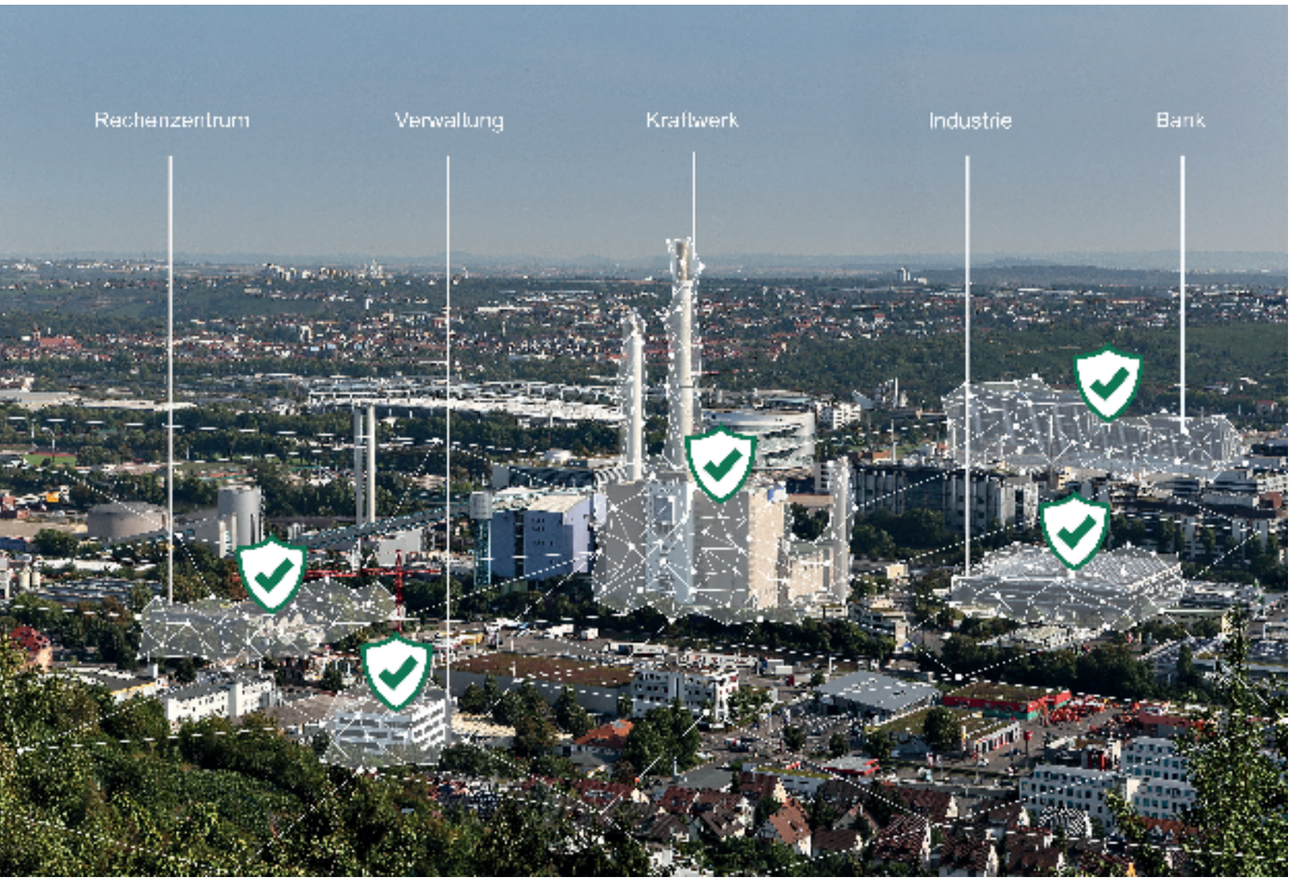
SICHERHEITSKONZEPT – Der Bedarf an Cybersecurity-Lösungen für kritische Infrastrukturen steigt. Im Idealfall sollten laufende Prozesse nicht behindert, aber jede noch so kleine Störung zuverlässig gemeldet werden. Die Lösung Silent Defense macht genau das.

DIE ABWEHR STEHT



Um ihre technischen Prozesse zu steuern, setzen Kritis-Betreiber Industrial Control Systems wie etwa Scada ein, mit dem übergeordnete Steuerungsdaten gesammelt werden können. Tatsache ist, dass Angreifer detailliertes Know-how über Systeme dieser Art besitzen.

