

USB als Angriffsvektor: Was Unternehmen wirklich über Ladekabel wissen sollten

Ein Blick hinter die Steckdose – aus der Perspektive der Informationssicherheit

Ein Ladekabel ist ein Ladekabel – oder etwa nicht? Wer so denkt, unterschätzt einen der ältesten und zugleich am häufigsten übersehenen Angriffsvektoren in der Unternehmens-IT. USB-Schnittstellen sind allgegenwärtig: im Konferenzraum, im Homeoffice, an öffentlichen Ladestationen – und genau dort beginnen die Risiken.

In der Praxis sehen wir immer wieder, dass USB-Schnittstellen in Risikoanalysen und ISMS-Dokumentationen entweder gar nicht oder nur oberflächlich behandelt werden – obwohl der Angriffsvektor seit Jahren bekannt ist und real genutzt wird.

1. Wie ein USB-Angriff in der Praxis abläuft

Der klassische Angriffspfad beginnt nicht mit einem Hackertool – er beginnt mit Menschenverstand. Das bekannteste Beispiel ist Baiting: Ein präparierter USB-Stick wird auf dem Firmenparkplatz oder in der Hotellobby abgelegt. Die Neugier tut den Rest.

Ist das Gerät eingesteckt, greift die Automatik: Das Betriebssystem erkennt das Gerät, lädt den passenden Treiber – vollständig ohne Benutzerinteraktion. Genau hier liegt das strukturelle Problem: Windows und Linux vertrauen USB-Geräten standardmäßig.

Die wichtigsten Angriffsvarianten im Überblick:

Variante	Funktionsweise	Wirkung
BadUSB / Rubber Ducky	USB-Stick emuliert eine Tastatur (HID)	Automatische Codeausführung in Sekunden
O.MG Cable	Präpariertes USB-C-Kabel mit eigenem MCU	Vollständige Kompromittierung, unsichtbar
Juice Jacking	Öffentliche Ladestation leitet auch Datenleitungen	Datenabfluss oder Malware-Installation
USB Killer	Kondensatoren entladen sich mit Hochspannung	Sofortige Hardware-Zerstörung
Treiber-Exploit	Präpariertes Gerät triggert Kernel-Bug	Privilege Escalation, Kernel-Crash

2. Der unterschätzte Angriffsvektor: USB Power Delivery

Mit der flächendeckenden Einführung von USB-C und dem Power-Delivery-Protokoll (USB PD) ist eine neue Angriffsfläche entstanden, die bislang kaum CVEs aufweist – aber technisch hochrelevant ist.

USB PD ist kein einfaches Stromkabel. Es ist ein vollwertiges Kommunikationsprotokoll: Geräte verhandeln über sogenannte Configuration-Channel-Leitungen Spannung und Strom – und können dabei herstellerspezifische Nachrichten (Vendor Defined Messages, VDMs) austauschen.

Forschungsarbeiten der NTNU (Norwegen) haben gezeigt, dass VDMs für Firmware-Updates, Memory Dumps und sogar Backdoors genutzt werden können. Ein Angreifer, der ein gewöhnliches Netzteil optisch imitiert, kann über den PD-Stack des Kernels Code einschleusen – während das Notebook ganz normal lädt.

Das Besondere: Dieser Angriff operiert unterhalb des Windows-Sicherheitsmodells. Weder Microsoft Defender noch HVCI analysieren PD-Protokollinhalte auf CC-Leitungsebene.

3. Was Microsoft abfängt – und was nicht

Windows 11 bietet eine beeindruckende Schutzarchitektur für USB – die jedoch bei PD-basierten Angriffen strukturell an ihre Grenzen stößt:

Schutzfunktion	Schutzwirkung	Wirksamkeit gegen PD-Exploit
HVCI / Memory Integrity	Blockiert unsignierte Kernel-Treiber	Mittel – PD-Treiber sind MS-signiert
Vulnerable Driver Blocklist	Bekannte verwundbare Treiber	Deckt unbekannte Zero-Days nicht ab
Kernel DMA Protection	Thunderbolt DMA-Angriffe	Gut – aber nur für DMA, nicht PD
Defender Device Control	USB-Gerätezulassung per Policy	Gut – wenn konfiguriert
Smart App Control	Unsignierte Prozesse blockieren	Wirkt erst nach dem Exploit

Das strukturelle Problem: Der Windows USB-PD-Stack (ucsi.sys, UcmUcsiCx) ist ein Inbox-Treiber von Microsoft selbst. Er ist signiert, vertrauenswürdig – und wird niemals durch die Blocklist gefiltert. Ein Zero-Day in diesem Stack wäre für Windows unsichtbar.

4. Was das für Ihr ISMS bedeutet

Aus Sicht von ISO 27001:2022 und IEC 62443 müssen USB-Schnittstellen als physische Angriffsvektoren explizit in der Risikoanalyse adressiert werden. Folgende Controls sind direkt relevant:

- **A.7.2** (Physical entry controls): Zugang zu Arbeitsbereichen mit ungeschützten USB-Ports
- **A.8.12** (Data leakage prevention): USB als Datenexfiltrationspfad
- **A.8.9** (Configuration management): Treiber- und Gerätekonfiguration

Besonders für hochwertige Ziele (Geschäftsführung, kritische Infrastruktur, F&E) sollte das PD-Szenario explizit als Bedrohung im Statement of Applicability (SoA) und im Risikobehandlungsplan dokumentiert sein.

5. Praktische Gegenmaßnahmen

Technische Maßnahmen:

- USB-Ports per Gruppenrichtlinie oder Endpoint Security auf Whitelist beschränken
- USB-C-Port im BIOS auf „Charge only“ konfigurieren (unterbindet Datenkommunikation vollständig)
- Secured-Core PC mit DRTM als Hardwarebasis wählen
- EDR-Lösung einsetzen, die HID-Anomalien erkennt (z. B. Tastatureingaben > 200 Zeichen/Sekunde)
- USB-Data-Blocker bei fremden Ladestationen verwenden

Organisatorische Maßnahmen:

- Richtlinie zum Verbot privater USB-Geräte und nicht autorisierter Ladekabel
- Sensibilisierungsschulung zu Baiting und Social Engineering
- Clear-Desk-Policy zur Minimierung unbeaufsichtigter Endgeräte
- Physische USB-Port-Blocker für stationäre Arbeitsplätze

Fazit

USB ist längst kein simpler Datenstecker mehr. Mit USB-C und Power Delivery ist eine Schnittstelle entstanden, die Strom, Daten und Protokollkommunikation vereint – und damit eine Angriffsfläche schafft, die weit unterhalb klassischer Sicherheitskontrollen operiert.

Die gute Nachricht: Die Gegenmaßnahmen sind bekannt und umsetzbar. Die schlechte Nachricht: In den meisten ISMS-Dokumentationen fehlen sie noch immer.

Kommentieren Sie gerne über konkrete Umsetzungsmöglichkeiten in Ihrer Organisation – ob im Rahmen eines ISO-27001-Audits, einer IEC-62443-Zertifizierung oder einer gezielten Risikoanalyse.