Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Incidentresponsplan Ransomware

De incidentrespons cyclus, toegepast op ransomware

Versiebeheer

Versie	Aanleiding / wijzigingen	Datum
0.1	Eerste opzet	Nov. 2021
0.3	Review vanuit NCSC thema incidentresponsprocessen	Nov. 2021
0.8	Review binnen NCSC unit operatie	Jan. 2022
0.9	Externe review	Maart 2022
1.0	Definitieve opmaak	Mei 2022

Dit stuk is tot stand gekomen met bijdragen van Ahold Delhaize, de Betaalvereniging, CIBG, Equens, en de Politie.

Toegestane verspreiding: TLP WHITE
(Traffic Light Protocol)

Deze handreiking bevat het label TLP: WHITE en wordt door het NCSC verspreid. Het NCSC gebruikt het Traffic Light Protocol (TLP) om eenduidig te definiëren wat er met de informatie mag gebeuren. Wanneer informatie is voorzien van een TLP-aanduiding weet u met wie u deze informatie mag delen. Dit staat beschreven in de standaard First (www.first.org/tlp). Ontvangers mogen de informatie uit deze handreiking delen binnen en buiten hun organisatie, daarnaast mag de informatie openbaar publiek gemaakt worden.

Uw reacties zijn welkom op info@ncsc.nl.

Inhoudsopgave

Beoogd gebruik van dit plan

Dit plan is bedoeld als voorbereiding op en ter ondersteuning van incidentrespons. In het Engels ook wel playbook genoemd, staat dit plan ten dienste van organisaties die getroffen zijn, of denken getroffen te kunnen worden door een ransomware-aanval. Hierbij is het van belang om te benadrukken dat een goede voorbereiding essentieel is voor een effectieve incidentrespons. Ransomware kan een ernstige bedreiging van (ICT) dienstverlening voor een organisatie betekenen met een langdurige en kostbare impact. In het licht van zo'n mogelijk ernstig incident, is het goed om niet zelf van nul af aan te hoeven bedenken wat te doen, maar om een eerste opzet te hebben om van uit te gaan.

Dit stuk is ingedeeld volgens de stappen zoals beschreven in de SANS incidentresponscyclus[1]. Indien het wordt gebruikt om de weerbaarheid te verhogen tegen een ransomware-incident, zal met name de eerste fase van belang zijn. Daarin is een groot aantal uiteenlopende aspecten opgenomen, die niet voor alle organisaties even geschikt zullen zijn. Allereerst gaat het om basismaatregelen die ingezet kunnen worden bij herstelwerkzaamheden. Daarnaast zijn er meer geavanceerde maatregelen om de impact van een aanval te beperken of om een aanval vroegtijdig te detecteren. Vanwege het uiteenlopende karakter van de maatregelen, zal de implementatie ervan ook sterk variëren. Soms kunnen bestaande maatregelen worden aangescherpt om ze effectiever te maken. In andere gevallen omvat de invoering een heel traject, inclusief passende processen en procedures.

Wanneer een organisatie al getroffen is door een ransomware-aanval, is een effectieve respons essentieel en kunnen de fasen vanaf 'identificatie' een handvat bieden in de aanpak.

Bij gebruik van dit plan is het van belang om alleen de relevante onderdelen te selecteren en te vertalen naar de actuele situatie. Daarnaast zullen voor de organisatie specifieke maatregelen en activiteiten toegevoegd moeten worden om een passende aanpak te krijgen.

[1] Zie het SANS Incident Handler's Handbook: https://www.sans.org/white-papers/33901/.

Incidentrespons

Definitie

Voor dit incidentresponsplan definiëren we een **ransomware-incident** als een digitale aanval die systemen of bestanden onbruikbaar maakt door ze te versleutelen waardoor data gegijzeld is. Deze gijzeling gaat gepaard met afpersing, waarbij ontsleuteling wordt aangeboden tegen een betaling, meestal in crypto-valuta.

Er zijn variaties van ransomware-afpersing waarbij naast versleuteling ook data gestolen wordt en gedreigd wordt om deze te lekken wanneer er niet betaald wordt *(double-extortion)* en waarbij gedreigd wordt om gegevens bekend te maken aan klanten of om klanten af te persen met de buit gemaakte gegevens *(triple-extortion)*.

In bijlage 1 is een schematische weergave opgenomen van hoe een ransomware-aanval werkt, zoals beschreven door het Nieuw-Zeelandse nationale CERT (CERT NZ).

Belangrijk is hierbij om op te merken dat *ransomware niet alleen een technisch probleem is*. In de meeste gevallen gaat het om zware, georganiseerde cybercriminaliteit. Politie en OM spannen zich in om dit te bestrijden, maar kunnen dat alleen als er samenwerking met hen gezocht wordt. Dat kan door aangifte te doen of een melding te maken bij de politie.

Bij het verrichten van incidentrespons is het van belang om een aantal aandachtspunten altijd te hanteren. Onder druk bij het verhelpen van de verstoring worden deze gemakkelijk uit het oog verloren. We benoemen ze hieronder.

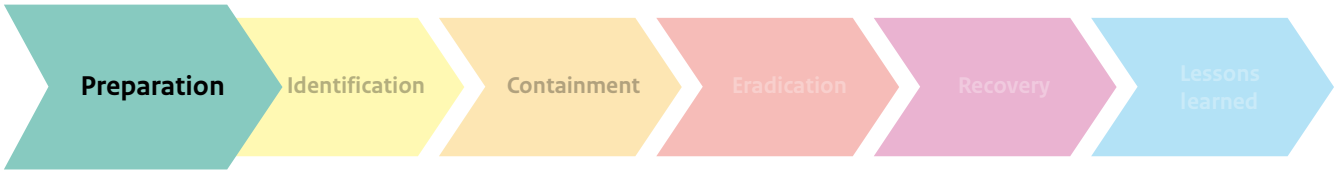
Aandachtspunten voor de incidentrespons

- Houd je aan de afgesproken incidentrespons-procedures en –afspraken;
- Ga planmatig te werk;
- Maak notities van je bevindingen en activiteiten (houd een logboek bij op datum en tijd);
- Beperk je bij het communiceren en vastleggen tot feiten, vermeld expliciet welke conclusies worden getrokken en vermijd aannames;
- Zorg dat alle betrokkenen op de hoogte blijven van de actuele status en informatie;
- Communiceer regelmatig en kondig telkens het volgende communicatiemoment aan;
- Blijf kalm en houd contact met het incident respons team, CERT of CSIRT.

Communicatie

Communicatie is een van de strategische processen die helpen om een calamiteit en/of crisis te managen. Voor de interne organisatie is het van belang om medewerkers helderheid te bieden om ruis en onrust op de werkvloer te voorkomen. Naar de buitenwereld wordt communicatie ingezet om de reputatie van en het vertrouwen in de organisatie te beschermen en/of te herstellen. Dit vereist dat zo veel mogelijk onzekerheid wordt weggenomen door zorgvuldig informatie te verstrekken, een handelingsperspectief te bieden en duiding te geven aan wat er gebeurt. Stakeholders zijn vooral gebaat bij open communicatie om vervolgschade te beperken.

Voorbereiding



In de voorbereiding op dit type incident kunnen per thema onderstaande acties worden uitgevoerd.

Continuïteitsmanagement

- In voorkomende gevallen zal er behoefte zijn aan een integrale - met netwerkpartners gecoördineerde - aanpak. Zorg daarom voor contracten en service level agreements (SLA's) waarin de aanwezigheid en beschikbaarheid van de betrokken partners geregeld is;
- Borg dat er 24x7 stand-by-managers zijn die piketdiensten draaien voor de kritieke voorzieningen. Let daarbij op de toepassing en naleving van de arbeidsrechtelijke voorwaarden;
- Zorg voor (snel) beschikbare images om kritieke systemen te kunnen voorzien van een basis inrichting bij het uitrollen in een schone omgeving;
- Zorg voor (snel) beschikbare reserve hardware en beschikbare software om kritieke systemen opnieuw uit te rollen in een schone omgeving;
- Zorg voor een herstelplan (afhankelijkheden, wijze en volgorde van herstel, verantwoordelijkheden, systeemeigenaren) van de ICT-systemen en de kritieke systemen en test en actualiseer dit regelmatig.

Back-up

- Bepaal welke vorm van back-up (incremental of full) noodzakelijk is en welke retentietijd gehanteerd moet worden;
- Zorg voor een periodieke offline back-up van centrale en decentrale data;
- Zorg voor een periodieke back-up van alle systemen en virtuele machines (VM's);
- Controleer elk back-up resultaat en periodiek het back-up proces op mogelijke fouten;
- Verifieer de integriteit van de back-up regelmatig (door o.a. een restore uit te voeren);
- Test de back-up regelmatig tegen de overeengekomen recovery point objective (RPO) en recovery time objective (RTO) (*zie gerelateerde informatie*);
- Sla back-ups of back-up media offline en off-site op;
- Zorg ervoor dat online en offline back-ups niet met dezelfde accounts toegankelijk zijn; gebruik hiervoor andere accounts dan standaard beheeraccounts (inclusief multi-factor authenticatie).

Inrichting en inrichtingsprincipes

- Segmenteer het netwerk op basis van zowel functionaliteit als beveiligingsniveau. Volg hierbij bij voorkeur het *zero trust* principe *(zie gerelateerde informatie)*;
- Pas systeem hardening toe volgens de richtlijnen van leveranciers of CIS benchmarks *(zie gerelateerde informatie)*;
- Geef gebruikers en administrators minimale rechten, pas het *principle of least privilege* toe;
- Gebruik een veilige VPN-oplossing die voldoet aan de TLS-richtlijnen *(zie gerelateerde informatie)*;
- Sluit management interfaces uitsluitend aan op een management (V)LAN;
- Maak gebruik van sterke wachtwoorden en hergebruik deze wachtwoorden niet. Vul waar mogelijk de authenticatie aan met multi-factor authenticatie (MFA) *(zie gerelateerde informatie)*;
- Beperk het gebruik van lokale beheeraccounts;
- Zorg ervoor dat lokale beheeraccounts op verschillende systemen verschillende (random) wachtwoorden hebben. Gebruik hiervoor bijvoorbeeld de Microsoft Local Administrator Password Solution (LAPS);
- Beperk, bescherm en monitor het gebruik van Active Directory domain administrator accounts;
- Zet toegang tot systemen via RDP uit, tenzij het niet anders kan. Beveilig – als het niet anders kan – remote access kanalen en RDP met onder meer MFA en een VPN-oplossing en log het gebruik.

Inventarisbeheer en configuratiebeheer

- Identificeer kritieke systemen en bepaal de impact wanneer deze geraakt worden door ransomware;
- Zorg voor een actueel en compleet overzicht van systemen en onderlinge afhankelijkheden;
- Leg bij iedere wijziging de configuratie van systemen vast;
- Ontwikkel en onderhoud infrastructuurontwerpen met kritieke systemen en datastromen. Houd hierbij rekening met ketenpartners en uitbestede dienstverlening;
- Zorg dat productkaarten en architectuurplaten van de kritieke voorzieningen op efficiënte beschikbaar en up-to-date zijn.

Monitoring en detectie

- Zorg voor beveiliging van de e-mailomgeving, waaronder het scannen op bijlagen of internet-koppelingen;
- Zorg voor (beveiligde en centrale) logging in het netwerk van:
  - Uitgevoerde (powershell) scripts en pogingen tot het uitvoeren van (powershell) scripts;
  - Event-Ids voor authenticatie;
  - Event-Ids voor het creëren van services en persistente processen;
  - (Grote) uitgaande datastromen;
  - Event-Ids voor creatie of aanpassing van (privileged) accounts
- Gebruik canary files (documenten of bestanden die niet gebruikt en aangepast zouden moeten worden) om ongeoorloofde wijzigingen op het bestandssysteem te detecteren;
- Monitor het gebruik van gevoelige beheeraccounts, zoals Domain Admin accounts.

