Firmen-LANs sind per Fax angreifbar

Unternehmen schützen ihre IT-Infrastruktur mittlerweile sehr aufwendig vor Hackerangriffen, doch uralte Einfallstore bleiben unbeachtet: Forscher der israelischen Sicherheitsfirma Check Point haben ein Angriffsszenario über eine **Lücke im Faxprotokoll** gefunden. In vielen Büros stehen Multifunktionsgeräte mit Fax, die etwa Scans zwar im abgesicherten LAN verteilen können, zum Faxen aber weiterhin eine von der IT-Security bislang unbeachtete Telefonleitung verwenden.

Mit einem manipulierten Fax konnte Check Point verschiedene Büromultifunktionsgeräte von HP kapern und Schadcode einschleusen. Ist der Faxdrucker wie meist üblich mit dem LAN verbunden, kann sich der Schadcode auf alle PCs verteilen und zum Infizieren weiterer Geräte passende Trojaner aus dem Netz laden. Infizierte Firmware könnte den Faxversand sowie Dokumentenscans an den Hacker weiterleiten. Ebenso denkbar ist das Manipulieren von Faxen vor dem Versand oder von Sendeprotokollen, was die Gerichtsfestigkeit von Faxen infrage stellen könnte – bisher ein wichtiger Grund für den anhaltenden Einsatz dieser technischen Altlast.

Da sich die Sicherheitslücke auf das alte, von allen Faxgeräten verwendete Faxprotokoll bezieht, rechnen die Forscher damit, dass die „Faxploit“ genannte Lücke auch bei vielen Faxgeräten anderer Hersteller und sogar bei Online-Faxdiensten funktioniert. Von HP betrifft die Faxlücke laut einer Herstellerliste über 150 Tintengeräte von den PageWide-Schnelldruckern über die Officejet-Serie bis zu den Deskjet- und Envy-Geräten für den Heimgebrauch. Da HP die betroffenen Faxmodems und die dazugehörige Firmware auch in Laserjet-Druckern einsetzt, dürften auch viele Büro-Laserdrucker betroffen sein. Für die Tintengeräte stellt HP bereits Firmware-Updates bereit. Faxnutzer sollten beim jeweiligen Hersteller auf Patches für die mit CVE-2018-5924 und CVE-2018-5925 bezeichneten Lücken achten.

Auch das für technische Prüfungen und Zertifikate zuständige VDE-Institut rät zu einer Neubewertung veralterter Techniken wie dem Faxgerät und empfiehlt, die Faxfunktion von Multifunktionsgeräten zu deaktivieren und alte Faxgeräte vom Telefonnetz zu trennen. Letzteres dürfte übertrieben sein, da alte dedizierte Faxmodelle in der Regel nicht mit dem LAN verbunden sind und für einen Faxploit-Schadcode zu wenig Ressourcen wie Speicher und Rechenleistung haben. Wichtige Fax-Multifunktonsgeräte im LAN sollte man allerdings möglichst schnell updaten. *(rop@ct.de)*

Ein manipuliertes Fax kann Multifunktionsgeräte wie die HP-Modelle PageWide Pro MFP 477dw (rechts) und OfficeJet Pro 8720 (links) kapern und Schadcode einschleusen; HP stellt gepatchte Firmwares bereit.