

ICS vor Malware schützen – ohne Security Software zu installieren

OT Security



MANCHE SECURITY-ANFORDERUNGEN KÖNNEN SIE GAR NICHT ERFÜLLEN

Sie stecken in einem Dilemma: Einerseits müssen Sie Security-Standards einhalten und sollten dafür Endpoint Security-Lösungen auf Ihren Produktionsmaschinen installieren. Andererseits dürfen Sie das auf vielen Systemen gar nicht, weil sonst die Herstellergarantie erlischt. Häufig lassen sich noch nicht einmal Patches einspielen. Die Krux: ICS, die über keine Security-Software verfügen und einen alten, ungepatchten Betriebssystem-Stand haben, sind besonders verwundbar durch Cyberangriffe. Selbst wenn diese Maschinen in einem abgeschotteten Netzwerk betrieben werden, sind sie nicht sicher.



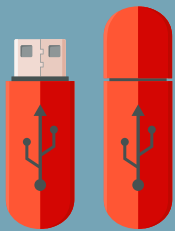
Denn komplett von der digitalen Außenwelt isoliert sind sie nie. Zumindest der Wartungstechniker kommt regelmäßig vorbei und schließt seine Geräte an die Systeme an. Sind diese mit Malware infiziert, gelangen Viren, Trojaner & Co ungehindert auf die Produktionsmaschinen. Welchen Schaden das verursachen kann, wollen Sie sich lieber nicht vorstellen. Beispiele für Angriffe mit WannaCry oder NotPetya kennt man ja zur Genüge. Doch mittlerweile gibt es sogar Kryptotrojaner, die speziell auf Produktionsmaschinen abzielen, etwa LockerGoga, Snake/Ekans oder DoppelPaymer.

SECURITY-SOFTWARE IST KEINE OPTION

Wie aber lassen sich solche OT-Systeme vor Cyberangriffen schützen? Das bereitet vielen Experten Kopfzerbrechen, denn:

- Die Herstellergarantie geht über die Security. Daher können Sie keine Security-Software installieren.
- Selbst wenn manche Systeme über einen Virenschanner verfügen, kann dieser womöglich keine aktuellen Patterns herunterladen, da er keinen Internetzugang hat.
- Sie können nicht prüfen, ob die Geräte, die der Wartungstechniker mitbringt, mit Malware infiziert sind.
- Aus Compliance-Gründen können Sie auch keine Security-Software auf den Geräten des Wartungstechnikers installieren.

WAS JETZT?



Sie brauchen eine Lösung, mit der Sie Systeme vor Malware schützen können, ohne dass Sie dafür Software installieren müssen. Die Lösung sollte sich in einen Security-Prozess einbinden lassen und es ermöglichen, sowohl ICS regelmäßig auf Malware zu scannen als auch Geräte des Wartungstechnikers zu prüfen, bevor er sie anschließt. Das gelingt mit einem kleinen, spezialisierten Tool in Form eines USB-Sticks, das die Funktion eines Virenschanners übernimmt. Zunächst konfigurieren Sie die Security Policy über Ihr Arbeitsnotebook und laden die aktuellen Viren-Patterns herunter. Anschließend ist der Stick einsatzbereit. Er wird einfach an den USB-Anschluss der Maschinen oder an das Notebook des Wartungstechnikers angesteckt, scannt die Geräte automatisiert auf Malware und kann gefundene Schädlinge eliminieren. Außerdem sammelt er Systeminformationen Ihrer Produktionsmaschinen, sodass Sie über den aktuellen Stand - und mögliche Schatten-IT - informiert werden. LED-Signale signalisieren den Status des Scans. Anschließend stecken Sie das Tool wieder an Ihr Arbeitsnotebook an, um die Informationen zentral auszuwerten und zu speichern.

TIPP

Haben Sie Produktionsmaschinen, auf denen Sie zwar Software installieren können - aber der Platz reicht nicht für einen kompletten Virenschanner? Dann versuchen Sie es doch einmal mit einer Application Lockdown-Lösung. Sie braucht nur minimale Ressourcen und arbeitet mit einer Whitelist. So kann nur autorisierte Software auf dem System ausgeführt werden.

IHRE VORTEILE



- Sie stellen sicher, dass OT-Systeme nicht mit Malware infiziert sind - ohne, dass Sie dafür Software auf den Maschinen installieren müssen.
- Mit einem einzigen Stick können Sie die verschiedensten Betriebssysteme scannen.
- Der Malware-Scan lässt sich ganz einfach in einen Security-Prozess einbinden.
- Maschinen werden ohne direkten Internetzugang stets mit aktuellen Patterns gescannt.
- Indem auch der Wartungstechniker den Stick nutzt, um sein Notebook zu scannen bevor es an kritische Systeme angeschlossen wird, können Sie verhindern, dass Malware eingeschleppt wird.
- Sie gewinnen Informationen zum aktuellen Systemstatus. Das erleichtert das Auditieren.
- Sie decken Schatten-IT auf.

DER PARTNER AN IHRER SEITE



Mit Trend Micro TXOne erhalten Sie eine einfach anzuwendende Lösung, um Systeme in abgeschotteten Netzwerken abzusichern. TXOne ist ein Joint Venture von Trend Micro und Moxa und verbindet führende IT-Security und OT-Security mit industrietauglicher Hardware.

Trend Micro (börsennotiert in Tokyo) hat über 30 Jahre Erfahrung als Spezialist für Sicherheitslösungen. Das Unternehmen wird seit 15 Jahren erfolgreich von seiner Mitgründerin Eva Chen geleitet, die als Leading Woman in IT international anerkannt ist. Seit der Gründung im Jahr 1988 achtet sie mit ihrem Managementteam darauf, dass das Unternehmen gesund wächst und reinvestiert auch in Krisenzeiten umfangreich in Forschung und Entwicklung.

Ihr Credo: „Unsere einzige Konkurrenz sind Cyberkriminelle, denen man Einhalt gebieten muss.“



Copyright © 2023 Trend Micro Incorporated. Alle Rechte vorbehalten. Trend Micro, das Trend Micro Logo und das T-Ball-Logo sind Marken oder eingetragene Marken von Trend Micro Incorporated. Alle anderen Firmen- bzw. Produktnamen sind Unternehmenskennzeichen oder eingetragene Marken ihrer jeweiligen Eigentümer. Die in diesem Dokument enthaltenen Informationen können sich ohne vorherige Ankündigung ändern. Trend Micro, das Trend Micro Logo und das T-Ball-Logo tragen das Registered-Trade-Mark-Symbol der USA. Einzelheiten darüber, welche personenbezogenen Daten wir erfassen und warum, finden Sie in unserer Datenschutzerklärung auf unserer Website unter: https://www.trendmicro.com/de_de/about/legal/privacy.html.