Moet ik losgeld betalen bij ransomware?

https://aucuba.nl/kennisbank/uncategorized/moet-ik-losgeld-betalen-bij-ransomware/

Het betalen van ransomware-losgeld wordt sterk afgeraden door cybersecurity-experts en autoriteiten wereldwijd. Er is geen garantie dat je data terugkrijgt na betaling, je financiert criminele activiteiten, en het maakt je een aantrekkelijk doelwit voor toekomstige aanvallen. Bovendien kunnen er juridische consequenties zijn, vooral wanneer het gaat om betalingen aan gesanctioneerde groepen. Dit artikel beantwoordt de belangrijkste vragen over ransomware-aanvallen en wat je het beste kunt doen als je ermee geconfronteerd wordt.

Wat is ransomware en hoe werkt een losgeldeis precies?

Ransomware is een vorm van malware die bestanden op je computer of netwerk versleutelt, waardoor je geen toegang meer hebt tot je eigen data. Cybercriminelen eisen vervolgens losgeld in ruil voor een decryptiesleutel om je bestanden weer toegankelijk te maken. De communicatie verloopt meestal via anonieme kanalen en betaling wordt vrijwel altijd in cryptocurrency zoals Bitcoin geëist.

Het proces begint vaak met een **phishing-email** of een gecompromitteerde website. Zodra de malware je systeem binnendringt, verspreidt deze zich door het netwerk en versleutelt systematisch alle toegankelijke bestanden. Je ziet dan een melding op je scherm met instructies voor de losgeldbetalingen, vaak met een deadline om de druk op te voeren.

Er bestaan verschillende varianten van ransomware, waaronder:

- Crypto-ransomware: versleutelt bestanden maar laat het systeem functioneren
- Locker-ransomware: blokkeert toegang tot het hele systeem
- Scareware: doet zich voor als beveiligingssoftware en eist betaling voor nepbedreigingen
- Doxware: dreigt gevoelige informatie openbaar te maken
- RaaS (Ransomware-as-a-Service): waarbij criminelen ransomware verhuren aan anderen

De werkwijze wordt steeds geavanceerder. Moderne ransomware-groepen gebruiken dubbele afpersing waarbij ze eerst data stelen voordat ze deze versleutelen. Als je weigert te betalen, dreigen ze de gestolen informatie openbaar te maken of te verkopen aan de hoogste bieder.

Waarom raden experts af om losgeld te betalen bij ransomware?

Beveiligingsexperts en autoriteiten zoals het NCSC en Europol raden consequent af om losgeld te betalen. De belangrijkste reden is dat er geen enkele garantie bestaat dat je na betaling daadwerkelijk toegang krijgt tot je bestanden. Onderzoek toont aan dat een aanzienlijk deel van de slachtoffers na betaling geen werkende decryptiesleutel ontvangt of slechts gedeeltelijk hun data terugkrijgt.

Door te betalen financier je **criminele organisaties** en stimuleer je verdere aanvallen. Het geld wordt gebruikt voor het ontwikkelen van nog geavanceerdere malware en het uitvoeren van nieuwe cyberaanvallen. Je draagt dus onbedoeld bij aan een groeiend probleem dat andere bedrijven en organisaties treft.

Betalen maakt je bedrijf ook een aantrekkelijk doelwit voor toekomstige aanvallen. Criminelen delen onderling informatie over bedrijven die bereid zijn te betalen. Dit verhoogt de kans dat je opnieuw slachtoffer wordt, mogelijk met een hogere losgeldeis. Sommige groepen verkopen zelfs toegang tot je netwerk aan andere criminelen.

Daarnaast zijn er praktische problemen met het betalingsproces zelf. Het omzetten van grote bedragen naar cryptocurrency is complex en tijdrovend. De communicatie met criminelen is onbetrouwbaar en je hebt geen verhaal als ze hun beloften niet nakomen. Ook bestaat het risico dat de decryptiesleutel niet werkt door technische fouten in de ransomware zelf.

Wat zijn de juridische gevolgen van het betalen van ransomware-losgeld?

In Nederland bestaat geen expliciet verbod op het betalen van ransomware-losgeld, maar er zijn wel degelijk juridische risico's. Europese sanctiewetgeving verbiedt betalingen aan bepaalde criminele groepen of individuen op sanctielijsten. Als de ransomware-aanval uitgevoerd wordt door een gesanctioneerde groep, kan betaling leiden tot boetes en strafrechtelijke vervolging.

De Algemene Verordening Gegevensbescherming (AVG) speelt ook een belangrijke rol. Bij een ransomware-aanval waarbij persoonsgegevens zijn getroffen, moet je binnen 72 uur melding maken bij de Autoriteit Persoonsgegevens. Het niet melden of te laat melden kan leiden tot boetes tot 4% van de jaaromzet of 20 miljoen euro.

Voor bedrijven gelden aanvullende verantwoordelijkheden:

- Meldplicht bij de politie voor aangifte van computercriminaliteit
- Informatieplicht richting betrokkenen waarvan persoonsgegevens zijn gelekt
- Documentatieplicht van alle genomen maatregelen en beslissingen
- Mogelijke aansprakelijkheid bij onvoldoende beveiliging van systemen

Verzekeringsmaatschappijen hebben vaak specifieke voorwaarden rond ransomware. Sommige **cyberverzekeringen** dekken losgeldbetalingen, maar alleen als aan strikte voorwaarden is voldaan. Het eigenmachtig betalen zonder overleg met de verzekeraar kan leiden tot het vervallen van de dekking. Ook kunnen premies significant stijgen na een incident.

