Bescherming tegen gijzelsoftware

Bad Rabbit, Spider, GoldenEye; zijn namen bekende gijzelsoftware, en bedoeld om online geld te stelen. Maar dit is maar het topje van de cybercriminele ijsberg. Er worden dagelijks nieuwe versies losgelaten op het internet. Veelal vallen cybercriminelen alles en iedereen aan op het internet, omdat ze op die maner de grootste kans hebben om ergens binnen te kunnen dringen en hun slag te slaan.

Wat is ransomware?

Ransomware is schadelijke software, of malware, die computers en bestanden gijzelt. Vandaar de Nederlandse naam 'gijzelsoftware'. Criminelen blokkeren of versleutelen je computers, bestanden, of soms zelfs hele netwerken, en geven die pas weer vrij als je losgeld betaalt. Volgens experts is dubbele versleuteling in opkomst: de ransomware versleutelt je data dan niet één keer, maar twee keer. Voor beide sleutels moet je betalen.

Bestanden gegijzeld

Een aanval kan op meerdere manieren verlopen. Via links, via bijlages in e-mail, advertenties, maar ook via gerichte aanvallen op servers proberen criminelen hun schadelijke software een systeem binnen te loodsen. Is de ransomware eenmaal binnen, dan kan deze zichzelf verspreiden. De software blokkeert dan de toegang tot je computer of netwerk, of versleutelt bestanden. In een pop-up eisen de criminelen betaling, vaak in bitcoin of een andere cryptovaluta.

Aangevallen, wat nu?

Wat moet je doen als je bent aangevallen? Neem altijd contact op met je IT-beheerder, als je die hebt. Verder kun je het volgende doen:

1. **Onderzoek om welke ransomware het gaat**

Van oudere software is soms de decryptiesleutel bekend, waarmee je je bestanden weer ontsleutelt. Dit controleer je op nomoreransom.org, een internationaal samenwerkingsverband tussen beveiligingsbedrijven en politie. Ransomware verwijderen is een vak apart, dus het is slim om daarbij hulp in te roepen van een expert.

2. **Betaal geen losgeld**

Dat is natuurlijk makkelijk gezegd. Soms hebben bedrijven geen andere optie. In januari en februari 2021 betaalde 32% van organisaties wereldwijd losgeld na een aanval met schadelijke software. Vaak is het een verzekeraar die het losgeld betaalt. Toch is betalen niet de oplossing voor het probleem.

Op die manier heeft de crimineel succes en zal die doorgaan met dit soort aanvallen.
De Nederlandse politie adviseert dan ook bij een ransomware-aanval: betaal niet. Doe wel aangifte en meld de aanval ook bij de Fraudehelpdesk.

3. **Investeer in back-ups**

Een back-up is een goede maatregel, vooral als je deze op een externe plek bewaart. Zo hoef je niet te overwegen om losgeld te betalen voor je gegevens. Uit het eerder genoemde onderzoek van Sophos bleek dat wereldwijd 57% van aangevallen organisaties hun data uiteindelijk terugkregen via hun eigen back-ups.

4. **Zorg voor goede antivirusprogramma's**

Het is een open deur, maar alleen met goede virusscanners die ook ransomware herkennen, ben je goed beschermd. Van de Nederlandse bedrijven die begin 2020 werden aangevallen, wist bijna een kwart de aanval tegen te houden met antivirussoftware voordat er bestanden waren versleuteld.

5. **Update je software**

Cybercriminelen gebruiken zwakke plekken in software om je systeem met ransomware binnen te dringen. Zorg dat je kwetsbaarheden op tijd repareert, en update dus altijd de software die je gebruikt.

6. **Gebruik adblockers en vooral geen privémail**

Mensen zijn een zwakke schakel in de beveiliging van data. Op een link is zo geklikt, een bijlage is zo geopend: wees daar dus voorzichtig mee. Gebruik adblockers en wantrouw mails van onbekenden, en zorg ook dat eventuele medewerkers geen privémail ontvangen via het zakelijke mailadres.

Meer informatie en hulp

- De Fraudehelpdesk kan bij een aanval adviseren en doorverwijzen.
- Het Digital Trust Center (DTC), opgericht door het ministerie van Economische Zaken en Klimaat, geeft meer uitleg over wat je kunt doen als je computersysteem door software gegijzeld is.
- Het Nationaal Cyber Security Center (NCSC), opgericht door het ministerie van Justitie en Veiligheid, bestrijdt cybercrime in Nederland. Het NCSC publiceert regelmatig over het voorkomen van cybercrime, in 2020 bijvoorbeeld over securitytesten.
- Op Hackhelpdesk.nl vind je een stappenplan en praktische oplossingen waarmee je verdere schade voorkomt.

Gebruikte bronnen: KvK, Fraudehelpdesk, DTC, NCSC en de Hackhelpdesk