Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Bundesamt für Cybersicherheit BACS

Cybertipp: Präparierte USB-Sticks als Einfallstor für Cyberangriffe

12.01.2023 - USB-Sticks gehören schon lange zum Computeralltag und werden genutzt, um Daten zu speichern, oder diese von einem Computer auf den anderen zu transferieren. Viele wissen aber nicht, dass präparierte USB-Sticks auch dazu verwendet werden können, um Computer zu hacken.

Ein solcher USB-Stick sieht auf den ersten Blick wie ein normales, unscheinbares USB-Flash-Laufwerk aus. Schliesst man diesen allerdings an einen Computer an, wird dieser vermeintlich als Tastatur erkannt. Dann werden vordefinierte Tastatureingaben abgespult, welche bestimmte bösartige Befehle auf dem Computer auslösen können. Solche so genannten «Rubber Duckies» können mehr als 1000 Wörter pro Minute generieren. Auf dem angegriffenen System lassen sich so beispielsweise Hintertüren installieren, Dokumente oder Passwörter stehlen oder erweiterte Rechte auf dem Computer einrichten.

Rubber Duckies – keine harmlosen Entchen

Beim Wort «Rubber Duckies» oder zu Deutsch «Gummi-Entchen» denkt man zuerst an Kinderspielzeug. Doch in der Hacking-Szene versteht man unter diesem Namen etwas ganz Anderes: Ein solcher Bad-USB-Stick ist ein beliebtes Hacking-Tool.

Der Name «Rubber Ducking» stammt aus der Geschichte der Programmierung. Bei einer Methode, einen Fehler im Programmiercode zu finden, wird einer gelben Plastik-Ente Zeile für Zeile vorgelesen und der Code erklärt. Mit dem Erklären fallen den Programmierern allfällige Fehler auf. Die Gummi-Ente dient als Zuhörerin und hat den Vorteil, dass keine Person damit gestört werden muss. Bei den «Rubber Duckies» werden ebenfalls Befehle Zeile für Zeile abgearbeitet. Um Administrationsaufgaben zu automatisieren wurde dazu ein Tool entwickelt, welches das Tippen von Befehlen auf einer Tastatur nachahmt. Immer wiederkehrende Befehle werden durch das Gerät Zeile für Zeile generiert und ausgeführt. Allerdings war damit auch die Idee einer Keystroke-Injection-Attacke geboren, also dem Einschleusen von Tastaturbefehlen über einen USB-Stick. Dies hat sich bis heute zu einem ausgeklügelten Hacking-Tool entwickelt.

Wie funktioniert die «Keystroke-Injection-Attacke»?

Das USB-Tool gibt sich gegenüber dem Computer als Tastatur aus und verfügt so über die gleichen Nutzerrechte wie das Opfer, welches vor dem Computer sitzt. Auf dem Tool, dem «Rubber Ducky», sind dann die auszuführenden Tastatureingaben, beziehungsweise Befehle, mit der Script-Sprache «Ducky Script» gespeichert. Einmal am Computer angeschlossen, wird der Stick als Tastatur erkannt und die vorprogrammierten Tastatureingaben resp. Befehle am Rechner ausgeführt.

Vorsicht vor geschenkten oder gefundenen USB-Sticks

Wie bringt man nun aber ein Opfer dazu, einen solchen USB-Stick in seinen Computer einzustecken? Dies geschieht mittels Social Engineering. Bei dieser Art von Angriff werden Eigenschaften wie Vertrauen, Angst, Respekt vor Autoritäten oder Neugier von den Angreifern geschickt ausgenutzt. Eine Untervariante des Social Engineerings ist das sogenannte Baiting (zu Deutsch: Ködern). Hier verlassen sich die Angreifer auf die Neugier des Opfers. Die bekannteste Art von Baiting ist, USB-Sticks im Eingangsbereich eines Firmengeländes zu platzieren und darauf zu spekulieren, dass Mitarbeitende den Stick finden und aus Neugier sofort in ein Firmengerät einstecken. USB-Sticks können aber auch über Werbegeschenke verteilt werden. Solche Sticks werden in vielen Varianten an Konferenzen oder Ausstellungen unter die Besucher gebracht. Nicht alle werden aber in guter Absicht verteilt, darunter können sich auch präparierte «Rubber Duckies» befinden». Aber auch ein unbeaufsichtigtes Notebook zum Beispiel im Zug oder an einer Konferenz kann durch einen Angreifer mit dieser Methode kompromittiert werden, wenn dieser es schafft, den Stick unbemerkt über eine kurze Zeit an das Gerät anzuschliessen.

Neue Tool-Version ist noch ausgeklügelter

Im August 2022 veröffentlichte ein Hacking-Hardware-Hersteller eine neue Version seines Tools. Bereits frühere Versionen konnten gefälschte Popup-Fensters erstellen, um die

Anmeldedaten eines Benutzers abzugreifen oder den Browser dazu zu bringen, alle gespeicherten Passwörter an den Webserver eines Angreifers zu senden. In der neuesten Version können gestohlene Daten auch wieder zurück auf das USB-Gerät gespeichert werden. So kann ein Angreifer den Stick für ein paar Sekunden einstecken und diesen dann mit allen gespeicherten Daten wieder abziehen. Dabei wird auch keine Internetverbindung zum Senden der Daten mehr benötigt.

Tipps:

- **Stecken Sie nie unbekannte USB-Devices in den Computer ein.**
- **Lassen Sie den Computer an öffentlichen Orten nie unbeaufsichtigt.**

Letzte Änderung 12.01.2023

https://www.ncsc.admin.ch/content/ncsc/de/home/aktuell/im-fokus/2023/cybertipp-rubberducky.html