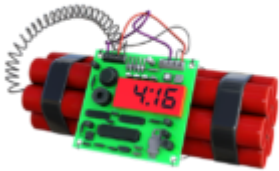


De aldoor tikkende tijdbom in de zorg die Windows heet



In de digitale wereld gebruikt men op zeer veel plaatsen het besturingssysteem Windows, zowel in de privésfeer als zakelijk. Ook in de zorg is het gebruik van Windows, afkomstig van Microsoft zeer dominant. Het probleem met besturingssystemen is dat ze na verloop van tijd verouderen. Kwetsbaarheden in de software vereisen het continu updaten van besturingssystemen naast grotere eisen die aan de performance worden gesteld. Op een gegeven moment stopt Microsoft met de ondersteuning met updates van de oude versie en dient men op de nieuwe versie over te stappen (upgrade). Gebruikers dienen goed te beseffen dat het niet op tijd tussentijds updaten de systemen kwetsbaar maakt. Helemaal kwetsbaar maakt men zich door niet over te stappen op een nieuwe versie van het besturingssysteem. Nu Windows 7 in januari 2020 geen ondersteuning meer krijgt van Microsoft zal men de overstap naar Windows 10 moet gaan maken. Anders vormt Windows een tikkende tijdbom.

Wisselende levensduur besturingssystemen

[Windows XP](#) hield het bijzonder lang vol: van 2001 tot 2014. [Windows Vista](#) hield het echter maar zes jaar vol, van 2006 tot 2012, terwijl [Windows 7](#) van 2009 tot januari 2020 ondersteund werd. Het betekent dat systeembeheerders alert moeten zijn en tijdig capaciteit vrij moeten maken voor een upgrade naar de volgende versie van Windows.

Zorg

In de zorg gaat het om zeer privacygevoelige data die goed beschermd dienen te zijn. Het besef dat er op tijd gedacht

moet worden aan een updates en upgrades heeft men in de zorg niet altijd. Dat is een heel zorgelijk probleem. Uiteraard gaat het om grote aantallen systemen die in zorginstellingen bijgewerkt moeten worden. Het digitaal werken brengt echter verantwoordelijkheden en verplichtingen met zich mee. In het Verenigd Koninkrijk heeft men recent becijfert dat in de National Health Service(NHS) op dit moment instellingen [zeker 500.000 werkplekken nog niet gemigreerd hebben naar Windows 10](#). Dat maakt ze zeer kwetsbaar voor aanvallen door hackers op de nog onder Windows 7 (of nog erger: eerdere versies) draaiende systemen

Problemen

Het is absoluut geen zeldzaamheid dat zorgICT-systemen aangevallen worden door hackers. Het meest duidelijk was dat toen in het Verenigd Koninkrijk [in mei 2017 het Wannacry-virus](#) toesloeg. Dat maakte gebruik van een kwetsbaarheid in Windows-systemen waarvoor al een softwarepatch aanwezig was, maar die op zeer veel plekken niet geïnstalleerd was.

Zeer oude versies Windows

Binnen de zorg zie je geregeld foto's opduiken van werkplekken waarop oude besturingssystemen van Windows zich zelf verraden. Zo moet men niet vreemd opkijken om op een systeem binnen een instelling Windows XP te zien draaien. Berucht zijn de besturingssystemen op de computers die gekoppeld staan aan bijv. MRI- of CT-scanners. Omdat die systemen ook gekoppeld staan aan een instellingsnetwerk kan zo'n systeem zelfs [een specifiek doelwit](#) vormen voor hackers. Het griezelige is dat tegenwoordig ook de mogelijkheid bestaat [radiologisch beeldmateriaal te manipuleren](#). Dat geldt zowel voor de afbeeldingen als ten aanzien van de vermelde diagnose of de tenaamstelling.

Noodzakelijkheden

Om te voorkomen dat Windows-tijdbom ooit bij een gebruikers afgaat dient men zich te houden aan de volgende punten:

- Installeer altijd onverwijld de updates van het actuele besturingssysteem.
- Installeer tijdig de opvolger van een besturingssysteem waarvan de uiterste houdbaarheidsdatum in zicht komt. Dus **voor** de uiterste houdbaarheidsdatum.
- Loop regelmatig alle werkstations af om (zwaar) verouderde versies van een besturingssysteem op te sporen.

De mensen waarvoor u werkt, de patiënten, dienen op uw commitment te kunnen vertrouwen.

W.J. Jongejan, 14 februari 2020

Afbeelding van [kalhh](#) via [Pixabay](#)