Sicherheitslücke in Word bedroht Outlook, Teil 1
Versionen: Outlook 2013, 2010, 2007 und 2003

Ende März veröffentlichte Microsoft eine Warnung vor einer offenbar gravierenden Sicherheitslücke in Microsoft Word: Mit speziell präparierten RTF-Dokumenten können Angreifer schädlichen Programmcode in Ihr System einschleusen. Das Fatale daran: Die Sicherheitslücke lässt sich auch in E-Mails ausnutzen, die Sie in Outlook lesen. Unter Umständen genügt schon das bloße Anzeigen der E-Mail im Lesebereich. In Outlook sind Sie damit im Grunde einem höheren Risiko ausgesetzt als in Word. Wir empfehlen deshalb dringend, Abwehrmaßnahmen einzuleiten. Wie Sie sich schützen, verraten wir Ihnen in diesem Tipp der Woche.

Leider sind Sicherheitslücken in Word auch immer ein Problem für Outlook, denn spätestens seit Outlook 2007 dient Word als E-Mail-Editor, ob Sie wollen oder nicht. Dazu muss Word nicht einmal auf Ihrem PC installiert sein. In diesem Fall setzt Outlook eine abgespeckte Version von Word zum Lesen oder Bearbeiten von E-Mails ein.

In Outlook 2003 haben Sie immerhin die Wahl, den Outlook-internen Editor oder Word zu benutzen. Darum lautet unsere erste Empfehlung für Outlook 2003: Verwenden Sie Word nicht zum Lesen von Nachrichten. Hier die entsprechenden Einstellungen:

1. Wählen Sie *Extras-Optionen* an und wechseln Sie danach auf die Registerkarte *E-Mail-Format*.
2. Deaktivieren Sie das Kontrollkästchen *Rich-Text-Nachrichten mit Microsoft Office Word 2003 lesen*.
3. Klicken Sie auf *Ok*.

Outlook 2003 verwendet jetzt immer den internen Editor, wenn Sie eine RTF-Nachricht per Doppelklick öffnen und in einem separaten Nachrichtenfenster lesen. Für den Lesebereich gilt das sowieso. Obwohl Sie damit einigermaßen sicher sind, sollten Sie weiterlesen. Schließlich sind Sie immer noch ungeschützt vor Viren und Trojanern, die sich in RTF-Dateianhängen befinden.

Solange es kein Update für Word gibt, das die Sicherheitslücke durch RTF-Dateien beseitigt, empfiehlt sich generell das Einspielen der aktuellen "Fix it"-Lösung, die Microsoft auf folgender Internetseite anbietet:

[**https://support.microsoft.com/kb/2953095**](https://support.microsoft.com/kb/2953095)

Beachten Sie, dass auf der Seite zwei "Fix it"-Lösungen angeboten werden: Nr. 51010 unter *Enable this fix it* schaltet den RTF-Schutz ein, Nr. 51011 unter *Disable this fix it* hebt den Schutz wieder auf.

In beiden Fällen werden Sie zum Download einer MSI-Datei aufgefordert, die sich jeweils per Doppelklick aus dem Windows Explorer installieren lässt.

Die "Fix it"-Lösung blockiert das Öffnen und Bearbeiten von RTF-Dokumenten in Word, indem bestimmte Zugriffsschutzeinstellungen in der Registry gesetzt werden.

Für Outlook ist die Blockade von RTF-Dokumenten allerdings nur bedingt hilfreich. Immerhin schützt sie vor E-Mail-Anhängen, die schadhaften Code einschleusen könnten, denn auch das Öffnen einer angehängten RTF-Datei wird mit einer Hinweismeldung abgeblockt.

Was die Blockade aber nicht verhindert, ist die Anzeige von E-Mails im RTF-Format. Über ein Nachrichtenfenster, in dem Sie eine E-Mail öffnen, oder über den Lesebereich von Outlook könnten sich also Viren einschleichen.

Dagegen hilft derzeit nur, alle E-Mails als reine Textnachrichten anzeigen zu lassen. Das erreichen Sie mit folgender Einstellung:

**Outlook 2013, 2010**

1. Wählen Sie *Datei-Optionen* an und wechseln Sie zur Kategorie *Trust Center* bzw. *Sicherheitscenter*.
2. Klicken Sie auf die Schaltfläche *Einstellungen für das Trust Center / Sicherheitscenter*.
3. Im nun angezeigten Dialogfenster wechseln Sie zur Kategorie *E-Mail-Sicherheit*.
4. Schalten Sie im Bereich *Als Nur-Text lesen* das Kontrollkästchen *Standardnachrichten im Nur-Text-Format lesen* ein.
5. Verlassen Sie die geöffneten Dialogfenster jeweils mit *Ok*.

