INFORMATIE
BEVEILIGINGS
DIENST

RANSOMWARE

Ransomware is een chantagemethode op internet door middel van malware. Letterlijk vertaald betekent ransom: losgeld. Het is een verzamelnaam voor verschillende malware-varianten die computers ontoegankelijk maken of gegevens die erop staan versleutelen. Cybercriminelen vragen vervolgens van de gebruiker geld om de computer of de gegevens weer te 'bevrijden'. Betalen leidt echter niet altijd tot vrijgave van de computer of gegevens. Ransomware is een toenemende bedreiging voor de ICT-infrastructuur en de daarbinnen aanwezige bedrijfsinformatie.

Gezien het aantal meldingen van besmettingen bij de Informatiebeveiligingsdienst voor gemeenten (IBD), kan geconcludeerd worden dat ransomware-aanvallen ook bij gemeenten nog steeds effectief zijn. Het is dan ook de verwachting dat de komende tijd nieuwe varianten hiervan opduiken waarbij cybercriminelen steeds weer gebruikmaken van nieuwe technieken. Alle computers van zowel particulieren als organisaties kunnen besmet raken met ransomware. Deze leaflet bevat achtergrondinformatie over ransomware en gaat verder specifiek in op preventieve en repressieve maatregelen die u kunt nemen. Ook vindt u hierin meerdere tips om medewerkers in de gemeentelijke organisatie bewust te maken van de risico's van ransomware. Tot slot geven wij u tips over wat u kunt doen als uw gemeente slachtoffer is geworden van ransomware.

KWALITEITSINSTITUUT NEDERLANDSE GEMEENTEN IN OPDRACHT VAN VERENIGING VAN NEDERLANDSE GEMEENTEN

VERSCHILLENDE RANSOMWARE-VARIANTEN

Er zijn verschillende varianten van ransomware aanwezig.

Ransomware

Deze vorm van ransomware is een chantagemethode en betreft malware die de *computer* van het slachtoffer ontoegankelijk maakt (vergrendelt). Het werkt als een soort 'computergijzeling'; de computer toont na besmetting een melding dat de vergrendeling ongedaan wordt gemaakt als het slachtoffer 'losgeld' betaalt aan de digitale afpersers. Betalen leidt echter niet altijd tot ontsluiting van de computer, dus dit wordt sterk afgeraden. Bovendien moedigt u met het toegeven aan de eisen van de criminelen het versturen van meer ransomware verder aan. Het komt dan ook niet zelden voor dat personen of bedrijven twee keer slachtoffer worden van ransomware.

Cryptoware

Bij Cryptoware is het doel van de gijzeling niet de computer zelf, maar de *bestanden* op de computer. Kortom: 'bestandsgijzeling'. Het kan gaan om bestanden in alle formaten op onder meer de harde schijf van de computer, bedrijfsnetwerken, de virtuele (Cloud)-disk, de externe harde schijf en usb-sticks die tijdens een besmetting kunnen worden versleuteld. Tot voor kort werden besmettingen met Cryptoware uitsluitend in het buitenland waargenomen. Inmiddels zijn ook Nederlandse bedrijven slachtoffer geworden. Met name het MKB en gemeenten kunnen vatbaar zijn voor besmetting met Cryptoware. Meer informatie over Cryptoware is ook te vinden op de website veiliginternetten.nl.

Ransomweb

Het doel van deze nieuwe aanvalstechniek is niet om bestanden op een computer te versleutelen, maar om *gegevens* in databases te versleutelen. Met deze aanval breekt een aanvaller in op een webapplicatie en modificeert hij scripts op de webserver. Gebruikers van de webapplicaties merken hier in eerste instantie niets van. Als de cybercriminelen uiteindelijk de encryptiesleutel van de remote webserver verwijderen, is de database en website onbruikbaar. De cybercriminelen eisen vervolgens 'losgeld' voor de encryptiesleutel. Ook hier geldt dat betaling niet altijd tot versleuteling van de gegevens leidt, dus dit wordt sterk afgeraden.

