Nationaal Cyber Security Centrum
Ministerie van Justitie en Veiligheid

Ransomware

Maatregelen voor het voorkomen, beperken en herstellen van een ransomware-aanval

Factsheet FS-2020-02 | versie 1.0 | mei 2020

Sinds enkele jaren neemt de dreiging van ransomware wereldwijd toe. Deze kwaadaardige software kan elke organisatie treffen die niet de juiste maatregelen heeft genomen. De laatste jaren is er een nieuwe trend zichtbaar: kwaadwillenden voeren meer gerichte ransomware-aanvallen uit, op doelwitten die een hoger losgeldbedrag kunnen betalen.

Deze factsheet geeft een overzicht van de verschillende soorten ransomware, beschrijft enkele maatregelen die je als organisatie kan nemen om een ransomware-aanval te voorkomen en geeft advies over wat te doen als uw organisatie geïnfecteerd is met ransomware.

Achtergrond

Het verdienmodel van ransomware voor criminelen was gebaseerd op schaalvoordeel: aanvallen waren ongericht op grote hoeveelheden gebruikers van kwetsbare systemen. Vaak werd er een laag losgeldbedrag gevraagd.

De laatste jaren is er een nieuwe werkwijze in opkomst: kwaadwillenden voeren meer gerichte ransomware-aanvallen uit op doelwitten die een hoger losgeldbedrag kunnen betalen. Nadat ze toegang weten te krijgen tot het systeem van een doelwit, wordt dit systeem gedurende langere tijd grondig geanalyseerd. Zo weet een crimineel wat de 'waarde' is van deze organisatie, waarna het gevraagde losgeld wordt aangepast aan deze subjectieve waarde.

Doelgroep

Chief Information Officers, Chief Information Security Officers, security officers en informatiebeveiligers.

Samenwerkingspartners

Tot stand gekomen in samenwerking met CERT-BE, NCSC-UK, Digital Trust Center (DTC), Universiteit Maastricht, Z-CERT, De Volksbank, Achmea, Ahold Delhaize, ASML, KPN, Heineken.

Copyright

De belangrijkste feiten

1. De impact van ransomware-aanvallen neemt toe.
2. Maatregelen tegen ransomware werken ook tegen andere malware.
3. Het verdienmodel van ransomware is veranderd. Kwaadwillenden voeren meer gerichte ransomware-aanvallen uit op doelwitten die meer losgeld kunnen betalen.

Wat is ransomware?

Ransomware is malware die de databestanden van gebruikers versleutelt, met als doel om deze later te ontsleutelen in ruil voor losgeld. In extreme gevallen blokkeert de ransomware de toegang tot het IT-systeem door ook systeembestanden te versleutelen die essentieel zijn voor de goede werking van het systeem. Gezien het destructieve karakter van ransomware-aanvallen is het vaak moeilijk om de logbestanden te herstellen en te achterhalen wat er daadwerkelijk is gebeurd. Hackers kunnen intellectueel eigendom of persoonsgegegevens hebben gestolen, waarbij zij ransomware inzetten om hun echte bedoelingen te verbergen.

Er zijn twee soorten ransomware: een *locker* vergrendelt het toegangsscherm van een systeem. Een *cryptor* versleutelt de bestanden op het geïnfecteerde systeem met behulp van encryptie algoritmes. Geavanceerde soorten ransomware kunnen naast lokale IT-systemen ook harde schijven, databases, back-ups, USB-sticks en gegevens in de cloud versleutelen. Beide soorten ransomware eisen dat het slachtoffer een losgeldbedrag (de 'ransom') betaalt, om de computer weer normaal te kunnen gebruiken. Dit losgeld wordt vaak geëist in de vorm van een *crypto-currency*, zoals Bitcoin.

Ransomware-infecties verschillen nauwelijks van andere malware-infecties. De maatregelen die een organisatie hiertegen kan nemen zijn ook grotendeels hetzelfde. Afhankelijk van de volwassenheid van uw organisatie kan de impact van een ransomware-aanval uiteenlopen van een minieme irritatie tot een grootschalige verstoring van het primaire proces.

