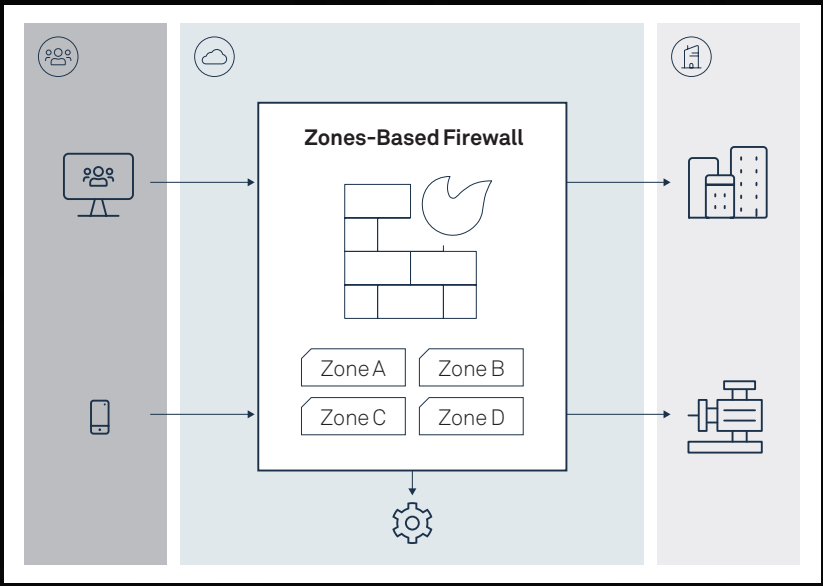
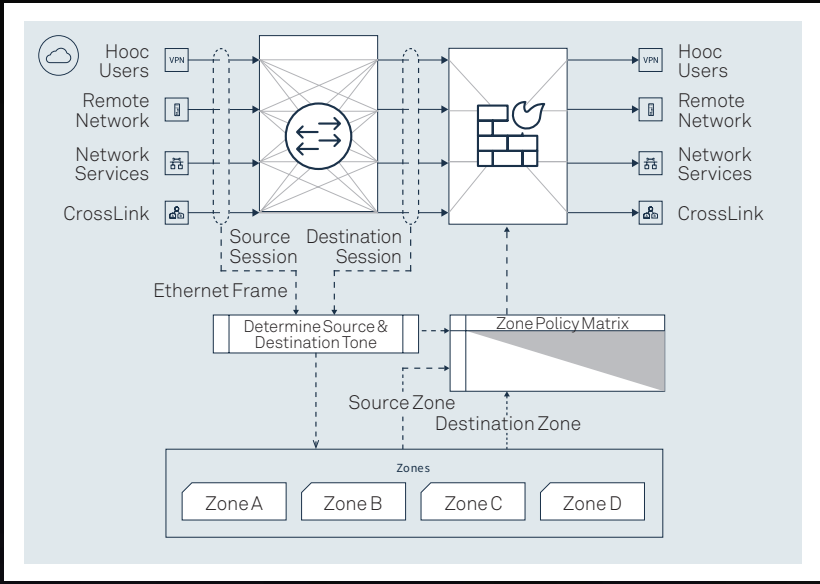
STORY HOOC AG

IST DEIN VPN-SYSTEM NOCH STATE OF THE ART?

Es ist doch so: Was in der OT-Branche vor ein paar Jahren noch State of the Art war, ist heute überholt. Viele Firmen wähnen sich dennoch auf dem neuesten Stand. HOOC bietet Lösungen, damit sie den Anschluss nicht verpassen.

HOOC AG | 8930 Visp | www.hooc.ch





Wo früher ein firmenintern aufgebautes VPN-System mit beliebigen Hardwarekomponenten genügte, braucht es heute zertifizierte Lösungen, die Zero-Trust und Mikrosegmentierung ermöglichen. Was derzeit also noch nach einem «Nice to have» klingt, wird in naher Zukunft zum Standard. Denn nicht nur der Markt, sondern auch der Staat fordert – mit Gesetzgebungen wie dem Cyber Resilience Act – maximale Sicherheit, um potenzielle Einfallstore für Cyberangriffe zu schliessen. Unternehmen, die hier nicht mithalten, verlieren nicht nur an Glaubwürdigkeit, sondern zwangsläufig auch Kunden. Damit dies nicht geschieht, liefert HOOC nicht nur innovative und einfach umsetzbare, sondern auch nach IEC 62443 4-1/4-2 zertifizierte Lösungen.

