ICTWaarborg

Microsoft Partner

Van Drie Computerzorg Brabant

Ringbaan West 123
5037 PA Tilburg
013- 889 3433
www.v3cb.nl
info@v3cb.nl
KvK nummer 5232 1746

WAT IS RANSOMWARE?

Ransomware is schadelijke software die wordt gebruikt door internet criminelen waarmee de persoonlijke bestanden van een getroffen computer worden 'gegijzeld' totdat er betaald wordt. Dit is een steeds bedreigender vorm van cybercriminaliteit met zeer vervelende consequenties voor gebruikers: namelijk, je bent je bestanden kwijt. Half mei j.l. was de grootste actieve wereldwijde ransomware aanval tot nu toe. Een nieuw gevaar is dat de laatste generatie ransomware ook instructies bevat om de software automatisch te installeren op meerdere Windows computers in hetzelfde netwerk. Apple en Linux computers liepen bij deze aanval geen risico.

HOE KAN RANSOMWARE OP MIJN COMPUTER TERECHTKOMEN?

Deze software kan op uw Windows computer terecht komen door met de muis te klikken op een 'link' of bijlage in een phishing e-mail. Het bericht lijkt misschien betrouwbaar maar het is een nagemaakte e-mail om de gebruiker te misleiden. Ook onbetrouwbare websites kunnen de gebruiker verleiden ergens op te klikken en zonder dat de gebruiker het doorheeft wordt de software op de achtergrond geïnstalleerd.

Computer criminelen zijn ook actief aan het hacken bij grote bedrijven door gebruik te maken van bestaande veiligheidslekken in Windows. Computers zonder de Windows updates van maart 2017 lopen een groot risico omdat er een kwetsbaar veiligheidslek aanwezig blijkt te zijn waarmee de hackers zich toegang kunnen verschaffen. *Met* installatie van deze maart-update is actief hacken op deze manier i.i.g. niet meer mogelijk en het 'lek' gedicht. Het is wel de eigen verantwoordelijkheid van het bedrijf of de gebruiker om zelf tijdig updates te installeren.

WAT GEBEURD ER ALS IK RANSOMWARE OP MIJN COMPUTER HEB EN HOE KAN IK DAT ZIEN?

Als ransomware wordt geïnstalleerd merk je dat niet meteen maar op de achtergrond worden razendsnel alle persoonlijke bestanden zoals documenten, foto's en video's versleuteld, m.a.w. zodanig veranderd dat er geen toegang meer is tot deze gegevens. Zowel de naam, de extensie als de inhoud van bestanden wordt gewijzigd. Daarna krijgt de gebruiker een melding op het bureaublad dat er betaald moet worden om de versleuteling weer ongedaan te maken. Wanneer er wordt betaald, wat u overigens niet moet doen, is het allerminst zeker dat de instructie verstuurd zal worden waarmee de bestanden weer in de 'oude' staat gebracht kunnen worden. Zonder deze 'sleutel' is de kans zeer groot dat de bestanden verloren blijven. Veiligheidsexperts zijn op zoek naar oplossingen en anti virus bedrijven werken aan anti-ransomware software. De computer moet worden opgeschoond en hopelijk kunt u wel terugvallen op een back-up.

HOE KAN IK MIJ BESCHERMEN TEGEN RANSOMWARE?

1. Met deze 4 eenvoudige tips bent u beschermd. **Zorg altijd dat Windows up-to-date is** van alle computers in uw netwerk. Volgens de standaard instellingen gaat dat automatisch.
2. Check de beveiliging op de aanwezigheid van **een anti virus programma**. In Windows 10 zit deze al ingebouwd genaamd Windows Defender. Dat is voldoende.
3. **Kijk altijd kritisch en met gezond wantrouwen naar binnenkomende e-mails**. Zogeheten phishing e-mails lijken op echte e-mails van bedrijven waar u vaker e-mails van krijgt, maar het zijn nep-mails om u te verleiden ergens op te klikken zodat schadelijke software geïnstalleerd kan worden. Check bij twijfel de afzender. Deze lijkt op het oorspronkelijke bedrijf maar is het niet, alhoewel de naam van het bedrijf er wel in voor kan komen. Wanneer de nep e-mail is verwijderd en de prullenbak geleegd is er geen gevaar meer.
4. **Zorg voor een actuele back-up**.

Voor bedrijven met veel computers in hetzelfde netwerk is de nieuwste generatie ransomware een extra risico omdat in korte tijd meerdere computers van personeel geïnfecteerd kunnen worden. Het is zeker zo belangrijk om bezoekers of gasten die met hun eigen computer gebruik maken van de lokale internetverbinding niet met hetzelfde netwerk te laten verbinden als het personeel maar op een gescheiden (gast)netwerk en het liefst eentje waarin deze gebruikers elkaar niet kunnen zien. Dat kan ingesteld worden op de meeste routers. Je kunt je eigen bedrijfsveiligheid wel op orde hebben maar je hebt geen zicht op hoe het ervoor staat met de veiligheid van computers van bezoekers en gasten. De meeste gebruikers zijn zich zelf ook niet bewust van de risico's.

IK HEB EEN BACKUP, WORDT DEZE DAN OOK VERSLEUTELD?

Dat is wel mogelijk maar dat hangt af van een aantal zaken. Welke back-up software wordt gebruikt; op welk tijdstip worden er back-ups gemaakt; wordt er continue real-time gesynchroniseerd of is er een tijdsinterval; worden bestanden met nieuwe namen toegevoegd aan de bestaande back-up of worden ze vervangen of gesynchroniseerd; is het back-up medium altijd beschikbaar of aangesloten. Back-up in 'de Cloud' (bijv. Onedrive en Dropbox) kan in dit opzicht ook risico's met zich meebrengen omdat er continue wordt gesynchroniseerd. Als dat de enige back-up is dan loop je ook daar grote risico's.

Voor vragen kunt u e-mailen naar info@v3cb.nl of bel 013 – 889 3433.