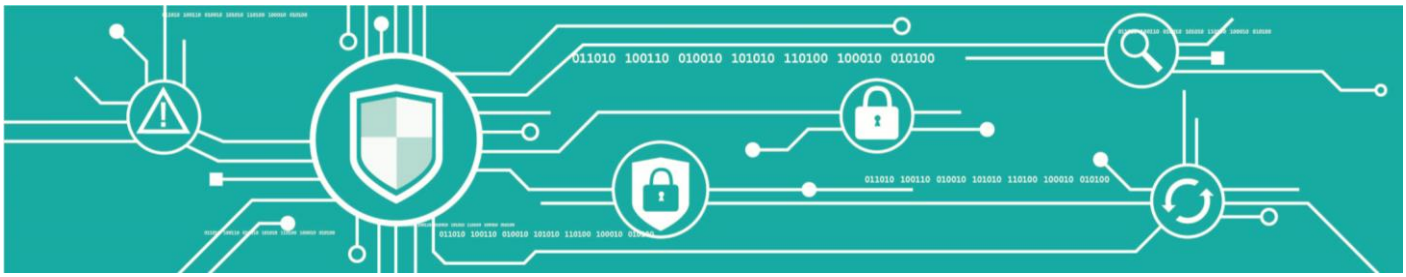

Dramatische Sicherheitslücke in Virenschutz-Software von Windows geschlossen

Microsoft hat eine schwerwiegende Lücke in der **Antiviren-Engine von Windows** beseitigt. Angreifer können verwundbare Systeme durch die Lücke auf vielfältige Weise infizieren. Betroffen sind alle Windows-Versionen sowie die Microsoft Security Essentials. Mit einem Notfall-Patch schliesst Microsoft eine hochkritische Sicherheitslücke in fast allen Windows-Versionen (einschliesslich Server). Angreifer können die Lücke ausnutzen, um die Kontrolle über ein System zu übernehmen. Die Google-Forscher Tavis Ormandy und Natalie Silvanovich hatten die Schwachstelle entdeckt und vergangenen Freitag an Microsoft gemeldet. Über Twitter kündigten sie an, auf eine "unfassbar schlimme" Windows-Lücke gestossen zu sein – wie die veröffentlichten Details zeigen, hatten die Forscher damit nicht übertrieben.

Was ist das für eine Sicherheitslücke?

Die Lücke ist in Microsofts Virenscanner-Engine, die seit Windows 8 in Form des **Defender** fester Bestandteil des Betriebssystems ist. In älteren Windows-Versionen ist sie Teil des gleichnamigen Antispyware-Programms sowie in der kostenlosen Virenschutz-Software Microsoft Security Essentials (MSE) erhalten. Die Engine untersucht vom System verarbeitete Daten vor der Ausführung auf Schadcode. Hält die Engine den Inhalt von Netzwerkpaketen oder Dateien etwa für JavaScript-Code, führt sie ihn zu Analysezwecken aus. Ormandy hat die Entdeckung der Lücke vergangenen Freitag über Twitter bekannt gegeben. Dabei leistet sich die Microsoft Malware Protection Engine (MsMpEn) allerdings einen fatalen Fehler, wie der Bericht der Google-Forscher offenlegt: Es kommt dabei unter bestimmten Umständen zu einer sogenannten Type Confusion. Eine Funktion des JavaScript-Interpreters überprüft die Eingabewerte nicht ausreichend, was letztlich dazu führt, dass ein Angreifer die Kontrolle über den Prozess übernehmen kann. Fatalerweise läuft dieser Prozess mit SYSTEM-Rechten und wird nicht von einer Sandbox geschützt. Der Angreifer erlangt also höchstmögliche Rechte über das verwundbare System.

Auswirkungen und Gefahren

Um die Lücke auszunutzen, muss der Angreifer die **Malware Protection Engine** dazu bringen, den Angriffscode zu verarbeiten. Und das ist einfach, da sie an vielen Stellen aktiv wird. Es genügt zum Beispiel, dem Opfer eine Mail zu schicken.

Sobald die Nachricht vom Mail-Client abgerufen wurde, wird der Schadcode ausgeführt – es ist nicht notwendig, dass das Opfer eine Mail oder gar einen Anhang öffnet. Genauso gut könnte der Angreifer sein Opfer auf eine angriffslustige Website locken. Auch Instant-Messenger-Nachrichten können für das Opfer fatale Folgen haben. Windows-Server sind gleichermassen gefährdet: Hier kann ein Angreifer den verwundbaren Prozess etwa durch das Hochladen von Dateien in Gang setzen. Kurzum: Die verwundbare Engine ist omnipräsent, der Kreativität des Angreifers sind keine Grenzen gesetzt.
Für Angreifer ist die Lücke hochinteressant, da sie extrem viele Systeme betrifft. Ferner ist sie leicht ausnutzbar und vielfältig einsetzbar. Es ist daher wahrscheinlich nur eine Frage von Stunden, bis sie für echte Infektionen ausgenutzt wird.

Für Abhilfe sorgt ein Notfall-**Update** der Microsoft Malware Protection Engine, das laut Microsoft automatisch installiert wird. Die abgesicherte Version lautet Microsoft Malware Protection Engine 1.1.13704.0.

Ist meine Anlage Bedroht?

Nein - Generell wird dieser Dienst auf den Anlagen Computer ausgeschaltet und ein autonomes Antiviren-Programm eingesetzt.

Update Service
Mit dem Update Service übernimmt Rittmeyer das testen und installieren der Patches und Hotfix von Microsoft. Besonders für das Betriebssystem wird empfohlen, in regelmässigen Abständen alle verfügbaren Sicherheitsupdates zu installieren, um bekannte Sicherheitslücken zu schliessen.

Backup Service
Das Daten-Backup von Rittmeyer ist eine vollständige, Cloudintegrierte Lösung. Gespeichert werden dabei nicht nur die Leitsystemdaten, wie beim manuellen Backup üblich, sondern auch die jeweilige Anlagekonfiguration mit allen Einstellungen. Diese Sicherung ist immer aktuell, da sie täglich durchgeführt wird.

ICT-Security
Wir unterstützen Sie dabei, potenzielle Schwachstellen und Bedrohungen frühzeitig zu erkennen und helfen Ihnen, gezielte Schutzmassnahmen zur IT-Sicherheit einzuführen. Unsere zertifizierten ISO-27001-Experten stehen Ihnen dabei von der Ist-Analyse über das Erstellen und Umsetzen eines individuellen IT-Sicherheitskonzepts bis hin zur strukturierten und nachhaltigen Verbesserung von Sicherheitsstandards zur Seite.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity