KNOKKi audio technologies
t 020-6620375; www.knokki.com; dojo@knokki.com
Van Breestraat 100, 1071 HT Amsterdam

Wat te doen tegen ransomware?

update mei 2017 nav WannaCry

Wat is er aan de hand? Door een beveiligingslek in de besturingssystemen van Windows (Linux- en Mac-gebruikers ontspringen dus de dans) kunnen computers van buitenaf worden benaderd zonder dat daar een handeling door een gebruiker voor nodig is. Daar is door kwaadwillenden gebruik van gemaakt door VAN BUITENAF het worm-virus WannaCry te installeren dat als een razende alle bestanden van de computer - EN andere computers waarmee deze computer verbonden is via het netwerk - versleutelt. Het is in dit geval dus NIET zo dat gebruikers zelf iets stoms hebben gedaan, bijvoorbeeld door een dubieus bestandje te openen. Verschillende experts hebben wat dit betreft echt de plank misgeslagen op radio, TV en internet. De versleutelde bestanden worden alleen tegen betaling weer ontsleuteld, vandaar de naam ransomware. Thuisgebruikers lijken vooralsnog niet getroffen te zijn.

Om het lek te dichten heeft Windows medio maart j.l. een update uitgebracht en met computers die latere Windows versies draaien (7, 8.1 en 10) en netjes zijn bijgewerkt zou dan ook niks aan de hand moeten zijn. In het onderhavige geval heeft Windows zelfs voor XP nog een patch uitgebracht Dat het uitsluitend bedrijven zijn die slachtoffer zijn geworden, komt waarschijnlijk omdat juist bedrijven vaak met oudere software draaien EN in dit geval de patch nog niet hadden geïnstalleerd. Dat juist bedrijven vaak met oudere besturingssystemen draaien komt doordat zij vaak heel specifieke software hebben laten ontwikkelen die niet zo maar draait op een nieuwer Windows platform. Upgraden naar nieuwere Windows-versies gaat dan gepaard met significante kosten en de rest laat zich raden.

Met beveiligingslekken moeten we leren leven. We moeten het geluk hebben dat de software-ontwikkelaars - als er een lek gevonden wordt - sneller een oplossing hebben dan kwaadwillenden een aanval kunnen doen. Die oplossing moet iedereen dan wel meteen installeren natuurlijk. Meer geld voor cybersecurity e.d. kan dit soort problemen nauwelijks voorkomen en ik vind dan ook dat de Nationale Coördinator Terrorismebestrijding Dick Schoof mensen op het verkeerde been zet door te zeggen dat er meer geld naar IT-beveiliging moet.

Wat kan je zelf doen? Er is eigenlijk niets nieuws onder de zon. Het belangrijkste is regelmatig een back-up maken. Als je daarbij nog risico's uit wil sluiten kan je dat het beste doen op een externe schijf die niet aan het netwerk hangt. Dat kan ook een USB-stick zijn. Daarnaast dien je je computer up-to-date te houden en moet je Firewall aanstaan. Last but not least moet je blijven nadenken bij het openen van bestanden e.d. (zie volgende pagina). En ja, het moet gezegd, werk je met besturingssystemen van Linux of Mac, dan kan je echt rustiger gaan slapen!

KNOKKi audio technologies
t 020-6620375; www.knokki.com; dojo@knokki.com
Van Breestraat 100, 1071 HT Amsterdam

Pas op voor ransomware!

Er is al enige tijd een ander soort computervirus actief: ransomware. Waarom dit soort virus speciale aandacht behoeft, is dat het virus wanneer het geactiveerd wordt al je bestanden versleutelt. Het tast je programma's niet aan, dus de computer blijft gewoon werken, maar AL JE BESTANDEN inclusief dus Word- en Excel-documenten en foto's zijn niet meer op te roepen. De enige tot nu toe bekende manier om je bestanden terug te krijgen is de betaling van minimaal zo'n 500$ in Bitcoins aan een 'derde', waarna je een bestand krijgt toegestuurd waarmee je alles weer kan ontsleutelen.
Het virus zit verpakt in een bestand dat een bewerking uitvoert ('executable') en dergelijke bestanden zijn moeilijk herkenbaar. Een voorbeeld dat mij bekend is, betreft een sollicitatie waarin een link naar Dropbox waarin een foto en een uit te pakken CV. In dat CV zat het virus. In dit geval is 'goed' te zien dat er een bewerking zal worden uitgevoerd, want de extensie .EXE staat voor 'executable'.

In the campaign observed by Sumalapao, the Dropbox folder came with two files: a stock photograph .JPG and a self-extracting executable.

The latter file loaded a trojan onto the machine that surreptitiously downloaded Petya onto a user's machine.

Het tweede voorbeeld betreft een meegestuurd .docm bestand. Een .doc bestand is een regulier Word-bestand, net als een nieuwer .docx bestand. Deze bestanden leveren géén gevaar op. Een .docm bestand is eveneens een Word-bestand, maar dan voorzien van een geel uitroepteken dat aangeeft dat er een 'makro' in zit die moet worden geïnstalleerd. Een 'makro' is een executable die als het ransomware is je computer gijzelt. Mails etc. met .docm-bestanden dus meteen weggooien.

Tot welk advies leidt dit nu? Het eerste advies is: maak dagelijks een back-up! Eigenlijk is dit ook het tweede tot en met het negende advies. Het tiende advies is 'obvious': klik niet op links of bijlages in mails van onbekende herkomst. Alleen een virusscanner o.i.d. is onvoldoende. Succes!