WO HERKÖMMLICHE SICHERHEITSKONZEPTE AN IHRE GRENZEN STOSSEN

In vielen Systemen erfolgt der Anlagenfernzugriff nach wie vor über Port-Forwardings, fehlende Authentifizierungen oder unverschlüsselte Verbindungen. Was bereits in geschlossenen Netzwerken problematisch sein kann, wird bei hybriden OT/IT-Infrastrukturen erst recht zum Sicherheits-

1 Eine zonenbasierte Firwall ist in alle Lösungen von HOOC integriert.

2 Genau bestimmte Zugriffsrechte sorgen für hohe Sicherheit.

risiko. Denn eine Lücke im OT-System exponiert mitunter auch das IT-System. Dabei ist den Systemintegratoren die Problematik durchaus bewusst: Was man früher einmal implementiert hat, würde man heute vielfach kaum mehr so umsetzen. Meist handelt es sich daher also um sogenannte «vergessene» Zugänge, die früher zwar nach damaligem Fachwissen korrekt realisiert worden sind, heute aber ein schwelendes Risiko darstellen, weil niemand mehr daran denkt oder sich dafür zuständig fühlt.

WANN HOOC INS SPIEL KOMMT

Um dem entgegenzuwirken, bietet HOOC neben dem verschlüsselten VPN-Fernzugriff auch ein zentralisiertes Nutzermanagement. Das macht Fernzugriffe nicht nur sicherer, sondern auch spezifischer und rückverfolgbar. Alle Zugriffsrechte sind übersichtlich gelistet und werden an einem einzigen Ort verwaltet. So geht bestimmt kein Zugang mehr verloren.

Das Motto von HOOC heisst nicht umsonst: Wir entwickeln. Immer. Weiter. Will heissen: Ausruhen auf Bestehendem «ist nicht». Um den steigenden Anforderungen im Bereich Zero-Trust-Netzwerksicherheit gerecht zu werden, hat das Unternehmen deshalb neu eine zonenbasierte Firewall (ZBF) standardmässig in seine Lösung integriert. Dabei handelt es sich um ein Sicherheitsinstrument, das Netzwerke in unterschiedliche Zonen (z. B. Lüftung, Heizung, Leittechnik) unterteilt, denen verschiedene IP-Geräte oder Ports zugewiesen werden. Mittels individuell parametrierbarer Allow- und Deny-Regelungen sowie einer übersichtlichen Matrixdarstellung können den Nutzenden die jeweiligen Zonen bzw. Geräte in einem nächsten Schritt zugewiesen werden.

WIE DAS IN DER PRAXIS AUSSIEHT

Dank den ZBF erhält also jede Person nur auf diejenigen Zonen bzw. diejenigen Anlagen und Endgeräte Zugriff, die sie betreut. In einem Industriebetrieb kann so beispielsweise der für die SPS zuständige Techniker aus der Ferne auf die Steuerung und das dazugehörende Touchpanel zugreifen, während beim Industrieroboter lediglich das Supportteam des Herstellers Zugriff hat. Will man aber nicht nur verschiedenen Nutzern anlagenspezifische Zugriffe erteilen, sondern die Netzwerke von SPS und Industrieroboter als solche komplett trennen, so kann dies durch die Aktivierung der auf dem HOOC-Gateway parametrierbaren Netzwerkschnittstelle SEP erreicht werden.

WARUM ZERO-TRUST NICHT BEI EINEM NETZWERK AUFHÖRT

In Kombination mit der standortübergreifenden Anlagenvernetzung (HOOC CrossLink) muss sich die zonenbasierte Firewall also nicht auf ein einziges Netzwerk beschränken. Beispielsweise können Immobilienbewirtschafter ihre über mehrere Standorte verteilten Gebäude über ein HOOC-Gateway in der HOOC-Cloud vernetzen und dann die zuständigen Techniker als Nutzer erfassen. Nehmen wir einmal an, dass bei den Heizungen in allen Gebäuden und Standorten die Produkte desselben Anbieters, bei den Lüftungen hingegen Produkte verschiedener Hersteller eingesetzt wurden: Mit der HOOC-Lösung hat der Heizungsinstallateur nun Zugriff auf alle Heizungsanlagen, während den verschiedenen Lüftungsanlagenbauern lediglich Zugriff auf die jeweils von ihnen betreuten Anlagen in den jeweiligen Gebäuden gewährt wird.

WER NICHT REAGIERT, VERLIERT

Heute muss also kein Unternehmen mehr eigene Sicherheitslösungen «from scratch» entwickeln: Dafür liefert HOOC die entsprechenden in Schweizer Datenzentren betriebenen und nach IEC zertifizierten Standardlösungen mit integrierten Firmware-Updates, einem Remote-Management-System und einer zonenbasierten Firewall, damit Zero-Trust auf jeden spezifischen Anwendungsfall umgemünzt und mit ein paar wenigen Klicks im HOOC Management-Portal umgesetzt werden kann. So dass sich in Sachen IT Security niemand mehr rausreden kann. Denn eines ist klar: Unwissen schützt vor Strafe – sprich: Cyberangriff – nicht.