Unternehmen

- Partner: KORAMIS
- Web: http://www.koramis.de
- Branche: Industrial Security
- Hauptsitz: Saarbrücken, Germany
- Mitarbeiter: 35

Herausforderung

KORAMIS, einer der wichtigsten Symantec Partner im wachsenden Markt für IoT-Sicherheit, zählt zu den führenden Systemhäusern im Bereich Industrial Security – und gilt als ausgemachter Spezialist für den Schutz von IIoT-Umgebungen vor Malware und Cyberattacken.

Lösung

- Symantec Critical System Protection
- Symantec Industrial Control System Protection

Leistungen

- Ganzheitliche Beratung bei der Absicherung kritischer Industrieumgebungen
- Signaturloser Schutz historisch gewachsener, heterogener Produktionsumgebungen vor Advanced Threats und Cyberattacken
- Malware-Analyse, Monitoring und Policy-Enforcement für eine sichere Einbindung von Wechseldatenträgern in IIoT-Umgebungen
- Verlängerung des EOL/EOB kritischer Steuersysteme

KORAMIS

Sicherheit für Industrie 4.0-Umgebungen

Wie KORAMIS mit Symantec-Technologie anspruchsvolle Industrial Internet of Things (IIoT)-Netze schützt

Die Digitalisierung der Industrieumgebungen schreitet rasant voran: Wer heute im globalen Wettbewerb bestehen will, ist auf offene, vernetzte Infrastrukturen und flexible, immer öfter Cloud-basierte Technologien angewiesen. Mit Industrie 4.0 und IIoT (Industrial Internet of Things) halten in den Unternehmen nahtlos integrierte Produktionsanlagen, webfähige Endpoints und hochkomplexe Embedded Systems Einzug.

Mit Blick auf die Produktivität, die Effizienz und die Wettbewerbsfähigkeit der Unternehmen ist dies eine positive Entwicklung. Unter Sicherheitsgesichtspunkten ist die Öffnung und Erweiterung der Netze aber durchaus problematisch. Denn mit jedem neuen System vergrößert sich die Angriffsfläche der Unternehmen – und auch die Komplexität der Infrastrukturen nimmt rasant zu.

Die Folge: Weltweit geraten Industrieumgebungen immer öfter in das Visier von Cyberkriminellen. Die Angreifer infiltrieren Produktionssysteme mithilfe von mehrstufigen Angriffen, Zero-Day-Exploits und Advanced Persistent Threats, und versuchen, kritisches Know-how zu stehlen, sensible Systeme zum Absturz zu bringen oder die Unternehmen mit der Androhung von Schäden zu erpressen.

Die Absicherung von IIoT-Umgebungen stellt selbst erfahrene Security-Integratoren oft vor eine erhebliche Herausforderung: Während sich die klassische Business-IT der Unternehmen in der Regel mit bewährten Best Practices aus dem Bereich Enterprise-Security schützen lässt, gehorchen die Produktionsnetze eigenen Gesetzen: Historisch gewachsen, vereinen sie unterschiedlichste Hardware- und Software-Plattformen mit einem bunten Mix mehr oder weniger exotischer Betriebssysteme – von Windows NT über diverse Linux-Derivate bis hin zu proprietären, nicht zu wartenden Embedded Systems.

Vom ICS-Entwickler zum IIoT-Security-Spezialisten

Der Symantec-Partner KORAMIS hat sich vor über zehn Jahren auf die Absicherung von IIoT-Umgebungen spezialisiert und gehört in diesem Umfeld heute zu einem kleinen Kreis weltweit führender Experten. Zu den wichtigsten Differenzierungsmerkmalen der Saarbrücker gehört dabei, dass KORAMIS ursprünglich selbst als Integrator und Programmierer industrieller Steuer- und Kontrollsysteme (ICS) gegründet wurde – und damit die Situation, die Anforderungen und die Prioritäten produzierender Unternehmen bestens einschätzen kann.

