MEINUNGEN

DAS PARADOX DES USB-STICKS IM INDUSTRIELLEN BEREICH

Vincent Nicaise
Industrial Partnership and Ecosystem Manager, Stormshield

Der USB-Stick für die Industrie ist eigentlich ein Paradox. Er spielt eine führende Rolle beim Funktionieren der Betriebsumgebung, kann aber bei falscher Handhabung für Zwischenfälle verantwortlich sein. Er stellt auch einen der begehrtesten Angriffsvektoren für Cyberkriminelle dar. Lagebericht zur ambivalenten Rolle des USB-Sticks im industriellen Umfeld. Zwischen operativer Notwendigkeit und Effizienz und beabsichtigter oder zufälliger Gefahr.

Fabriken, Produktionsstätten, Maschinen... auch wenn sie gut abgeschirmt sind, so muss sich die Industrie und ihre operativen Netzwerke dieser Bedrohung durch USB-Sticks stellen. Eine Bedrohung, die man eher mit böswilliger Absicht vermutet, die aber auch zufällig passieren kann. In der Tat befürchten CISOs im industriellen Bereich eher die versehentliche Übertragung von Malware, die Schaden an der Produktionslinie anrichten könnte. Das kann zum Beispiel über den USB-Stick eines Mitarbeiters geschehen, den dieser zuvor in einem persönlichen Umfeld verwendet hat. Es ist schwierig, jemandem die Schuld zu geben, der nur eine *scheinbar* harmlose Datei auf seinen USB-Stick kopiert hat. Und doch...

Bedeutet das, dass **die Industrie von USB-Sticks Abstand nehmen sollte**? Ist das überhaupt für alle Industriezweige durchführbar? Können USB-Sticks durch alternative Lösungen ersetzt werden, die sich besser den Bedürfnissen der operationellen Infrastruktur anpassen? Wie kann die IT-Sicherheit eines Standorts gewährleistet werden, ohne die Produktion zu belasten oder herunterzufahren? Es gibt also viele Fragen und die Probleme, die die Branche betreffen, sind sehr real. Ein Versuch, darauf zu antworten.

DER USB-STICK: EIN UNVERZICHTBARES INSTRUMENT FÜR OT-SYSTEME

Während all der Jahre, in denen die Maschinen und Arbeitsplätze des OT nicht an das Internet angeschlossen waren, stellte der USB-Stick das bevorzugte, wenn nicht sogar das einzige Instrument zum Datenaustausch dar. Darüber hinaus war die Industrie lange Zeit in dem Glauben, dass das Risiko von Cyber-Angriffen eher vom Computernetzwerk (Internet) als von physischen Geräten ausgehen würde. Der USB-Stick hat daher einen historischen Wert in der OT, die sich zudem langsamer entwickelt und verändert als der IT-Bereich. *„OT betrachtet die Gegebenheiten von einem anderen Blickwinkel, da sie sich mit einem Anwendungskontext befasst, der nicht gestoppt oder verlangsamt werden darf. In der Industrie sieht das Paradigma im Vergleich zu anderen Sektoren genau umgekehrt aus: Ein durchgehender und reibungsloser Ablauf ist wichtiger als die Sicherheit. Man geht lieber das Risiko ein, USB-Sticks zu verwenden, als das Risiko, die Produktion zu unterbrechen*“, sagt **Thierry Hernandez**, Global Account Manager bei Stormshield.

„Man geht lieber das Risiko ein, USB-Sticks zu verwenden, als das Risiko, die Produktion zu unterbrechen“

Thierry Hernandez, Global Account Manager Stormshield

Darüber hinaus gibt es eine Funktion, die dem Industriebereich eigen ist: Die mit der Wartung von Industrieanlagen (Maschinen, Sensoren usw.) beauftragten Personen sind externe Dienstleister, die nicht immer die Möglichkeit haben, sich an das Netz anzuschließen. Mobile Datenträger – und hier eben auch USB-Sticks – sind für diese Akteure unverzichtbar, sie diese Medien für alle Arten von Vorgängen wie die Installation von Updates oder Backups verwenden. Andererseits gibt es an einem Industriestandort keine Garantie dafür, dass diese von Drittfirmen durchgeführten Maßnahmen die gleichen Sicherheitsvorkehrungen beachten, die das Unternehmen selbst einhält. Das kann natürlich ein Risiko bilden.

In einigen Industriezweigen kann sich der Verzicht auf USB-Sticks und diese Art der Funktionsweise in der OT als besonders komplex erweisen. Etwa in der Schwerindustrie, wie z. B. Lebensmittelverarbeitung, Eisen und Stahl, Wasser, Chemikalien, sind die Arbeitsplätze und Maschinen nur sehr wenig vernetzt. Um dort direkt an jedem Arbeitsplatz eingreifen zu können, sind USB-Sticks unerlässlich. Aber zum praktischen Aspekt dieses spezifischen Peripheriegeräts kommt also ein potenzieller Vektor zur Infizierung hinzu.

EIN USB-STICK ALS ÜBERTRÄGER FÜR MALWARE

Im Wesentlichen ermöglicht der USB-Stick den Austausch beliebiger Daten und überträgt unbekannte Elemente in ein Netzwerk. Sensible Elemente, insbesondere innerhalb eines Industriestandortes. Darüber hinaus durchläuft der USB-Stick nicht alle Perimeter-Abwehrmaßnahmen einer Struktur, sondern gelangt direkt in den Computer des Benutzers. *„Auf einem USB-Stick kann alles Mögliche sein, und Nachlässigkeit seitens der Benutzer, die nicht daran denken, den Inhalt eines USB-Sticks zu überprüfen, bevor sie ihn in eine Maschine einstecken, kommt sehr häufig vor und ist gefährlich*“, sagt Thierry Hernandez.

„Auf einem USB-Stick kann alles Mögliche sein, und Nachlässigkeit seitens der Benutzer, die nicht daran denken, den Inhalt eines USB-Sticks zu überprüfen, bevor sie ihn in eine Maschine einstecken, kommt sehr häufig vor und ist gefährlich.“

Thierry Hernandez, Global Account Manager Stormshield

Mit dem Aufkommen von Industrie 4.0 sind die Fabriken zunehmend vernetzt und daher immer anfälliger für Malware. Für Angreifer stellen USB-Sticks ein Einfallstor dar, um sich in ein System einzuschleusen und ein Netzwerk ganz oder teilweise zu infizieren. Das Blockieren der Produktionslinie, das Installieren von Malware, sogar Fernspionage oder das Verschlüsseln von Daten... die Cyberrisiken sind vielfältig.

Bei böswilligen Angriffen stellen vor allem kritische Infrastrukturen ein begehrtes Ziel dar. Nach Angaben von SANS gehen 56 % der Sicherheitsvorfälle, von denen sie betroffen sind, auf USB-Sticks zurück. Darüber hinaus zeigen Cyber-Kriminelle immer mehr Einfallsreichtum und Kreativität und finden immer wieder neue Formen von Cyber-Angriffen in der Industrie über USB-Sticks. 2005 hat die AutoRun-Funktion von Microsoft, das Programme automatisch startete, sobald ein USB-Stick in einen Computer eingesteckt wurde, die Kasse der Hacker klingeln lassen. Es genügt diese einfache Verbindung mit dem Computer, um die am Stick enthaltene Schadsoftwares oder schädliche Codes automatisch auszuführen. Anfang 2010 wurde der Angriff über USB-Stick mit RubberDucky für Cyberkriminelle zu einer gängigen Methode, um IT-Systeme zu hacken. Gleiches gilt für den Angriff PHUKD (Programmable HID USB Keystroke Dongle), der die Aktivität einer Tastatur oder Maus nachahmt. Im Jahr 2014 taucht der Exploit BadUSB auf, eine Schwachstelle, der von einigen Forschern als für industrielle Steuerungssysteme kritisch angesehen wird. 2017 ist dann das Jahr von P4wnP1, einem Programm, das Angriffe über die Peripheriegeräte Raspberry Pi Zero et Raspberry Pi W ausführt. Ein paar Jahre später ist BashBunny an der Reihe. In jüngerer Zeit kann mit dem Angriff USB Killer ein Computer in wenigen Sekunden buchstäblich zum Absturz gebracht werden, einfach nur durch das Einstecken des Sticks in den betreffenden Computer.