Processen en procedures

Communicatie

- Houd rekening met het uitvallen van reguliere communicatiekanalen (telefoon, e-mail, toegang tot adresboek, chat), bereid vertrouwelijke alternatieven of uitwijkmogelijkheden voor, test deze en houdt ze up-to-date;
- Bepaal een interne en externe communicatiestrategie. Zorg dat stakeholders (medewerkers, woordvoering/persvoorlichting, ketenpartners, klanten, raad van bestuur, data protection officers,) tijdig worden geïnformeerd en houd rekening met:
  - De inkoopafdeling kan wellicht helpen bij het verstrekken van een overzicht van leveranciers;
  - Betrek de juridische afdeling in de voorbereiding en laat een extern communicatiehandboek eventueel vooraf goedkeuren;
- Bepaal de communicatiestrategie wanneer gestolen data wordt gepubliceerd, waaronder:
  - Welke verzenders en ontvangers zijn van belang;
  - Welke berichten moeten worden verstuurd;
  - Welke toezichthouder(s) (onder meer Autoriteit Persoonsgegevens) moeten worden geïnformeerd;
  - Welke andere organisaties geïnformeerd moeten worden (NCSC, politie, etc.);
- Bepaal een strategie voor het omgaan met de ransom note. Contact opnemen met de gijzelnemers kan van belang zijn om zekerheid te krijgen of data ontvreemd is en welke databronnen geraadpleegd zijn. Daarnaast moeten criminelen tijdens het onderhandelen informatie delen; dit verhoogt de kansen op succesvolle opsporing. *Daarbij is het van belang om op te merken dat contact hebben met de gijzelnemers niet inhoudt dat er losgeld betaald moet worden*. Het dringende advies van de politie en vanuit het Kabinet blijft om geen losgeld te betalen na een ransomware-aanval, aangezien dit het crimineel verdienmodel in stand houdt[2]. Betaling geeft bovendien niet de garantie geeft dat het probleem is opgelost: er zijn gevallen bekend waarbij ook na betaling de ontsleuteling niet (geheel) plaatsvindt; de aanvaller kan zich ook na betaling nog steeds in uw netwerk bevinden; de aanvaller kan uw data hebben weggesluisd en u daarmee later opnieuw afpersen (de dader weet nu dat u bereid bent tot betalen). Houd voor het contact over de ransom note rekening met:
  - Wie moet worden ingeschakeld om een gesprek met de gijzelnemers te voeren;
  - Welke informatie moet in een onderhandeling/gesprek vastgesteld worden;
  - Hoe wordt met een eis tot losgeld omgegaan;
  - Wie doet wanneer aangifte of maakt een melding bij de politie.

Incidentrespons

- Stel een incidentresponsplan op, waarin onder meer is opgenomen:
  - Wie er betrokken moet worden bij een cybersecurity incident;
  - Hoe, op basis van welke criteria en door wie wordt vastgesteld dat sprake is van een security incident;
  - Wie verantwoordelijk is voor oplossen van het incident;
  - Hoe en wanneer er wordt aangesloten bij reguliere (ITIL) incidentmanagement procedures;
- Weet wie de interne sleutelfunctionarissen en de externe stakeholders zijn;
- Maak het mandaat van betrokkenen expliciet, in het bijzonder bij welke functionaris het stekkermandaat ligt om een voorziening uit te schakelen;
- Beschrijf de rol en het gestructureerde werkproces van het incidentresponsteam. Beschrijf tevens de gewenste invulling en competenties per rol van het team, in de vorm van functiebeschrijvingen;
- Voer een standaard overlegstructuur in voor crisisoverleggen, zoals de BOB structuur (Beeld, Oordeelsvorming, Besluitvorming) en oefen het overleg volgens deze structuur;

[2] https://www.nomoreransom.org/nl/ransomware-qa.html
https://www.politie.nl/nieuws/2020/februari/6/00-politie-%E2%80%98niet-betalen-bij-ransomware.%E2%80%99.html
https://www.tweedekamer.nl/kamerstukken/kamervragen/detail?id=2021Z16018&did=2021D37453

- Borg dat de leden van het incidentresponsteam voldoende rust- en slaapmomenten hebben tijdens het verrichten van de incidentrespons;
- Rust betrokkenen uit met middelen om ook buiten kantooruren snel en gemakkelijk als team in contact te kunnen treden. Maak het mogelijk dat betrokkenen ook buiten kantooruren vanuit de kantooromgeving (inclusief uitwijklocatie) kunnen werken;
- Aangezien uit diverse ransomware incidenten blijkt dat veelal op vrijdagavond ransomware wordt uitgevoerd op de systemen, is het nuttig om hier voor piketrollen en de beschikbaarheid van incidentresponsteam leden rekening mee te houden;
- Zorg voor een contract met een service verlener of incidentrespons partij voor ondersteuning en uitvoering van bijvoorbeeld recovery en forensisch onderzoek;
- Simuleer en oefen een ransomware-aanval met medewerkers. Evalueer deze oefening en gebruik dit als input om het incidentresponsplan waar nodig bij te werken;
- Houd rekening met richtlijnen, wetgeving en regelgeving (bijvoorbeeld voor het informeren van toezichthouders, stakeholders en autoriteiten) en verwerk dit in het incidentresponsplan. Houdt hierbij ook rekening met de mogelijkheid om een vrijwillige Wbni-melding te kunnen doen of een verplichte Wbni-melding te moeten doen bij het NCSC of bij CSIRT DSP;
- Wees voorbereid op het doen van aangifte of het maken van een melding bij de politie. Hierdoor krijgt de politie beter zicht op het fenomeen ransomware en kan het de juiste prioriteit krijgen. Raadpleeg hiervoor de brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten', die politie heeft opgesteld om maatregelen te nemen die het opsporingsonderzoek ondersteunen *(zie gerelateerde informatie)*. Het verrichten van aangifte of het doen van een melding kan tevens nieuwe aanvallen voorkomen. Zo kan de politie andere organisaties waarschuwen of servers met schadelijke software uitschakelen.