Hoeveel bedraagt het losgeld?

Er is een groot verschil tussen een opportunistische ransomware-aanval en een gerichte aanval. Bij een opportunistische aanval wordt geprobeerd om een aanzienlijk aantal slachtoffers te besmetten en wordt meestal een paar honderd of een paar duizend euro geëist. Het bedrag is bewust laag, zodat het betalen van losgeld de snelste en goedkoopste optie is om weer normaal verder te kunnen met uw IT-systemen.

Bij een gerichte, zorgvuldig voorbereide aanval door kwaadwillenden kan het losgeld oplopen tot miljoenen euro's. Kwaadwillenden willen dat de ransomware zoveel mogelijk impact heeft op hun doelwit. Dit kan grote gevolgen hebben: na een ransomware besmetting kan het zijn dat kritieke bestanden en processen niet langer toegankelijk zijn. Ook kan worden gedreigd de gegevens te wissen of juist publiek te maken. Dit type aanvallen komt steeds vaker voor.

Kwaadwillenden die meer geïnteresseerd zijn in gevoelige informatie, gebruiken ransomware ook om hun sporen uit te wissen. Hierbij gebruiken ze ransomware als een *wiper* (harde-schijfwisser). In sommige gevallen is het dan niet meer mogelijk om uw gegevens te herstellen.

Het NCSC adviseert om geen losgeld te betalen. Er is geen enkele garantie dat de sleutel (*decryptor*) of het wachtwoord aan u wordt overhandigd nadat u het gevraagde losgeld heeft betaald. Daarnaast zijn er cases bekend waarbij na betaling hetzelfde slachtoffer nogmaals werd geraakt.

Hoe infecteert ransomware uw systeem?

Er zijn verschillende manieren waarop een kwaadwillende uw systeem kan infecteren met ransomware. Ransomware is een vorm van malware. Het openen van een malafide bijlage in een e-mail of het bezoeken van een kwaadaardige webpagina is voldoende om geïnfecteerd te raken. Veel slachtoffers installeren ransomware zonder het te beseffen.

Ransomware-aanvallen maken ook gebruik van niet-gepatchte kwetsbaarheden in een systeem. Voorbeelden hiervan zijn kwetsbare webbrowsers, legacy protocollen zoals SMBv1, en de Remote Desktop Protocol (RDP) toegang. Andere malware, zoals trojans, kunnen ook worden ingezet om toegang te krijgen tot uw systeem.

Ransomware as a service

Er is sprake van specialisatie en professionalisering binnen cybercrime. Sommige groepen cybercriminelen hebben zich gespecialiseerd in het verkrijgen van toegang tot netwerken, om deze toegang vervolgens te verkopen.

Ook zijn er groepen cybercriminelen die gespecialiseerd zijn in het exploiteren van deze toegang, bijvoorbeeld via ransomware. Ze hebben verschillende manieren ontwikkeld om kwetsbare RDP-sessies te identificeren en te misbruiken. Hierbij worden bijvoorbeeld inloggegevens (*credentials*) en andere gevoelige informatie buitgemaakt. Het gebruiken van een toegang via RDP heeft voordelen: het is gemakkelijker om op te gaan in het netwerkgebruik van een slachtoffer door gebruik te maken van bestaande credentials. Doordat er bestaande credentials worden gebruikt kan een aanvaller zijn/haar handelingen vermommen en opgaan in het 'normale' netwerkgebruik. Juist doordat er weinig tot geen zichtbaar of kwaadaardig netwerkverkeer te zien is, wordt de aanvaller mogelijk minder snel opgemerkt door system monitoring of een oplettende sys-admin.

Ondanks de professionalisering van *ransomware as a service*, vereist het uitvoeren van zowel ongerichte- als gerichte ransomware-aanvallen nog steeds specialistische kennis.

