Ransomware Encounter Rate

Microsoft Windows 10

Diejenigen, die eine Aktualisierung auf Windows 10 vermieden haben oder denen die Motivation zum Einsatz von Windows 10 fehlt, sollten sich mal mit den beängstigen Ransomware Zahlen beschäftigen.

Ransomware ist unter uns und kann nicht mehr gestoppt werden!

Wir befinden uns in einer Zeit, in der das Internet nicht mehr wegzudenken ist. So gut wie jedes Gerät hat einen Zugang zum Internet und ist den wachsenden Gefahren ausgesetzt. Server, Workstations, Netzwerkkomponenten, Drucker – alles ist miteinander verbunden und tauscht sich aus.

Aus diesem Grund appelliere ich an ein höheres Bewusstsein für Sicherheit.

Ransomware kommt entweder per E-Mail oder über den Browser. Es ist nicht damit getan Mitarbeiter zu sensibilisieren oder organisatorische Anweisungen zu verhängen. Das Problem muss gesamtheitlich betrachtet und Schutzmaßnahmen müssen schnellstmöglich ergriffen werden.

Auch der Mitarbeiter muss sich sicher fühlen und nicht ständig von Angst begleitet werden, derjenige zu sein, der nachweislich die Schadsoftware ins Unternehmen gebracht hat.

Schleust sich eine Infektion ein, verbreitet sich diese schneller als dass man die Möglichkeit hat, rechtzeitig zu reagieren, um die Ausbreitung zu stoppen.

An dieser Stelle fange ich gerne damit an, den Begriff „digitale Seuche" zu benutzen. Seit 2015 verzeichnet Microsoft einen Anstieg an Ransomware von 400%.

Bis zum Juli letzten Jahres zählte Microsoft ebenfalls 58 Millionen Versuche, Computer mit Ransomware zu infizieren.

Die Grafik zeigt ganz klar auf, dass Windows 10 die Wahl des einzusetzenden Betriebssystems sein sollte. Windows 10 ist das bisher sicherste Windows aller Zeiten.

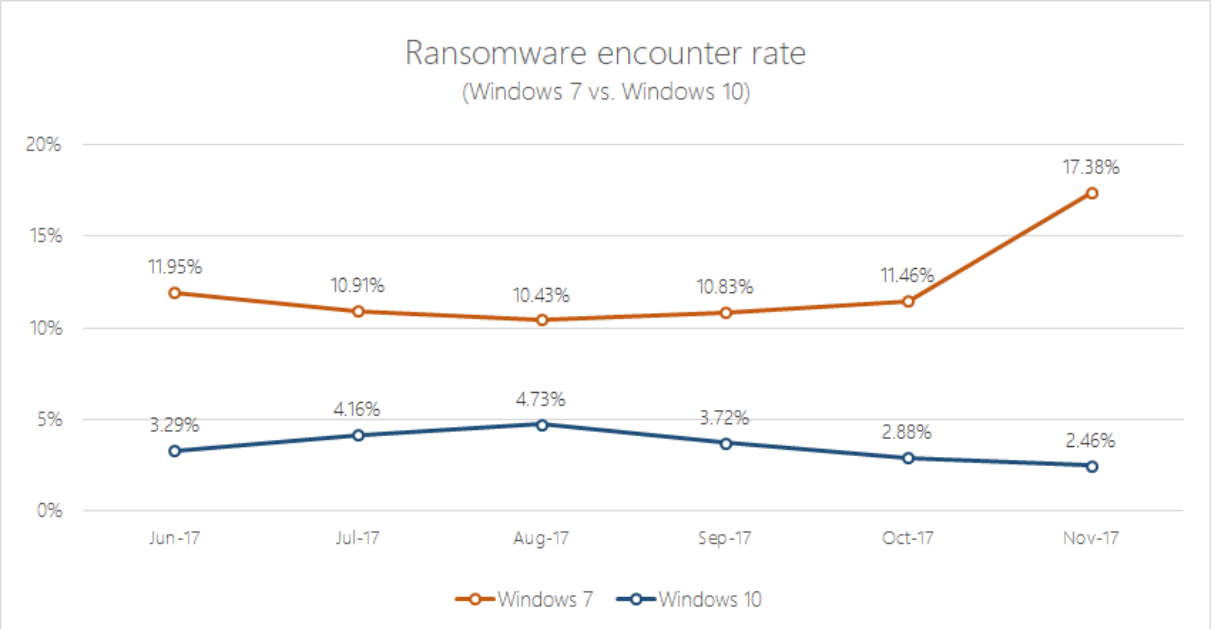

Bild: Microsoft

Erstellt von Jörn Walter **12.01.2018**

Ransomware Encounter Rate

Im November 2017 sind 15% mehr Windows 7 Rechner mit Ransomware infiziert worden als Windows 10 Systeme.

Was passiert, wenn Redmond am 14. Januar 2020 den Support-Stecker für Windows 7 zieht? Dann sind alle Anwender noch höheren Risiken ausgesetzt. Sicherheitslücken innerhalb des Systems werden nicht mehr geschlossen, und nun?

Clientbetriebssysteme	Aktuelles Update oder Service Pack	Ablauf des grundlegenden Supports	Ablauf des erweiterten Supports
Windows Vista	Service Pack 2	10. April 2012	11. April 2017
Windows 7 *	Service Pack 1	13. Januar 2015	14. Januar 2020
Windows 8	Windows 8.1	9. Januar 2018	10. Januar 2023
Windows 10 **	Siehe verfügbare Updates	13. Oktober 2020	14. Oktober 2025

https://support.microsoft.com/de-de/help/13853/windows-lifecycle-fact-sheet

Was ist dann mit denen, die ihre Zertifizierung nach dem PCI-DSS Standard erhalten, wie zum Beispiel das Bankenwesen?!

Microsoft Office 2016

Makros in Office Dokumenten sind ein weiteres Einfallstor für Malware. In Office 2016 besteht nun die Möglichkeit Makros zu blockieren die eine Verbindung zum Internet aufbauen und den Schadcode unbemerkt herunterladen.

Über aktuelle Gruppenrichtlinien ist es nun möglich diese Funktion zentral zu deaktivieren und zu steuern.