Success Story

Bell AG

secured by ARP-GUARD

Cybersecurity e rilevamento di dispositivi sconosciuti rendono la produzione di carne di Bell ancora più sicura

Da oltre 130 anni il marchio Bell AG è sinonimo di qualità eccellente dei suoi prodotti. Quella che era una piccola macelleria è oggi l'azienda Bell AG, di gran lunga il più grande produttore di carne in Svizzera. Lo conferma anche la grande notorietà del marchio Bell: oltre il 90% della popolazione svizzera conosce l'azienda tradizionale di Basilea. Ogni anno vengono prodotte 130.000 tonnellate di carne e, secondo le statistiche, nel Paese vengono venduti circa 50 prodotti Bell al secondo.

Riconoscere e gestire gli accessi di dispositivi sconosciuti presso Bell

Nell'ambito di un'espansione continua delle infrastrutture aziendali, sia nella sede centrale che nelle sedi esterne e negli impianti di produzione distribuiti sul territorio, è stata posta una maggiore attenzione alla sicurezza IT interna. Oltre alle soluzioni firewall già esistenti, era necessario riconoscere e gestire correttamente gli accessi da parte di dispositivi sconosciuti o non conformi, indipendentemente dal tipo di dispositivo o dal sistema operativo. „Nelle nostre sedi di produzione e stoccaggio distribuite in maniera capillare e che utilizzano vari sistemi mobili e cablati, abbiamo bisogno di una protezione assolutamente affidabile e semplice da adattare e gestire", afferma Peter Kunimünch, direttore IT del gruppo Bell. „Inoltre, gli accessi alla rete devono essere forniti in maniera più granulare possibile, per consentire anche a persone esterne (ad es. fornitori o collaboratori) di poter accedere alla rete in maniera sicura e con accessi specifici".

ARP GUARD by ISL

ARP-GUARD Network Access Control (NAC): una decisione semplice

Dopo un'intensa fase di valutazione insieme allo specialista di cybersecurity Omicron AG (in qualità di partner per il progetto e l'implementazione) la decisione è stata presa all'unanimità a favore della soluzione ARP-GUARD, una soluzione ben pensata in ogni aspetto. „A convincere Bell, oltre alle funzionalità di sicurezza, sono state in particolare la semplicità di implementazione e di gestione, così come il funzionamento ad alta disponibilità e prestazioni dell'appliance di ARP-GUARD", afferma Thomas Stutz, CEO del fornitore svizzero di servizi di cybersecurity Omicron AG. „Inoltre, ARP-GUARD soddisfa i requisiti di conformità attuali e futuri grazie a potenti funzionalità di reporting, poiché solo ai dispositivi conformi alle normative viene concesso l'accesso alla rete aziendale", aggiunge Thomas Stutz.

Il test di resistenza superato con successo

Con il sistema di ARP-GUARD, Omicron, in qualità di partner, è riuscito a creare e implementare con successo uno scudo protettivo attivo e altamente disponibile contro dispositivi sconosciuti non autorizzati, nonché contro attacchi interni. „Né i dispositivi collegati via WLAN né quelli collegati direttamente alla rete trovano accesso alla rete aziendale di Bell senza autorizzazione esplicita“, spiega Thomas Stutz, CEO di Omicron AG. „La soluzione di Network Access Control (NAC) ARP-GUARD rileva e impedisce in tempo reale l'accesso ai dispositivi non autorizzati e segnala, se necessario, il tentativo di connessione da parte di questi. Le lacune di sicurezza colmate grazie ad ARP-GUARD non possono essere risolte né dalle firewall tradizionali né dai sistemi di Intrusion Detection. Un'altra dimostrazione dell'elevata consapevolezza della qualità e della sicurezza dell'azienda Bell“, aggiunge Thomas Stutz di Omicron. „ARP-GUARD può essere implementato senza problemi e con un dispendio minimo di tempo“, aggiunge Peter Kunimünch di Bell. „Rispetto ad altre soluzioni, che richiedono installazioni e configurazioni lunghe per un funzionamento ottimale, questo è un punto assolutamente a favore“, afferma soddisfatto Peter Kunimünch.

L'espansione dell'infrastruttura non è più un problema

Secondo i primi risultati, oltre ad una sicurezza notevolmente rafforzata, è stato possibile aumentare in modo significativo la visibilità dei dispositivi connessi alla rete, e completare e monitorare meglio il sistema di gestione dell'inventario interno. Contemporaneamente, i tempi di intervento reattivo sono stati notevolmente ridotti grazie ad informazioni migliori e più trasparenti su chi, come, quando e dove si è collegato alla rete. „La soluzione ARP-GUARD che abbiamo in uso ci consente di guardare con ottimismo a nuovi servizi di rete, come ad es. la telefonia IP con numerosi nuovi dispositivi. Non c'è quindi nulla che ostacoli un'ulteriore espansione della nostra infrastruttura in termini di quantità e qualità“, conclude Peter Kunimünch.