Voorkom ransomware

1. Bescherm tegen phishing
2. Organiseer vulnerability management, patch management en netwerk segmentering
3. Beperk de mogelijkheden van code execution
4. Filter webbrowser verkeer
5. Beperk USB-gebruik

Er bestaat geen wondermiddel tegen ransomware-aanvallen. Ransomware is een van vele varianten van malware. De maatregelen die u kunt nemen tegen ransomware komen daarom grotendeels overeen met maatregelen die uw systemen beschermen tegen andere malware.

Het doel van ransomware is vaak financieel gewin. Het is daarom aan te raden om uw netwerk te beschermen met een *in-depth* verdedigingssysteem, zodat een kwaadwillende meer moeite moet doen voor het uitvoeren van een succesvolle ransomware-aanval. Criminelen zullen de potentiële winst inschatten, en opgeven als de aanval waarschijnlijk te veel tijd in beslag neemt in verhouding tot het losgeld dat ze kunnen krijgen.

1. Bescherm tegen phishing

Phishing is een vorm van social engineering waarbij mensen verleid worden tot het overhandigen van gevoelige gegevens. De meest gebruikte phishing-methode is het versturen van vervalste e-mails die afkomstig lijken van betrouwbare afzenders. Veelal bevatten de e-mails een link naar een nagemaakte internetpagina. Daarop wordt een besmet bestand aangeboden of wordt de ontvanger gevraagd persoonlijke gegevens in te vullen. Phishing tegengaan vereist zowel een technische- als een mensgerichte aanpak. Enerzijds kunt u uw werknemers trainen om phishing-mails te herkennen; anderzijds zijn er ook technische maatregelen die u kan nemen. De volgende maatregelen raden wij sowieso aan:

- Verbeter de veiligheid van e-mails met SPF, DKIM en DMARC. Zie hiervoor ook de factsheet *Bescherm domeinnamen tegen phishing* [1] van het NCSC. Controleer ook binnenkomend e-mail verkeer met deze standaarden. Op deze wijze voorkomt u dat kwaadwillenden namens uw organisatie e-mails kunnen versturen.
- Maak gebruik van spamfilters om te voorkomen dat phishing-mails medewerkers kunnen bereiken.
- Voer regelmatig phishingtests uit. Maak gebruikers bewust van het belang om niet op alles te klikken en leer hen hoe ze spam- en phishingmails kunnen herkennen. Stem deze tests goed af binnen uw organisatie, om ongemak te voorkomen.
- Richt een proces in waarmee gebruikers phishingmails kunnen melden en train uw personeel hoe zij hiermee om moeten gaan. Vaak worden bijna identieke phishingmails verzonden, waarbij bijvoorbeeld alleen de link naar de geïnfecteerde pagina miniem verschilt.
- Verhoog de awareness van uw medewerkers en hanteer een positieve veiligheidscultuur: zorg ervoor dat medewerkers weten waar ze phishing kunnen melden en dat ze dit durven, ook als ze zelf al op een malafide link hebben geklikt.
- E-mailsoftware bevat soms visuele hulpmiddelen om gebruikers alert te maken op malafide e-mails. Het is daarmee bijvoorbeeld mogelijk om externe e-mails een label te geven.

2. Organiseer vulnerability management, patch management en netwerk segmentatie

Sommige varianten van ransomware misbruiken kwetsbaarheden in operating systems, webbrowsers, browser plug-ins en applicaties. Vaak zijn deze kwetsbaarheden al enige tijd publiek en zijn er patches beschikbaar die het risico op infectie kunnen mitigeren.

Updates

Het uitvoeren van updates op uw systemen maakt het aanzienlijk moeilijker om deze te infecteren met recente kwetsbaarheden. De meeste software wordt regelmatig bijgewerkt middels updates. Deze updates kunnen patches bevatten om de software beter te beschermen tegen nieuwe dreigingen.

Het is belangrijk om alle systemen in uw netwerk tijdig te patchen, niet enkel de systemen die direct zijn verbonden met het internet. Zeker bij een gerichte aanval is het mogelijk dat een aanvaller lateraal door uw netwerk beweegt. Door alle systemen tijdig te patchen is het voor een aanvaller die toch weet binnen te dringen, moeilijker zich verdere toegang tot uw netwerk te verschaffen.

