Referenz

Bell AG

secured by ARP-GUARD

IT-Sicherheit und Fremd-hardwareerkennung bei Bell machen den Fleischgenuss noch sicherer

Seit über 130 Jahren steht die Marke Bell AG für Genuss und Top-Qualität ihrer Erzeugnisse. Am Anfang stand eine kleine Metzgerei, heute ist die Firma Bell AG der mit Abstand größte Fleischverarbeiter der Schweiz. Dies bestätigt auch der große Bekanntheitsgrad der Marke Bell: Über 90% der Schweizer Bevölkerung kennen das Basler Traditionsunternehmen. Jährlich werden dabei 130.000 Tonnen Fleisch verarbeitet und statistisch gesehen rund 50 Bell Produkte pro Sekunde in der Schweiz verkauft.

Fremde Geräte im Netzwerk – Aber nicht bei Bell

Im Zuge eines kontinuierlichen Ausbaus der betriebseigenen Infrastrukturen, im Hauptsitz, aber auch in den Außenstellen und verteilten Produktionsstätten, wurde als wichtiger Bestandteil jeder Infrastruktur ein erhöhtes Augenmerk auf die eigene IT-Sicherheit gelegt. Neben bereits vorhandenen Firewall-Lösungen sollten, unabhängig vom Gerät oder Betriebssystem, neu angeschlossene oder nicht konforme Gerätschaften im Netzwerk erkannt und entsprechend behandelt werden können. „Bei unseren weit verteilten Produktions- und Lagerstellen und den verschiedensten mobilen, aber auch kabelgebundenen Systemen, benötigen wir einen absolut verlässlichen und unkomplizierten Schutz, welcher leicht anzupassen und zu verwalten ist“, äußert Peter Kunimünch, Leiter IC der Bell Gruppe seine Wunschvorstellung. „Dabei sollen die Netzwerkzugänge möglichst granular zur Verfügung stehen, um auch externen Dienstleistern oder Besuchern, zum Beispiel in Sitzungszimmern, einen verwendbaren, wenn auch eingeschränkten Zugang zu ermöglichen.“

ARP GUARD by ISL

ARP-GUARD Network Access Control (NAC) – Eine einfache Entscheidung

Nach einer intensiven Evaluationsphase, zusammen mit dem Walliseller IT-Sicherheitsspezialisten Omicron AG als Projekt- und Implementierungspartner, fiel der Entscheid einstimmig auf die durchwegs durchdachte Lösung ARP-GUARD. „Dabei überzeugten neben den Sicherheitsfunktionen speziell die einfache Implementierung und Verwaltung, aber auch der hochverfügbare und performante Betrieb der Network Access Control (NAC) Appliance den Fleischverarbeiter Bell“ meint Thomas Stutz, CEO des Schweizer IT-Sicherheitsdienstleisters Omicron AG. „Aber auch heutige und zukünftige Compliance Anforderungen werden damit adressiert und durch starke Reporting-funktionalitäten unterstützt, denn nur richtlinienkonformen Geräten wird der Zugang zum Firmennetzwerk überhaupt gewährt“, ergänzt Thomas Stutz.

Den Härtetest im Praxiseinsatz bestanden

Mit dem hochwirksamen System ARP-GUARD hat Omicron als Schweizer Partner einen aktiven und hochverfügbaren Schutzschild gegen fremde, nicht autorisierte Geräte, aber auch vor internen Angriffen erarbeitet und erfolgreich implementiert. „Weder WLAN- noch direkt am Netzwerk angeschlossene Geräte finden, ohne explizite Erlaubnis, den Weg ins Bell Firmennetz“, erklärt Thomas Stutz, CEO der Omicron AG. „Die Network Access Control (NAC) Lösung ARP-GUARD erkennt und verhindert in Echtzeit den Zugriff und meldet bei Bedarf den unerwünschten Anschlussversuch. Die somit geschlossenen Sicherheitslücken können bisweilen weder von üblichen Firewalls noch von Intrusion Detection Systemen geschlossen werden. Ein weiteres Merkmal des hohen Qualitäts- und Sicherheitsbewusstseins der Firma Bell“, fügt Thomas Stutz von Omicron hinzu. „ARP-GUARD lässt sich ohne Probleme und mit geringem Zeitaufwand implementieren und produktiv schalten“, ergänzt Peter Kunimünch von Bell. „Verglichen mit anderen Lösungen, welche langwierige Installationen und Konfigurationen für einen optimalen Betrieb mit sich bringen, ein absoluter Pluspunkt“, stellt Peter Kunimünch zufrieden fest.

Neue Services und zukünftige Geräte können kommen

Nach den ersten Erkenntnissen kann, neben der markant verstärkten Sicherheit, die Visibilität der Gerätschaften im ganzen Netzwerk markant erhöht und das interne Inventarsystem besser vervollständigt und überprüft werden. Stark reduziert wurden nebenbei die Zeitaufwände für reaktive Eingriffe durch bessere, transparente Informationen - wer, wie, wann und wo am Netzwerk angeschlossen ist. „Die im Einsatz stehende ARP-GUARD Lösung lässt uns optimistisch auf neue Netzwerkservices wie zum Beispiel der IP-Telefonie, mit vielen neuen Endgeräten, blicken. Einer weiteren Expansion unserer Infrastruktur in puncto Quantität und Qualität steht somit nichts mehr im Wege“, erklärt Peter Kunimünch.