Checklist: Voorkom ransomware op je systeem

De meeste malware probeert zich op je systeem te nestelen zonder dat je het door hebt. Ransomware– ook wel cryptomalware genoemd – is daar een uitzondering op. Deze malware gijzelt je systeem of belangrijke bestanden en eist losgeld om ze weer vrij te geven. Het is verschrikkelijke als dit je overkomt, maar met deze checklist kun je je voorbereiden op en beschermen tegen ransomware.

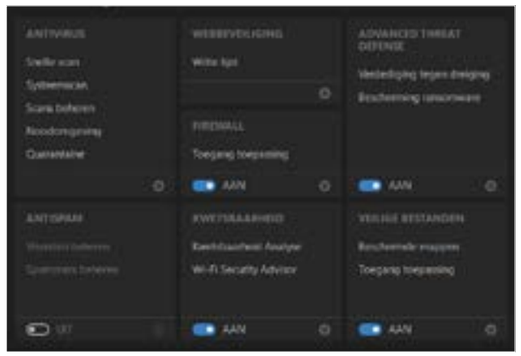
Wees niet naïef

Regelmatig horen we argumenten als 'ik doe toch niks geks op het internet' en 'ik heb nog nooit malware op mijn pc gehad'. Windows-pc's zijn echter ook kwetsbaar voor besmetting zonder dat je iets opvallends of verkeerds doet. Een kwetsbaarheid wordt achter je rug om uitgebuit, zodat je pc besmet raakt. Dit kan in iedere Windows-versie gebeuren, dus ook in Windows 8 of 10, waar Windows Defender standaard is ingeschakeld. Een besmetting is zelden je eigen schuld, maar denken dat je geen gevaar loopt is naïef. Overigens zijn ook Mac's kwetsbaar.

Beveiligingssoftware

Windows 8 en Windows 10 hebben met Defender standaard malwarebeveiliging aan boord, maar voor Windows 7 moet je dit zelf nog verzorgen. Gebruik je Windows Vista, XP of zelfs nog een oudere Windows-versie? Dan is het de hoogste tijd over te stappen naar Linux of een Windows-variant die nog wél ondersteund wordt door Microsoft, want het gebruik van een oudere versie dan Windows 7 is vragen om problemen.

Windows Defender vormt een prima basisbescherming, maar je kunt natuurlijk ook kiezen voor uitgebreide beveiliging. Zo kun je beveiligingssoftware kiezen met extra beveiliging tegen ransomware. Hiermee wordt er ook naar het gedrag van programma's gekeken en verdachte processen worden direct afgebroken. Bijvoorbeeld dus wanneer een programma opeens allerlei bestanden begint te versleutelen. Beveiligingssoftware die goed scoort is Bitdefender Internet Security 2019.



Apparatuur scheiden

Ransomware kan ook je Android-smartphone of -tablet kapen, maar dat is wel een behoorlijk zeldzaam fenomeen. Besmetting vindt niet achter je rug om plaats, maar kan alleen het gevolg zijn van eigen handelen: wanneer je apps buiten de Play Store om installeert en vervolgens alle permissies en apparaatbeheer-toegangsrechten toekent. Een mobiele virusscanner op je Android is daarom niet nodig. Installeer géén apps buiten de Play Store om, wees altijd erg kritisch op permissies die apps (ook uit de Play Store) vragen en geef nooit apparaat- en toegankelijkheidsbeheer weg.

Permissies

Ransomware kan ook je Android-smartphone of -tablet kapen, maar dat is wel een behoorlijk zeldzaam fenomeen. Besmetting vindt niet achter je rug om plaats, maar kan alleen het gevolg zijn van eigen handelen: wanneer je apps buiten de Play Store om installeert en vervolgens alle permissies en apparaatbeheer-toegangsrechten toekent. Een mobiele virusscanner op je Android is daarom niet nodig. Installeer géén apps buiten de Play Store om, wees altijd erg kritisch op permissies die apps (ook uit de Play Store) vragen en geef nooit apparaat- en toegankelijkheidsbeheer weg.

Updaten

Besmetting met ransomware en andere vormen van malware op je pc gebeurt door de uitbuiting van kwetsbaarheden in je systeem en geïnstalleerde programma's. Programma's die vaak uitgebuit worden zijn Java, Adobe Reader en Internet Explorer. Gebruik je deze niet, maar heb je ze wel? Dan kun je het beter van je systeem verwijderen. Wanneer een kwetsbaarheid in een programma en in het besturingssysteem wordt gevonden, dan kan het lek worden gedicht door middel van updates. Windows 10 updatet zichzelf automatisch. Voor je overige programma's kun je een software-updater gebruiken, bijvoorbeeld Patch My PC Updater, of Filehippo App Manager.

Back-up

De vorige tips waren vooral bedoeld om ransomware te voorkomen. Maar het kan natuurlijk altijd gebeuren dat je pc toch te grazen wordt genomen. Wanneer je zorgt voor een actuele back-up blijft de impact natuurlijk minimaal. Zorg dus altijd voor een back-up, die niet op dezelfde pc (zoals de D-schijf) staat. Bewaar deze bij voorkeur op een externe locatie, zoals een externe harde schijf, cloudopslag of netwerklocatie. Een tweede back-up-schijf op een andere locatie (bijvoorbeeld bij kennissen) is ook handig voor andere rampspoed, zoals brand. Dit heet een off-site back-up. Windows heeft een eigen back-upfunctie ingebouwd. Voor uitgebreide opties kun je ook uitwijken naar het gratis programma EaseUs Todo Backup Free.

Back-up locatie

Heb je Dropbox (of een andere cloud-opslagdienst) op je systeem geïnstalleerd, zodat je handig via de verkenner bij je bestanden kunt? Heb je netwerk-shares – zoals een nas –zodat je ook op dezelfde manier bij je back-ups kunt op je netwerk? Bewaar je je back-ups op een externe schijf die permanent gekoppeld is aan je systeem? Bedenk dan: wanneer jij er zonder inlog in je verkenner bij kunt, dan kan ransomware dat na besmetting ook! Zorg er dus altijd voor dat je moet inloggen of aankoppelen voordat je bij je geback-upte bestanden kunt komen, hoe onhandig dat soms ook kan zijn. Wanneer een besmetting met ransomware heeft plaatsgevonden, benader dan pas je back-up wanneer je er zeker van bent dat je systeem schoon is.

Toch besmet?

Heb je Dropbox (of een andere cloud-opslagdienst) op je systeem geïnstalleerd, zodat je handig via de verkenner bij je bestanden kunt? Heb je netwerk-shares – zoals een nas –zodat je ook op dezelfde manier bij je back-ups kunt op je netwerk? Bewaar je je back-ups op een externe schijf die permanent gekoppeld is aan je systeem? Bedenk dan: wanneer jij er zonder inlog in je verkenner bij kunt, dan kan ransomware dat na besmetting ook! Zorg er dus altijd voor dat je moet inloggen of aankoppelen voordat je bij je geback-upte bestanden kunt komen, hoe onhandig dat soms ook kan zijn. Wanneer een besmetting met ransomware heeft plaatsgevonden, benader dan pas je back-up wanneer je er zeker van bent dat je systeem schoon is.