ICS / IPS-Schleuse

Die Gefährdungslage

Stuxnet, Duqu, Flame, Mahdi, Gauss, Shamoon, ihre Varianten und Nachkommen legen Produktionssysteme lahm. Die Sicherheit der Systeme ist dort angekommen wo es weh tut: beim Geld, der Verfügbarkeit der Produktion.

Dokumentiert ist eine steigende Anzahl von Security Vorkommnissen im Industrial Control Systems (ICS), SCADA und IPS Umfeld mit direkten Auswirkungen auf die Verfügbarkeit, Qualität oder Produkthaftung – also die Kosten bzw. den Gewinn des Betreibers. VDMA , und BSI zeigen die Risiken auf. Besonders perfide ist, dass die Angriffe, obwohl erfolgreich, häufig noch schlummern und auf den richtigen Moment warten. Auch Komponentenangriffe, die erst nach dem Zusammenführen und Nutzen verschiedener Angriffsvektoren ihren Schaden anrichten, nehmen zu.

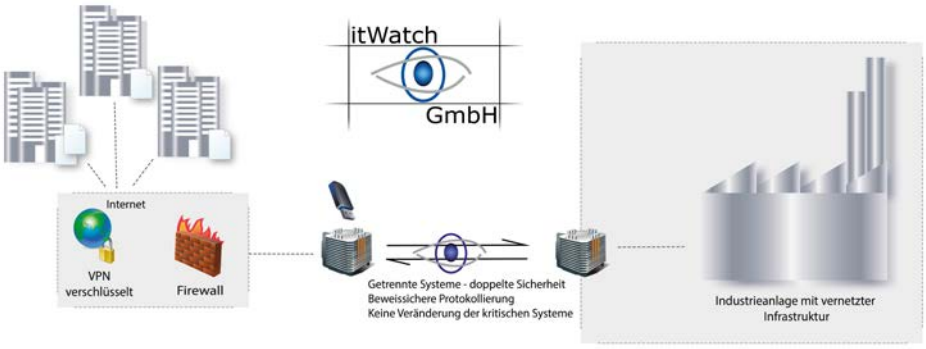

Bild: IST-Stand der IT-Sicherheit sind im besten Fall VPN und Firewall, wodurch sich der Schadcode verschlüsselt ausbreitet und kein Schutz vor wild wachsendenm Datentransfer in der Produktionsanlage über USB-Stick etc. besteht.

Die Herausforderung

Kommunikation zwischen den Systemen war schon immer nötig. Die Integrität und die Sicherheit der Verfahren lagen durch organisatorische Richtlinien hauptsächlich in der Hand der beteilgten Menschen. Kosten können durch Vernetzung statt manueller Datentransporte gesenkt werden. USB Sticks – direkte Vernetzung stehen in allen Facetten (Protokollierung, Dateninegrität, Authentizität, …) im Widerspruch zur Sicherheit. Der Betreiber steht vor unterschiedlichen Kostenbetrachtungen:

- Verschiedene Systeme dürfen nicht verändert werden, weil sonst die Haftung und Service Levels verloren gehen
- Wartungszugriffe von außen ermöglichen schnelle Reaktionen in kritischen Situationen und verbessern die Produktivität. VPN und Firewall genügen aber nicht, da die Angriffe dann verschlüsselt übertragen werden.
- Das Beschaffen von Qualitäts- und weiteren Daten aus der Produktion über remote Zugriffe gefährdet zum einen die Sicherheit der Systeme und zum anderen ist die Vertraulichkeit der Daten, was in vielen Industriezweigen in den Zeiten der Industrie- und Wirtschaftsspionage immer höhere Bedeutung bekommt
- Die Kostensenkung durch Vernetzung muss durch Kosten in die Schutzsysteme aufgefangen werden.

Die Umsetzung effizienter Sicherheitsmechanismen im industriellen Umfeld ist deshalb eine komplexe Herausforderung. ICS Anlagen (Automatisierungs-, Prozessteuerungs- und Leitsysteme) bestehen aus mehrschichtigen Systemen, z.B. Automatisierungsgeräten wie SPS Systemen und gegebenenfalls Human-Machine-Interfaces (HMI) und Industrie-PCs (IPC). Die unterschiedlichen Teilsysteme haben verschiedene Anforderungen an:

- Heterogenität der Umgebungen (z.T. sehr alte OS)
- Teilvernetzte Systeme
- Fehleranfälligkeit
- Wartungsfähigkeit
- Verfügbarkeit und Integrität

Statt der klassischen IT-Sicherheitsmachanismen wie Authentisierung, Zugriffskontrolle etc., die hohe Kosten in der Administration bergen, ist eine vollautomatisierte Verfahrenskontrolle hier der effizientere Weg. itWatch nutzt die Vorteile der Verfahrenskontrolle eine patentierte Lösung. Alle Zugriffe und Datenmanipulationen werden erkannt und entsprechend des zugeordneten Verfahrens erlaubt oder verboten und revisionssicher protokolliert. Vertrauliche Ergebnisse werden mit unternehmenseigenen Schlüsseln geschützt.

Die Lösung

Die bewährte Technologie des itWatch nutzt verschiedenen Produktkomponenten und Expertisen und führt sie in einem Produkt zum Schutz von Industriesystemen zusammen.

