INDUSTRIELLE SICHERHEIT – ZU ENDE GEDACHT

Endpoint-Security-Lösungen für eine geschützte und störungsfreie Produktion

Endpoint Security gehört für Unternehmen zum Pflichtprogramm – und zwar längst nicht mehr nur in der klassischen, sondern auch in der Produktions-IT. Denn: Die zunehmende Vernetzung der Operational Technology (OT) mit der IT und die Entwicklung hin zur Smart Factory potenzieren nicht nur die Mehrwerte für Unternehmen, sondern auch die Angriffsflächen für Cyberkriminelle.

2017 sorgten die schwerwiegenden Folgen eines Cyberangriffs durch das Schadprogramm WannaCry weltweit für große Aufmerksamkeit – und rüttelten viele Unternehmen auf. Denn bis zu diesem Zeitpunkt wurden Endpoint-Schutzmaßnahmen in Produktions- und Werkhallen häufig vernachlässigt. Dabei ist eine Endpoint-Security-Strategie von zentraler Bedeutung, um die Verfügbarkeit der Produktion zu gewährleisten. Zudem sollte der gesamte Lebenszyklus eines Endpoints betrachtet werden – denn im Gegensatz zur Office-Umgebung sind Betriebszeiten von bis zu 20 Jahren keine Seltenheit.

Die Herausforderungen sind in der Produktion daher meist größer als in der klassischen IT, nicht zuletzt aufgrund der Komplexität der Prozesse und der Heterogenität der Systemlandschaft. Die Endpoint Services von Computacenter berücksichtigen sowohl die Abhängigkeiten von Faktoren wie Systemkritikalität und aktuellem Lebenszyklus auch die Vorgaben von Systemintegratoren.

MALWARE IN DER PRODUKTION? NICHT MIT GANZHEITLICHEN ENDPOINT-SCHUTZMASSNAHMEN

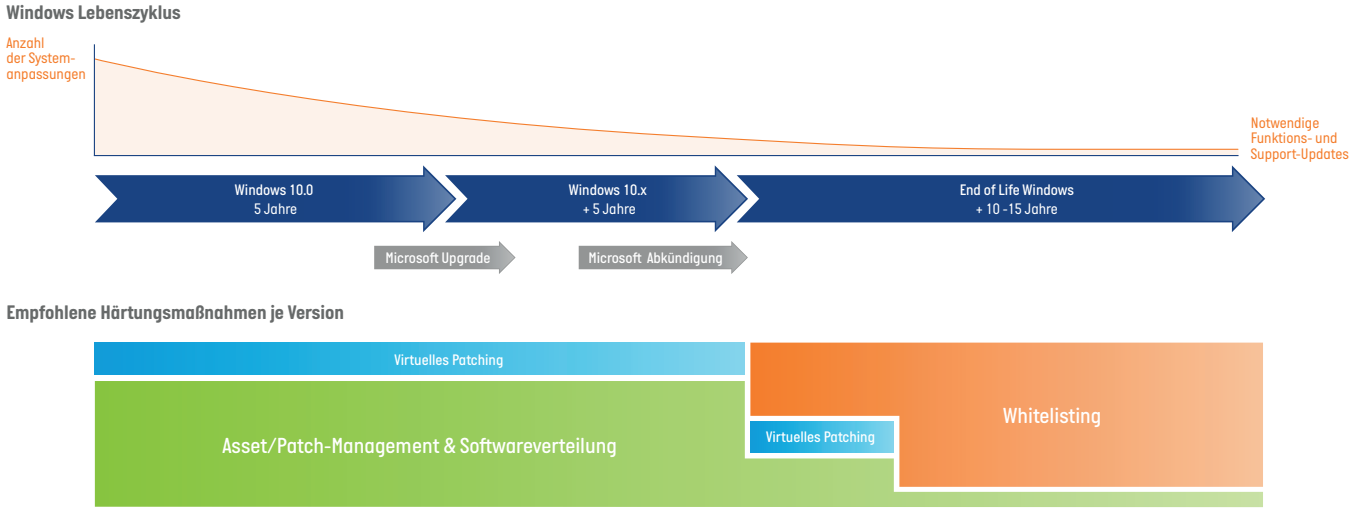
Unverzichtbare Basis für die Endgerätesicherheit bilden etablierte Sicherheitsmaßnahmen – wie zum Beispiel das **Patchen von Betriebssystemen**. Moderne Patch-Plattformen speziell für Produktionsumgebungen ermöglichen eine intelligente Verteilung von Patches mit dedizierten Freigabeprozessen und automatisierten Aufgaben, die für den Rollout von Betriebssystem-Updates eingesetzt werden können. Die von der Plattform ausgerollten Systemagenten überführen den Client zusätzlich in einem gemanagten Status. Zentral gesteuert, können damit weitere Funktionalitäten wie Softwareverteilung oder Backup- und Recovery-Prozesse durchgeführt werden.