1 https://www.ncsc.nl/binaries/ncsc/documenten/factsheets/2019/juni/01/factsheet-bescherm-domeinnamen-tegen-phishing/20151028+-Factsheet-Bescherm-domeinnamen-tegen-phishing.pdf

Het NCSC raadt de volgende maatregelen aan:

- Volg de NCSC RSS –feed met beveiligingsupdates voor veel gebruikte software. Vraag daarnaast aan uw leveranciers om u op de hoogte te houden van updates in hun product.
- Installeer de laatste updates van uw operating system.
- Periodiek updates installeren is een must. Het is goed om hierbij een stapsgewijze aanpak (testfase en vervolgens ingebruikname) te hanteren.
- Zorg ervoor dat de antivirussoftware up-to-date is en dat alle relevante functies zijn ingeschakeld.

Netwerk monitoring

Een succesvolle ransomware-aanval berust op timing: kwaadwillenden proberen zo lang mogelijk onopgemerkt te blijven. Bij het voorkomen (of beperken) van een ransomware-aanval is het daarom zaak om deze activiteiten zo snel mogelijk te herkennen. Het NCSC raadt de volgende maatregelen aan:

- Creëer en beheer een actuele inventaris van uw assets: u moet een duidelijk overzicht hebben van wat er op uw netwerk aanwezig is. Bij een infectie met ransomware is het noodzakelijk om te kunnen traceren van wie een systeem is, en waar deze zich bevind in het netwerk.
- Herken het basisgedrag van het netwerk: gebruik een oplossing die weet wat normaal is voor uw netwerk.
- Richt detectie in om zicht te krijgen op dreigingen van digitale aanvallen of malafide activiteiten. Detectie is van belang om een aanval snel op te merken en te stoppen. Zie hiervoor ook de NCSC webpagina over detectie [2]. Hier vindt u de publicaties *Handreiking voor implementatie van detectie-oplossingen* en *Factsheet Indicators of Compromise*.
- Monitor of credentials mogelijk gecompromitteerd zijn.
- Zorg ervoor dat logging op een centrale locatie plaatsvindt.
- Naast logging is het ook goed om monitoring in te richten: bepaal welke logs sowieso een alarm moeten genereren en richt een proces in om daarop te acteren. Denk hierbij bijvoorbeeld aan een alarm op het moment dat uw antivirus uitgeschakeld wordt.
- Verbeter de zichtbaarheid van veiligheidsincidenten. Onderzoek of het mogelijk is om een *Security Information and Event Management* (SIEM) systeem te implementeren.
- Onderzoek of het mogelijk is om *Endpoit Detection and Response* (EDR) sotware te implementeren. Deze software biedt de mogelijkheid om continue de endpoints (veelal pc's) in uw organisatie te monitoren. Hiermee kan ook in real-time op een aanval gereageerd worden.

Netwerksegmentatie

Netwerksegmentatie biedt een extra laag beveiliging in uw netwerk. Het is van groot belang bij het voorkomen van *lateral movement* door uw netwerk. Lateral movement houdt in dat een kwaadwillende probeert om diepere en bredere toegang tot uw netwerk te krijgen. Door uw netwerk op te delen in functionele segmenten is het lastiger voor een kwaadwillende om zijn of haar doel te bereiken. Immers: het deel van het netwerk waar deze aanvaller binnen is gekomen kan totaal afgeschermd zijn van het beoogde doel. Het NCSC raadt de volgende maatregelen aan:

- Beperk de toegang tot systemen en hun interfaces van buitenaf tot strikt noodzakelijk verkeer. Zorg dat medewerkers alleen via een VPN-verbinding toegang krijgen tot uw interne netwerk.
- Segmenteer uw netwerk. Systemen die geen onderlinge interactie of communicatie nodig hebben, moeten in verschillende segementen worden opgedeeld. Gebruikers krijgen alleen toegang tot de segmenten die zij nodig hebben. Blokkeer segment-overstijgend verkeer. Impliciet gaat dit uit van het zero trust principe: sta alleen dat verkeer toe dat expliciet vertrouwd is.
- Beperk de administratorrechten en het delen daarvan.
- Zorg dat aanvallers niet de kans krijgen om van buitenaf in te loggen op uw systemen. Gebruik lange, complexe wachtwoorden en implementeer een beleid voor accountvergrendeling om u te beschermen tegen brute-force aanvallen. Authenticeer gebruikers via Multi-Factor Authenticatie (MFA).

