Herken én voorkom de versleuteling van uw belangrijke data

Het aantal RansomWare aanvallen is de afgelopen maanden wederom explosief gestegen. RansomWare is de verzamelnaam van schadelijke software die cybercriminelen gebruiken om alle data op de computer van een gebruiker te versleutelen. Hierdoor is er geen toegang meer mogelijk tot bestanden, foto's en vaak gebruikte applicaties.

RansomWare komt meestal binnen via een advertentie op een vage website of een goed vervalste e-mail zodat deze betrouwbaar lijkt. Deze e-mail bevat een bijlage of een link. Bij het openen ervan versleutelt de RansomWare, zonder dat je dit direct in de gaten hebt, alle bestanden (op alle locaties waar je rechten hebt!)

Hoe kan je zelf besmetting voorkomen

- ✓ Open alleen e-mails van bekende afzenders
- ✓ Vertrouw alleen een e-mail waarvan het logisch is dat je deze ontvangt
- ✓ Voordat je op een link in een e-mail klikt, blijf er dan even met de muis boven hangen zodat zichtbaar wordt waar deze naar verwijst. Klik nooit op deze link als deze verwijst naar een 'vage' website
- ✓ Bezoek nooit een website naar aanleiding van telefonische acquisitie of spontaan contact
- ✓ Voer geen gegevens in, of download niets van websites zonder (groen) slot in de adresbalk
- ✓ Open alleen 'betrouwbare' websites bij het browsen op Internet
- ✓ Klik niet op 'vage' advertenties op Internet
- ✓ Sluit direct 'Pop-Ups' die vragen om inlognamen, wachtwoorden of het installeren van een programma
- ✓ Blijft altijd alert bij het downloaden van software en tools
- ✓ Bij twijfel niet openen, klikken of opstarten
- ✓ Check de laatste alerts en het laatste nieuws over RansomWare op www.fraudehelpdesk.nl

Technische preventie

- ✓ Zorg ervoor dat alle programmatuur inclusief de virusscanner altijd up-to-date is
- ✓ Zorg ervoor dat er een back-up gemaakt wordt van de belangrijke bestanden
- ✓ Controleer regelmatig de inhoud en de betrouwbaarheid van de back-up
- ✓ Zorg ervoor dat de back-up niet rechtstreeks benaderbaar is voor gebruikers. RansomWare zal in dat geval ook de back-up versleutelen
- ✓ Ga zorgvuldig om met instellingen van Macro's
- ✓ Overleg met de ICT verantwoordelijke voor eventuele verdere technische stappen

Bij het eerste vermoeden dat uw werkstation geïnfecteerd is, zet deze per direct uit! **BETAAL NOOIT DE HACKER**, overleg eerst met de ICT verantwoordelijke!

Trivision Automatisering, Overschieseweg 76, 3044EH Rotterdam, 010 – 246 92 40, support@trivision.nl