Ein weiterer Schutz gegen Schadsoftware bieten die speziell für den OT-Bereich entwickelten **Next-Generation-Antivirus-Applikationen**. Sie bieten nicht nur optimierte Sicherheits-Engines und -Module für Produktionsressourcen, sondern sind auch eigens für die Detektion von ICS-relevanter Schadsoftware ausgelegt.

Da das Zeitfenster zwischen dem Bekanntwerden von Schwachstellen und der Möglichkeit, diese zu schließen, beim Endpoint-Schutz besonders kritisch ist, empfiehlt sich zudem der Einsatz **virtueller Patching-Maßnahmen**. Dieses Vorgehen ist bereits von der Produktionsfirewall bekannt, kann jedoch auch für die Absicherung von einzelnen Systemen – via Mikrosegmentierung – durch Edge-IPS-Lösungen eingesetzt werden. Ergänzt wird die Funktion von Endpoint Detection and Response (EDR)-Lösungen, die die Maßnahmen direkt auf dem Client ausführen.

Nicht immer können jedoch alle geforderten Sicherheitskomponenten auf einem System installiert werden. Hier setzt Computacenter auf eine moderne, portable **AV-Scanner-Lösung**. Diese kann sowohl bei „Non-Touchable"-Systemen als auch bei Systemen ohne Netzwerkanbindung eingesetzt werden. Der Vorteil: Nicht nur Scan-, sondern auch Asset-spezifische Informationen lassen sich zentral in einer Management-Plattform zusammenführen. Dies sorgt für maximale Transparenz über den Sicherheitsstatus all Ihrer Systeme hinweg.

HÄRTUNGSMASSNAHMEN IM LEBENSZYKLUS
Beispiel Windows OS



HÄRTUNG DER PRODUKTIONS-IT: DAS WHITELISTING-PRINZIP

Gerade im Produktionsumfeld sind nach wie vor viele End-of-Life-Systeme im Dauerbetrieb. Eine Härtung ist daher unverzichtbar. Am Markt hat sich dabei das Whitelisting-Prinzip etabliert. Diese Härtungs-Maßnahme bietet nicht nur einen soliden Basisschutz, sondern ist auch für einen flächendeckenden Rollout geeignet. Möglich macht das die automatische Konfiguration, die nach einer Anlernphase und einem automatisierten System-Scan das Security-Regelwerk eigenständig erstellt und im Anschluss aktiviert. Je nach Anbieter können zusätzlich weitere Schutzfunktionen für Endpoints wie beispielsweise Daten- und USB-Schutz konfiguriert werden.

UMFASSENDER USB-SCHUTZ

Gerade Datenübertragungen von Fremdsystemen über Wechseldatenträger gelten als klassisches Einfallstor für Cyberkriminelle. Um Wechseldatenträger – wie beispielsweise USB-Sticks – abzusichern, werden AV-Schutzprozesse etabliert, die Daten auf Schadsoftware untersuchen. Im Vergleich zur klassischen USB-Schleuse hat Computacenter in Zusammenarbeit mit einem Hersteller einen **portablen Security-Stick** entwickelt, der den AV-Scanprozess direkt beim Kopiervorgang mittels integrierter Scan-Engine des Sticks absichert. Mit diesem Verfahren entfällt nicht nur der Weg zu zentral installierten USB-Schleusen, man spart auch kostbare Zeit beim Update.

SICHERHEIT AUF GANZER LINIE

Dank der Verknüpfung spezifischen Wissens rund um die Produktions-IT in Kombination mit einem tiefen Security-Verständnis über alle Infrastrukturebenen hinweg kann Computacenter Lösungen zum Schutz Ihrer Endpoints entwickeln, die zu den Herausforderungen Ihres Unternehmens passen und die auf etablierten Standards in der OT basieren. Dabei berücksichtigen wir nicht nur die Sicherheitsfunktionen und betrieblichen Aspekte, sondern auch die betriebswirtschaftlichen Aufwendungen. Mit der Konzeption, Implementierung und dem Rollout von Sicherheitsmaßnahmen unterstützen wir Sie im gesamten Prozess. Darüber hinaus sind wir in der Lage, das Security-Niveau kontinuierlich an die aktuelle Gefahrenlage anzupassen und das Risiko eines Ausfalls Ihrer Produktionssysteme zu minimieren.

Haben Sie Interesse, mehr zu erfahren?
Sprechen Sie Ihren Account Manager an oder kontaktieren Sie uns über unsere Webseite:
www.computacenter.com/de/it-agenda/digital-factory

Computacenter

Computacenter AG & Co. oHG
Computacenter Park 1, 50170 Kerpen

computacenter.de
+49 (0)2273 5970