

Netzwerk- und Sicherheitsdienste sind unabdingbar

WLAN gilt heute als unverzichtbare Erweiterung einer drahtgebundenen Vernetzung. Das effiziente Management und Monitoring mit AI sollte genauso selbstverständlich sein, fordert Thomas Wehrich von der Wehrich Informatik GmbH aus Kreuzlingen.



Thomas Wehrich:
Sicherheit verbessern.

Längst gehören fixe Arbeitsplätze nicht mehr zum Regelfall. Das mobile WLAN wird dabei als unverzichtbare Erweiterung einer drahtgebundenen Vernetzung vorausgesetzt.

Eine WLAN-Erweiterung oder Erneuerung des Netzwerkes unterstützt den Unternehmenserfolg dann, wenn im Vorfeld die genauen Bedürfnisse ermittelt werden. Moderne WLAN-Lösungen basieren auf dem WiFi-6-Standard und einer Gigabit-Netzwerkinfrastruktur mit einer Bandbreite mit bis zu 10 Gbit/s.

Klarsicht statt Blindflug

Genauso selbstverständlich wie eine gut verfügbare und sichere LAN/WLAN-Struktur sollte ein effizientes Management der eingesetzten Geräte sein. Doch: Viele Unternehmen führen immer noch manuelle Inventarlisten, und auch die Wartung, das Beheben von Störungen und das Überwachen der Sicherheit werden vielerorts noch manuell durchgeführt.

Um die Kosten für den Betrieb und Unterhalt des IT-Systems zu optimieren sowie Sicherheit und Verfügbarkeit der Dienste zu steigern, gibt es seit längerer Zeit Software-Lösungen, die bisher manuell ausgeführte Tätigkeiten automatisieren und in Echtzeit relevante Kenngrössen ausweisen. Ein umfassendes, sich automatisch aktualisierendes Inventar ist dabei ein willkommenes Nebenprodukt solcher Lösungen zur Verwaltung von Arbeitsplätzen, Servern und Netzwerken («Managed-Workplace-Lösungen»).

Kern der Lösung ist die proaktive Echtzeit-Überwachung aller integrierten Komponenten wie Server, Arbeitsplätze, Switches, WLAN, Firewalls oder Drucker. Beim Erreichen von vordefinierten Schwellwerten werden Alarmer ausgelöst. In regelmässigen Abständen erstellt die Managed-Workplace-Lösung Berichte, Fehler werden konsequent protokolliert und regelmässig erforderliche Bereinigungen und Optimierungen der Systeme automatisch ausgeführt.

Auswertung und Beurteilung der Sicherheit einer EDV-Anlage werden anhand von Vergleichswerten und teils auf künstlicher Intelligenz basierenden Analysemethoden erstellt und mit Charts sichtbar gemacht. Gleichzeitig werden geeignete Massnahmen zur Verbesserung der Sicherheit aufgezeigt.

Autopilot mit AI anstelle Sichtflug mit Risiko

In den letzten Jahren hat sich der Einsatz von Virenschutzlösungen auch im KMU-Umfeld etabliert. Diese EDR-Sicherheitslösungen basieren auf meist lokalen Funktionen, die einen ungewollten Zugriff anhand eines Regelwerkes verhindern.

In grösseren Unternehmungen gehören komplexe Überwachungs- und Managementwerkzeuge wie SIEM (Security Information and Event Management) und SOAR (Security Orchestration, Automation and Response) seit einiger Zeit zum Standard. Solche Lösungen zur Risikominimierung bereitzustellen und zu betreiben, überstieg bis vor Kurzem die Möglichkeiten eines KMU-Betriebes – werden aber benötigt, da auch kleinere KMU-Betriebe von Cyber-Attacken betroffen sind.

Um Wahrscheinlichkeit und Folgen einer Attacke zu reduzieren, stehen heute auch für KMU Lösungen als Dienst zur Verfügung, wie diese in grossen Unternehmungen eingesetzt werden. Basis bildet dazu eine weiterentwickelte XDR-Virenschutzlösung, kombiniert mit einem Security Operation Center (SOC). Ihr IT-Dienstleister installiert und betreibt diese Lösung in Kooperation mit dem Hersteller und kann so auch einem KMU Funktion und Dienstleistung eines Security Operation Center (SOC) mit SIEM- und SOAR-Diensten 7×24 h zur Verfügung stellen.

Text: Stephan Ziegler
Bild: zVg