Accounts en rechten

- Verwijder onnodige of niet gebruikte useraccounts en -groepen;
- Ken minimale domein-, admin- en rootrechten toe aan accounts;
- Beperk de toegang tot domain controllers tot een afzonderlijke domain administrator-groep;
- Beperk de rechten van de domain administrator groep en gebruik de accounts die lid zijn enkel voor het beheer op de domain controllers. Maak aparte administrator accounts voor andere beheertaken;
- Log het gebruik en aanmelden van beheeraccounts (zowel gelukte als mislukte inlogpogingen).

Overig

- Zorg dat in het netwerk in beeld te brengen is:
  - Welke (onbekende) bestanden zijn of worden uitgevoerd;
  - Welke (powershell) scripts zijn of worden uitgevoerd;
  - Welke 'lateral movement' (laterale bewegingen tussen werkstations/endpoints) plaatsvindt of heeft plaatsgevonden;
  - Welke (grote hoeveelheden) data wordt of is geëxfiltreerd;
  - Wie op welk systeem is ingelogd of gebruik heeft gemaakt van resources;
- Stel een procedure op voor het maken van een forensisch image van werkstations en servers en test deze regelmatig;
- Zorg voor een geïmplementeerd patch- en upgrade beleid en update systemen (servers en werkstations) regelmatig; baseer de prioriteit en planning van het patchen op de ernst van de verholpen kwetsbaarheden;
- Zorg voor een emergency patch en update proces om kritieke kwetsbaarheden direct te kunnen mitigeren.

Technische maatregelen

- Installeer een Endpoint Detection and Response (EDR) tool zowel op clients als op servers;
- Implementeer network segmentatie gebaseerd op functie (ontwikkel, test, acceptatie en productie) en data classificatie (openbaar, intern, vertrouwelijk, geheim, persoonsgegevens, bijzondere persoonsgegevens);
- Voer multi-factor authenticatie (MFA) in;
- Onderhoud antivirussoftware en controleer deze; scan alle software die van het internet wordt gedownload alvorens deze uit te voeren;
- Zet macro's in office-software centraal uit, zodat macro's in geïnfecteerde bestanden niet uitgevoerd kunnen worden;
- Zet het volgen van weblinks of het openen van afbeeldingen in e-mails uit;
- Zet het Remote Desktop Protocol (RDP) aan de internetzijde uit (ransomware verspreidt zich vaak door kwaadwillenden die organisaties hebben gecompromitteerd via RDP);
- Controleer de periferie van het netwerk op de aanwezigheid van management interfaces aan de buitenzijde en schakel deze uit;
- Overweeg de toepassing van PowerShell constrained language mode om PowerShell gebruik te limiteren;
- Overweeg aanvullende PowerShell log maatregelen toe te passen, zoals: Module logging, Script-Block logging en Transscript logging;
- Overweeg - als u Windows besturingssystemen gebruikt - Applocker en Windows Defender Application Control toe te passen om het gebruik van ongewenste scripts en software te limiteren;
- Maak gebruik van de 'Protected Users' Active Directory groep in Windows Active Directory voor privileged user accounts om de kans op pass-the-hash aanvallen te bemoeilijken;
- Overweeg applicatie whitelisting;
- Installeer geen extra software op domain controllers of op andere systemen en verwijder reeds geïnstalleerde software die niet nodig is;
- Schakel onnodige services uit op domain controllers en andere servers en schakel de print spooler service uit op domain controllers;
- Blokkeer internetconnectiviteit op de domain controllers. Updates kunnen worden opgehaald via een WSUS-oplossing;

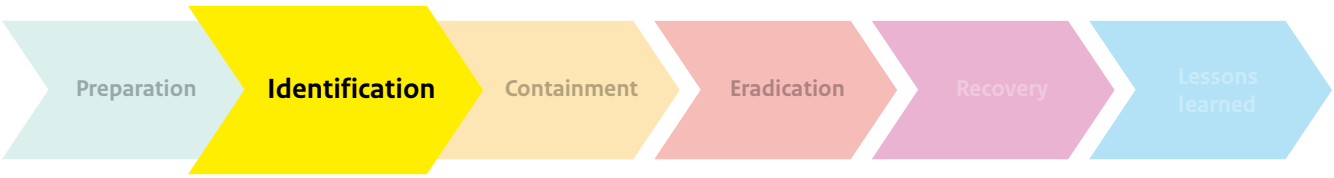
- Overweeg op Windows servers extra Local Security Authority (LSA) beveiliging in te voeren (het LSA proces valideert (lokale en externe) gebruikersaanmelding en zorgt voor de toepassing van beveiligingsbeleid (policies));
- Bepaal en configureer het gebruik van Bit-Locker of andere disk encryptie (indien niet gebruikt kan het gebruikt worden door aanvallers);
- Blokkeer het gebruik van ongeautoriseerde USB-apparatuur en configureer het toegestane gebruik van geautoriseerde USB-apparatuur;
- Overweeg uitgaand verkeer te filteren op de firewall, configureer welke applicaties en servers naar buiten mogen communiceren.

Medewerkersbewustzijn

Denk bij medewerkers ook aan inhuurkrachten, adviseurs en gedetacheerde medewerkers.

- Zorg voor kennis en bewustzijn bij medewerkers over:
  - Phishing varianten en het herkennen hiervan;
  - Het signaleren van social engineering;
  - De verspreiding van malware en ransomware;
  - Het herkennen van een ransomware-besmetting en hoe hierop te reageren;
  - Hoe verdachte waarnemingen of mogelijke besmettingen gemeld kunnen worden;
  - Het gebruik van verschillende wachtwoorden voor verschillende systemen en omgevingen (ondersteun medewerkers hierin door een wachtwoordmanager aan te bieden);
  - Het gewenste gebruik van bedrijfseigendommen en mobiele apparaten;
  - Het social mediabeleid van de organisatie;
- Maak het voor medewerkers eenvoudig om verdachte e-mail berichten te melden, bijvoorbeeld door hiervoor een menu-optie of knop aan te bieden;
- Maak een lijst met sleutelfunctionarissen en wijs ze op de mogelijke spionagerisico's vanwege hun functie of positie binnen de organisatie;
- Zorg voor een beleidsplan voor opleiden, trainen en oefenen van onder meer bovenstaande aspecten en voer het plan uit.

