

Microsoft und itWatch arbeiten Hand in Hand

Wirksam vor den rtf Angriffen über MS Word schützen!

München, 31.März 2014 RTF (Rich-Text-Format) Textdateien stellen erneut eine Bedrohung dar. Das BSI pflegt seit langem Listen über Angriffsvektoren in bestimmten Contents – RTF war schon häufiger als Träger von Angriffen dokumentiert. Aktuell ist es, wie in Spiegelonline beschrieben, Hackern gelungen, mit Schadcode versehene RTF zu erstellen und erfolgreich in den Umlauf zu bringen. Durch diesen Schadcode kann der Angreifer fremde Rechner mit den Rechten des angemeldeten Nutzers übernehmen. Das Öffnen von diesen RTF Dateien in der Anwendung Word genügt, um den Schadcode auszuführen. Es genügt auch schon über einen Download mit dem Browser oder die Preview Funktion in beliebigen Email Programmen solche RTF Anhänge implizit zu öffnen, wenn Word die textverarbeitende Software dahinter ist.

Microsoft bietet Fix an

Microsoft bietet den Fix an, RTF Dateien von der Anwendung Word zu entkoppeln, also nicht standardmäßig mit Word zu öffnen. Für viele Kunden ist das ein gangbarer Weg und bietet 100%igen Schutz vor dem Angriff.

Mit XRayWatch Inhalte prüfen

Wer weiterhin RTF Dateien in Word bearbeiten muss, sich aber trotzdem gegen diese Angriffe schützen will, kann sich mit der itWatch Enterprise Security Suite gegen diese Angriffe schützen. Kunden der itWatch finden in dem Kunden-Download unter www.itWatch.de die geeignete, schon vorbereitete Lösung.

Mit der Content Filter Technologie und der Pattern Definition Sprache in XRayWatch ist es möglich die semantische und syntaktisch beliebig genaue Prüfung der Inhalte einer Datei (die so genannte Pattern Prüfung) durchzuführen und sich so vor diesen Schadcodes zu schützen. Zum einen werden per Content Filter RTF und DOC Dateien mit aktivem Code geblockt, d.h. das Lesen solcher gefährlicher Inhalte wird verhindert oder virtualisiert. Zusätzlich wird durch den Content Filter verhindert, dass Word ausführbare Codes in die Temporär-Bereiche des Benutzers schreibt. Dieser ist kundenseitig beliebig modifizierbar und kann auch auf externe Massenspeicher (z.B. USB-Sticks oder CDs), Netzwerkshares und Cloud-Dienste ausgeweitet werden, um somit einen sicheren Rundumschutz zu bieten.

Durch diese Technologie der itWatch GmbH wird zusätzlich verhindert, dass Benutzer ohne es zu merken gefährliche Dateien öffnen, erzeugen oder bestehende verändern. Mit XRayWatch in Kombination mit ApplicationWatch definieren Sie, wer oder welche Anwendung welche Daten von wo lesen und wohin schreiben darf – sei es im Netzwerk, der Cloud, lokal auf der Festplatte oder auf mobilen Datenträgern.

[zur Pressemeldung](#)