Spyware: Apps mit unerwünschten Erweiterungen

Sicherheitsforscher haben bei einer Routineüberprüfung ein Software Development Kit für Werbeeinblendungen entdeckt, das Schnüffelfunktionen besitzt. Dieses war in mehr als 500 Apps enthalten, darunter Spiele- und Wetter-Apps, die im offiziellen Google Play Store angeboten wurden, so ein Artikel auf heise.de. Die Spionagefunktion ist in der Lage, Werbung einzublenden und Befehle von einem Server zu empfangen und auszuführen. dies geschieht allerdings nur, wenn der Nutzer oder die Nutzerin bei der Installation der Apps entsprechende Berechtigungen erteilt hat. Mittlerweile hat Google die Apps gelöscht beziehungsweise die Funktion entfernt.

Worauf Sie bei der Installation einer App auf Ihrem Android-Gerät und der angeforderten Berechtigungsvergabe achten sollten, erfahren Sie auf der Webseite BSI für Bürger. [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*

Schwachstelle: Automatische Link-Updates in Word bergen Risiken

Sicherheitsexperten haben eine Funktion entdeckt, mit der Cyber-Kriminelle mittels Microsoft Word Systeme mit Malware infizieren. Dazu nutzen sie eine eingebettete Verlinkung, die sich immer wieder automatisch aktualisiert, sobald der Nutzer oder die Nutzerin das Word-Dokument öffnet, so ein Blogbeitrag auf botfrei.de. Ziel ist es, eine bösartige "PE-Netwire RAT"-Datei über einen PowerShell-Befehl-Programmbefehl herunterzuladen und auf dem betroffenen System zu starten.

Sie können Ihre Geräte schützen, indem Sie dafür sorgen, dass Ihr Betriebssystem und alle verwendeten Applikationen stets mit Updates auf dem aktuellen Stand gehalten werden. Zudem sollten Sie niemals Office-Dateien öffnen, die von nicht vertrauenswürdigen Quellen stammen. Wie wichtig Patch-Management in diesem Zusammenhang ist, erfahren Sie auf der BSI für Bürger Webseite [LINK zur Website]. *[Quelle: Buerger-Cert-Newsletter] SICHER • INFORMIERT vom 31.08.17]*