**Outlook 2007**

1. Wählen Sie *Extras-Vertrauensstellungscenter* an.
2. Wechseln Sie zur Kategorie *E-Mail-Sicherheit*.
3. Schalten Sie im Bereich *Als Nur-Text lesen* das Kontrollkästchen *Standardnachrichten im Nur-Text-Format lesen* ein.
4. Klicken Sie auf *Ok*.

**Outlook 2003**

1. Wählen Sie *Extras-Optionen* an und wechseln Sie auf die Registerkarte *Einstellungen*.
2. Klicken Sie auf die Schaltfläche *E-Mail-Optionen*.
3. Aktivieren Sie das Kontrollkästchen *Standardnachrichten im Nur-Text-Format lesen*.
4. Schließen Sie die geöffneten Dialogfenster jeweils mit *Ok*.

Ab sofort lesen Sie alle Nachrichtentexte nur noch als reinen Text - ohne Formatierungen, Bilder usw. Damit haben manipulierte RTF-Nachrichten keine Chance mehr.

Leider werden jetzt aber auch HTML-Mails komplett unformatiert angezeigt, was zum Beispiel bei Newslettern unvorteilhaft ist. Im Bedarfsfall haben Sie deshalb die Möglichkeit, einzelne Nachrichten wieder in der Originalformatierung anzeigen lassen. Dazu klicken Sie im Nachrichtenkopf auf die Infoleiste mit dem Text "Diese Nachricht wurde in das Nur-Text-Format konvertiert" und wählen im aufklappenden Kontextmenü *Als HTML anzeigen* an.

Achten Sie aber genau auf den Kontextmenübefehl. Wenn dort *Als RTF (Rich-Text) anzeigen* angeboten wird, sollten Sie misstrauisch werden. Wählen Sie diesen Befehl nur an, wenn Sie dem Absender der E-Mail vertrauen und Sie sicher sein können, dass sich in der Nachricht keine Viren verstecken.

So sind Sie schon gut vor den Gefahren in RTF-Dokumenten geschützt. Was Sie sonst noch tun können, erfahren Sie im zweiten Teil dieses Tipps.

Sicherheitslücke in Word bedroht Outlook, Teil 2
Versionen: Outlook 2013, 2010, 2007 und 2003

RTF-Dokumente stellen potenziell eine Bedrohung für Word und damit auch für Outlook dar. Für eine gerade bekannt gewordene Sicherheitslücke in den RTF-Komponenten von Word gibt es bislang kein Update, das die Gefahr bannt. So bleibt Ihnen nur, bestehende Sicherheitsfunktionen auszunutzen, um eine Bedrohung durch E-Mails oder Dateianhänge im RTF-Format weitgehend auszuschließen. Akute Maßnahmen haben wir Ihnen im ersten Teil dieses Tipps vorgestellt. In diesem Teil geht es um weitere Möglichkeiten, das Risiko durch RTF-Dokumente zu minimieren.

Selbst Virenscanner sind im Moment kein hundertprozentiger Schutz vor der Bedrohung durch manipulierte RTF-Dokumente. Erst müssen eindeutige Kennungen gefunden werden, durch die sich entsprechende Angriffe identifizieren lassen. Aber es gibt ein Tool, das schon jetzt recht zuverlässig den schadhaften Programmcode aus RTF-Dokumenten blockiert: Microsofts "Enhanced Mitigation Experience Toolkit" (EMET).

In den Outlook Weekly-Ausgaben vom 8.1.2014 und 15.1.2014 hatten wir bereits ausführlich über EMET berichtet. Dort finden Sie auch Hilfestellungen zur Installation und Konfiguration des Toolkits. An dieser Stelle deshalb nur ein kurzer Überblick:

EMET ist ein Hilfsprogramm, das die Ausführung laufender Programme überwacht und Alarm schlägt, wenn es virentypische Verhaltensmuster entdeckt. So kann auch Schadsoftware ausgeschaltet werden, die bislang noch gar nicht bekannt war. Das gilt unter anderem auch für die Angriffe durch RTF-Dokumente bzw. RTF-formatierte E-Mails - so behauptet es jedenfalls Microsoft in seinem "Security Research and Defense Blog".

Besonders erfreulich ist, dass Microsoft das "Enhanced Mitigation Experience Toolkit" kostenlos zum Download anbietet. Die aktuelle Version 4.1 ist über folgende Internetseite erhältlich: