Hallo,
mein Artikel zur Nutzung von Windows 7 bezog sich auf Nutzer, die den PC für den rein alltäglichen Gebrauch anwenden. Also Text bearbeiten, Bilder anschauen und mit allgemeiner SW bearbeiten, ins Internet gehen zum Shoppen. Die meiste Zeit des Tages benötigen sie für andere Dinge und Tätigkeiten. Näheres Fachwissen ist nicht nötig, da man nur ab und zu am PC seine Zeit verbringt.
Ich habe den Artikel von Steffen gelesen und nicht alle Begriffe verstanden wie z.B: addon, adguard, baidau. Auch ich bin nur ein Greenhorn auf dem Gebiet der Computer. Also habe ich einen Profi gefragt (Schwiegersohn) der Jahrzehnte schon im IT-Geschäft tätig ist und sich bestens auskennt zu Fragen der PC-Sicherheit. Ich habe ihn Steffens Artikel geschildert und folgende Frage gestellt.
Geht ein „PC-Normalverbraucher“ da nicht ein zu großes Risiko ein?
Hier einige Passagen aus seiner Antwort:
…Hallo Fred,
ja, das tut man, und du hast mit deiner Einschätzung Recht.
Der Weiterbetrieb veralteter Betriebssysteme, insbesondere Windows 7 ab 2020, grenzt an grobe Fahrlässigkeit. Es geht hier um grundlegende Sicherheitslücken im Betriebssystem, die ab dem Supportende nicht mehr durch MS-Sicherheitsupdates gestopft werden. Das hat nichts mit Viren, Skripten, Sandboxen oder Ransomware zu tun, die ein signaturbasierender Scanner neutralisieren könnte. Es handelt sich um Fehler in den Programmierungen der Codebibliotheken.
Besagte Sicherheitslücken, sogenannte „Exploits“, erlauben das Einschleusen und Ausführen beliebigen Programmcodes in den Betriebssystemkernel oder in Teile davon. Vor den Gefahren offener Lücken im Quellcode des Betriebssystems kann keine Zusatzsoftware oder was auch immer schützen. Virenscanner, Firewall, Sandbox & Co. können das Risiko zwar minimal mindern, aber keinesfalls auf null reduzieren. ***Sicherheitslücken zeichnen sich ja gerade dadurch aus, dass man mit ihrer Hilfe ein System an anderen Schutzmaßnahmen vorbei angreifen kann.***
Im Klartext: Am 14.01.2020 gibt es zum letzten Mal kostenlose Sicherheits-Updates für Windows 7, danach ist für Otto Normal Verbraucher Schluss damit. Alle nach diesem Zeitpunkt entdeckten Sicherheitslücken werden also nicht mehr gestopft. Und es werden weiterhin welche gefunden werden, darauf kann man sich verlassen: Von den rund 1000 Schwachstellen in Win7, die die einschlägige Datenbank „CVE Detail“ seit Erscheinen von Win 7 im Jahr 2009 insgesamt verzeichnete, wurde 229 erst im Jahr 2017 gefunden; 2018 waren es auch schon wieder 139. Von den insgesamt 269 besonders dramatischen Lücken wurden gar 47 erst 2017 und 30 im Jahr 2018 entdeckt.
Eine Kostprobe: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=windows+7
Der o. g. Link ist die offizielle Schwachstellenliste von Windows 7.

Und das nutzen die „bösen Jungs“, um ihre Angriffe vorzubereiten:
https://www.exploit-db.com/
Hier gibt es den Programmcode und die Anleitungen, um die Schwachstellen auszunutzen. Wir reden also von einer ganz realen Gefahr.
Letztendlich ist jeder selbst verantwortlich über die Nutzung seines Betriebssystems.
Trotzdem sollten wir unseren Kunden über die Gefahren bei weiterer Anwendung von Win 7 ab 2020 hinweisen.
Wir sollten bedenken, dass unsere Kunden auch nur größtenteils als „PC-Normalverbraucher“ eingestuft werden.
Was geschieht wenn das Kind in den Brunnen fällt?
Eine falsche Beratung und das Image vom Club ist dahin. Nicht jeder der am PC arbeitet hat ein fundiertes Wissen auf dem Gebiet der SW.
Mit freundlichen Grüßen
Fred Arnhardt