HOE GAAN CYBERCRIMINELEN TE WERK?

Nadat de bestanden ongemerkt zijn versleuteld, tonen de cybercriminelen een melding op het scherm waarin staat dat de bestanden versleuteld zijn door de malware. Deze melding bevat een aftelklok die aangeeft hoeveel tijd het slachtoffer heeft om losgeld te betalen om de bestanden weer terug te krijgen. Afhankelijk van de ransomware-variant wordt in elke map die versleutelde bestanden bevat een of meerdere bestanden geplaatst met een uitleg wat te doen na deze besmetting.

HOE RAAKT MIJN COMPUTER BESMET MET RANSOMWARE?

Een ransomware-besmetting kan men overal op het internet oplopen en is, helaas, nooit helemaal te voorkomen. De computer van een slachtoffer raakt doorgaans besmet doordat hij op het internet aan het surfen is en ongewild wordt doorgeleid naar een webpagina waarop een exploit-kit de kwetsbaarheden van zijn computer verkent. Een exploit-kit is een programma dat beveiligingslekken in verschillende programma's en plug-ins misbruikt. Deze worden vervolgens uitgebuit om de malware te plaatsen. Hier merkt de gebruiker in eerste instantie niets van. Cybercriminelen verstoppen ransomware ook in pop-ups en advertenties op internet of via bestanden als bijlage in een e-mail (spam/phishing) en hyperlinks en filmpjes op sociale netwerksites.

WAT KAN IK DOEN OM BESMETTING TE VOORKOMEN?

Ransomware wordt steeds geavanceerder en het is daarom noodzakelijk om continu te beoordelen welke beveiligingsmaatregelen passend zijn en deze indien nodig bij te stellen. Hiervoor is het belangrijk om te zorgen dat informatiebeveiliging structureel binnen de gemeente wordt georganiseerd. Voorkomen is immers beter dan genezen.

"ALS UW GEMEENTE SLACHTOFFER IS GEWORDEN VAN RANSOMWARE OF CRYPTOWARE KUNT U HIERVAN AANGIFTE DOEN BIJ DE POLITIE. NEEM OOK ALTIJD CONTACT OP MET DE IBD"

Preventieve maatregelen

Om besmettingen van malware zoveel als mogelijk te voorkomen, zijn er veel preventieve maatregelen die u als gemeente kunt nemen.