Hardening van beheer-interfaces

Een beheer-interface – zoals het Remote Desktop Protocol (RDP) – maakt het mogelijk om op afstand toegang te krijgen tot systemen en deze te bedienen. Dit biedt functionele voordelen: zo hoeft een medewerker bijvoorbeeld niet fysiek op locatie te zijn. Deze directe toegang via het internet maakt beheer-interfaces ook een geliefd doelwit van kwaadwillenden. Dit wordt onder andere misbruikt door SamSam ransomware, die probeert om vanaf het internet toegankelijke RDP-servers met zwakke wachtwoorden uit te buiten.
Het beperken van toegang tot het netwerk van een organisatie wordt ook wel *system hardening* genoemd. Virusscanners en firewalls dragen hier aan bij, maar ook het beperken van toegang via beheer-interfaces verdient aandacht. Hierbij is het van groot belang om enkel relevante netwerkinterfaces open te stellen en specifieke toegangsrechten tot productieomgevingen/gegevens af te scheiden.

- Ga na of het nodig is om RDP open te hebben op systemen en, zo ja, beperk de verbindingen dan tot specifieke en betrouwbare hosts (*whitelisting*).
- Bescherm uw (RDP) verbindingen ook tegen *brute-force attacks*: zorg dat gebruikers via een VPN verbinding maken en authenticeer deze gebruikers via Multi-Factor Authenticatie (MFA).
- Zorg ervoor dat cloudomgevingen voldoen aan recente best practices. Beperk ook in deze omgevingen het gebruik van RDP-poorten.
- Scherm het gebruik van RDP - inclusief de poorten - goed af.

NB: bij informatiebeveiliging is het van belang dat u een eigen risicoanalyse maakt, toegespitst op uw organisatie. De bovenstaande omschrijving is geen uitputtende lijst en niet alle maatregelen zijn voor elke organisatie geschikt.

2 https://www.ncsc.nl/onderwerpen/detectie

3. Beperk de mogelijkheden van code execution

Overweeg om uw organisatie te beschermen tegen *unauthorised code excecution*: het uitvoeren van kwaadaardige code en malware. Een veelgebruikte aanvalsmethode is het gebruik van macro's: een kwaadwillende verleidt gebruikers om malafide code uit te voeren door macro's toe te staan in het document dat ze hebben geopend. Deze aanval kan voorkomen worden door in uw organisatie macro's uit te schakelen.

Vanuit een beveiligingsperspectief is het daarnaast wenselijk om eindgebruikers niet de mogelijkheid te geven om software op hun eigen device te installeren. Er zijn natuurlijk ook legitieme redenen om software te installeren of code uit te voeren op een device. Creëer een proces om gebruikers hierin te faciliteren. Dit voorkomt dat ze in de verleiding komen om dit buiten uw zicht te doen.

De volgende maatregelen raden wij sowieso aan:

- Gebruik applicatiewhitelisting, zodat enkel goedgekeurde programma's op uw computersystemen kunnen draaien.
- Schakel de macro's in Office-bestanden uit.
- Schakel ActiveX in Office-bestanden uit.
- Schakel automatisch afspelen ('AutoPlay') uit.

4. Filteren van webbrowser verkeer

Het is raadzaam om uw uitgaande webverkeer via een *proxy* naar buiten te leiden. Dit maakt het mogelijk om de websites die uw gebruikers willen bezoeken te filteren, zoals het blokkeren van bekende malafide websites.

5. Beperk USB-gebruik

Gegevensdragers zoals USB-sticks kunnen een systeem besmetten met malware. Het is mogelijk om USB-poorten dicht te zetten dan wel USB-opslag te blokkeren. Ook kunt u USB-opslag beperken tot specifieke gebruikers die met speciale USB-sticks werken. Overweeg of een van deze maatregelen past in uw organisatie.

