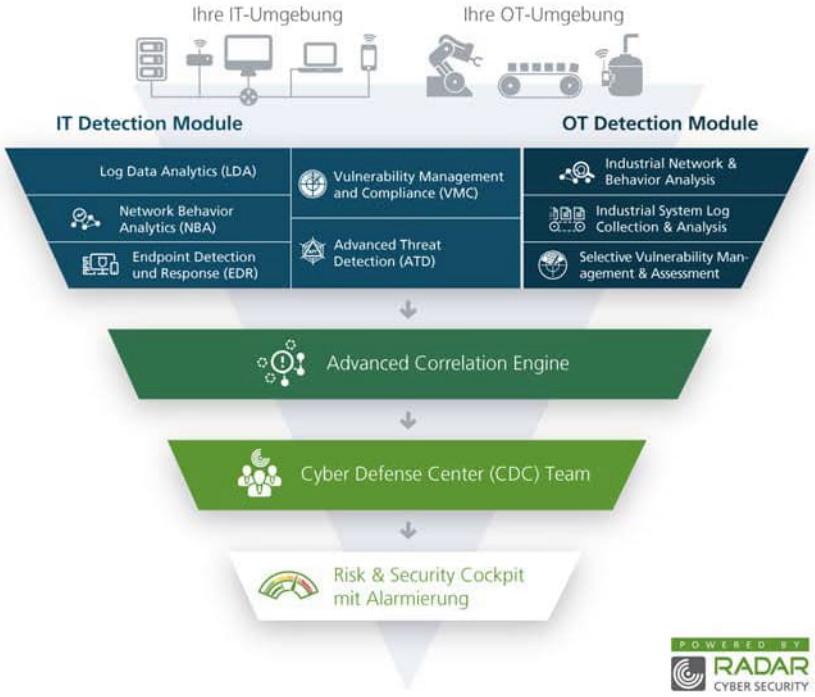

Foto: Radar Cyber Security

Informationen aus unterschiedlichen Sicherheitsmodulen werden automatisiert, mit menschlichem Know-how aufbereitet und im Risk & Security Cockpit übersichtlich visualisiert.

Königsklasse der IT-Security

Ein Security Operations Center (SOC) agiert mit 360-Grad-Blick als Kommandozentrale zur Abwehr von Cyberangriffen.

HANS-JÜRGEN MITZSCHER & DANIEL WEBER

Cyberangriffe werden in dem Moment zur realen Gefahr, in dem sich Industrieanlagen direkt oder indirekt mit dem Internet verbinden. Was Betreiber Kritischer Infrastrukturen (Kritis) schon immer wussten, dringt durch die gestiegene Cyber-Bedrohungslage und die verschärften Vorgaben des IT-Sicherheitsgesetzes 2.0 auch ins Bewusstsein anderer Industriebereiche: Die Systeme der OT (Operational Technology) sind keine in sich abgeschotteten Insellösungen mehr. Denn intelligente Lösungen wie Smart Grid und digitale Dienstleistungen wie Netzwerküberwachungen oder Fernwartung brauchen einen regen Datenaustausch. Dafür muss sich die OT in rasanter Geschwindigkeit vernetzen, und das macht sie angreifbar.

Die Königsklasse der Cyberabwehr sind Security Operations Center (SOC). Sie kombinieren Prozesse, technische Tools und Cybersecurity-Experten, die mit einem 360-Grad-Blick alle sicherheitsrelevanten Systeme eines Unternehmens integrieren, analysieren und überwachen. Während es in der Welt der IT schon seit Längerem SOC gibt, ist das für die OT Neuland und stellt sie bei der Umsetzung vor echten Herausforderungen. Das beginnt damit, dass sich Softwarelösungen, die zum Schutz typischer IT-Produkte wie Serversysteme oder Router entwickelt wurden, nicht einfach 1:1 auf die OT übertragen lassen. Die Programme sprechen nicht dieselbe Sprache und können etwa Industrieprotokolle von Anlagensteuerungen nicht verstehen. Dass IT nicht gleich OT ist, wird offenkundig bei so etwas Selbstverständlichem wie Updates. Die Betreiber haben die nicht unberechtigte Sorge, dass das Patchen älterer Bestandsanlagen problematisch sein kann. Die Anlagenverfügbarkeit hat höchste Priorität und die Folgen eines ungeplanten Maschinenstillstands sind wesentlich gravierender als der kurzfristige Ausfall eines Büro-PCs.

„Am Anfang stehen immer grundlegende Dinge, wie sichere Passwörter, sauber segmentierte Netze oder ein etabliertes Patch-Management. Was in der IT zum Standard gehört, ist in der OT noch selten."

Hans-Jürgen Mitzscher, Service Manager bei Telent.

