Ladegeräte spionieren Laptops gezielt aus - Experten warnen User vor gedankenloser Nutzung von Beamern und Co im öffentlichen Raum

Die meisten Laptops sind verletzlich, wenn periphere Geräte angeschlossen werden, wie Forscher der University of Cambridge und der Rice University herausgefunden haben. Hacker können sich sekundenschnell Zugang zu unbeaufsichtigten Geräten verschaffen, indem sie beispielsweise eine präparierte Stromversorgung anschliessen oder den Laptop auf ein berührungsloses Ladegerät legen.

Einfallstor Thunderbolt

Betroffen sind insbesondere Geräte mit einer sogenannten Thunderbolt-Schnittstelle, die von Intel in Zusammenarbeit mit Apple entwickelt worden ist. Seit 2012 wird sie auch für Geräte mit Windows genutzt. Betroffen sind ausserdem Geräte mit den Betriebssystemen macOS, Linux und FreeBSD. Zunehmend findet die Schnittstelle auch für Computer Anwendung.

Laut den Forschern ermöglichen selbst harmlos erscheinende Geräte, die mit einem Laptop oder Computer verbunden werden, die totale Kontrolle. Dazu zählen beispielsweise Beamer, die korrekte Bilder liefern, nebenbei aber einen Angriff auf den Laptop starten. Die peripheren Geräte haben einen Speicherdirektzugriff, der die Schutzmechanismen des Laptops umgeht.

Verhindern lässt sich eine solche Attacke mit der Input-Output-Memory-Management-Unit (IOMMU), die aber nicht in allen Geräten steckt. Oft wird diese Funktion ausgeschaltet, sagen die Forscher um Theodore Markettos, Computerwissenschaftler in Cambridge. Kompletten Schutz biete aber auch IOMMU nicht. "Gegen besonders raffinierte Angriffe ist auch dieser Schutzmechanismus unwirksam", unterstreicht Brett Gutstein, der zum Team gehört.

Externe Videogeräte

Die Forscher arbeiten mittlerweile mit Apple, Intel und Microsoft zusammen, um Gegenmassnahmen zu entwickeln. Andererseits eröffnen Weiterentwicklungen der Thunderbolt-Schnittstelle Angreifern neue Möglichkeiten. Diese dienen gleichzeitig der Stromversorgung, der Datenübermittlung an externe Videogeräte und dem Anschluss anderer peripherer Geräte.

Vor diesem Hintergrund werden weitere Anstrengungen der Hersteller zur Eindämmung der Gefahren gefordert. Gleichzeitig mahnen die Forscher Nutzer, die ihre Laptops beispielsweise auf Kongressen nutzen, um Power-Point-Präsentationen zu zeigen, sich der Risiken stets bewusst zu sein. Es gebe bereits Schutzmassnahmen, die grosse Unternehmen anböten. Sie seien auf die Angriffsmöglichkeiten fixiert, die sie aufgedeckt hätten. Es sei allerdings wichtig, diese Schutzprogramme regelmässig upzudaten.