Wat is de impact van een ransomware-aanval?

Ransomware beperkt de toegang tot systemen of data totdat er een oplossing is gevonden. Dit kan leiden tot serieuze schade: denk hierbij aan onveilige (werk)situaties, financiële schade en reputatieschade. Ransomware heeft niet alleen impact op uw eigen organisatie, maar ook op uw omgeving. Zelfs met zorgvuldig ingerichte back-ups kan het enige tijd duren voor de primaire processen van uw organisatie weer op orde zijn. Gedurende deze *downtime* moet een organisatie mogelijk haar business continuity processen in werking stellen.

Bij gerichte ransomware-aanvallen heeft een kwaadwillende toegang tot de IT-systemen van uw organisatie. Dit brengt mogelijk de integriteit en de vertrouwelijkheid van uw data in gevaar. Verder kan het zo zijn dat het systeem ook met andere types malware is geïnfecteerd naast de ransomware.

Een succesvolle ransomware-aanval treft niet alleen de versleutelde data. Het levert potentieel ook indirecte of zelfs blijvende schade op.

Beperk de impact van een ransomware-aanval

1. Limiteer de toegang tot gegevens en filesystems
2. Creëer een back-upstrategie

1. Limiteer de toegang tot gegevens en filesystems

U kunt voorkomen dat ransomware zich onbeperkt kan verspreiden binnen uw organisatie: beperk de toegang tot gegevens en file systems tot die personen (of systemen) met een valide reden om ze te gebruiken. Vergeet niet dat ook uw back-upsystemen en cloudvoorzieningen baat hebben bij deze maatregel.

Het is zeer belangrijk om goede access controls te implementeren, ofwel het hanteren van strikte gebruikersrechten. Hierbij is het van belang om een goede administratie te hebben van uw gebruikers. Houdt zicht op het *joiners-movers-leavers* proces in uw organisatie: pas de toegangsrechten aan wanneer een gebruiker een andere rol krijgt of wanneer deze de organisatie verlaat.

Bij *administratoraccounts* (admin) zijn goede access controls nog relevanter: deze accounts vereisen verregaande rechten en toegang tot systemen. Gebruikers (met de systemadmin-rol) behoren niet met admin-accounts te mailen of browsen, of ingelogd te zijn op werkplek systemen. Deze maatregel kan een ransomware-aanval beperken tot specifieke domeinen van de infrastructuur.

Ook het principe van *zero trust* is in opkomst. Binnen dit informatiebeveiliging framework wordt er niet vertrouwd op het bestaan van een 'veilig eigen netwerk'. Het onderscheid tussen het interne en externe netwerk vervalt hiermee. Dit denkkader kan bijvoorbeeld handvatten bieden bij organisaties die een open *Bring Your Own Device* (BYOD) beleid hanteren. Maatregelen die risico's op dit vlak kunnen mitigeren zijn bijvoorbeeld micro-segmenteren of een *Privileged Access Management* (PAM) oplossing. Micro-segmenteren houdt (onder andere) in dat een organisatie per systeem aangeeft waar deze toegang tot heeft (whitelisting). Ook kan er per systeem monitoring worden toegepast, aanvullend op de monitoring van het gehele netwerk. Bij Privileged Access Management gaat het om het monitoren en loggen van admin-activiteiten en het bewust autoriseren van gebruikers voor specifieke taken. Deze autorisaties gelden voor een beperkte tijd: de gebruiker mag voor een korte tijd deze taak uitvoeren. Deze oplossing kan een aanvulling zijn op uw bestaande Identity Access Management systeem.

2. Creëer een back-upstrategie

Back-ups zijn essentieel om uw bestanden te herstellen na een incident met ransomware. Een back-up maken van al uw vitale bestanden en systemen kan de impact van een ransomware-infectie beperken.