Gebündeltes Know-how in IT und OT

IT-Security-Kenntnisse allein reichen nicht aus, um maßgeschneiderte Sicherheitskonzepte für die OT zu entwickeln. Zusätzlich braucht es ein tiefes Verständnis der OT-Infrastrukturen und ihrer Automatisierungs-, Prozess- und Netzleittechnik, wie sie telent durch die langjährige Betreuung von Kommunikations- und Datennetzen insbesondere in Kritis-Umgebungen besitzt. Seit Kurzem ist das interdisziplinäre Fachwissen in einem neugegründeten SOC für IT und OT gebündelt. Die technische Basis ist eine Softwareplattform, die beide Bereiche automatisiert auf Sicherheitsprobleme überprüft. Mit

menschlichem Know-how werden die Ergebnisse analysiert, und zwar immer passend zu speziellen Erkennungsszenarien. Dafür werden im Vorfeld für jeden Kunden gemäß seiner kritischen Geschäftsprozesse Gefährdungssituationen definiert, sogenannte „Use-Cases".

Zu einem modular aufgebauten SOC gehört ein breites Spektrum an Managed Services. Für Unternehmen, die nicht an die strengen Vorgaben des Kritis-Sektors gebunden sind, hat das den Vorteil, dass sie ihre Schutzmaßnahmen stufenweise aufbauen und erweitern können. Am Anfang stehen immer grundlegende Dinge, wie sichere Passwörter, sauber segmentierte Netze oder ein etabliertes Patch-Management. Was in der IT zum Standard gehört, ist in der OT noch selten. Doch die Basismaßnahmen sind unerlässlich, damit die Sicherheitsfachleute im SOC überhaupt ein modernes Security Information and Event Management (SIEM) realisieren können.

Hohe Transparenz für schnelle Reaktion

Eine der wichtigsten Anwendungen des SIEM ist das Security-Modul „Log Data Analytics" (LDA). Es identifiziert Tausende von Logdaten, die alle zur Infrastruktur gehörenden IT- und OT-Komponenten erzeugen. Dann kategorisiert und analysiert es automatisiert die Daten in Bezug auf ihre Sicherheitsrelevanz. Mit diesem Tool erfüllen Unternehmen ihre Pflicht nach dem IT-SiG 2.0, Sicherheitsvorfälle zu protokollieren, zu detektieren sowie darauf reagieren zu können. Die definierten Use-Cases erhöhen die Produktivität des LDA erheblich, da die Korrelationsregeln, Compliance-Standards und bekannte Gefährdungslagen jederzeit verfügbar sind und nach der Implementierung sofort für alle Anwendungen bereitstehen. Den Security-Analysten im SOC liefert LDA genau die Transparenz und Visualisierung, um Daten noch besser zu interpretieren und in kürzester Zeit zu reagieren. Sinnvoll flankiert wird LDA von weiteren Sicherheits-Modulen, wie „Vulnerability Management & Compliance" (VMC). Die Software scannt automatisiert in regelmäßigen Abständen die komplette IT/OT-Infrastruktur in so hoher Güte, dass Produktionsanlagen nicht gestört werden. Sie zeigt Unternehmen auf, ob ihre Systeme bekannte Sicherheitslücken enthalten, die Cyberkriminellen eine Angriffsfläche bieten. Daneben erkennt das Modul „Network Behaviour Analytics" (NBA), ob gefährliche Malware, Anomalien und andere Bedrohungen im Netzwerk unterwegs sind.

KMU sollten externen Spezialisten vertrauen

Die technischen Tools sind aber nur die Basis. Der echte Mehrwert für Unternehmen in puncto Cybersecurity entsteht durch Security-Analysten mit umfassenden Kenntnissen in IT- und OT-Umgebungen.

„Mit dem Security-Modul LDA erfüllen Unternehmen ihre Pflicht nach dem IT-SiG 2.0, Sicherheitsvorfälle zu protokollieren, zu detektieren sowie darauf zu reagieren."

Daniel Weber, Senior Manager Security Solutions bei Telent.

Letztlich entscheidet sich die Qualität eines SOCs an der Kompetenz der darin arbeitenden Menschen, die ein gleichermaßen breites wie tiefgehendes Spezialwissen besitzen müssen. Denn nur mit diesem Sachverstand sind sie in der Lage, aus der Vielzahl der Meldungen echte Sicherheitsvorfälle herausfiltern und richtig zu reagieren.

Sicherheit ist Vertrauenssache. Deswegen bleiben alle Daten innerhalb der Kundensysteme und Telent verbindet sich nur mittels verschlüsselter Datenübertragung. Unternehmen können natürlich ein eigenes SOC aufbauen und betreiben. Doch vor allem für kleinere mittelständische Unternehmen (KMU) wird es der günstigere Weg sein, diese Kapazitäten einzukaufen. Hinzu kommt: Ein auf IT-Sicherheit und OT-Infrastrukturen spezialisierter Dienstleister beschäftigt sich täglich mit Cyberrisiken und ist bestens über aktuelle Entwicklungen informiert. Mit diesem 360-Grad-Blick gelingt es, als Kommandozentrale für mehr Cybersecurity zu sorgen. ■

telent GmbH:
www.telent.de