Identificatie



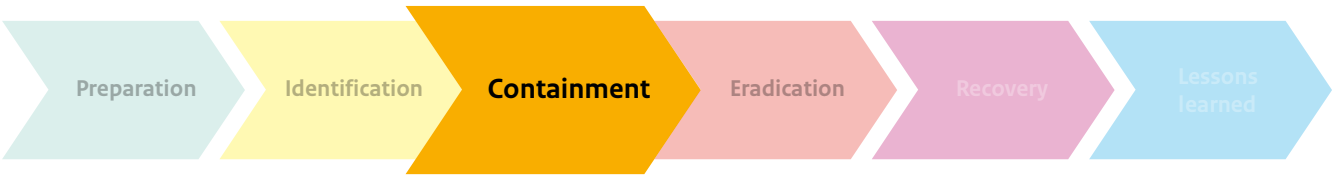
Opmerking vooraf: Het kan zijn dat een ransomware-incident zich manifesteert met een grootschalige verstoring van (ICT) dienstverlening doordat bestandssystemen versleuteld zijn. Hierdoor kan het nodig zijn om meteen te beginnen met het herstellen van een (schone) omgeving om zo snel mogelijk de dienstverlening te kunnen hervatten. ***Het blijft ook dan echter noodzakelijk om parallel aan het herstel de incidentresponscyclus te doorlopen, te beginnen met identificatie.*** Het is immers zaak om kwaadwillenden uit het netwerk te weren en ook in de toekomst buiten het netwerk te houden.

Onderstaande zaken kunnen een indicatie zijn van een ransomware incident. Hierbij staan ook een aantal activiteiten, die kunnen worden uitgevoerd ter identificatie:

- Ongebruikelijke facturen of andere zakelijke e-mails, mogelijk voorzien van malafide bijlagen of koppelingen;
- Ransomware berichten op het bestandssysteem;
- Ransomware meldingen op het beeldscherm;
- Ransomware berichten via e-mail;
- Medewerkers melden dat zij hun bestanden niet meer kunnen openen;
- Grote hoeveelheden bestanden worden (achtereenvolgens) aangepast op een (netwerk) bestandssysteem;
- Een ongebruikelijk(e) (grote) hoeveelheid data wordt weggesluisd;
- Systeemanalyse leidt tot identificatie van server-side versleuteling. Onderzoek:
  - In Windows onder computermanagement bij “Sessions” en bij “Open Files “; controleer op verbonden systemen/gebruikers;
  - Eigendom van versleutelde bestanden; controleer het account dat deze bestanden wegschrijft;
  - De RDP-eventlog; controleer op onverwachte, succesvolle RDP-connecties;
  - De Windows Security-log en SMB-log; controleer op authenticatie events;
  - Netwerkcommunicatie via het SMB-protocol om open verbonden systemen te identificeren;
- Op een systeem wordt ongebruikelijke activiteit gezien of malware aangetroffen ie een bestandssysteem kan versleutelen (of modules kan downloaden die een bestandssysteem kunnen versleutelen). Onderzoek:
  - Ongebruikelijke binaries;
  - Forensische images van het geheugen;
  - Ongebruikelijke processen;
  - Ongebruikelijke taken in de Taakplanner
  - Ongebruikelijke patronen van e-mail bijlagen;
  - Ongebruikelijke netwerk- of web-browse-activiteit, bijvoorbeeld TOR-verkeer of verkeer naar cryptocurrency betaalsites;
- Er vindt mogelijk malafide communicatie of netwerkverkeer plaats. Denk daarbij onder meer aan:
  - Bekende patronen van exploit kits;
  - Verbindingen met (bekende) C2-servers;
  - Ongebruikelijk netwerkverkeer of web-browse-activiteit, bijvoorbeeld TOR-verkeer of verkeer naar cryptocurrency betaalsites;
  - E-mails met koppelingen naar verdachte of malafide websites;
  - Ongebruikelijke bijlagen in e-mails (bijlagen van een type dat een medewerker normaal niet ontvangt, bijlagen van een verzender die normaal geen bijlagen stuurt of bijlagen van een onbekende afzender);
- Er worden aankondigingen gedaan van een geslaagde ransomware-aanval door bekende actoren op het darkweb;
- Er worden geëxfiltreerde gegevens of bestanden aangeboden op het darkweb, afkomstig van een ransomware-aanval;
- Er wordt een phishing-aanval gedaan met kenmerken die te herleiden zijn tot bekende ransomware-aanvallen (gebruik hiervoor eventueel DMARK logs of DNS logs);
- Zorg na de waarneming van een ransomware-aanval voor een actueel situationeel beeld (welke systemen zijn getroffen en wat is de functie van die systemen, wie is verantwoordelijk voor dat systeem) en een impactassessment zodat te nemen maatregelen daarop aansluiten;

- Het is belangrijk om “Patient Zero” te identificeren om te kunnen begrijpen hoe de aanvaller binnengekomen is en in een later stadium de toegang te ontzeggen (er kan onder meer worden gezocht naar waar ongebruikelijke activiteit ontstond na ontvangst van een phishing mail, waarvandaan C2 communicatie plaatsvindt of waar gebruik wordt gemaakt van veelvoorkomende ransomware-gerelateerde tooling zoals installatie van een keylogger, exploitatie van een kwetsbaarheid middels Metasploit, uitvoering van Mimikatz of Cobalt Strike);
- Bepaal op basis van het actuele situationele beeld of het nodig is om een vrijwillige of verplichte Wbni-melding te verrichten bij het NCSC of bij CSIRT DSP;
- Monitor ketenpartners (klanten, leveranciers of samenwerkingspartners) op berichten over mogelijke ransomware-besmettingen.

Inperking



Om de gevolgen van dit type incident in te perken kunnen de volgende acties worden ondernomen:

- Koppel direct systemen los van het netwerk (op alle interfaces: bekabeld, wifi of mobiel) waarvan is vastgesteld of het vermoeden bestaat dat ze gecompromitteerd zijn (met ransomware) (loskoppelen kan ook door de vliegtuig-modus te activeren);
- Zet systemen niet uit, maar breng ze in slaapstand of mogelijk sluimerstand (indien beschikbaar, bijvoorbeeld op laptops). Dit om de toestand van het systeem niet te verstoren en zo het beste beeld te kunnen verkrijgen, het verlies van eventueel aanwezig sleutelmateriaal te voorkomen en om geen forensische sporen te verliezen voor mogelijk onderzoek;
- Bij een grote aanval kan worden overwogen om netwerk-infrastructuur, zoals wifi, routers en switches en internet-connectiviteit te ontkoppelen; verbreek indien mogelijk de verbinding met netwerken of netwerkdelen die nog niet zijn getroffen door de ransomware;
- Koppel direct externe apparaten los, zoals USB-/externe-schijven, mobiele telefoons of andere apparaten die besmet kunnen raken;
- Verbreek de verbinding met de netwerk-bestandsopslag indien een systeem niet kan worden geïsoleerd of losgekoppeld van het netwerk;
- Blokkeer of deactiveer alle accounts die (mogelijk) bij de ransomware-aanval betrokken zijn;
- Reset wachtwoorden en andere vormen van authenticatie voor administrator- en andere systeem- of services-accounts (**let op**: een reset van het wachtwoord van de KRBTGT service-account moet tweemaal achtereen worden uitgevoerd anders blijft toegang met het oude wachtwoord mogelijk) *(zie gerelateerde informatie)*;
- Reset wachtwoorden van gebruikers;
- Ontneem schrijfrechten op bestandssystemen aan processen of accounts waarmee ransomware wordt uitgevoerd;
- Controleer of MFA nog is ingesteld op de accounts en voor de toegang tot services waar dit de bedoeling is en corrigeer waar nodig indien een kwaadwillende de MFA heeft uitgeschakeld;
- Blokkeer het verkeer met mogelijk vastgestelde C2 servers;
- Lever de (kenmerken van) nog onbekende malware die gevonden is in het incidentresponsproces of de forensische analyse aan bij de endpoint securityprovider en het NCSC;
- Lever nog onbekende malafide URL's, domeinnamen of IP-adressen aan bij de netwerksecurityprovider en het NCSC;
- Rapporteer het incident zo vroeg mogelijk om verdere schade zo veel mogelijk te voorkomen (contactinformatie staat aan het einde van dit document);
- Verzamel mogelijk relevante logbestanden, zoals: Windows Security logs, Emaillogs, Firewall logs en Linux System logs;
- Indien een ketenpartner mogelijk besmet is geraakt, blokkeer dan de uitwisseling van e-mail en netwerkverkeer met deze organisatie totdat duidelijk is dat het besmettingsrisico geweken is;
- Overweeg in deze incidentresponsfase al om de politie te informeren. Het is voorgekomen dat de politie kon interveniëren bij het wegsluizen van informatie naar leak pages. Ook kan het mogelijk zijn dat de politie tijdig andere (potentiele) slachtoffers kan waarschuwen. Daarnaast is het in deze fase al relevant om te denken aan het veiligstellen van bewijs, zoals onder meer communicatiekanalen en BTC-adressen. Raadpleeg hiervoor de brochure 'Samen tegen Cybercrime, Stappenplan voor IT-specialisten', die politie heeft opgesteld om het opsporings-onderzoek ondersteunen *(zie gerelateerde informatie)*.

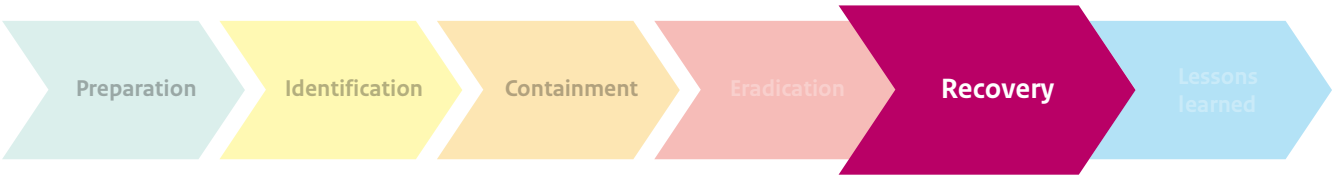
Eliminatie

Opmerking: *Ga pas over tot eliminatie als duidelijk is dat de gehele scope van de aanval in kaart is gebracht en er geen nieuwe geïnfecteerde machines meer worden gevonden. Te snel overgaan tot eliminatie kan een aanvaller informeren over de ondernomen incidentrespons acties en laat mogelijk een backdoor van de aanvaller of slapende malware achter.*

Om de inbreuk of impact van dit type incident te elimineren, kunnen de volgende acties worden ondernomen:

- Verwijder de malafide binaries en indien van toepassing bijbehorende registry waarden van (centraal opgeslagen) gecompromitteerde gebruikersprofielen en systemen (denk ook aan %ALLUSERPROFILE%, %APPDATA% en %SystemDrive%). Als opschonen niet mogelijk is, overweeg dan om (centraal) opgeslagen gebruikersprofielen te verwijderen;
- Herinstalleer de getroffen systemen met een schone image nadat eventueel lokaal opgeslagen data en bestanden in quarantaine zijn geplaatst;
- Noteer metadata, zoals signatures en oorsprong van de malware, domeinen en ip-adressen en blokkeer bekende malware(communicatie);
- Update antivirus signatures zodat de geïdentificeerde malware wordt geblokkeerd;
- Identificeer het systeem waarop de eerste inbreuk heeft plaatsgevonden en verhelp de oorzaak of mogelijke kwetsbaarheden.
- Voer de vastgestelde interne en externe communicatiestrategie uit. Zorg dat stakeholders (medewerkers, ketenpartners, klanten, raad van bestuur,) tijdig worden geïnformeerd.

