

Tosibox bietet einfache und sichere zentralisierte Zugangsverwaltungslösung für IoT-Geräte einer führenden Einzelhandelskette

Fernverbindungslösung bewältigt IT/OT-Konvergenz-Herausforderung



Herausforderung

Wie alle großen Organisationen muss auch eine Einzelhandelskette mit hunderten Verkaufsstellen externen Partnern Zugang zu ihrem IT-Netzwerk und ihren Systemen gewähren, wozu Gebäudeautomation, Kameraüberwachung, Tiefkühlgeräte, Flaschenrecyclingmaschinen und Zutrittskontrolle zählen. Wenn diese Geräte gehackt werden, drohen erhebliche Schäden. Die Einzelhandelskette musste Sicherheit gewährleisten, noch bevor es zu bedauerlichen Situationen kommen konnte.

Aus der IT-Perspektive stellt jeder Nutzer ein potenzielles Risiko dar, weshalb Fernzugriffsrechte extrem sorgfältig verwaltet werden. Allerdings erwies sich sorgfältige Zugriffsverwaltung von 2000 Geräte als extrem arbeits- und zeitintensiv, was sich chronisch negativ auf die Betriebsabläufe auswirkte.

Die Einzelhandelskette plante, ein umfassendes IoT- (Internet of Things) Sicherheitsprojekt durchzuführen. Der Einzelhandel ist mit denselben Problemen konfrontiert, die auch viele andere Branchen beherrschen: die Verbindung von Geräten, die nicht ursprünglich darauf ausgelegt wurden, Gefahren durch offene Netzwerke abzuwehren. Die Einzelhandelskette sah vor, sichere Verbindungen zu ihren Geräten herzustellen.

Lösung

TOSIBOX®-Fernverbindungstechnologie wurde zur Verbesserung der Cybersicherheit sowie zum Testen der Fernverbindungen zunächst in einigen Verkaufsstellen getestet. Anschließend wurden die Industrierouter TOSIBOX® Lock in den Läden installiert, zu denen über einen TOSIBOX® Key eine Fernverbindung hergestellt werden sollte; auf diese Weise entstand ein vollkommen sicherer VPN-Tunnel zwischen den Geräten. Tosibox half bei der Erstellung eines kontrollierten IoT-Netzwerks ständig aktiver VPN-Verbindungen für Fernwartung, kontinuierliche Überwachung, Echtzeitdatenerfassung und Datenprotokollierung.

Nach einer erfolgreichen Implementierung wurde die Lösung mühelos auf hunderte Verkaufsstellen erweitert. Dies versetzte die Einzelhandelskette in die Lage, ein Netzwerk aufzubauen, das den Herausforderungen des operativen Geschäfts gerecht wird – unabhängig von der IT. TOSIBOX® Virtual Central Lock ermöglichte die Kombination von IT- und OT-Netzwerk, ohne dass Nutzer auf Geräte oder andere Teile des Netzwerks zugreifen können, für die sie keine Zugangsrechte besitzen. Das Virtual Central Lock reduzierte den Zeitaufwand zur zentralisierten Zugangsverwaltung von Tagen auf Minuten, ermöglicht einfache Verwaltung großer Netzwerke ohne besondere IT-Kenntnisse.

Nun kann die Einzelhandelskette ein sicheres Netzwerk aus Geräten und Verkaufsstellen aufbauen, auf die sogar externe Nutzer mühelos zugreifen können – ohne Beeinträchtigung der Cybersicherheit. Dank des TOSIBOX® Virtual Central Lock können sie Sichtbarkeit und Zugriff ihrer Geräte für externe Auftragnehmer effizient begrenzen, sparen dadurch Zeit und Aufwand, während die Cybersicherheit ihrer IoT-Infrastruktur stets gewährleistet bleibt.

Vorteile

- Zugangsgruppen erstellen und verwalten: Zugang beschränken, neue Nutzer und Objekte durch einfaches Ziehen-und-Ablegen ergänzen
- IT/OT-Konvergenzprobleme behoben
- Sichere Lösung: Ein TOSIBOX® Lock schützt alle sich anschließenden Geräte.
- Unbegrenzte Erweiterbarkeit und Flexibilität

„Mit der TOSIBOX®-Lösung dauert die Verwaltung von Zugangsrechten nur wenige Minuten, während die gleiche Aufgabe bei den altmodischen IT-Netzwerken noch Tage oder sogar Wochen in Anspruch nahm.“