- Hou het besturingssysteem en programma's altijd up-to-date met beveiligingsupdates/-patches om eventuele beveiligingslekken te dichten. Maak zoveel mogelijk gebruik van automatische updates en controleer regelmatig (minimaal eens per maand) of er updates beschikbaar zijn en installeer deze. Lees hierover meer in het BIG OP-product 'Patchmanagement voor gemeenten'.
- Zorg ervoor dat alle gemeentelijke systemen, zoals firewalls, werkplekken, laptops, mobiele apparaten en servers voorzien zijn van anti-malware software. Dit zorgt voor een continue bescherming van uw ICT-infrastructuur. De anti-malware software dient automatisch voorzien te worden van nieuwe updates van virusdefinities en dit wordt centraal bewaakt. Lees hierover meer in het BIG OP-product 'Anti-malware Beleid'.
- Maak dagelijks back-ups zodat verloren, vernietigde of versleutelde informatie hersteld kan worden. Back-up en recovery is een belangrijke beschikbaarheidsmaatregel die ervoor zorgt dat corrupte, verloren of vernietigde bedrijfsinformatie hersteld kan worden. Zorg ook voor voldoende beveiligingsmaatregelen zodat de back-ups zelf niet besmet of versleuteld kunnen worden. Dit kan bijvoorbeeld middels een logische toegang en compartimentering van het netwerk. De back-up en herstelprocedures dienen regelmatig (minimaal eens per jaar) getest te worden om de betrouwbaarheid ervan vast te stellen. Lees hierover meer in het BIG OP-product 'Back-up en recovery gemeente'.
- Zorg indien mogelijk voor IP- en URL-reputatie filtering op bijvoorbeeld de firewall en spamfilter. Hiermee wordt de toegang tot bekende, aan malware gerelateerde, sites geblokkeerd.
- Breng de functionaliteiten en rechten van systemen terug tot het minimum dat noodzakelijk is voor het uitvoeren van de taak (hardening). Ook dienen de beveiligingsinstellingen zo te worden ingesteld dat hiermee de mogelijkheden om een systeem te compromitteren worden verlaagd en een maximale veiligheid ontstaat. Het gaat hierbij ook om het verwijderen van niet gebruikte of onnodige gebruikersaccounts en het wijzigen van standaard wachtwoorden die op systemen aanwezig kunnen zijn. Hierbij is het verzamelen en beoordelen van systeemdata en -waarschuwingen van bijvoorbeeld applicaties, netwerk infrastructuur, servers en pc's van groot belang om te verifiëren dat er geen instellingen zijn aangepast. Lees hierover meer in het BIG OP-product 'Hardening-beleid voor gemeenten'.
- Zorg voor een logische toegangsbeveiliging waarmee onbevoegden minder makkelijk toegang kunnen krijgen tot gemeentelijke informatiesystemen en de informatie binnen deze systemen. Geef gebruikers alleen toegang tot systemen en bestanden die zij voor hun werkzaamheden nodig hebben. Het toekennen van meer rechten resulteert in een hoger risico. Controleer regelmatig of de huidige autorisatie-instellingen noodzakelijk zijn. Het veranderen van schrijfrechten naar leesrechten van schijven of bestanden kan de schade bij besmetting minimaliseren. Lees hierover meer in het BIG OP-product 'Beleid logische toegangsbeveiliging'.
- Meld u aan voor de community van de IBD. Een digitaal platform waarop u als gemeente samen met collega-gemeenten informatie kunt delen, vragen kunt stellen en documenten uit kan wisselen.

Repressieve maatregelen

Als gemeente kunt u ook een aantal repressieve maatregelen nemen om besmettingen van malware te voorkomen.

- Zorg voor logging en monitoring en verzamel en beoordeel systeemdata en -waarschuwingen van bijvoorbeeld applicaties, servers, desktop pc's en het netwerkinfrastructuur om te verifiëren dat er geen instellingen zijn aangepast en/of ongewenste activiteiten plaatsvinden. Lees hierover meer in het in het BIG OP-product 'Aanwijzing Logging'.
- Leg de beoordeling en behandeling van het melden van incidenten neer bij een deskundige functionaris. Lees hierover meer in het BIG OP-product 'Voorbeeld incidentmanagement en responsebeleid'. Belangrijke incidenten moeten gemeld worden aan de IBD en daarvoor moet een speciale contactpersoon aangewezen worden. Zie hiervoor de factsheet 'Aansluitproces bij de IBD'.

Bewustwordingstips voor medewerkers

Om besmettingen op malware zoveel als mogelijk te voorkomen is het belangrijk medewerkers in de organisatie bewust te maken van de risico's van ransomware. Geef instructies over hoe de kans op besmetting verkleind kan worden. Bijgaand een aantal tips. Meer informatie hierover is te lezen in het in het BIG OP-product 'Handreiking Communicatieplan Informatiebeveiliging'.