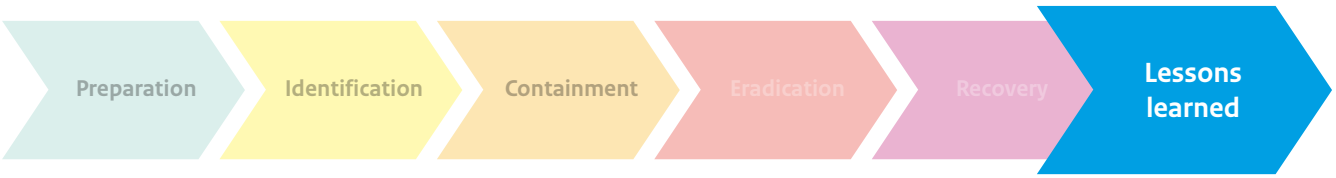
Herstel



Om te herstellen van dit type incident kunnen de volgende acties worden uitgevoerd:

- Overweeg bij een grote aanval het netwerk en bijhorende systemen parallel aan de bestaande omgeving op te bouwen. Importeer geen systemen of gegevens zonder deze grondig te controleren op de aanwezigheid van malware. Sluit geen systemen op de schone omgeving aan die verbonden zijn geweest met de besmette omgeving;
- Als het niet mogelijk is om parallel aan de bestaande omgeving een nieuwe omgeving op te bouwen bij een grote aanval met mogelijke compromittatie van de Active Directory, overweeg dan om een nieuwe rechtenstructuur op te bouwen met nieuwe accounts, waaronder ook beheer- en service-accounts, en alle oude accounts (permanent) te verwijderen;
- Gebruik voor herstel alleen zorgvuldig veilig verklaarde systemen;
- Zorg ervoor dat alle malafide binaries die aanwezig waren verwijderd zijn van de systemen als ze opnieuw moeten worden aangesloten en niet heringericht kunnen worden;
- Ga na of er bij het No More Ransom project *(zie gerelateerde informatie)* bekende decryptiesleutels of –software beschikbaar is voor de ransomware die is gebruikt in dit incident;
- Neem contact op met opsporingsdiensten voor het doen van aangifte en het verkrijgen van mogelijke decryptiesleutels;
- Deel (technische) informatie over het incident met de politie. Dat kan bij een aangifte, maar kan ook los van een aangifte worden gedaan. Dit kan de (internationale) opsporing en verstoring van dadergroepen helpen en het kan leiden tot het notificeren van andere (potentiele) slachtoffers;
- Scan back-ups op malware voordat deze worden hersteld. De kwaadwillenden zijn mogelijk al langere tijd in het netwerk waardoor malafide bestanden in de back-ups terecht kunnen zijn gekomen;
- Scan in quarantaine geplaatste data en bestanden en verwijder aangetroffen malware;
- Herstel versleutelde of gecompromitteerde servers of systemen uit een niet gecompromitteerde back-up;
- Herstel versleutelde bestanden uit een niet gecompromitteerde back-up;
- Als het niet lukt om de informatie te ontsleutelen of te herstellen uit een back-up en er is dataverlies, dan kan een kopie van de versleutelde informatie bewaard worden. Wanneer er dan later eventueel wel een methode komt om de informatie te ontsleutelen, kan deze eventueel alsnog teruggehaald worden.
- Corrigeer ongewenste configuratieaanpassingen die eventueel door de kwaadwillenden zijn doorgevoerd;
- Test en verifieer of het afwijkende gedrag (o.a. netwerkverkeer) is verdwenen na het herstellen van alle systemen en processen;
- Monitor het netwerk enige tijd extra intensief om er zeker van te zijn dat de aanvaller uit het netwerk verdwenen is en er niet meer in terug kan komen;
- Upgrade en update verouderde software en systemen.

Leerpunten



Uit dit soort incidenten kunnen na het herstellen lessen worden geleerd, die weer kunnen leiden tot verdergaande voorbereidingsacties. Omdat deze leerpunten voor elk incident specifiek zijn, kunnen ze niet vooraf worden vastgesteld. Het is echter wel van groot belang dat deze fase doorlopen wordt. Ook alle voorbereidende acties die al uitgevoerd zijn, kunnen in deze stap worden geëvalueerd. Om een goede terugkoppeling te krijgen voor de leerpunten, kan bij afsluiting van de actieve incidentrespons een after-action review met de betrokkenen gedaan worden, zodat ervaringen vers vanuit de beleving gedeeld kunnen worden.

Het komt de kwaliteit van verslaglegging ten goede als er altijd iemand aanwezig is die in alle fasen de rol van verslaglegging vervult zodat alle stappen, besluiten, bescheiden en dergelijke juist, tijdig, volledig en op controleerbare wijze zijn vastgelegd (aanvullend op de individuele logs die medewerkers bijhouden).

Geadviseerd wordt om de leerpunten in een rapportage op te nemen. Aanbevolen wordt om aandacht te besteden aan onder meer de volgende zaken:

- Verspreiding: wie gaan de rapportage ontvangen;
- Doelgroep van rapportage;
- Initiële besmetting;
- Activiteiten en tijdlijn;
- Geraakte systemen;
- Impact op beschikbaarheid;
- Invloed op of afhankelijkheden van (keten)partners, klanten, leveranciers of andere stakeholders;
- Kenmerken van de gebruikte ransomware (IOC's);
- Risico's van mogelijk gelekte gegevens in de buitenwereld;
- Effectiviteit en uitvoering van het incidentrespons proces (wat ging goed en wat kon beter);
- Kosten en doorlooptijd van het incident;
- Welke documentatie dient aangepast te worden op basis van de geleerde punten en wie dat gaat doen;
- Hoe breng je de organisatie op de hoogte van die wijzigingen;
- Door te voeren wijzigingen om toekomstige vergelijkbare incidenten te voorkomen of de impact ervan te verkleinen, met betrekking tot:
  - Systeemaanpassing en technische wijzigingen;
  - Aanpassingen in procedures en beleid;
  - Aanpassingen in incidentresponsprocedures of in specifieke incidentreponsplannen;
- Deel gevonden indicatoren en de rapportage met het NCSC, zodat andere organisaties gewaarschuwd of geïnformeerd kunnen worden.