Diese in der industriellen Umgebung angewandten Infektionsmethoden haben zu zahlreichen Fällen von Cyberangriffen geführt. Im Jahr 2017 war eine kritische Infrastruktur im Nahen Osten das Ziel der Malware Copperfield, die über einen USB-Stick auf einen Arbeitsplatz übertragen wurde, den Dutzende von Mitarbeitern in der betreffenden Struktur gemeinsam nutzen. Copperfield ist ein Remote Access Trojaner (RAT) und zielt speziell auf kritische Industriezweige ab. Sobald der infizierte USB-Stick in einen Computer eingesteckt wird, breitet sich die Malware aus, insbesondere durch Umgehen der Software Windows Script Host, um die Kontrolle über den Computer zu übernehmen. Im selben Jahr warnten mehrere Akteure des maritimen Sektors in ihrem Bericht *The Guidelines on Cyber Security Onboard Ships* vor den Risiken, die mit USB-Sticks für ihren Sektor verbunden sind. Der Bericht beschreibt zahlreiche Cyber-Angriffe, von denen zwei durch die Verwendung von USB-Sticks ermöglicht wurden. Der erste Angriff steht im Zusammenhang mit der Nachlässigkeit oder Unkenntnis der Schiffsbesatzung. So soll ein Mitglied des Sicherheitsteams eines Schiffs der Handelsmarine angeblich unbeabsichtigt einen infizierten Schlüssel in das IT-System des Schiffes eingesteckt haben. Der USB-Stick hätte dann Malware in den Systemen verbreitet. Die Besatzung sei erst einige Tage später aufmerksam worden, da sie anormales Verhalten der besagten Systeme festgestellt haben. Ein weiteres Beispiel stammt aus dem Zentrum des Systems zur Energieversorgung eines Schiffes. IT-Serviceleute, die für die Systeme des Schiffes zuständig waren, entdeckten ruhende Malware. Die Malware war inaktiv, weil das Gerät noch nicht mit dem Internet verbunden war, hätte sich aber in den Systemen verbreitet, sobald sie mit dem Netzwerk verbunden worden wäre. Schließlich entging die Automobilindustrie in jüngster Zeit nur knapp einem Angriff, der große Ausmaße hätte annehmen können. Im August letzten Jahres wurde ein Mitarbeiter der Tesla-Gruppe von einem russischen Cyberkriminellen angesprochen, der ihm die bescheidene Summe von einer Million Dollar anbot, um mit Hilfe eines infizierten USB-Sticks Malware in den Informationssystemen der Gruppe zu verbreiten. Hätte der Mitarbeiter nicht das FBI alarmiert und den Angriff verhindert, wäre Tesla möglicherweise ebenfalls als der Opfer von Angriffen über USB-Stick auf einer langen Liste aufgeschienen.

Die Industrie steht von zwei Seiten unter Druck: einerseits die Notwendigkeit, eine kontinuierliche und reibungslose Geschäftstätigkeit aufrechtzuerhalten, andererseits die Anforderung, Risiken zu berücksichtigen, die durch die Verwendung von USB-Sticks in Unternehmen gegeben sind.

USB-STICK: SICHER MACHEN ODER ERSETZEN

Um sich zu schützen und die Risiken zu begrenzen, setzen einige Unternehmen auf Softwarelösungen zur Kontrolle der USB-Sticks. Ziel ist, den Nutzen dieser Peripheriegeräte zu erhalten und gleichzeitig die Kontrolle über die ausgetauschten Daten zu verstärken. „*So kann eine sogenannte Datenschleuse eingesetzt werden, um die Verwendung des USB-Sticks innerhalb eines Unternehmens zu sichern*“, erklärt **Adrien Brochot**, Produktmanager bei Stormshield. *Dazu gehört das Scannen des Laufwerks, um sicherzustellen, dass keine Malware vorhanden ist, aber auch die Abbildung seines Inhalts, um seinen aktuellen Status zu bestimmen, und die Überprüfung des mobilen Datenträgers, sobald er in einen zu schützenden Computer eingesteckt wird. Wenn dieses Abbild geändert wurde, muss dann geprüft werden, ob diese Änderungen, die auf einem internen, ebenfalls geschützten Computer vorgenommen wurden, autorisiert sind. Wenn nicht, wird der Zugang blockiert.*“ USB-Sticks zu überprüfen bedeutet, einige davon abzulehnen: In vertrauenswürdigen Domänen können nur autorisierte USB-Sticks verwendet werden. Zur Sicherung dieser USB-Sticks können auch Endpoint-Sicherheitslösungen eingesetzt werden. In jedem Fall ist die Gewährleistung der Vertrauenswürdigkeit eines USB-Sticks besonders wichtig für Computer in kritischen Industrien, insbesondere für solche, die Überwachungsvorgänge durchführen.