Tomi Liias,
Vertriebsleiter,
Tosibox Oy

Finland

sales@tosibox.com

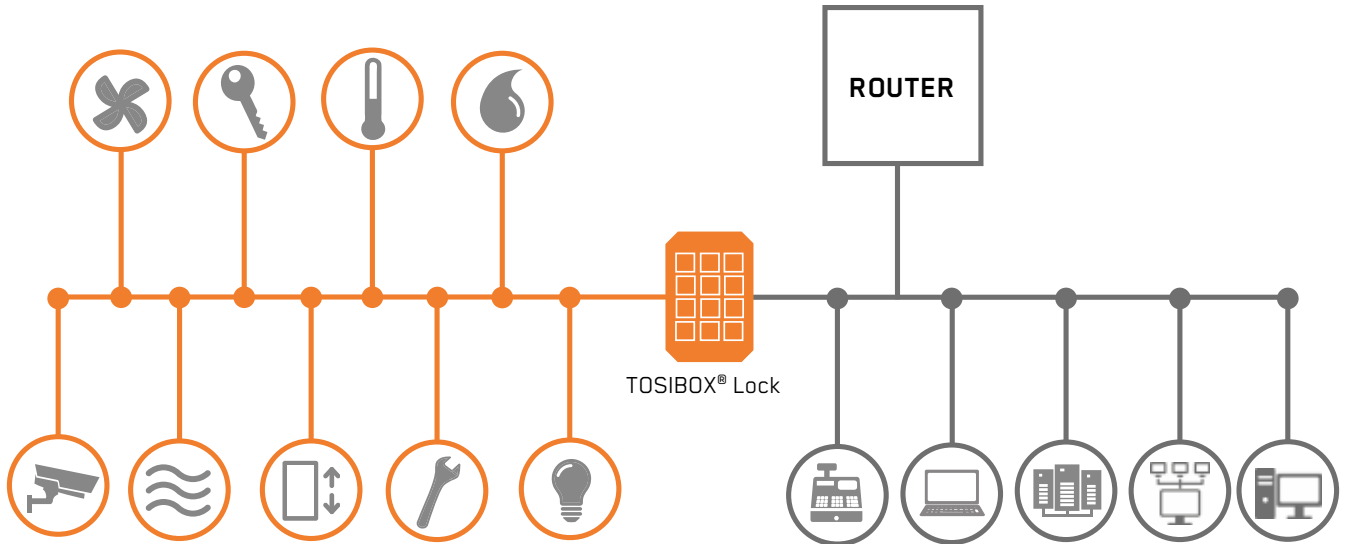
support@tosibox.com

Sales, Finland, tel. 044 709 0100

Sales, International, tel. +358 44 709 0200

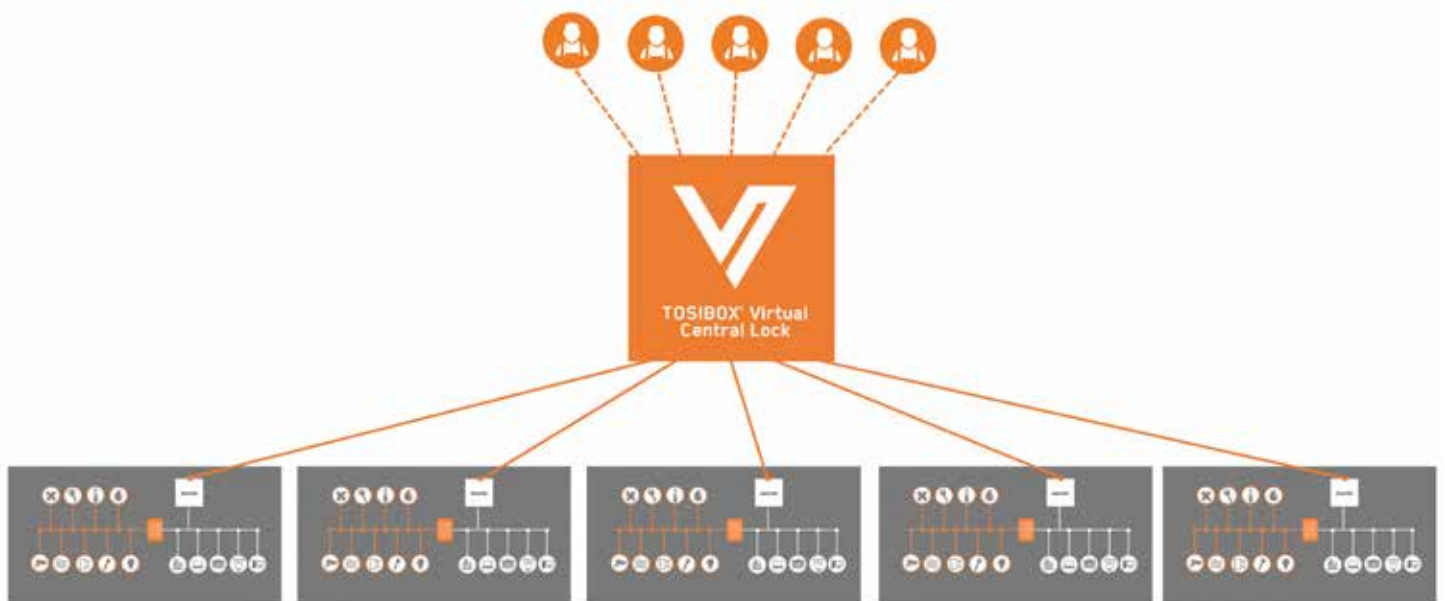
www.tosibox.com

Installationsdiagramme



Mit dem Router TOSIBOX® Lock verbundene Systeme, auf die Auftragnehmer über TOSIBOX® Key zugreifen können.

Im privaten IT-Netzwerk der Einzelhandelskette laufende Systeme.



TOSIBOX® Virtual Central Lock ermöglicht Konvergenz von IT- und OT-Netzwerken, sodass externe Nutzer nur Geräte oder Teile des Netzwerks nutzen können, für die sie zugangsberechtigt sind.