NETZWERKE INTELLIGENT ÜBERWACHEN UND SCHÜTZEN

Für ein durchdachtes Sicherheitskonzept eignet sich ein System für Anomalieerkennung. Anomalie bezeichnet eine Normabweichung beziehungsweise ein unerwartetes Verhalten, das auf verschiedene Arten auftreten kann; sei es ein Netzwerkgerät, das von jetzt auf gleich ein anderes Kommunikationsprotokoll nutzt, oder Netzwerkverkehr, der plötzlich eine neue Route nimmt. Um Abweichungen zu definieren, ist es entscheidend, zuerst den Normalzustand zu erfassen. Das System beobachtet dazu die gesamte IT-Architektur und lernt, ohne sich bemerkbar zu machen.

Im Fall eines Angriffs erkennen solche Systeme das Verhalten einer Schadsoftware als abnormales Angriffsmuster. Dazu zählt etwa das Installieren und Manipulieren von Treibern oder der Versuch, eine Verbindung ins Internet herzustellen. Neben der Angriffserkennung ermöglicht moderne Anomaly Detection, alle Teilnehmer der Netzwerkkommunikation zu identifizieren und sie über ein entsprechendes Monitoring abzubilden. Das System bereitet zudem alle Logfiles automatisch auf, alarmiert bei Auffälligkeiten und entlastet so Administratoren in IT-Abteilungen, die diese Daten ansonsten manuell überprüfen müssten.

EIN LERNFÄHIGES ABWEHRSYSTEM

Der Systemintegrator Telent und die auf Cybersicherheit spezialisierte Tochter Koramis setzen die Securitylösung Silent Defense von Security Matters ein. Es handelt sich um eine passive Überwachungslösung, die eine umfassende Bestandsaufnahme aller Komponenten von Infrastrukturen ermöglicht. Sie analysiert das Verhalten von Netzwerknutzern und angeschlossenen Systemen, um Prozessanomalien, Maschinenstatus, unsicheren Zugriff und potenziell schädliche Aktivitäten zu identifizieren. Silent Defense nutzt patentierte maschinelle Lernfunktionen zur Überwachung von ICS-Netzwerken, -Protokollen und -Semantik und liefert damit umfassendere Daten als konkurrierende Technologien.

Grundvoraussetzung für die Überwachung ist eine Inventarisierung des Netzwerkzustands, die Identifikation aller Geräte im Netzwerk sowie die Analyse der Kommunikationsflüsse. Sensoren an den jeweiligen Schnittstellen speichern sämtliche Informationen, Parameter und Werte und lernen so Verhaltensmuster, die per Network Map festgehalten werden. Die Lösung erkennt Netzwerk-, Betriebs- und Sicherheitsprobleme sowie Bedrohungen out of the box.

Darunter fallen beispielsweise unerlaubte Zugriffe und Datenflüsse, Manipulations- und Zugangsversuche von außen sowie Fehlkonfigurationen von Firewall- und Netzkomponenten. Darüber hinaus informiert es auch über unsichere Protokolle, falsche Messergebnisse, Verbindungsprobleme zwischen Geräten, Softwarebugs, instabile Prozesse, nicht eingehaltene Protokoll-Spezifikation, Anomalien beziehungsweise Stillstand der Schaltanlagen sowie unkontrollierte Regelschalterbedienung.

Die Lösung ist kompatibel mit mehr als 40 Industrieprotokollen, umfasst eine umfangreiche Bibliothek für industrielle Bedrohungen mit über 1.300 ICS-spezifischen Prüfungen und stellt zeitnah Updates zu neuen Bedrohungen bereit.

Dominic Iselt/Koramis, Nico Werner/Telent

www.telent.de

FAKT

Immunsystem geschwächt

Der Computerwurm Stuxnet wurde vor einigen Jahren speziell zum Angriff auf zentrale Kontrollsysteme von Uranan-reicherungsanlagen entwickelt. Die Malware nutzte eine Schwachstelle in der Firmware eines ICS-Systems aus. Stuxnet zielte darauf ab, Zentrifugen in einer nuklearen Anlage durch Veränderung der Motorgeschwindigkeit zu beschädigen. Aufgrund seiner Komplexität und Flexibilität wurde das Schadprogramm nicht erkannt und konnte sich unbemerkt im Netzwerk verbreiten.

Bild: wm-foto.com