- Het ondoordacht openen van e-mails vormt een risico. Open daarom geen berichten en onbekende bestanden die u niet verwacht of niet vertrouwt. Wees alert en ga hier niet op in, zelfs niet wanneer u de afzender kent. Accepteer het bericht alleen als u dit bericht van de afzender verwacht.
- Controleer het webadres (URL) om vast te stellen of u een veilige website bezoekt. Gebruik zoveel mogelijk bladwijzers voor websites die u vaak bezoekt en wees alert bij het openen van verkorte URL's.
- Wees alert bij het downloaden van software en populaire bestanden. Ook apps voor uw mobiele apparaten kunnen kwaadaardige software bevatten. Installeer apps daarom alleen via de officiële applicatiewinkels en gebruik geen illegale kopieën.
- Sluit pop-ups in uw browser af met Alt+F4. Klik nooit op akkoord, ok, de 'X' of nee om een pop-up af te sluiten; u kunt hiermee per ongeluk alsnog kwaadaardige software installeren. Installeer eventueel een pop-up-filter om pop-ups te blokkeren.

WAT TE DOEN ALS MIJN COMPUTER TOCH BESMET IS MET RANSOMWARE?

Is uw gemeente slachtoffer geworden van ransomware? Raak dan vooral niet in paniek en ga niet over tot betaling; betaling leidt immers *niet altijd* tot vrijgave van het systeem of bestanden. Bijgaand nog een aantal tips dat u kunt opvolgen wanneer uw gemeente besmet is.

- Wanneer u slachtoffer bent van ransomware, kan besloten worden om een coördinator aan te stellen en in het uiterste geval een (crisis)team te formeren die de verdere coördinatie van de incidentafhandeling op zich neemt.
- Incidenten dienen altijd zo snel mogelijk te worden gemeld bij de IBD.
- Betrek indien noodzakelijk externe expertise bij het oplossen van de besmetting, bijvoorbeeld de leverancier van de anti-malware software.
- Zorg voor een goede en afgewogen communicatie over de besmetting naar zowel het management en de bestuurder als de rest van de gemeentelijke organisatie. Lees hierover meer in de factsheet 'Incidentcoördinatie crisiswoordvoering' van de IBD.
- Als is vastgesteld hoe de besmetting heeft plaatsgevonden, isoleer of verwijder de bron van deze besmetting, bijvoorbeeld door:
  - het gebruikersaccount en/of gebruikersprofiel uit te schakelen of te verwijderen of verwijder (tijdelijk) de rechten van de gebruiker van waaruit de besmetting heeft plaatsgevonden;
  - de gevirtualiseerde desktop (VDI) en/of pc te verwijderen;
  - indien mogelijk alle (besmette) bestanden te bewaren en isoleren voor nader onderzoek en/of het herstellen van de inhoud.
- De website fraudehelpdesk.nl bevat informatie over hoe ransomware verwijderd kan worden.
- De versleuteling van bestanden door Cryptoware is een onomkeerbaar proces. Anti-malware software kan de malware wel van de computer verwijderen, maar de bestanden niet terugbrengen; de versleuteling is niet te doorbreken. Maak dus regelmatig meerdere back-ups.

MEER INFORMATIE

MEER INFORMATIE OVER ONZE DIENSTVERLENING VINDT U IN DE ANDERE FACTSHEETS VAN DE IBD EN OP DE WEBSITE WWW.IBDGEMEENTEN.NL. HIER KUNNEN GEMEENTEN BOVENDIEN VIA DE COMMUNITY RELEVANTE INFORMATIE MET ELKAAR DELEN, VRAGEN AAN ELKAAR STELLEN EN DOCUMENTEN UITWISSELEN. DE HELPDESK VAN DE IBD IS TE BEREIKEN TIJDENS KANTOORUREN VAN 9:00 TOT 17:00 UUR OP HET NUMMER 070 373 8011 OF VIA HET E-MAILADRES INFO@IBDGEMEENTEN.NL. TIJDENS DEZE KANTOORUREN REAGEERT DE IBD BINNEN 30 MINUTEN OP EEN INCIDENTMELDING. BUITEN KANTOORUREN IS DE IBD OP HETZELFDE NUMMER BEREIKBAAR VOOR SPOEDEISENDE MELDINGEN EN ZAL DE IBD BINNEN 60 MINUTEN REAGEREN OP EEN TELEFONISCHE OPROEP.