Alte Technik, neue Risiken:
Fast jedes zweite Produktionssystem ist über fünf Jahre alt

Befragung von Sophos unter Industrieunternehmen zeigt: Viele OT-Systeme sind in die Jahre gekommen. Die Mehrheit der Unternehmen hält sie durch Updates, Backups und externe Prüfungen einsatzfähig.

Gebaut für die Ewigkeit, anfällig für Cyberangriffe
Die Steuerungssysteme in deutschen Produktionshallen sind echte Langstreckenläufer. Bei knapp der Hälfte aller 211 befragten Unternehmen (48,8 Prozent) sind die kritischen Systeme bereits fünf bis zehn Jahre im Einsatz. In Betrieben mit 250 bis 999 Mitarbeitenden ist es sogar etwas mehr als die Hälfte. Noch älter – über zehn Jahre – sind die Systeme bei 11,4 Prozent der Befragten. Ihre mechanische Zuverlässigkeit ist ein Qualitätsmerkmal, aus Sicht der Cybersicherheit jedoch ein wachsendes Problem.

„Produktionssysteme sind robust gebaut und laufen oft jahrzehntelang zuverlässig. Doch gerade diese Langlebigkeit bringt in Zeiten wachsender Cybergefahren auch Risiken mit sich“, erklärt Michael Veit, Security-Experte bei Sophos. „Was damals als isolierte Anlage konzipiert wurde, ist heute oft vernetzt und damit angreifbar.“

Gewissenhaft gepflegt und trotzdem ausfallgefährdet
Die meisten Betriebe kümmern sich aktiv um die Pflege ihrer Systeme. 82,5 Prozent führen regelmäßige Updates durch, um Schwachstellen zu schließen und die Anlagen am Laufen zu halten. Nur ein verschwindend kleiner Anteil von 0,5 Prozent verzichtet komplett darauf.

Diese wichtige Routine bleibt jedoch nicht ohne Nebenwirkungen: Bei mehr als drei Viertel der Befragten führten Software- oder Sicherheitsupdates in den letzten drei Jahren zu ungeplanten Produktionsausfällen. Jedes vierte Unternehmen (24,6 Prozent) erlebte sogar mehrfache Stillstände, weitere 52,6 Prozent bestätigten zumindest vereinzelte Unterbrechungen. Der Grund: In der Fertigung greifen viele Systeme millimetergenau ineinander. Schon kleine Softwareänderungen können dazu führen, dass Schnittstellen nicht mehr reibungslos funktionieren, Abläufe ins Stocken geraten oder Maschinen kurzzeitig stillstehen.
Damit zeigt sich ein zentrales Dilemma: Maßnahmen zur Erhöhung der Sicherheit können die Verfügbarkeit gefährden.

White Hacker, Backups, Schulungen: die Top-Strategien
Um sich gegen Cyberangriffe und technische Ausfälle zu wappnen, setzen die Unternehmen auf verschiedene Strategien. Am häufigsten greifen sie zu professionellen Schwachstellenanalysen und Penetrationstests durch externe Sicherheitsexperten – 54 Prozent nutzen diese Dienste regelmäßig.
An zweiter Stelle stehen spezielle Backup-Strategien für Produktionssysteme (51,2 Prozent). Anders als bei Büro-IT geht es hier nicht nur um Daten, sondern auch um System-konfigurationen und Maschinenparameter.
Auf Platz drei folgen gezielte Mitarbeiterschulungen (46,4 Prozent); ein wichtiger Baustein, da viele Vorfälle durch menschliche Fehler entstehen, sei es ein unsicherer USB-Stick oder ein unbedacht geöffneter E-Mail-Anhang.

Interne und externe technische Lösungen
Zusätzlich setzen 38,9 Prozent der Betriebe auf Sicherheitszentren (SOC/SIEM), die Systemaktivitäten kontinuierlich überwachen und bei Unregelmäßigkeiten Alarm schlagen.

37 Prozent haben ihre Netzwerke segmentiert, sodass kritische Produktionsbereiche vom restlichen Unternehmensnetz getrennt sind. Auf diese Weise lässt sich verhindern, dass Angreifer aus dem Firmennetzwerk in die Fertigung gelangen.
Externe Unterstützung spielt ebenfalls eine wichtige Rolle: 37,9 Prozent der Unternehmen lassen sich beim Schutz ihrer Systeme von spezialisierten Dienstleistern unterstützen. Knapp ein Drittel probt zudem regelmäßig den Ernstfall mit Notfallübungen.

Die Lieferkette im Blick
Eine früher oft übersehene Schwachstelle haben viele Unternehmen inzwischen erkannt: ihre Partner in der Lieferkette. Mehr als die Hälfte der Befragten (57,3 Prozent) hat mittlerweile vertragliche Anforderungen zur Cybersicherheit an Zulieferer formuliert, ein Drittel zumindest teilweise. 8,5 Prozent planen entsprechende Vereinbarungen.

Dem Prinzip „Verträge sind gut, Kontrollen sind besser" folgen knapp zwei Drittel (64,9 Prozent) der Unternehmen. Sie prüfen die IT-Sicherheit ihrer Lieferanten regelmäßig, weitere 19,4 Prozent zumindest gelegentlich. Allerdings verzichten 12,3 Prozent vollständig auf solche Prüfungen – und öffnen damit potenziell Angreifern die Tür.

Modernisierung bleibt unvermeidlich
„Langfristig führt kein Weg an der Modernisierung der Produktionslandschaft vorbei", betont Michael Veit. „Entscheidend ist, dass Unternehmen den technischen Ist-Zustand kennen und Sicherheitsroutinen konsequent umsetzen. Wer hier vorausschauend plant und schrittweise modernisiert, kann seine Fertigung langfristig gegen moderne Bedrohungen absichern, ohne dabei die Stabilität zu opfern, die deutsche Produktionsqualität ausmacht."

Sophos empfiehlt fünf Maßnahmen für mehr Cybersicherheit in der Produktion:

1. **Regelmäßige Updates:** Sie schließen Sicherheitslücken und sind ein unverzichtbarer Baustein, auch wenn sie manchmal störanfällig sind.
2. **Backup-Strategie etablieren:** Produktionsdaten und Maschinenparameter regelmäßig sichern – am besten getrennt vom Produktionsnetzwerk.
3. **Mitarbeitende schulen:** Viele Angriffe beginnen beim Menschen. Schulungen sensibilisieren für die wichtigsten Gefahrenquellen.
4. **Prüfung der Lieferkette:** Zulieferer sind Teil des eigenen Sicherheitsnetzes. Verträge und regelmäßige Kontrollen schaffen Verlässlichkeit.
5. **Verzahnung von IT und Produktion:** Sicherheit gelingt nur gemeinsam. Regelmäßige Abstimmungen helfen, Risiken frühzeitig zu erkennen.

Über die Umfrage
Die Befragung wurde im Juli und August 2025 von techconsult im Auftrag von Sophos durchgeführt. Befragt wurden 211 Produktionsbetriebe in Deutschland.

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Pressekontakt:

Sophos
Jörg Schindler, Senior PR-Manager EMEA Central
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de