Welke alternatieven heb je als je geen losgeld wilt betalen?

Het belangrijkste alternatief voor losgeldbetalingen is het herstellen van data vanaf back-ups. Voorwaarde is wel dat je recente, geteste back-ups hebt die niet door de ransomware zijn aangetast. Offline of immutable back-ups bieden de beste bescherming. Het herstelproces kan tijd kosten, maar je behoudt controle over de situatie zonder criminelen te financieren.

Professionele hulp inschakelen is vaak de beste keuze. Cybersecurity-experts kunnen de schade inventariseren, systemen veilig herstellen en adviseren over vervolgstappen. Een managed service provider met ervaring in incident response kan het herstelproces aanzienlijk versnellen en de kans op verdere schade minimaliseren.

Er zijn ook gratis decryptietools beschikbaar voor sommige ransomware-varianten. Initiatieven zoals No More Ransom, een samenwerking tussen politie en beveiligingsbedrijven, bieden tools om bestanden te ontsleutelen zonder te betalen. Het identificeren van de specifieke ransomware-variant is cruciaal voor het vinden van de juiste tool.

Andere praktische alternatieven omvatten:

- Forensisch onderzoek om mogelijk niet-versleutelde kopieën van bestanden te vinden
- Samenwerking met autoriteiten die mogelijk decryptiesleutels hebben van eerdere onderzoeken
- Herbouw van systemen en data uit andere bronnen zoals e-mail, cloudopslag of partnersystemen
- Onderhandeling met criminelen over gedeeltelijke data-vrijgave zonder betaling
- Acceptatie van dataverlies en focus op toekomstgerichte maatregelen

Hoe voorkom je dat je überhaupt voor deze keuze komt te staan?

Preventie begint met regelmatige, geteste back-ups volgens het 3-2-1 principe: drie kopieën van belangrijke data, op twee verschillende media, waarvan één offsite. Test maandelijks of je back-ups daadwerkelijk werken door een volledige restore uit te voeren. Immutable of write-once back-ups bieden extra bescherming tegen ransomware die back-ups probeert te versleutelen.

Employee awareness training is essentieel omdat de meeste ransomware-aanvallen beginnen met menselijke fouten. Train medewerkers om phishing-emails te herkennen, verdachte links te vermijden en onbekende bijlagen niet te openen. Regelmatige phishing-simulaties helpen om het bewustzijn scherp te houden.

Technische maatregelen die ransomware-aanvallen voorkomen:

- Patch management: installeer beveiligingsupdates direct na release
- Netwerksegmentatie: beperk de verspreiding van malware door netwerkscheiding
- Endpoint protection: gebruik moderne antivirus met gedragsdetectie
- E-mailbeveiliging: implementeer geavanceerde spamfilters en sandboxing
- Toegangscontrole: beperk gebruikersrechten volgens het least-privilege principe

Voor MKB-bedrijven zonder interne IT-afdeling is samenwerking met een managed service provider vaak de meest effectieve preventie. Zij zorgen voor proactief beheer, continue monitoring en snelle respons bij verdachte activiteiten. Dit vermindert niet alleen het risico op ransomware, maar zorgt ook voor sneller herstel als er toch iets misgaat.

Wat moet je direct doen als je slachtoffer wordt van ransomware?

De eerste 24 uur na een ransomware-aanval zijn cruciaal. Begin direct met het isoleren van geïnfecteerde systemen door netwerkverbindingen te verbreken. Trek letterlijk de netwerkkabel uit de computer en schakel wifi uit. Dit voorkomt verdere verspreiding van de ransomware naar andere systemen en beperkt de schade.

Documenteer vervolgens alles wat je ziet en doet. Maak foto's van het ransomware-bericht, noteer tijdstippen en bewaar alle communicatie. Deze informatie is waardevol voor forensisch onderzoek en eventuele aangifte. Verander niets aan de getroffen systemen totdat experts de situatie hebben beoordeeld.

Het **stappenplan voor de eerste 24 uur**:

1. Isoleer direct alle verdachte systemen van het netwerk
2. Identificeer welke systemen en data zijn aangetast
3. Maak melding bij de politie via cybercrime.nl
4. Informeer je cyberverzekeraar als je die hebt
5. Schakel professionele hulp in voor incident response
6. Communiceer intern volgens je crisisplan
7. Beoordeel of melding bij de Autoriteit Persoonsgegevens nodig is
8. Start niet eigenmachtig met herstelpogingen

Communicatie met stakeholders vereist zorgvuldigheid. Informeer het managementteam direct maar voorkom paniek. Wees transparant over de situatie zonder technische details prijs te geven die criminelen kunnen helpen. Klanten en leveranciers informeer je pas als duidelijk is welke impact de aanval heeft op hun data of dienstverlening.

Een ransomware-aanval is een crisis die je niet alleen hoeft op te lossen. Professionele hulp van cybersecurity-experts maakt het verschil tussen weken stilstand en snel herstel. Als je vragen hebt over ransomware-preventie of hulp nodig hebt bij het opstellen van een incident response plan, neem dan contact met ons op voor deskundig advies.