Gerelateerde informatie

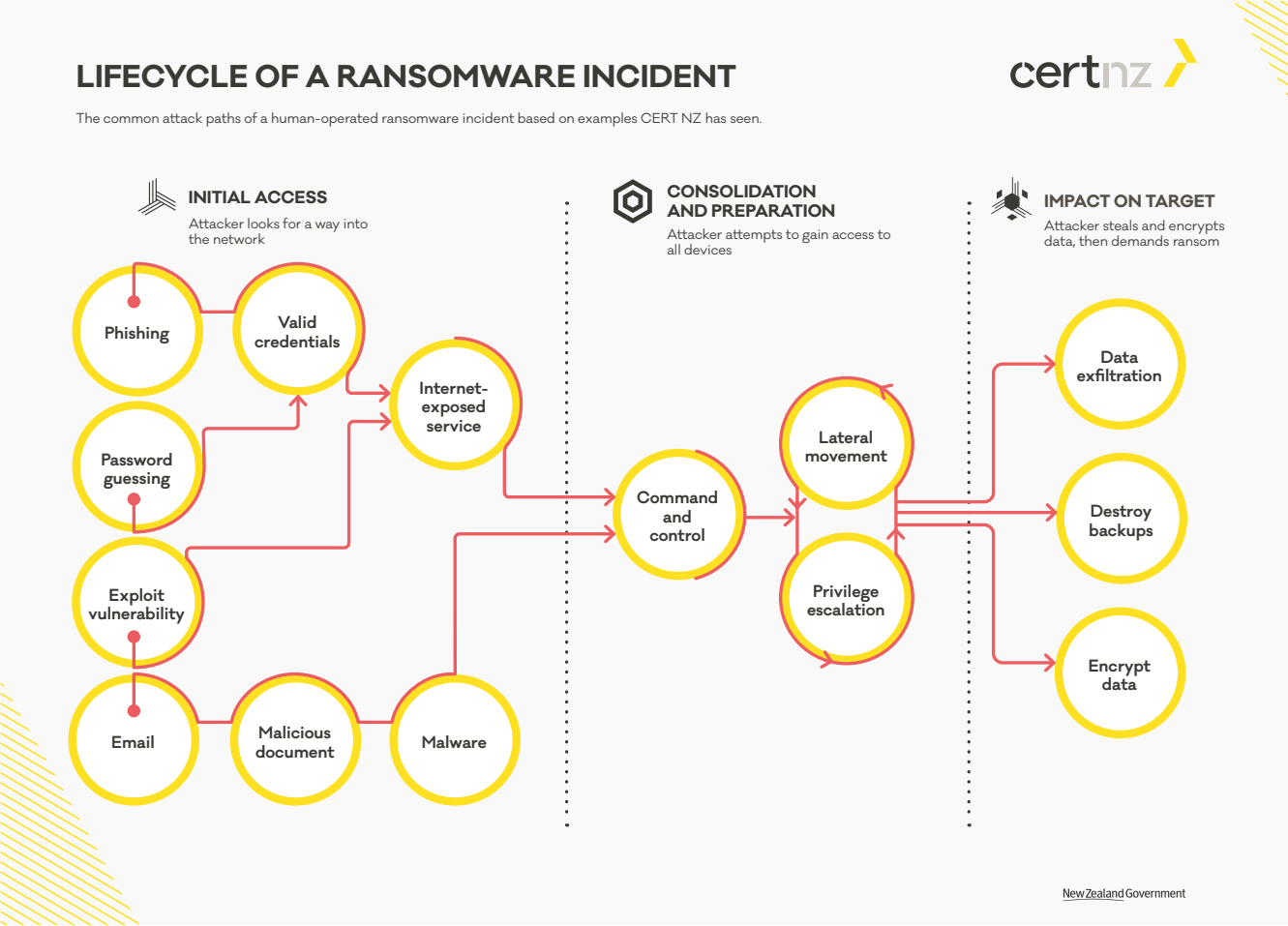
Informatiebronnen

Document	*Locatie*
NCSC factsheet ransomware	https://www.ncsc.nl/documenten/factsheets/2020/juni/30/factsheet-ransomware
NCSC fastsheet 'Bereid u voor op Zero Trust'	https://www.ncsc.nl/documenten/factsheets/2021/augustus/18/factsheet-bereid-u-voor-op-zero-trust
NCSC ICT-beveiligingsrichtlijnen voor Transport Layer Security (TLS) v2.0	https://www.ncsc.nl/documenten/publicaties/2019/mei/01/ict-beveiligingsrichtlijnen-voor-transport-layer-security-tls
NCSC Factsheet Gebruik tweefactorauthenticatie	https://www.ncsc.nl/documenten/factsheets/2019/juni/01/factsheet-gebruik-tweefactorauthenticatie
No More Ransom project	https://www.nomoreransom.org/nl/index.html
Ransomware Guide (CISA)	https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C_.pdf
Infographic Ransomware (Politie)	https://www.politie.nl/binaries/content/assets/politie/onderwerpen/ransomware/infographic-cybercrimes-ransomware.pdf
Back-up strategie	https://www.digitaltrustcenter.nl/back-up/geavanceerde-informatie-over-back-ups
CIS benchmarks	https://www.cisecurity.org/cis-benchmarks/
Microsoft white paper 'Mitigating Pass-the-Hash and Other Credential Theft, version 2'	http://download.microsoft.com/download/7/7/A/77ABC5BD-8320-41AF-863C-6ECFB10CB4B9/Mitigating-Pass-the-Hash-Attacks-and-Other-Credential-Theft-Version-2.pdf
Samen tegen Cybercrime, Stappenplan voor IT-specialisten	https://www.politie.nl/binaries/content/assets/politie/algemeen/algemeen/brochure-stappenplan-cybercrime.pdf

Contactinformatie

Organisatie	*Contactinformatie*
NCSC waakdienst	cert@ncsc.nl
NCSC algemeen	info@ncsc.nl
Politie (aangifte)	https://www.politie.nl/aangifte-of-melding-doen

Bijlage 1: schematische weergave van een ransomware-aanval



Bron: https://www.cert.govt.nz/it-specialists/guides/how-ransomware-happens-and-how-to-stop-it/.

Uitgave
Nationaal Cyber Security Centrum
(NCSC)
Postbus 117, 2501 CC Den Haag
Turfmarkt 147, 2511 DP Den Haag
070 751 5555

Meer informatie
www.ncsc.nl
info@ncsc.nl

mei 2022