Whitepaper

telent
service • commitment • value

Kleine Ursache, großer Schaden

Wie der Einsatz einer Datenschleuse das Eindringen von Schadsoftware über USB-Stick und andere mobile Datenträger effektiv verhindern kann.

Wenn kleine Dinge große Schäden anrichten

Die größte Cybergefahr für Systeme der Fertigungs- und Prozessautomatisierung – in Fachkreisen Industrial Control Systems (ICS) genannt - droht von Schadsoftware, die über USB-Sticks und andere Wechseldatenträger, eingeschleust wird. Das ist das Resultat der Veröffentlichung ‚Industrial Control System Security – Top 10 Bedrohungen und Gegenmaßnahmen 2019' des Bundesamts für Sicherheit in der Informationstechnik (BSI). Auch jenseits der produktionsnahen IT, insbesondere in Office-Umgebungen, ist ein nicht unerheblicher Teil der Incidents auf einen zu nachlässigen Umgang mit USB-Sticks, Speicherkarten, Mobiltelefonen und anderen Wechseldatenträgern zurückzuführen.

Top 10 Bedrohungen	Trend seit 2016
Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware	↗
Infektion mit Schadsoftware über Internet und Intranet	↗
Menschliches Fehlverhalten und Sabotage	↑
Kompromittierung von Extranet und Cloud-Komponenten	↑
Social Engineering und Phishing	↘
(D)DoS Angriffe	↑
Internet-verbundene Steuerungskomponenten	→
Einbruch über Fernwartungszugänge	→
Technisches Fehlverhalten und höhere Gewalt	↘
Kompromittierung von Smartphones im Produktionsumfeld	→

Die Top-10-Bedrohungen für Industrial Control Systems 2019 (Quelle: BSI)

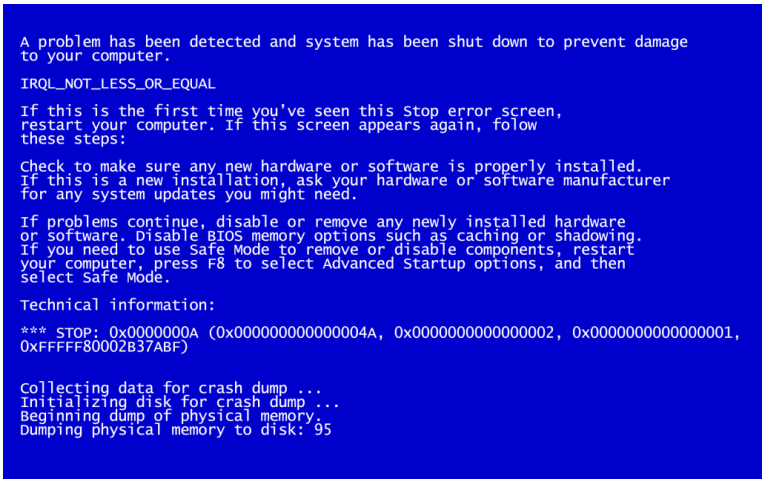
Ohne die Kontrolle von Wechseldatenträgern können Viren, Schadprogramme und Malware ins Firmennetzwerk gelangen und mitunter großen Schaden verursachen. Vor allem in sensiblen Umgebungen, wie in industriellen Anlagen oder Kritischen Infrastrukturen, in Entwicklungsabteilungen oder Forschungseinrichtungen, aber auch in Verwaltungen und Büroumgebungen, kann es zu drastischen Datenverlusten kommen. Egal ob in der Produktion oder im Office, solche Vorfälle stören den Betriebsablauf massiv und die wirtschaftlichen Folgen sind mitunter unberechenbar.

Wenn Schadsoftware über USB-Sticks eingeschleust wird

Das Problem dabei: Meistens ist den Verursachern gar nicht bewusst, welche Gefahr von ihren kleinen Helferlein ausgehen kann. Folgender fiktive, an bekannte Vorfälle aus der Realität angelehnte, Fall verdeutlicht die Problematik und zeichnet ein gutes Bild der Auswirkungen.

8:57 Uhr - Stillstand

Plötzlich gehen die Lichter aus. Alles steht still – jede Maschine, jedes Band. Alle Versuche, die Produktion wieder anzufahren scheitern. Erste Untersuchungen zeigen: Die Anlage ist mit Malware infiziert. Der Schaden - sowohl wirtschaftlich als auch auf das Image bezogen - ist groß.



Auch unbeabsichtigt eingeschleppte Schadsoftware kann kritische Systemfehler verursachen.

