Operational Support Systems, OSS Appliance

Situation

Regelmäßig erfahren wir aus der Presse über realisierte Angriffe auf essentielle, teilweise kritische IT-Infrastrukturen bei Energie- oder Wasserversorgung, Produktivumgebungen der verarbeitenden Industrie oder neuerdings auch der Gebäudeleittechnik. Was ist da los?

Nach langen Jahren der dem Kostendruck geschuldeten unreglementierten Einführung und Installation von Compute- und Storagekomponenten in der Automatisierungstechnik und bei SCADA-Systemen, kommen inzwischen fast ausschließlich standardisierte Ethernet-Schnittstellen und die aus der Büro-IT bekannten Betriebssysteme wie Windows oder Linux zum Einsatz. Industrial Ethernet Infrastrukturen und IoP (Internet of Production) sind in OT-Umgebungen mittlerweile State-of-the-Art.

Damit einhergehend wurden automatisch auch alle aus der Büro-IT bekannten Bedrohungsszenarien auf die OT-Umgebungen weitervererbt, jedoch besteht ein unterschiedlicher Schutzbedarf im Vergleich zur Office-IT. Deshalb können bekannte Sicherheitslösungen und Sicherheitsmechanismen aus Büroumgebungen nicht 1:1 auf die OT adaptiert werden.

Erschwerend kommt hinzu, dass in der OT meist keine oder nur eine unzureichende IT-Expertise vorhanden ist.

Herausforderung

Um dem Schutzbedarf von OT-Umgebungen gerecht zu werden, ist die Einführung und Adaption von etablierten Mechanismen zur Gewährleistung von anerkannten Sicherheitsstandards in Anlehnung an das BSI Grundschutzkompendium und branchenspezifische Regelwerke (VDE usw.) erforderlich. In der Regel sind mehrere Maßnahmen durchzuführen, wie beispielsweise:

- Einführung von **Triple-A Strukturen** (Authentication, Authorization, Accounting) zur Steuerung von Zugriffsrechten und Protokollierung von Zugriffen.
- **Absicherung von Remotezugängen:** Eng verwandt mit den AAA-Strukturen werden die Mechanismen einer Network Access Control (NAC) oder Zero Trust Network Access (ZTNA) eingesetzt, um Zugriffe von außen auf die Produktionsmittel zu reglementieren.
- **Monitoring, Logging, Analytics:** Das Kommunikationsverhalten der beteiligten Elemente und die Einhaltung der Regelwerke muss überwacht, sowie zumindest bei Zugriffen Dritter auch protokolliert werden. Auffälligkeiten müssen durch geeignete Cyber Security Elemente wie Security Incident Event Management (SIEM), Vulnerability Assessment Systeme (VAS) oder Behavioral Analytics erkannt und ggf. Maßnahmen zur Gefahrenabwehr eingeleitet werden.
- **Datensicherung, Datenschutz:** Schaffung sicherer Repositories, Einführung von Backup- und Restore-Mechanismen, Etablierung von Data Loss Prevention Systemen, Schutz vor Malware u. ä.

Für all diese bekannten Problemstellungen muss ein breitgefächertes Lösungsinstrumentarium mit vergleichsweise geringem User- und Endgerätespektrum geschaffen werden, d. h. es wird zwar ein vollständiges Setup aller Unterstützungssysteme (Operational Support) für einen sicheren Betrieb von IP-basierten Netzwerken benötigt, dieses muss jedoch nur eine „kleine“ Skalierung abdecken.

Unser Angebot

Controlware bietet mit der OSS Appliance eine Lösung, die mit dem bestehenden Fachpersonal handhabbar ist.

OSS-Appliance Size M

Dabei handelt es sich um eine vollständige „Out-of-the-box“-Lösung mit einem von Controlware etablierten Hardwareunterbau, der als solcher auch von unserem Customer Service Center unter Wartung genommen werden kann.

Die OSS-Appliance beinhaltet einen vollständigen, aufeinander abgestimmten und kontinuierlich validierten System-Stack bestehend aus Instanzen aller benötigten Supportsysteme mit einheitlicher Benutzeroberfläche. Das Sizing erfolgt auf Basis der vom Kunden ausgewählten modular einsetzbaren virtuellen Systeminstanzen, wie beispielsweise:

- **Administration Services:** Das Cockpit ist eine Webkonsole, die einen Systemüberblick gibt und grundlegende administrative Funktionen erfüllt.
- **Authentication Services:** beinhaltet Single Sign On, User-/Group-/Sudo-/Host-Management, LDAP, DNS, DHCP, WebGui zur Verwaltung des DHCP-Services (Kea), PKI.
- **RADIUS Services:** AAA-Funktion mit einer Vielzahl unterstützter Protokolle.
- **File Services:** unterstützt SMB, CIFS, NFS
- **File Services (Free NAS):** unterstützt SMB, CIFS, NFS, AFP, FTP, WebDAV, iSCSI, VMware VAAI, Microsoft ODX und Windows Server Clustering
- Upload Services

Ihr Nutzen

Zuerst einmal ist die OSS-Appliance kostengünstiger als die jeweils „große“ Lösung etablierter Anbieter. Darüber hinaus ergeben sich viele Vorteile bei Einführung und Betrieb:

- Der vollständige, aufeinander abgestimmte und kontinuierlich validierte System-Stack führt dazu, dass sich sehr schnell ein nachweisbarer Sicherheitsstandard etablieren lässt.
- Das System ist auditierbar und führt in einigen Branchen zu deutlich verringerten Versicherungsleistungen.
- In Verbindung mit dem gewünschten Care Service wird die OSS-Appliance mit von Controlware zusammengestellten Update-Paketen kontinuierlich aktuell gehalten.
- Es besteht Wahlfreiheit, die Appliance mit dem vorhandenen technischen Personal zu betreiben oder auch vollständig durch Controlware betreiben zu lassen.

Die OSS-Appliance reduziert Ihren Bereitstellungsaufwand erheblich

- Das System ist ohne aufwändige Einzelschulungen bedienbar.
- Die Appliance ist vor allem für mittlere und kleinere Unternehmen geeignet und bietet durch seine Konzeption einen kostengünstigen Einstieg in die erforderlichen Technologien.
- Bei Bedarf kann die OSS-Appliance jederzeit durch eine „große“ Lösung eines frei wählbaren etablierten Anbieters ersetzt werden, so dass kein Vendor-Lockin entsteht.
- Darüber hinaus werden durch den Einsatz der OSS-Appliance Abhängigkeiten zur bestehenden Office-IT vermieden.

Warum Controlware

Die Controlware GmbH ist einer der führenden unabhängigen Systemintegratoren und Managed Service Provider. Das 1980 gegründete Unternehmen entwickelt, implementiert und betreibt anspruchsvolle IT-Lösungen für die Cloud-, Data Center-, Enterprise- und Campus-Umgebungen seiner Kunden mit nachgewiesener Servicequalität mit dem ISO 27001-zertifiziertem Customer Service Center.

Unsere Spezialisten verfügen über umfangreiche Expertisen in verschiedensten Branchen, mit vielfältigen Technologien und für unterschiedlichste Unternehmensgrößen.

Zentrale

Controlware GmbH
Waldstraße 92
63128 Dietzenbach
Tel. +49 6074 858-00
Fax +49 6074 858-108

info@controlware.de
www.controlware.de
blog.controlware.de

Besuchen Sie uns auf: