Erste Exploits für Bluekeep in Umlauf – umgehend Windows updaten!

Erste Exploits für Bluekeep in Umlauf – umgehend Windows updaten!

Großangelegte Cyber-Angriffe mit Schadprogrammen wie WannaCry und NotPetya haben 2017 Millionenschäden verursacht. Ein ähnlich bedrohliches Szenario ermöglicht jetzt die Microsoft-Windows-Schwachstelle Bluekeep. Die Sicherheitslücke wurde im Remote-Desktop-Protocol-Dienst (RDP) entdeckt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) rät dringend zur Installation der neuesten Sicherheitsupdates.

BSI warnt erneut vor gefährlicher Bluekeep-Schwachstelle

Bereits im Mai hatte das BSI auf eine extrem riskante Sicherheitslücke im Remote-Desktop-Protocol-Dienst (RDP) von älteren Windows-Versionen hingewiesen. Die Bluekeep-Schwachstelle ermöglicht einen Angriff mit Schadsoftware, die sich wurmartig aus- und selbstständig weiterverbreitet. Besonders bedenklich: Cyber-Attacken über Bluekeep können aus der Ferne und ohne Zutun des PC-Benutzers erfolgen. Inzwischen sind erste Exploits aufgetaucht, die die Ausnutzung der Lücke ermöglichen könnten. In Deutschland dürften derzeit mindestens 14.000 Computer unmittelbar über das Internet und unzählige weitere über Netzwerke angreifbar sein. Das BSI warnt daher erneut und sieht dringenden Handlungsbedarf für Unternehmen, Institutionen und Behörden.

Sofortige Installation von Sicherheitsupdates empfohlen

Von der gefährlichen Schwachstelle betroffen sind die älteren Windows-Versionen Windows XP, Windows Server 2003, Windows 7,

Windows Server 2008 R2 und Windows Server 2008. Obwohl diese Varianten nicht mehr unterstützt werden, stellt Microsoft wegen der akuten Bedrohungslage **Updates zur Verfügung,** die die Sicherheitslücke schließen. Das BSI rät betroffenen Nutzern dringend, die von Microsoft zur Verfügung gestellten Patches umgehend einzuspielen und eventuell erforderliche Kompatibilitätsprüfungen beschleunigt durchzuführen. Neuere Windows-Varianten sind laut Auskunft von Microsoft nicht anfällig für Bluekeep, sollten aber dennoch regelmäßig mit allen verfügbaren Sicherheitsupdates auf den aktuellen Stand gebracht werden.

DIE VSMA GMBH: EIN STARKER PARTNER IM KAMPF GEGEN CYBER-RISKEN

Als 100%iges Tochterunternehmen des VDMA e.V. bietet Ihnen auch die VSMA GmbH Unterstützung bei der Minimierung der wachsenden Bedrohung aus dem World Wide Web. Kostenlose Publikationen mit praxisbezogenen Tipps und ein Online-Tool zur Prüfung Ihres Cyber-Risikos bereiten Sie auf den Ernstfall vor. Eine speziell auf die Branche ausgerichtete Cyber-Versicherungslösung sichert Sie umfassend ab.

- **Branchenversicherung VDMA CYBER-POLICE: https://cyber.vsma.de**
- **Cyber-Risiko Prüfung: https://www.vsma.de/vdma-cyber-risiko-pruefung**
- **Broschüre "Tipps für den Cyber-Schadenfall": https://cyber.vsma.de**
- **Video „Cyberrisiken im Maschinen- und Anlagenbau": https://cyber.vsma.de**

Beitragsbild: Bilgehan Tuzcu / iStock

Kontakt:
Herr Thomas Völker
VSMA GmbH – ein Unternehmen des VDMA
Telefon +49 69 6603-1520
tvoelker@vsma.org

VDMA Cyber-Police