Absturz statt Update

Rückblick: Beginn der Nachtschicht, knapp zehn Stunden vor dem Blackout. Noch ist alles in Ordnung. Der externe Dienstleister Peter Müller kommt zur regelmäßigen Wartung der von ihm betreuten Anlage vorbei.
Heute spielt er, wie geplant, ein Update der Steuereinheit ein. Dazu hat er seinen USB-Stick mitgebracht, auf dem er das Update abgelegt hat. Leider nicht nur das Update. Auf dem USB-Stick, den er auch zu privaten Zwecken nutzt, hat sich unbemerkt Schadsoftware eingenistet. Diese gelangt zusammen mit dem Update auf die gewartete Maschine – und pflanzt sich von dort aus im Netzwerk fort. Dabei hat sie leichtes Spiel. Alle Endpunkte innerhalb der Anlage werden, wie in solchen Umgebungen üblich, ohne aktiven Virenschutz betrieben. Resultat: Zehn Stunden später steht die gesamte Anlage still.

Vermeidbarer Schaden

Der geschilderte Vorfall und der durch den Stillstand entstandene Schaden wäre durchaus vermeidbar gewesen, wenn im betroffenen Betrieb Sicherheitsrichtlinien, am besten im Zusammenspiel mit einer technischen Lösung, bezüglich des Umgangs mit Wechseldatenträgern, vorhanden gewesen wären.

Verbot ist keine Lösung

Natürlich könnte eine Sicherheitsrichtlinie vorschreiben, dass die Nutzung von USB-Sticks, SD-Karten und anderen portablen Speichermedien untersagt ist. Allerdings ist das in dieser Form kaum umsetzbar, da der Import und Export von Daten, wie Updates, Programmstände oder Logdateien, nur auf diesem Wege möglich ist. Daher muss eine Lösung her, die den Einsatz der mobilen Datenträger ermöglicht und zugleich sicherstellt, dass keine Schadsoftware über USB-Sticks und Co auf diesem Weg in die Anlage verbracht wird.

Eine Datenschleuse sorgt für mehr Sicherheit

In diesem Fall bietet sich der Einsatz einer Datenschleuse an. Eine Datenschleuse ist ein System, um Wechseldatenträger auf Schadsoftware zu untersuchen, bevor diese mit einer sicheren Netzwerkumgebung in Berührung kommen.
Wie beispielsweise unsere Datenschleuse InDEx Ihnen die Datenkontrolle erleichtert und Ihre Security erhöht, erläutern wir im Folgenden. Einsatzmöglichkeiten und Vorteile einer Datenschleuse haben wir in einem kurzen Video zusammengefasst.

Einsatzmöglichkeiten der Datenschleuse InDEx: https://youtu.be/A5vlobn0zC4

So funktioniert die Datenschleuse

Eine Datenschleuse bietet die Möglichkeit, den wechselseitigen Datenstrom in und aus der eigenen Infrastruktur zu überwachen. Die Lösung, wie etwa die Datenschleuse „InDEx“ (Intelligent Data Exchange), besteht aus einem dedizierten Rechner mit einem robusten Gehäuse mit Schnittstellen und hochprofessioneller Software zum Scannen von Wechseldatenträgern.

Die Datenschleuse InDEx gibt es in zwei Varianten: Als Office- und als Shopfloor-Version (unten)

Das System bezieht automatisch Updates und Virensignaturen über eine verschlüsselte Verbindung. Die Schleuse zeichnet sich durch eine einfache Bedienungsoberfläche mit Touchscreen aus und dient quasi als digitaler Pförtner für Wechselmedien in Unternehmen.

Die Lösung kann beispielsweise im Eingangsbereich von Unternehmen platziert werden. Die Daten auf Wechseldatenträgern, wie beispielsweise USB-Sticks, werden dann überprüft und gereinigt – und zwar bevor sie mit internen Systemen in Verbindung kommen. Besonders Unternehmen mit sensiblen Infrastrukturen stehen vor der Herausforderung, einen immer aktuellen Virenschutz bereitzustellen.

Dies ist mit „InDEx“ möglich, weil die Datenschleuse autark arbeitet und zeitnah mit den neuesten Updates versorgt wird. Die Kiosk-Lösung bietet mit seinem Rundum-Service aus Maintenance, Monitoring, Fernwartung, Patchmanagement, Signaturen-Updates und Vor-Ort-Austausch-Service einen wichtigen Baustein in einer ganzheitlichen Cybersecuritystrategie.

Technik und Prozess führen zum Erfolg

Wichtig ist, dass es einen sauberen Prozess, eine klare Richtlinie zum Einsatz der Lösung gibt. Beispielsweise könnte dieser folgendermaßen aussehen:

Grundsätzlich ist das Einbringen von Wechseldatenträgern verboten. Ist dies nicht vermeidbar, müssen diese zuvor an der vorhandenen Datenschleuse gescannt werden und ihre Verwendung, abhängig vom Ergebnis, von einer befugten Person erlaubt oder untersagt werden. Zusätzlich sollten Prozesse für die erwartbaren Scanergebnisse vorab definiert werden. Etwa:

1. Das Medium wird von der Datenschleuse ZUGELASSEN: Der Scanner hat alle auf dem USB-Stick vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht und hat keine Schadsoftware gefunden. Man kann davon ausgehen, dass auf dem Medium keine bekannten Schädlinge vorhanden sind.

2. Das Medium wird von der Datenschleuse zurückgewiesen, ein RISIKO wird gemeldet: Der Scanner hat alle auf dem Medium vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht. Schadsoftware wurde zwar nicht gefunden, allerdings konnte mindestens eine Datei nicht oder nicht vollständig gescannt werden (z. B. nicht normgerecht gepackte oder verschlüsselte .zip Dateien, die der Scanner nicht entpacken kann). In diesem Fall muss ein festgelegter Prozess starten, der vorschreibt, was zu tun ist. Dieser Prozess kann nur vom Betreiber der Datenschleuse an Hand seiner Security Policy festgelegt werden. Möglichkeiten sind:

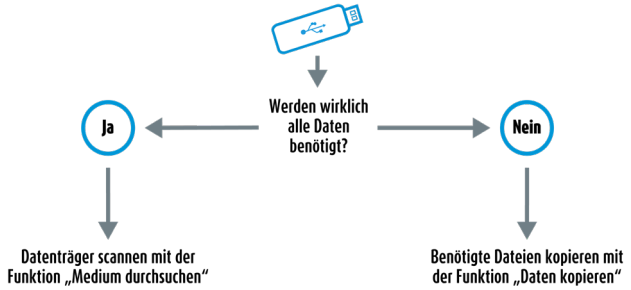
- Das Medium darf grundsätzlich nicht verwendet werden.
- Das Medium darf verwendet werden, wenn ein Entscheidungsträger dies genehmigt. Dieser Genehmigungsprozess sollte dokumentiert werden.
- Wurden nicht benötigte Dateien beanstandet, die aktuell benötigten Dateien jedoch als „sauber“ klassifiziert, können die „sauberen“ Dateien mit Hilfe der Datenschleuse auf ein sicheres Medium kopiert werden, das nach nochmaligem Scan dann zugelassen wird.

3. Das Medium wird von der Datenschleuse zurückgewiesen, ein VIRUS wird gemeldet: Der Scanner hat alle auf dem USB-Stick oder der SD-Card vorhandenen Dateien (incl. der in Archiven vorhandenen) auf Schadsoftware untersucht und hat Schadsoftware gefunden. Auch hier sollte ein festgelegter Prozess starten der vorschreibt, was zu tun ist. Dieser Prozess kann nur vom Betreiber der Datenschleuse an Hand seiner Security Policy festgelegt werden. Möglichkeiten wären:

- Das Medium darf grundsätzlich nicht verwendet werden.
- Die infizierten Dateien werden mit Hilfe der Datenschleuse gelöscht, danach muss das Scanergebnis nochmals bewertet werden.
- Wurden nicht benötigte Dateien als infiziert gemeldet, die aktuell benötigten Dateien jedoch als „sauber“ klassifiziert, können die „sauberen“ Dateien mit Hilfe der Datenschleuse auf ein leeres sauberes Medium kopiert werden, das dann zugelassen wird.

Auch einfache Regeln helfen

Die volle Wirksamkeit entfaltet eine solche Kombination aus technischer Lösung und passenden Prozessen dann, wenn dabei auch einfache, auf den ersten Blick ersichtliche Maßnahmen berücksichtigt werden. So sinkt beispielsweise das Risiko eines Vorfalls, wenn die Datenmenge auf dem Wechselmedium gering gehalten wird. Im Idealfall befinden sich auf dem Medium nur die aktuell benötigten Daten.



telent
service · commitment · value

telent GmbH
Gerberstraße 34 | 71522 Backnang
Tel.: +49 7191 900-0
E-Mail: info.germany@telent.de

KORAMIS
Cybersecurity by telent

www.telent.de