IT-Sicherheit USB – ein praktisches System…

Der Verizon 2016 Data Breach Investigations Report wies dem USB-Anschluss (Universal Serial Bus) den Platz drei bei Datenlecks zu. Jeder PC, jedes Tablet oder Smartphone besitzt in der Regel einen USB-Anschluss, der durch entsprechende Gerätschaften wie USB-Sticks oder USB-Festplatten als Einfallstor von Kriminellen missbraucht werden kann. Die kleinen Geräte sind für den schnellen Datenaustausch einfach zu nutzen, bieten aber besonders deshalb eine große Wahrscheinlichkeit des Verlusts. Durch die technischen Möglichkeiten der USB-Schnittstelle ist es sogar möglich, Schadsysteme in vorhandene Geräte, wie Tastatur oder Maus, zu integrieren. So schöpft der Anwender keinen Verdacht. Die IT-Sicherheit Ihrer Einrichtung ist womöglich in Gefahr.

Einige Angriffsszenarien

Infizierte Dateien:
Der einfachste Angriff besteht aus infizierten Dateien, die sich auf dem Datenspeicher befinden können. Denken Sie nur an den besitzerlosen USB-Stick auf dem Parkplatz.

Poisentap:
Der Angreifer steckt das modifizierte USB-Gerät an Ihr Endgerät (PC, Smartphone o.ä.), durch die Simulation einer falscher USB-Kennung, wird der Treiber automatisch vom Betriebssystem installiert. Dieses geschieht auch bei gesperrten Systemen. Dieser Angriff ist als Poisontap bekannt. In diesem Szenario wird ein USB-Netzwerkadapter vorgegaukelt und das WPAD-Protokoll (Web Proxy Autodiscovery Protocol) missbraucht, welches zum Auffinden eines Web Proxys innerhalb des Netzwerks verwendet wird. Zum Aufrufen der vermeintlichen WPAD-Konfigurationsdatei werden die Benutzerdaten verlangt, der NTLM-Hash. Ist der Angreifer im Besitz dieses Hash, kann er ihn zum Angriff nutzen, um sich so als legitimer Benutzer auszuweisen. Dieser Pass-the-Hash Angriff ist insbesondere aus dem Angriff auf die IT des deutschen Bundestags bekannt geworden. Zum anderen kann der Angreifer durch Brute-Force Attacken das Kennwort entschlüsseln. Hierzu sind lediglich Zeit und Rechenkapazitäten der begrenzende Faktor.

Umleiten und mitlesen des Datenverkehrs:
Der Angreifer kann einen Man-in-the-Middle Angriff starten, in dem er den Netzwerkverkehr um- und durchleiten. Hierbei wird das korrekte Zertifikat durch ein gefälschtes Zertifikat ausgetauscht und der Eindringling kann alle vertraulichen Informationen mitlesen und/oder verändern.

Ausgabe als Eingabegerät:
Auch kann der Angreifer eine Tastatur modifizieren, über die bis zu 60 Tastaturanschläge pro Sekunde eingegeben werden können. In dieser Geschwindigkeit bekommt das Opfer diese Eingaben gar nicht mit oder kann nicht schnell genug eingreifen. Auch kann dieser Angriff zur Entsperrung von Displaysperren von Smartphones genutzt werden.

Abwehrstrategien

An erster Stelle stehen alle Nutzer des Systems. Durch regelmäßige Schulungen und Informationen sollte das Bewusstsein für diese Problematik geschärft werden.

Des weiteren kann die Nutzung von privaten USB-Geräten mithilfe von Dienstanweisungen ausgeschlossen werden. Technisch kann dies durch Gruppenrichtlinien unterstützt und umgesetzt werden. Für die Verwendung von USB-Datenträgern sollte ein sogenannter LifeCycle erarbeitet und implementiert werden. Feste Vorgehensweisen bei Verlust und auch Entsorgung von nicht mehr benötigten Geräten sind dabei vorzugeben. Im weiteren sollte die Boot Reihenfolge der Systeme so angepasst, dass das Endgerät nicht alternativ über USB gestartet werden kann. USB-Datenträger sollten nur verschlüsselt genutzt werden, so können bei Verlust die darauf befindlichen Daten nicht mehr genutzt werden. Die USB-Anschlüsse an den Endgeräten müssen geschützt werden. Ist der PC länger unbeaufsichtigt, muss der Zugang verhindert werden oder der PC heruntergefahren werden. Steht der PC an öffentlichen Orten, muss mechanisch oder über Gruppenrichtlinien der USB-Anschluss gesperrt werden.

Die Härtung des Betriebssystems steht ebenfalls an. Updates müssen immer installiert sein. So wurde die Autorun Option bei Windows von Microsoft durch ein Update entfernt. Der Nutzer darf keine lokalen Administratorenrechte besitzen. Durch weitere Maßnahmen, wie lokale Virenscanner oder Firewall, können das Risiko weiter minimiert werden.