Michael Krammel, Geschäftsführer von KORAMIS, erklärt: „Als ehemalige ICS-Integratoren bringen wir ein tiefes Verständnis für die Prozesse unserer Kunden mit – und wissen, welchen hohen Stellenwert die Stabilität und Verfügbarkeit der IT in Industrieumgebungen genießen. Mit Symantec haben wir für diesen anspruchsvollen Markt einen wichtigen strategischen Partner gefunden. Die host-basierten Systeme schützen die Produktionsanlagen unserer Kunden zuverlässig, ohne den Betrieb zu beeinträchtigen, und stoppen dabei selbst gezielte Angriffe und dynamische Threats.“

„Mit Symantec haben wir für diesen anspruchsvollen Markt einen wichtigen strategischen Partner gefunden. Die host-basierten Systeme schützen die Produktionsanlagen unserer Kunden zuverlässig, ohne den Betrieb zu beeinträchtigen, und stoppen dabei selbst gezielte Angriffe und dynamische Threats."

– Michael Krammel, Geschäftsführer von KORAMIS

KORAMIS unterstützt Kunden aus der Industrie mit einem breiten Lösungs- und Beratungsportfolio bei der Absicherung ihrer Infrastrukturen. Im Fokus steht dabei neben dem Schutz vor internen und externen Angriffen zunehmend die zuverlässige Einhaltung gesetzlicher Compliance-Bestimmungen, etwa des IT-Sicherheitsgesetzes, der KRITIS-Vorgaben und der europäischen NIS-Direktive.

„Am Anfang unserer Projekte steht meist ein detailliertes Assessment der vorhandenen Systeme und Anwendungen. Dabei verschaffen wir uns auch einen Überblick über deren Schwachstellen und führen Penetrationstest durch, um alle Angriffspunkte zu lokalisieren", erläutert Daniel Buhmann, Business Unit Manager Security Solutions bei KORAMIS. „So schaffen wir gleich zu Projektbeginn die Voraussetzungen für ein fundiertes Risikomanagement und können tragfähige technische und organisatorische Maßnahmen zum Schutz der Systeme ableiten."

Schlüsselkomponente der von KORAMIS entwickelten IIoT-Security-Architekturen ist die Symantec Critical System Protection (CSP). Die kompakte, hostbasierte Security-Lösung kombiniert ein innovatives Sandboxing für Anwendungen mit integrierter Intrusion Detection & Prevention und leistungsfähigen Malware-Filtern, um Industriesysteme zu härten und vor allen gängigen Bedrohungen zu schützen.

„CSP ist für den Einsatz auf ICS, SCADA und Embedded Systems mit geringer Rechenleistung optimiert und funktioniert unabhängig vom Betriebssystem, ohne Signaturen, ohne Updates und ohne Internetanbindung", erklärt Olaf Mischkovsky, IIoT-Experte von Symantec. „Die Lösung schützt zwanzig Jahre alte Windows NT-Server also ebenso zuverlässig wie die brandaktuellen Embedded Systems eines Smartcars – und das, ohne den Betrieb in irgendeiner Weise zu beeinträchtigen."

Anwendungsisolierung und Whitelisting von Anwendungen

Um zu verhindern, dass kompromittierte Anwendungen auf dem ICS Schäden verursachen, unterstützt Symantec CSP ein granulares, policy-basiertes Whitelisting. Dieses sorgt dafür, dass auf dem Host stets nur freigegebene Anwendungen ausgeführt werden – und zwar ausschließlich in der vorgegebenen Art und Weise. Unbekannte Dienste und Anwendungen verschiebt Symantec CSP automatisch in eine isolierte Sandbox mit minimalen Rechten. Sie haben damit keinen Zugriff auf den Code oder den Funktionsumfang anderer Anwendungen und können sich weder über das Netzwerk verbreiten noch Schadcode über das Internet nachladen.

Integrierte IDP-Funktionalitäten

Über die Anwendungskontrolle hinaus setzt KORAMIS Symantec CSP bei Kunden als leistungsfähige Intrusion Detection- und Prevention-Lösung ein, um verdächtige Aktivitäten auf den Hosts zuverlässig zu identifizieren und proaktiv zu unterbinden. „CSP ist standardmäßig mit Tausenden vordefinierter Regeln hinterlegt und überwacht durchgehend die Files, die Einstellungen, die Logs, die Events und das Anwendungsverhalten auf dem Host-System", erklärt Daniel Buhmann. „Bei Anomalien und Verstößen gegen die Policy schlägt das System automatisch Alarm und unterbindet die entsprechenden Aktivitäten. So lassen sich gängige Angriffe zuverlässig stoppen."

„CSP ist standardmäßig mit Tausenden vordefinierter Regeln hinterlegt und überwacht durchgehend die Files, die Einstellungen, die Logs, die Events und das Anwendungsverhalten auf dem Host-System."

– Daniel Buhmann, Business Unit Manager Security Solutions bei KORAMIS

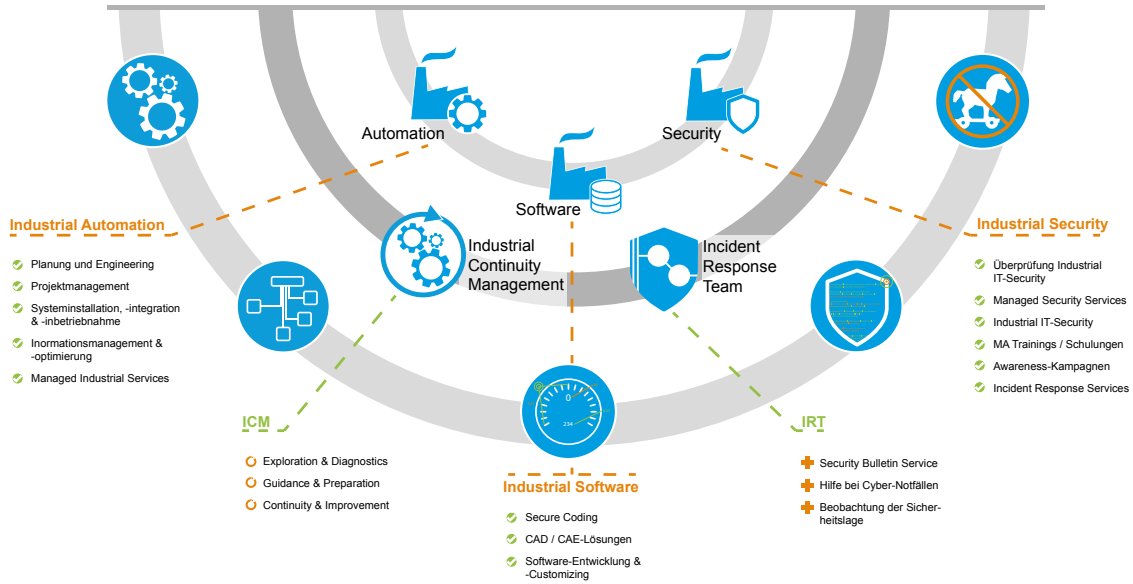
Die Kombination aus Härtung, Sandboxing und Whitelisting ermöglicht es KORAMIS, die Netzwerk-Zugriffe im Kundennetz anwendungsbasiert zu steuern, Back Doors zu schließen und den ein- und abgehenden Traffic zu minimieren. Auch Zero-Day-Exploits und gezielte Angriffe mit Malware lassen sich durch die restriktive Anwendungssteuerung zuverlässig unterbinden, um die ICS-Hosts und die Netzwerkumgebungen der Kunden zu schützen.

Dies ist umso wichtiger, als signaturbasierte Filter in Industrieumgebungen keine echte Alternative sind: Auf den meisten industriellen Steuersystemen stoßen sie schon wegen der hohen CPU-Anforderungen an ihre Grenzen. Hinzu kommt, dass sich die oft veralteten Betriebssysteme über Signaturen nicht zuverlässig schützen lassen, da viele Hersteller alte Pattern nach einigen Jahren herausrotieren, um die Pattern-Files nicht zu groß werden zu lassen.

