aruba
a Hewlett Packard Enterprise company

AT A GLANCE

MODERNIZING CYBERSECURITY IN HOSPITALITY

The hospitality industry has seen an increasing number of brazen cyberattacks in the past few years. Recently, a massive cyberattack at an international chain compromised personal information of nearly 400 million guests[1] including birthdates, passport and credit card information. These stolen details can become highly lucrative as they provide the necessary foundation to launch identity theft scams, phishing attempts, and a variety of financial and other cyberattacks at individuals and organizations.

BROAD ATTACK SURFACE

When addressing IT strategies, hospitality organizations globally are faced with new security and connectivity challenges. Millions of new connected devices are being added to the network every day and guests expect to connect with not just phones and PCs. The explosion of these unpredictable device types renders manual device profiling techniques inadequate and makes automation a key requirement for securing users and devices. To add to the complexity, many IoT devices are often connected to disparate overlay networks that typically support only one type of connectivity, such as Wi-Fi, Bluetooth or Zigbee. All this widens the attack surface and makes the infrastructure more difficult to secure.

CLOSING THE GAPS

Although the hospitality industry is increasing investments in cybersecurity, recent breach statistics suggest there are opportunities for improvement to stay ahead of threats.

Let's investigate how modern security solutions from Aruba can help hospitality vendors better:

- Gain visibility into everything connected to both wired and wireless networks
- Ensure that the appropriate IT access policies are applied to users and devices

Hotels are not known for being obvious cyberattack targets as hackers prefer financial or retail institutions, but the user data held by many hotels make them much more valuable. Known hacks have utilized electronic door locks, POS systems, Wi-Fi, and in one reported case, even a connected aquarium to hijack a casino's internal networks in search of corporate data[2].

Cyberattack incidents include:

- Phishing attacks and network breaches resulting in the disclosure of personal data
- Ransomware attacks
- DoS attacks
- Other cyber incidents resulting in disruptions and unauthorized disclosures

SECURE INFRASTRUCTURE

Aruba Secure Solutions for Hospitality

For over 15 years, Aruba has delivered high performance networks that include many built-in security features.

- The newest Wi-Fi certified protocol WPA3™ was co-authored by Aruba experts and delivers a range of security and ease of use features.
- Secure boot delivers anti-tampering features for access points.
- Military grade encryption and VPN ensure traffic is secure.
- The Aruba Policy Enforcement Firewall (PEF) enables user/application visibility and policy enforcement based upon user, role, application, device and location.

[1] Hotel News Now, Timeline: The growing number of hotel data breaches
[2] The Hotel Hackers Are Hiding in the Remote Control Curtains
[3] Marriott Faces $123 Million Fine For 2018 Mega-Breach

ACCESS CONTROLS

Security starts with visibility of who and what is connected to your network and what they are doing on the network at all times.

- **Know What is on the Network**
  Today, many IoT devices are built on standard hardware platforms. That can make it extremely difficult to know exactly what is on your network. For example, a security camera and smart thermostat could both be built on the same Linux platform. ClearPass Device Insight uses machine learning to identify devices based on multiple attributes, traffic destination, and communication frequency. Knowing what is on the network is the first step in protecting it.
- **"Zero Trust" Access to the Network**
  Aruba ClearPass NAC (Network Access Control) delivers discovery, profiling, authentication and authorization of users, their devices and IoT devices before letting them on the network or giving them access to IT resources. These pre-admission controls are critical because cybercriminals are adept at quickly advancing and moving laterally within seconds after gaining access to a network.
- **Precise Control of Access to IT Resources and Assets**
  ClearPass provides adaptive, granular policy-based access controls by user, device, role and location, including for applications. These controls ensure that each user, device or IoT only has access to the network and IT resources and assets they are approved for.
- **Intelligent Segmentation**
  Aruba Dynamic Segmentation leverages the Aruba secure infrastructure, PEF and ClearPass Policy Manager to deliver a network edge that securely isolates and separates user and device traffic across wired and wireless network.

NEXT STEPS FOR A HEALTHIER SECURITY POSTURE

With advanced access controls and interoperability with over 140 multi-vendor network and security solutions, you can rest assured with the visibility and confidence that your security posture is in a much healthier state.

LEARN MORE

https://www.arubanetworks.com/solutions/hospitality/

aruba
a Hewlett Packard Enterprise company

AAG_SecurityInHospitality_SK_012920 a00090830enw