Einige Unternehmen entscheiden sich stattdessen für Sicherheitsrichtlinien mit sehr eingeschränkten Listen von autorisierten USB-Geräten. Im Jahr 2019 griff die französische Nationale Agentur für Sicherheit der Informationssysteme ANSSI auch das heikle Thema der USB-Sticks auf und stellte ihr Open-Source-Projekt Wookey vor, das die Sicherheit von Arbeitsplätzen stärken und Angriffe wie BadUSB bekämpfen soll. Schließlich haben einige Unternehmen, wie z. B. die IBM-Gruppe oder die amerikanische Armee, die Verwendung von USB-Sticks einfach verboten, um das Risiko von Angriffen zu verringern.

INDUSTRIE 4.0 ALS ALTERNATIVE ZUM USB-STICK?

Darüber hinaus zeichnet sich auch im Bereich OT ein neuer Trend ab, der als mögliche Alternative zum USB-Stick die Verwendung von Servern wie in der IT vorsieht, Umgebungen zur gemeinsamen Nutzung von Dateien oder Workflows vorsieht.

„Es ist unbedingt notwendig, eine Alternative zum USB-Stick zu haben, bevor dessen Ersatz in Erwägung gezogen wird. Die Erhöhung der Kapazität der Netzwerkkonnektivität kann eine gute Option sein.“

Fabrice Tea, Technischer Leiter Digitale Transformation Schneider Electric

Der USB-Stick wird in einigen Unternehmen viel weniger benutzt als früher, und immer mehr Dateien sind über das Netzwerk in Umlauf. Netzwerkkonnektivität und Fernwartung könnten daher eine interessante Alternative zu diesen Peripheriegeräten sein. *„Das Ersetzen des USB-Sticks durch digitale Systeme kann Zeit sparen und sehr bequem sein. Die für die Backups von Industriestandorten zuständigen Personen könnten beispielsweise mit einem digitalisierten System 3 bis 4 Arbeitstage pro Monat einsparen*", sagt **Fabrice Tea,** Technischer Leiter für digitale Transformation bei Schneider Electric, und fügt hinzu: *„Es ist unbedingt notwendig, eine Alternative zum USB-Stick zu haben, bevor dessen Ersatz in Erwägung gezogen wird. Die Erhöhung der Kapazität der Netzwerkkonnektivität kann eine gute Option sein.*"

Aber Vorsicht: Der Ansatz 4.0 ist in der Industrie noch nicht allgemein verbreitet. Viele Unternehmen verfügen derzeit nicht über diesen Ansatz, und die Zusammenschaltung kritischer Computer kann im Hinblick auf die Cybersicherheit für operative Systeme heikel sein. Durch die Verbindung der Arbeitsplätze untereinander und insbesondere mit der Außenwelt vergrößert sich die gesamte Angriffsfläche industrieller Infrastrukturen. Dies gilt insbesondere für kleine Unternehmen, die nicht über die Ressourcen der Großindustrie verfügen. Den Herausgebern von Software kommt daher eine Schlüsselrolle zu, wenn es darum geht, Unternehmen bei ihrer Akkulturation an eine für Cyberangriffe unbedenkliche Industrie 4.0 zu unterstützen.

STORMSHIELD

Stormshield, eine hundertprozentige Tochtergesellschaft von Airbus CyberSecurity, bietet innovative End-to-End-Sicherheitslösungen zum Schutz von Netzwerken (Stormshield Network Security), Desktops (Stormshield Endpoint Security) und Daten (Stormshield Data Security). **www.stormshield.com**