Monitoring- & Security-Analysetool

für IT- und OT-Umgebungen

Neuerdings ist das OT (Operational Technology) Netzwerk häufig an das Internet angeschlossen, um Remote-Support und Firmware-Updates umzusetzen. OT-Umgebungen, die mal als geschlossene Systeme sicher vor Angriffen waren, müssen daher nun ebenfalls abgesichert werden. Während sich Monitoring-Systeme mit aktiven Scans für das IT (Information Technology) Netzwerk gut eignen, ist die Anwendung von aktiven Scans in OT-Netzwerken nicht empfehlenswert, da diese zu Ausfällen der Komponenten führen können. Passive Scans sammeln Daten ohne die OT-Komponenten zu überlasten, so dass der Betrieb der Anlage ohne Unterbrechung gewährleistet ist.

Das Monitoring- und Security-Analysetool ScanBox ist in der Lage aktive sowie passive Scans durchzuführen. So können Netzwerke der IT-Umgebung aktiv und passiv gescannt werden, während der aktive Scan für Netzwerke in der OT-Umgebung abgeschaltet ist. Auf diese Weise werden Schwachstellen in beiden Umgebungen entdeckt. Vorfälle werden automatisch in Risikostufen eingeordnet. Eine Tacho-Anzeige bildet die Risikostufen der Vorfälle ab, so dass mit einem Blick festgestellt werden kann, wie es dem Unternehmensnetzwerk gerade geht. Im Gegensatz zu reinen Analysetools werden so Bezüge der identifizierten Risiken des Unternehmens hergestellt. Nutzer erhalten konkrete Handlungsempfehlungen, deren Validität ebenfalls überprüft wird. Die empfohlenen Gegenmaßnahmen basieren auf den Empfehlungen des BSI zum IT-Grundschutz. Über die Integration der Common Vulnerabilities and Exposure (CVE) Datenbank wird ein Bezug zu den vom BSI entsprechend empfohlenen Gegenmaßnahmen hergestellt. Alle ScanBox-Komponenten kommunizieren verschlüsselt miteinander. Jeder Vorfall wird in einem integrierten Ticketsystem aufgenommmen und kann hierüber bearbeitet werden. Die Vorfälle lassen sich als Report archivieren und nachträglich offline analysieren.

Sind Sie daran interessiert, die ScanBox einzusetzen?

Um alle Rahmenbedingungen abzuklären, nehmen wir Ihre individuelle Konfiguration der Netzregeln und der Szenarien auf (z. B. welche Netzwerke gescannt werden sollen). Voraussetzung für den Einsatz der ScanBox ist ein Switch-Mirror-Port. Anhand der gesammelten Anforderungen wird eine ScanBox mit Basiskonfiguration erstellt und ausgeliefert. Diese kann kontinuierlich oder für einen bestimmten Zeitraum begrenzt eingesetzt werden.

Die ScanBox eignet sich für IT- sowie OT-Umgebungen. Gern stellen wir sie Ihnen persönlich vor.

Kontaktdaten

DECOIT® GmbH E-Mail: scanbox@decoit.de URL: www.scanbox-product.de

Funktionen der ScanBox im Überblick

■ Überwachung des Netzwerkverkehrs für IT und OT (passiver Scan)

- Mirrorports an den Switchen für Netzüberwachung
- Sammlung von Netzwerk- und Serverdaten über ScanBox-Sensoren
- Überwachung von verschiedenen Quellen, abhängig von Tageszeit und Wochentag
- Alarmierung bei unerwünschtem Netzwerkverkehr
- Regeln für den Netzwerkverkehr zwischen verschiedenen Netzen
- Sonderregeln für einzelne IP-Adressen

■ Schwachstellenscans für IT-Netzwerke (aktiver Scan)

- Umfangreiche Konfigurationsmöglichkeit der zu scannenden Netzwerke und Geräte
- Automatisierte und manuelle netzwerkweite Scans auf Schwachstellen
- Aktualisierung der Schwachstellen-Prüfroutinen (VTs) über das Internet
- Erstellen von Schwachstellen-Tickets zu jeder gefundenen Schwachstelle inkl. aktueller CVE (Common Vulnerabilities and Exposures) Informationen
- Überprüfung der Behebung der Schwachstellen durch erneuten Scan
- Anzeige von Compliance-Verletzung bei offenen Schwachstellen
- Möglichkeit den aktiven Scan in OT-Netzwerken auszuschalten

■ Integriertes Ticketsystem und Reporting

- Dashboard mit Netzwerkstatistiken: Nachvollziehbare und nachweisbare zentrale Sammlung aller sicherheitsrelevanten Informationen
- Übersichtliche Abarbeitung der gefundenen Vorfälle: Tickets Benutzern zuordnen/öffnen/schließen/Gegenmaßnahmen dokumentieren
- Nachverfolgbarkeit der getätigten Arbeiten
- Reporting mit flexiblen Ansichtstypen für die aufgenommenen Daten
- Nachträgliche Analyse der Daten, inkl. Offline-Analyse
- Archivierung als Report

Zwei starke Partner

TELCO TECH GmbH und DECOIT® GmbH bilden ein hervorragendes Team in der Bereitstellung und Entwicklung der ScanBox. Innerhalb des gleichnamigen Forschungsprojekts verwirklichten sie gemeinsam ihre Vision des „Out-of-the-Box"-Systems für eine anspruchsvolle Security-Analyse im Industrie-4.0-Umfeld.

Über TELCO TECH GmbH

Die TELCO TECH GmbH entwickelt seit 1993 IT-Sicherheitslösungen. Als einer der wenigen unabhängigen deutschen Produzenten von HighEnd Security-Systemen bietet das Unternehmen unter dem Markennamen LiSS (LAN Internet Support Station) moderne, technologisch ausgereifte Security-Appliances. Diese bieten mit neuen Sicherheitsfeatures als High Performance System die ideale Appliance für die ScanBox.

Über DECOIT® GmbH

Als Bremer IT-Systemintegrator verfügt die DECOIT® über mehr als 20 Jahre Erfahrung im Bereich IT-Sicherheit. Individuell auf Kundenwünsche zugeschnittene Lösungen bilden die Kerntätigkeit der DECOIT® in allen Abteilungen. ScanBox ist praxisnah aus der Notwendigkeit erhöhter Sicherheit in der Netzwerkabsicherung entstanden. Die DECOIT® entwickelt implementiert und betreut ganzheitliche Sicherheitskonzepte mit individuellen Komponenten.

Kontaktdaten

DECOIT® GmbH E-Mail: scanbox@decoit.de URL: www.scanbox-product.de