Angriffsvektor Wechseldatenträger

Ergänzend zu Symantec CSP empfehlen die KORAMIS-Experten ihren Kunden in der Regel den Einsatz einer Datenschleuse, wie etwa der Symantec ICSP (Industrial Control System Protection). Die kompakte und robuste Station ermöglicht es Anwendern, ihre USB-Wechseldatenträger vor der Anbindung an das Netzwerk einem schnellen Security-Check zu unterziehen. Dabei wird der Datenträger binnen weniger Sekunden mit einer Reihe leistungsfähiger Technologien gescannt: Die ICSP Station kombiniert klassische signaturbasierte Verfahren mit Reputationsanalysen, Machine Learning und innovativem Sandboxing, um Malware und Advanced Threats zuverlässig zu identifizieren.

„Da die meisten Produktionsnetze nicht an das Internet angebunden sind, gehören infizierte USB-Sticks in der Industrie zu den gefährlichsten Einfallstoren für Malware", erklärt Olaf Mischkovsky. „Mit der ICSP lässt sich dieser Angriffsvektor zuverlässig kontrollieren. In besonders kritischen Umgebungen können die Kunden auf ihren Produktionssystemen optional auch noch einen kleinen Agent installieren, der dafür sorgt, dass ausschließlich ICSP-geprüfte Datenträger verwendet werden dürfen. Das gibt den Betreibern noch ein zusätzliches Maß an Sicherheit, und verhindert, dass Mitarbeiter schlichtweg vergessen, ihre Sticks untersuchen zu lassen."



KORAMIS – eine Success Story im besten Sinn

Als ausgemachter Spezialist für die Absicherung von Industrie 4.0-Umgebungen ist KORAMIS in den vergangenen Jahren rasant gewachsen. Lag der Fokus in den ersten Jahren im Security-Geschäft noch auf Energieversorgungs- und Chemieunternehmen in der DACH-Region, sind die Saarbrücker heute weltweit tätig – und betreuen produzierende Unternehmen über alle Branchen und Unternehmensgrößen hinweg. Neben der Absicherung von ICS- und SCADA-Systemen engagiert sich KORAMIS inzwischen sehr erfolgreich im boomenden Markt für IoT-Security – auch dies ein Segment, in dem die Host-basierten Lösungen von Symantec ihre Stärken voll ausspielen können.

Erfahren Sie mehr über Symantec Critical System Protection unter:
https://www.symantec.com/products/embedded-security

Erfahren Sie mehr über Symantec Industrial Control System Protection unter:
https://www.symantec.com/solutions/industrial-control

Über Symantec

Symantec Corporation (NASDAQ: SYMC) ist einer der weltweit führenden Anbieter für Cybersicherheit. Symantec unterstützt Unternehmen, Regierungen und Menschen dabei, ihre wichtigen Daten zu schützen – egal, wo diese sich befinden. Organisationen auf der ganzen Welt bauen auf die strategischen und ganzheitlichen Lösungen von Symantec, um sich vor komplexen Attacken über Endgeräte, Cloud und Infrastrukturen hinweg zu schützen. Gleichzeitig vertrauen mehr als 50 Millionen Menschen und Familien weltweit auf Symantecs Norton-Produktreihe für Sicherheit zuhause und auf all ihren Geräten. Symantec betreibt eines der weltweit größten zivilen Cyber-Intelligence-Netzwerke. Dadurch ist das Unternehmen in der Lage, frühzeitig die ausgefeiltesten Bedrohungen zu erkennen und entsprechenden Schutz anzubieten. Erfahren Sie mehr unter www.symantec.com/de/de oder besuchen Sie uns auf Facebook, Twitter und LinkedIn.

Symantec™

Symantec (Deutschland) GmbH, Theatinerstraße 11, Fünf Höfe Business Center, 8. Stock, 80333 München | +49 (0) 89 710 422 430 | www.symantec.com/de/de