- Gegevens kunnen slechts worden hersteld tot het moment van de laatste back-up.
- Online back-ups kunnen ook geïnfecteerd raken. (Een *online* back-up betekent dat de back-up in verbinding staat met het netwerk, in tegenstelling tot offline back-ups. Voorbeelden van *offline* back-ups zijn een harde schijf in een kluis, of het gebruik van tapes.)
- Back-up bestanden mogen niet direct benaderbaar zijn vanaf een systeem dat mogelijk geïnfecteerd kan raken.
- Back-up bestanden moeten regelmatig worden getest: ga daarbij na of de data volledig en niet corrupt is.

Zorg dat back-ups niet uw enige bescherming zijn tegen ransomware: goede cybersecurity-maatregelen kunnen ervoor zorgen dat uw organisatie überhaupt niet geïnfecteerd wordt.

Als u moet beslissen over het aantal potentieel haalbare back-ups, evalueer dan welke informatie het meest kritiek is voor uw organisatie. Denk hierbij ook aan uw kritieke processen: welke functies moet uw organisatie (binnen enkele uren of dagen) weer kunnen vervullen?

- Pas de **3-2-1 regel** toe: zorg dat je minstens **drie** verschillende kopie□n van je data en applicaties hebt. Deze back-ups moeten minimaal **twee** verschillende dragers hebben. Zorg dat er □ drager op een andere locatie is. De **3-2-1-1 regel** stelt daarnaast dat □ van deze back-ups een offline kopie moet zijn.
- Beperk het aantal gebruikers dat toegang heeft tot uw back-ups. Hoe minder, hoe beter.
- De logs moeten ook een integraal onderdeel zijn van uw back-upstrategie.

Het is essentieel om na te gaan hoe lang het duurt om een back-up terug te zetten. Deze informatie is cruciaal voor het opstellen van uw *business continuity plan*: er is een groot verschil tussen een restore van een paar dagen of enkele weken. Definiëer een *recovery time objective* en pas uw back-upstrategie hierop aan. Test deze strategie vervolgens.

Het is een risico om de back-up op dezelfde technologie te laten berusten als de operationele infrastructuur. Overweeg om de back-up infrastructuur in een eigen omgeving te laten werken (waardoor lateral movement wordt beperkt) en overweeg om geheel andere technologie te gebruiken. Denk hierbij aan het gebruik van Linux-gebaseerde oplossingen voor de back-up van een Windows-systeem.

Wat te doen als uw organisatie is geïnfecteerd met ransomware

Ransomware versleutelt uw bestanden. Het terugzetten van data door middel van een back-up is de meest betrouwbare oplossing om weer over deze bestanden te beschikken.

Als het niet mogelijk is om de bestanden door middel van een back-up te herstellen, is het raadzaam om na te gaan of er een decryptor bestaat. Dit kan bijvoorbeeld op de website van het 'No More Ransom'-project [3], een initiatief van politiediensten en private partijen.

Bij een beperkte infectie:

Let op: bij de volgende stappen wordt het geinfecteerde systeem als verloren beschouwd. Dit kan een eventueel decryptieproces verstoren.

- Verwijder het geïnfecteerde systeem uit het computernetwerk.
- Verwijder de ransomware uit het geïnfecteerde computersysteem. Het systeem wordt indien nodig volledig opnieuw geïnstalleerd.
- Meld de infectie bij de politie.
- Herstel het IT-systeem met behulp van een back-up.

Bij een netwerkbrede infectie:

- Stel uw calamiteitenplan in werking.
- Sluit uw netwerk af van de buitenwereld. Dit kan bijvoorbeeld door het dichtzetten van uw firewall(s).
- Roep de hulp in van een cybersecurity expert en/of een cybersecurity samenwerkingsverband.
- Meld de infectie bij de politie.
- Herstel de IT-systemen met behulp van een back-up.

Ga ook na of u een meldplicht heeft bij het NCSC, een toezichthouder, een opdrachtgever of bij een andere instantie[4]. Kijk onder meer naar geldende privacy wetgeving, bijvoorbeeld als u verwerker bent.

