Ransomware

1. Wat is het?

Ransomware is kwaadaardige software (malware) die computers infecteert via e-mails, bijlagen of links naar besmette websites. Ransomware blokkeert de toegang tot een informaticasysteem of versleutelt gegevens zodat ze onbruikbaar worden. Het slachtoffer verneemt via een afpersbericht dat de toestand opnieuw genormaliseerd wordt na het betalen van losgeld.

2. Komt het vaak voor?

Het aantal verschillende soorten ransomware is de afgelopen jaren aanzienlijk gestegen, met 237 meldingen in 2017.[1] Ransomware is, naast phishing, de modus operandi bij uitstek voor internetoplichters.[2] Vooral kmo's zijn een interessant doelwit. Zij kunnen vaak minder geld besteden aan de beveiliging van hun informaticasystemen, maar hebben toch voldoende financiële middelen om losgeld te betalen.

3. Wat zijn de gevolgen?

Het losgeld voor particulieren ligt vaak tussen 300 en 500 euro. Voor bedrijven loopt dit bedrag op tot tienduizenden euro's. Betalen geeft echter geen garantie dat de computer en/of de gegevens opnieuw toegankelijk worden. Integendeel, wie betaalt, riskeert om sneller opnieuw slachtoffer te worden (voor een hoger bedrag). Bovendien gebruiken criminele organisaties dit losgeld om hun illegale activiteiten verder te zetten en nog meer slachtoffers te maken.

4. Wat kan je doen?

Sensibiliseer het personeel om de burger steeds door te verwijzen naar www.safeonweb.be of www.nomoreransom.org. Twee website met zeer duidelijke en nuttige tips.

Informeer burgers over de gevaren van ransomware en zorg dat ze hun computers, tablets en smartphones goed beveiligen, de verschillende besmettingsmogelijkheden herkennen en op regelmatige tijdstippen een back-up maken.

Ontraad slachtoffers te betalen en informeer dat er mogelijkheden bestaan om hun computers, mobiele apparaten of digitale bestanden gratis te ontgrendelen via de website www.nomoreransom.org.

Stimuleer slachtoffers om aangifte te doen via de lokale politie.

Download campagnemateriaal op de website www.safeonweb.be (affiches, banners, folders …)

- Sensibiliseer via website, sociale media en het gemeentelijk infoblad (bv. preventietips);
- Verdeel affiches en flyers in het straatbeeld, bij lokale clubs, verenigingen, kleine kmo's…;
- Organiseer initiatieven en activiteiten (presentaties, infomomenten, workshops …).

[1] Crime control barometer 2018
[2] Centrum voor Cybersecurity België 2018 en jaarverslag van Europol 2017

5. Wat biedt de dienst maatschappelijke veiligheid?

- uitwisselen van goede praktijken uit andere gemeenten en politiezones;
- preventietips om te plaatsen in het gemeentelijk infoblad, op de website of op sociale media;
- opleidingen voor personeelsleden om hun kennis rond het thema te vergroten in samenwerking met het PIVO;
- zoeken of aanreiken van namen van deskundigen die een infosessie kunnen geven aan de burger;
- presentaties, documentatie- en informatiemateriaal;
- sensibiliseringsmateriaal zoals brochures en gadgets (onder voorbehoud van beschikbaar budget).

Contactpersoon:

Marleen Piccard
Federale afdeling gouverneur Vlaams-Brabant, dienst maatschappelijke veiligheid
Provincieplein 1, 3010 Leuven
Telefoon: 016 26 78 42
E-mail: dmv.preventie@vlaamsbrabant.be

6. Interessante instanties en websites

No more ransom: www.nomoreransom.org
Een initiatief van het Team High Tech Crime van de Nederlandse politie, Europol's European Cybercrime Centre en McAfee met als doel slachtoffers te helpen bij het herstellen van hun versleutelde bestanden.

Centrum voor Cyber Security België (CCB): www.safeonweb.be
Algemene website van de overheid over cyberveiligheid met informatie en campagnemateriaal. De burger kan er terecht voor tips en nieuwsberichten.

Het federale Computer Emergency Response Team: www.cert.be
De operationele dienst van het Centrum voor Cybersecurity België (CCB). Een burger kan er terecht om ondersteuning te vragen bij het ontgrendelen van computers, mobiele apparaten of digitale bestanden.
Op hun website kan je de *brochure: 'ransomware, how to protect and respond'* downloaden. Deze brochure geeft een duidelijk overzicht van maatregelen die je kan nemen om je te beschermen tegen ransomware. Daarnaast vind je er ook tips in terug die je helpen wanneer je slachtoffer bent.