- Jede Datei kann nach spezifischen Vorschriften für den Inhalt geprüft werden. Die Vorschriften (Patterndefinitionen) können in einfacher Art an die Kundenbedürfnisse ohne Produktänderung angepasst werden.
- Entkoppelte Systeme (Remote Controlled Application Systems), deren Informationsübergabe mit zwei separierten Kontrollsystemen jedes Bit in beiden Richtungen kontrolliert. Dieses System kann auch mit Einweg-Dioden angereichert werden. Dadurch werden sichere Internet Verbindungen oder sichere Netzübergänge um die fehlenden Funktionen angereichert. Dieses System wird zwischen die offenen und die kritischen Systeme als Echtzeit-Schleuse gebracht.
- Alle Schnittstellen (Ports) und an diesen angeschlossene Geräte (Devices) eines Systems werden erkannt, authentisiert, überwacht und abhängig von den Dateninhalten frei gegeben oder gesperrt.
- Remote liegende Systeme können ohne das Aufbringen von Code in das Daten-Kontroll-System integriert werden.
- Verschlüsselung mit benutzerspezifischen oder Unternehmens Schlüsseln sichern die Vertraulichkeit entsprechend dem konkreten Bedarf.
- Protokollierung komplexer Systemzustände, Veränderungen an Systemen, Daten Zu- und Abflüsse und revisionsichere Beweiserhebung der Aktivitäten.
- Verfahrenskontrolle ermöglicht es unter Verwendung der notwendigen Privilegien automatisiert fest definierte Aktionen mit automatisch ermittelten oder über abgesicherte Benutzerdialoge eingegebenen Parametern protokolliert auszuführen.

Das System kann auf Standard-Systemen betrieben werden oder als Appliance in das Netz integriert werden. In besonderen Situationen wird das Gesamtsystem inklusive der Entkoppelten Systeme auch als mobiles Gerät geliefert.

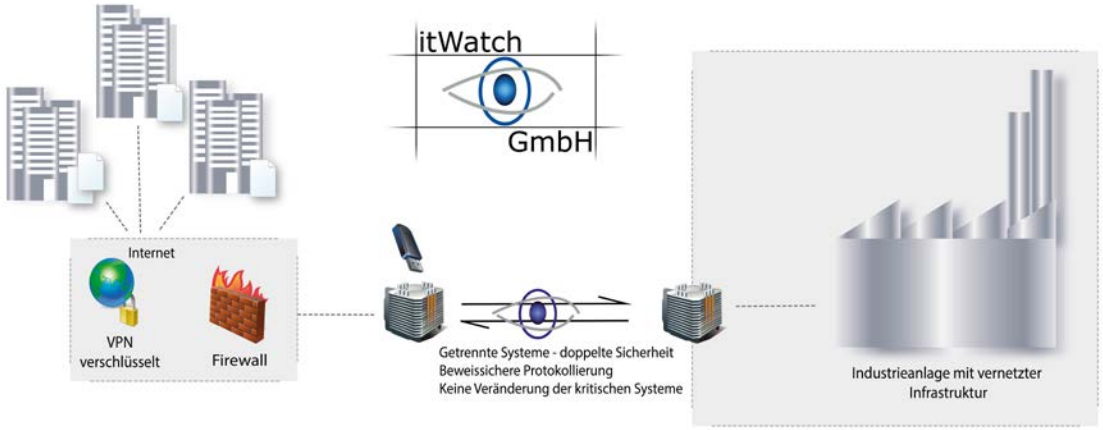

Bild: Daten- und Applikationsschleusen trennen die Netze logisch, transparent für alle Anwender ohne die Arbeitsprozesse zu verändern

Use Case

Nicht vertrauenswürdige Mitarbeiter im Ausland sollen Qualitätsdaten über einen mobilen Datenträger von den Messstationen einsammeln. Statt dem Mitarbeiter ein Login und das Recht zum Anstecken des Datenträgers und Lesen der Daten zu geben ermöglicht die ICS/IPS-Schleuse der itWatch hier folgende moderne und sichere Lösungsszenarien

Lösung 1 mit Code auf den Messrechnern: Auf einem speziellen authentisierbaren verschlüsselten Datenträger werden die Messdaten sofort beim Anstecken ohne Interaktion mit dem Mitarbeiter vollautomatisch, außerhalb der Benutzeranmeldung, sprich ohne Login auf den Messstationen, verschlüsselt aufgebracht.

Lösung 2 ohne Code auf den Messrechnern: Die betroffenen Systeme werden mit den Werkzeugen der ICS/IPS-Schleuse gekoppelt, ohne die Zielsysteme zu verändern. Die doppelten Schleusensysteme und die Automatisierung steuern den Datenfluß automatisch und bei Bedarf verschlüsselt. Dieses System kann feststehend gekoppelt oder als mobile Instanz integriert werden.

Die Produkte der itWatch haben eine über 15-jährige Tradition. Ihre Stabilität und Verfahrenssicherheit ist in vielen Millionen täglich aktiven Systemen dokumentiert. Die Produkte haben seit 2003 Freigaben für die Verwendung in GEHEIM klassifizierten Umgebungen und belegen dadurch die Robustheit gegen Angriffe.