BELDEN

12 Gründe für NAC in OT

Ich kann nur schützen, was ich kenne

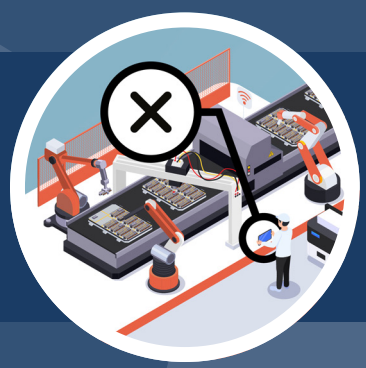
Die Übersicht und Segmentierung des gesamten Netzwerks und aller angeschlossenen Assets, unterstützt das Konzept der Sicherheitszonen.

Die Anlagenverfügbarkeit hat oberste Priorität

Ein NAC-System darf keine festen Umsetzungsstrategien vorgeben, sondern muss ausreichend Freiheiten einräumen, um den Aktionsradius eines NAC zu maximieren. Gleichzeitig darf ein NAC nicht im Widerspruch zu einer gleichbleibend hohen Anlagenverfügbarkeit stehen, um die Geschäftskontinuität zu gewährleisten.

Nachhaltige Umsetzung der Sicherheitsstrategie

Heterogene IT-/OT-Netze erfordern flexible und zukunftssichere Softwarelösungen. Ein NAC-System darf keine umfangreichen Hardware-Nachrüstungen im Netzwerk erfordern, um eine hohes Maß an Nachhaltigkeit zu erreichen.



Unerwünschte Geräte bleiben draussen

In einer gehärteten OT-Umgebung, die aus verschiedenen OT-spezifischen Geräten (z.B. Roboter, SPS) besteht, muss verhindert werden, dass unerwünschte Geräte eine Verbindung erhalten oder die Produktionsanlage negativ beeinflussen.

Erkennung von unerwünschten Netzwerkereignissen

Durch die Überwachung eines breiten Spektrums von Netzwerkereignissen wird unerwünschtes Verhalten sofort erkannt, unabhängig davon, ob es bewusst oder unbewusst verursacht wurde. Kritische Netzwerkereignisse (z. B. doppelte IP-Adressen) werden identifiziert, so dass automatisch oder manuell geeignete Gegenmaßnahmen ergriffen werden können.

Gesetzliche Anforderungen

Gesetzliche Anforderungen, wie ISO62443/ISO27001/ISO9001, erfordern eine zuverlässige Durchsetzung von Unternehmensrichtlinien und gesetzlichen Vorgaben für alle Bereiche des Netzwerks. Informationen aus angeschlossenen Lösungen können genutzt werden, um darin erkannte Bedrohungen automatisch zu isolieren.

Automatische Übertragung von Zugangsberechtigungen

Bei einem autorisierten Austausch von Endgeräten, sollten Zugangsberechtigungen sicher und dynamisch an neu einzubindende Endgeräte übertragen werden. Eine solche Veränderung muss einfach, schnell und ohne Einbindung von Netzwerkexperten möglich sein.

Compliance-Anforderungen

Die meisten OT-Assets können nicht durch herkömmliche Technologien, wie z. B. Endpoint-Security, geschützt werden, dennoch müssen auch Non-IT-Ressourcen bestimmte Compliance-Anforderungen erfüllen. Im Falle einer Kompromittierung müssen sofortige und gezielte Warnmeldungen und Reaktionen eingeleitet werden.

Zeitlich begrenzter Zugriff auf bestimmte Netzbereiche

Ein externes Unternehmen (z.B. technischer Dienstleister) benötigt für definierte Endgeräte (z.B. Notebooks, Steuergeräte) einen zeitlich begrenzten Zugriff auf ganz bestimmte Netzbereiche. Jeder darüber hinausgehende Zugriff soll automatisch unterbunden werden.

Granulare Zugriffssteuerung oder automatischer Ausschluss

Nicht autorisierte Netzwerkgeräte oder Endgeräte (z. B. private Router, nicht verwaltete Switches oder private Tablets) müssen von der Netzwerkkommunikation automatisch ausgeschlossen werden oder es muss ihnen limitierter Zugriff gewährt werden.

Lokalisierung von Geräten

Ein Handscanner oder Programmiergerät ist verloren gegangen. Es muss möglich sein, die Kommunikationshistorie eines solchen Gerätes schnell und einfach einzusehen, um in kürzester Zeit richtige und zielgenaue Maßnahmen einzuleiten.

Reduktion von Verwaltungsaufwänden

Trotz der massiven Zunahme von Bedrohungen für Netzwerke müssen Sicherheitslösungen, neben ihrer Kernfunktionalität, auch den damit verbundenen Verwaltungsaufwand klein halten, um eine hohe Akzeptanz im Unternehmen zu erhalten.

macmon nac

Übersicht Kontrolle und Sicherheit im Netzwerk