

| Produktion



Die Fertigung richtig absichern

OT Security



PRODUKTIONSUMGEBUNGEN ALS ZIEL VON CYBERKRIMINELLEN

Die Produktionsumgebung vor Cyberangriffen zu schützen war noch nie einfach. Schon seit Langem setzen Sie sich mit Security-Standards auseinander. Doch durch die Konvergenz von IT und OT kommen neue Herausforderungen hinzu. Neben den klassischen Szenarien wie einem Malware-verseuchten USB-Stick, der unbedacht angesteckt wird, müssen Sie sich jetzt auch mit direkten Angriffen aus dem Internet auseinandersetzen. Ein häufiges Einfallstor ist zum Beispiel die Fernwartung. Vor ein paar Jahren passierten Cyber-Attacken auf OT-Systeme noch eher zufällig, weil herkömmliche Ransomware wie WannaCry Kollateralschaden verursachte.



Mittlerweile haben Cyberkriminelle die Produktion jedoch als dezidiertes Ziel entdeckt und spezielle Malware dafür entwickelt, zum Beispiel LockerGoga, Snake/Ekans oder DoppelPaymer. Mit einer IoT-Suchmaschine wie Shodan ist es ein Kinderspiel, vernetzte Geräte aufzuspüren und sogar Details zum Betriebssystem zu ermitteln. So können Cyberkriminelle ganz einfach Ziele mit bekannten Schwachstellen anvisieren.

KOMPLEXER SCHUTZ

Natürlich dürfen Sie auf keinen Fall riskieren, dass die Fertigung wegen eines Cybervorfalls stillsteht oder Maschinen außer Kontrolle geraten. Doch die OT-Umgebung richtig abzusichern, bringt viele Herausforderungen mit sich:

- Sie wissen gar nicht genau, welche IT in den verschiedenen Produktionsmaschinen verbaut ist, welche Betriebssysteme laufen und in welchem Zustand sich diese befinden.
- Auch welche Geräte mit wem kommunizieren, ist oft nicht klar. Viele Hersteller bauen heute zum Beispiel einen Internetzugang in Maschinen ein, um Services wie Predictive Maintenance oder nutzungsbasierte Abrechnungsmodelle zu ermöglichen.
- Viele OT-Systeme lassen sich nicht patchen, weil es keine Freigabe der Hersteller für die Patches gibt. Manche Systeme sind auch zu alt oder ein Patch könnte den Betrieb beeinträchtigen. Dadurch bleiben Schwachstellen offen.
- Ältere Produktionsmaschinen haben keine integrierte Security. Neue leider meist auch nicht. Gängige Maßnahmen wie starke Authentifizierung und Verschlüsselung sind nicht implementiert und lassen sich auch nicht nachträglich einbauen.
- Auf vielen Maschinen können Sie keine Security-Software installieren, weil das technisch nicht möglich ist oder sonst die Hersteller-Garantie erlischt.
- Security-Systeme dürfen die Produktion nicht stören, müssen spezielle OT-Protokolle verstehen und mit den Umweltbedingungen auf dem Shopfloor zurechtkommen. Mehr zu den Besonderheiten von OT-Security erfahren sie in unserem aktuellen [Whitepaper](#).

SECURITY SPEZIELL DESIGNT FÜR OT



Sie brauchen eine Security-Lösung, die speziell für OT-Umgebungen designt wurde, aber gleichzeitig führende Technologien aus der IT-Security mitbringt. Sie sollte sowohl auf Netzwerkebene als auch am Endpoint für Sicherheit sorgen und drei grundlegende Funktionen erfüllen: Präventiv vor Cyberangriffen schützen, verdächtige Vorfälle schnell erkennen und durchgehend den Betrieb aufrechterhalten. Dafür empfehlen sich spezielle IPS-Systeme und Firewalls, die sämtliche im Netzwerk angeschlossenen Geräte und

Kommunikationswege transparent machen und kontrollieren. Sie ermöglichen es, das Netzwerk in Segmente zu unterteilen, um die Bewegungsfreiheit von Angreifern einzuschränken, und die Kommunikation zwischen Produktionskomponenten zu filtern. Mit virtuellem Patching lassen sich auch Systeme schützen, auf denen Sie keine realen Patches installieren können. Die Sicherheitslösung verhindert die Ausnutzung der Schwachstelle auf Netzwerkebene. Lernen Sie Anwendungsbeispiele in unserem [Best-Practice-Whitepaper](#) kennen.

ENDPUNKT-SCHUTZ FÜR LEGACY-SYSTEME

ICS, HMI/SCADA, POS, ATM und andere Embedded Systeme, die feste Funktionen haben, können Sie mit einer Application-Lockdown-Lösung vor einer Malware-Infektion und Manipulation schützen. Sie erlaubt nur autorisierte Aktionen, die auf einer Whitelist definiert sind. Ein spezieller Security-USB-Stick ermöglicht es zudem, Systeme zu scannen und Malware zu entfernen, ohne dass Sie Security-Software installieren müssen.



IHRE VORTEILE



- Sie schützen missionskritische ICS, ohne ihre Performance zu beeinträchtigen.
- Sie gewinnen Transparenz und Kontrolle im gesamten Netzwerk und decken Schatten-IT auf.
- Schwachstellen werden geschlossen, ohne dass Sie dafür die Produktionssysteme anfassen müssen.
- Sie erkennen Cyberattacken frühzeitig und können schnell Maßnahmen ergreifen.
- Sie minimieren Risiken, indem Sie Netzwerksegmente bilden.
- Das Security-Management wird einfacher, da Sie alle Funktionen von einer zentralen Konsole aus steuern.

DER PARTNER AN IHRER SEITE



Mit TXOne EdgeIPS und TXOne EdgeFire erhalten Sie einfach zu implementierende ICS Cybersecurity für die Shopfloor-Absicherung. 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.“



©2021 by Trend Micro Incorporated. All rights reserved. Trend Micro, and the Trend Micro t-ball logo, OfficeScan and Trend Micro Control Manager are trademarks or registered trademarks of Trend Micro Incorporated. All other company and/or product names may be trademarks or registered trademarks of their owners. Information contained in this document is subject to change without notice. For details about what personal information we collect and why, please see our Privacy Notice on our website at: <https://www.trendmicro.com/privacy>