Datenschutz-Newsletter 02-19

BadUSB – Wenn USB-Sticks angreifen

Aus Dr. Datenschutz

Ein gefundener USB-Stick im Flur oder auf dem Parkplatz kann schnell zur Gefahr für den privaten Computer oder ein ganzes Unternehmen werden. Welche Gefahren verstecken sich hinter den unscheinbaren USB-Geräten und wie kann man sich davor schützen?

Angreifen! Aber wie?

Durch USB-Schnittstellen ist es Angreifern möglich vollen Zugriff auf einen Computer und das gesamte Netzwerk zu gewinnen, wenn dieser nicht grade gesperrt ist. Ein BadUSB sieht wie ein gewöhnlicher USB-Stick aus, verhält sich aber nicht so.

Der USB-Stick „USB RUBBER DUCKY“ enthält statt des Flash-Speicher-Chips einen Prozessor, einen MicroSD Kartenleser und eine dazu passende Speicherkarte. Auf diese Speicherkarte können anschließend Skripte geladen werden, wodurch Angriffe auf dem System gestartet werden können.

Jedoch können auch alltagsübliche USB-Sticks so manipuliert werden, dass diese Schäden verursachen. Dies ist möglich, indem der Firmware-Speicherbereich neu beschrieben und in dem freien Speicherbereich zusätzlicher Code hinzugefügt wird.

Rechner erobern

In der Regel wird zu Beginn eines solchen Angriffs auf Windowssysteme der „Ausführen“- Dialog mittels der Tastenkombination Windows-Taste+R gestartet. Anschließend können die drei Buchstaben „cmd“ und Enter eingetippt werden und die Konsole wird geöffnet.

Nun stehen dem Angreifer die Tore offen. Im Folgenden werden drei mögliche Angriffe und die Folgen dargestellt. Natürlich gibt es noch viele weitere Anwendungsszenarien welche denkbar und realisierbar sind.

- Über einen erstellten Fernzugriff kann der Angreifer völlige Kontrolle aus der Ferne erlangen. Anschließender Datendiebstahl, oder die Veröffentlichung von Betriebsgeheimnissen kann die Folge sein.
- Der Computer oder das gesamte Netzwerk mit einem Virus infiziert, oder durch Ransomware angegriffen werden.
- Alternativ kann ein neues Netzwerk-Interface installiert werden, um den Internet-Datenverkehr umzulenken und mitzuschneiden. Daraufhin können Informationen über Internetnutzer gesammelt werden, um einen Identitätsdiebstahl zu begehen.

Prävention – wie kann ich mich schützen?

Die effektivste Möglichkeit, einen solchen Angriff von einem BadUSB zu verhindern ist es, das Anschließen von USB-Geräten physisch zu verhindern und die USB-Ports zu versiegeln. Jedoch liegt dies meist nicht im Sinne der Geschäftsleitung, da diese Entscheidung endgültig ist. Neben dem Zukleben aller USB-Ports an einem System gibt es noch weitere Möglichkeiten, wie Sie sich vor den Angriffen eines BadUSB schützen können.

„Device Control“

Generell ist dies durch eine Form der „Device Control“ möglich, die den Zugriff auf unbekannte USB-Geräte blockieren kann.

Unter Windows ist ebenfalls eine Einschränkung der USB-Geräte über Gruppenrichtlinien möglich. Hier kann festgelegt werden, ob neue, unbekannte USB-Geräte installiert werden dürfen, oder ob eine Blockade für neue USB-Geräte aktiviert wird.

„Whitelisting“

Eine weitere Möglichkeit zum Schutz ist das sogenannte „Whitelisting“. Dabei werden alle USB-Geräte, welche erlaubt sind wie z. B. die Seriennummer der physischen Tastatur und Maus, und ausgewählte Speichermedien, auf eine Liste der „gutartigen“ USB-Geräte geschrieben. Diese Liste kann jederzeit erweitert und verändert werden. Alle USB-Geräte, welche nicht auf dieser Liste stehen, können nicht verwendet werden.

Zur jeweiligen Einschränkung der benutzbaren USB-Geräte, sei es durch eine „Whitelist“ oder andere Richtlinien, können mehrere Identifikationsmerkmale herangezogen werden. Neben den 21 Geräteklassen, welche USB kennt, gibt es noch weitere Identifier wie:

- die Class ID,
- der Hersteller- oder Produkt ID sowie
- die Seriennummer.

Geräteklassen

Unter Linux kann in den Einstellungen festgelegt werden, welche USB-Ports welche Geräteklassen erlauben. Somit können die festgelegten USB-Ports für Tastatur und Maus dahingehend konfiguriert werden, dass die anderen USB-Ports nur Speichermedien zulassen. Wenn ein USB-Stick manipuliert wurde und sich als Tastatur und als Speichermedium ausgibt, wird unter diesen Einstellungen nur das Speichermedium installiert.

Bei den vorgestellten Möglichkeiten zum Schutz ist jedoch keine 100%ige Sicherheit gegeben. Bei allen USB-Geräten ist es möglich die Informationen, welche es mit sich führt, zu fälschen. Wenn dem Angreifer bekannt ist, welche USB-Geräte zugelassen werden, oder bereits ein zugelassenes besitzt, können diese USB-Geräte so manipuliert werden, dass der Zugriff auf den Computer dennoch gewährt wird.

Weitere Gefahren

Die genannten Risiken gelten nicht nur für USB-Sticks. Jedes USB-Gerät, auch Webcams, Smartphones und externe Festplatten, können so manipuliert werde, dass sie Schadsoftware enthalten. Daher ist bei allen unbekannten USB-Geräten Vorsicht geboten.

Je nach Gerät sollten unterschiedliche Vorsichtsmaßnahmen getroffen werden. Wenn es beispielsweise um das Laden von einem Smartphone geht, können sogenannte „Data Blocker“ oder „USB-Kondome“ verwendet werden. Diese sind Adapter für USB-Geräte, welche nur Strom durchlassen und keine Daten.

Impressum:
Datenschutzbeauftragter nach DSGVO und BDSG (neu)
Peter Brandmann
pb beratung & training
Schnepfenreuther Weg 51
90425 Nürnberg