hiervan, maar blijkbaar wordt dit onvoldoende overgebracht op de bestuurders van deze organisaties. Omdat grote organisaties hun zaken op dit gebied vaak beter op orde hebben (en omdat ze vaak in een heel specifieke context opereren) is het logisch om de focus op middelgrote en kleine organisaties te leggen. Een goede campagne zou de volgende elementen moeten bevatten:

- De campagne moet confronterende feiten bevatten, zoals de gemiddelde schade die slachtoffers ervaren.
- Bestuurders moeten worden geprikkeld om stil te staan bij hun eigen situatie. Dat kan door ze te vragen wat het effect op hun organisatie is als (1) alle gegevens openbaar worden of (2) ICT drie weken niet gebruikt kan worden of (3) losgeld betaald moet worden ter grootte van bijvoorbeeld 5 procent van de omzet.
- De campagne moet concrete handelingsperspectieven bevatten door duidelijk te maken hoe en wat een organisatie minstens op orde moet hebben om goed beschermd te zijn tegen ransomware-aanvallen . De interne risicofactoren sluiten hier goed bij aan.

- De inhoud van de campagne moet actief onder de aandacht gebracht worden en bestuurders moeten een persoonlijk gerichte boodschap ontvangen. Hiervoor zijn verschillende kanalen mogelijk, maar het lijkt zinnig om aan te sluiten bij bekende relaties van de bestuurder zodat er een betrouwbare en bekende bron wordt gehanteerd.
- Door de hoge mate van heterogeniteit van deze doelgroep lijkt een sectorale aanpak voor de hand te liggen. In combinatie met het vorige punt zouden branche- en sectororganisaties een belangrijke rol kunnen spelen.
- Tot slot kan het presenteren van een sociale norm een krachtig instrument zijn. Bestuurders moeten het gevoel krijgen dat vergelijkbare organisaties ook stappen nemen om zich te beschermen tegen ransomware.

Er zijn uiteraard ook andere mogelijkheden om gedragsverandering en bewustwording te bereiken. Zo zou een bepaald niveau van cybersecurity kunnen worden afgedwongen door klanten, leveranciers, verzekeraars of zelfs de overheid. Dit kan gelden voor zowel ICT-dienstverleners als reguliere organisaties.