Industrial Production Hardening

BASICS, DIE NICHT FEHLEN DÜRFEN

DIGITAL Trust.

Die Härtung der Informationstechnologie gehört für Unternehmen zum Pflichtprogramm – und zwar längst nicht mehr nur in der klassischen IT, sondern auch in der Operational Technology (OT). Denn: Die zunehmende Verschmelzung der OT mit der IT und die Entwicklung hin zur vernetzten Produktion potenzieren nicht nur die Mehrwerte für Unternehmen, sondern auch die Angriffsflächen für Cyberkriminelle.

Für die Ausrichtung der richtigen Härtungsmaßnahmen Ihrer Produktionsumgebung haben wir ein Vorgehensmodell etabliert, das auf verschiedenen Stufen aufbaut, aber auch individuell auf Ihren Anwendungsbereich oder die Ist-Situation angepasst werden kann. Im Modell evaluieren wir die Ist-Situation, definieren gemeinsam mit Ihnen die Vorgabe für die OT und reduzieren die Sicherheitsrisiken in Produktionsumgebungen durch verschiedene Schutzmaßnahmen wie zum Beispiel im Netzwerk- und Endpoint-Bereich.

TRANSPARENZ SCHAFFEN: RISK ASSESSMENTS DECKEN DEN IST-ZUSTAND AUF

Für den Abgleich von bereits implementierten Security-Maßnahmen mit den für den Anwendungsbereich erforderlichen Schutzmechanismen ist die Durchführung von Risk Assessments unerlässlich. Als besonders empfehlenswert hat sich ein Grey Box Assessment erwiesen, für das vorab partielle Informationen über die Umgebung geteilt werden, aber auch ein praktisches Assessment durchgeführt wird. Dieses Vorgehen ist speziell auf das Produktionsumfeld ausgerichtet und sichert aussagefähige, qualitativ gleichbleibende Ergebnisse:

- **Vorbereitungsphase:** Definition des Assessment-Fokus und Verifizierung der bereitgestellten Dokumente. Erstellung eines Anforderungskatalogs mit Interview-Checkliste.
- **Analyse des Ist-Zustands:** Interviews mit den Fachbereichen und den IT-Verantwortlichen. Vor-Ort-Check mit einer System- und Schwachstellenanalyse.
- **Auswertung und Bewertung:** Abgleich der Security-Level und Risikoanalyse. Maßnahmenplanung und Priorisierung.

STARRE IT-RICHTLINIEN? NICHT MIT UNS!

Da die IT/OT-Konvergenz weiter zunimmt, profitieren unsere Kunden aus dem produzierenden Gewerbe von unserer langjährigen Erfahrung aus der Office-IT-Security: Bestehendes und umfangreiches Wissen adaptieren wir auf die Herausforderungen der OT und stärken somit die Widerstandskraft Ihrer Anlagen.

Da sich nicht alle Unternehmensrichtlinien für Cyber Security eins zu eins auf die Produktions-IT übertragen lassen, unterstützen wir Unternehmen dabei, Anwendungsbereiche mit spezifischen Anforderungen zu definieren. So berücksichtigen wir sowohl aktuelle Technologien und Normen als auch deren Umsetzbarkeit in Brownfield-Anlagen und definieren diese in einer Security Baseline.

Bei Computacenter können Sie auf ein dediziertes Team von erfahrenen Industrial-Security-Expert:innen zurückgreifen und sicher sein: Wir verstehen nicht nur die Abhängigkeiten bei Produktionsprozessen und wissen um die Kritikalität von Produktionssystemen, sondern berücksichtigen auch den Einfluss von Automatisierungssystemen.

Maßnahmen zum Basisschutz bringen die schnellstmögliche Effektivität und lassen sich gut in die Betriebskonzepte der Produktions-IT einführen – der erste und wichtigste Schritt zur Erhöhung des Sicherheitslevels.

Rainer Leisen
Solution Manager Industrial Security

VERLÄSSLICHER MALWARE-SCHUTZ – MIT GANZHEITLICHEN ENDPOINT-SCHUTZMASSNAHMEN

Auch bei Schutzmaßnahmen für die Endpunkte in der Produktion gestalten sich die Herausforderungen meist größer als in der klassischen IT – nicht zuletzt aufgrund der Komplexität der Prozesse und der Heterogenität der Systemlandschaft. Mit unseren ganzheitlichen Endpoint Security Services berücksichtigen wir daher sowohl die Abhängigkeiten von Faktoren wie Systemkritikalität und aktueller Lebenszyklus als auch die Vorgaben von Systemintegratoren.

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.

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.

Bei End-of-Life-Systemen, die gerade im Produktionsumfeld nach wie vor noch im Dauerbetrieb sind, müssen alternative Maßnahmen angewendet werden. In der Praxis hat sich dafür die Härtung nach dem Whitelisting-Prinzip etabliert. Diese Härtungsmaßnahme bietet nicht nur einen soliden Basisschutz, sondern ist auch für einen flächendeckenden Rollout geeignet.

FIREWALLS IN DER PRODUKTION: MEHR ALS NUR EIN PERIMETERSCHUTZ

Die Trennung zwischen IT und OT ist heute integraler Bestandteil jedes Sicherheitskonzepts für die Produktion. Doch aufgrund der zunehmenden funktionalen Vernetzung der Office- mit der Produktionswelt treten immer wieder Herausforderungen bei der Kommunikation zwischen den beiden Welten auf. Zudem wird die Absicherung innerhalb der OT immer wichtiger, da vermehrt bekannte Angriffstechnologien aus der IT nun auch in Produktionsumgebungen angewendet werden und sehr hohen Schaden verursachen können. Das kann zum Beispiel das sogenannte „Lateral Movement" sein, bei dem sich Angreifende schrittweise vertikal und horizontal durch das Netzwerk bewegen.

Zur Erhöhung des aktuellen Schutzlevels kommen dann Firewallsysteme zum Einsatz, die sich beispielsweise mit IDP/IPS-Technologien in der IT etabliert haben, aber speziell auf die Anforderungen der OT angepasst wurden und Formfaktor oder unterstützte Produktionsprotokolle berücksichtigen.

Um bekannte, aber nicht zu lösende Sicherheitslücken zu schließen, kann eine Mikrosegmentierung eine geeignete mitigierende Maßnahme darstellen. Oft unterstützen zudem veraltete Komponenten nur noch unsichere Protokolle, deren Angriffsvektoren im Allgemeinen bekannt sind. Durch eine Isolation dieser Systeme mit einer integrierten Protokolltransformation, zum Beispiel von unverschlüsselt zu verschlüsselt, lassen sich auch diese Geräte bedenkenlos weiter betreiben. Hohe Kosten durch den Austausch oder Moderierung entfallen. Die aufgezeigten Maßnahmen lassen sich also geräuschlos in den laufenden Produktionsbetrieb einbinden und erhöhen somit deutlich die Informationssicherheit Ihrer Produktion.

Sie möchten mehr erfahren?
Sprechen Sie gern Ihr Account Management an oder kontaktieren Sie uns über
www.computacenter.com/de

Computacenter

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