Communiceren en zorg voor medewerkers

Er komt veel op u af als uw organisatie geraakt wordt door ransomware. Zeker in de eerste verkenning ('Hoe groot is het probleem?') heerst er veel onduidelijkheid en komen er veel vragen op u af. Het is daarom raadzaam om al in een vroeg stadium na te denken over uw communicatie over de ransomware-infectie – het liefst vóór dat er een aanval plaatsvindt.

Ga na hoe u betrokkenen kunt informeren wanneer ook uw e-mailsystemen versleuteld zijn. Andere organisaties hebben in dit soort situaties onder andere gebruik gemaakt van social media en/of fysieke informatiepunten. Leg deze plannen vast in een draaiboek en beoefen/evalueer deze geregeld.

Naast communicatie is het ook raadzaam om na te gaan welke (partner) organisaties u nodig hebt tijdens een ransomware aanval. Ga in de koude periode na welke processen vitaal zijn voor uw organisatie en stel een business continuity plan op.

3 https://www.nomoreransom.org/nl/index.html

4 https://www.autoriteitpersoonsgegevens.nl/nl/nieuws/datalek-door-ransomware-wat-moet-u-doen

Wees u ervan bewust dat een ransomware-infectie veel van betrokken medewerkers vraagt en dat de nadelige effecten weken kunnen aanhouden. Zorg ervoor dat uw medewerkers genoeg rust krijgen in deze periode. Zo behoudt u energie in de gehele herstelperiode.

Betalen of niet?

Het wordt niet aanbevolen om het losgeld te betalen, vooral omdat dit geen oplossing voor het probleem garandeert. De kans is groot dat er bij de ontsleuteling tal van problemen opduiken. De decryptor die door de cybercriminelen wordt geleverd, heeft vaak veel minder aandacht gekregen dan de versleutelingsoftware. Hierdoor zijn de gegevens in het slechtste geval niet meer te herstellen.

Het betalen van losgeld houdt een ecosysteem in stand: het moedigt cybercriminelen aan om ransomware te gebruiken aangezien het een winstgevende business is. Cybercriminelen zullen hun activiteiten vervolgens voortzetten en nieuwe manieren zoeken om systemen te exploiteren, met als gevolg meer infecties, meer slachtoffers en meer schade voor de samenleving.

Enkele slachtoffers die losgeld hebben betaald, gaven aan dat er na een eerste betaling een hoger bedrag van hen werd geëist. In sommige gevallen werden de slachtoffers na een tijdje opnieuw door dezelfde ransomware getroffen.

Aangifte doen

U kunt aangifte doen op een politiebureau. Maak hiervoor een afpraak via 0900-8844.

Ter voorbereiding van de aangifte, moet u ervoor zorgen dat degene die namens uw bedrijf aangifte doet daartoe een machtiging heeft. Neem eventuele logbestanden mee (deze bevatten mogelijk sporen, indicaties en bewijzen) en noteer alvast de (contact)gegevens van de aangever.

Bij een aangifte kunt u de volgende vragen verwachten:

- Welke systemen zijn geraakt?
- Wat zijn de netwerkadressen en hoe ziet de infrastructuur van het netwerk eruit?
- Welke veiligheidsmaatregelen (zoals virusscanners en firewalls) heeft u genomen?
- Was er een dreigement of waren er andere bijzondere omstandigheden?
- Wat is de geschatte (economische en imago)schade en hoeveel (persoons)gegevens zijn getroffen?
- Welke (herstel)acties heeft uw bedrijf ondernomen na het ontdekken van het incident?

Tot slot

Zolang organisaties niet voldoende aandacht besteden aan cybersecurity, blijft malware zoals ransomware bestaan. Het verdienmodel is gebaseerd op de gedachte dat een organisatie noodgedwongen moet betalen. Door een ransomware-aanval te voorkomen helpt u niet alleen uw eigen organisatie, maar draagt u bij aan het verstoren van deze criminele activiteit.

Tegelijkertijd kunnen niet alle ransomware aanvallen voorkomen worden. Zorg daarom dat u ook voorbereid bent op de mogelijke impact van een ransomware-aanval.

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
@ncsc_nl

FS-2020-02 | versie 1.0 | juni 2020