Centralized security

Jonathan Stone, aviation solutions division manager at Leidos, explains the importance of bridging the gap between data rights, privacy and open architecture in relation to cybersecurity

ACCORDING TO EASA, **1,000 CYBERATTACKS** HAPPEN AT AIRPORTS EVERY MONTH

From flight information displays to passenger wayfinding, the airport experience is becoming increasingly digital

The aviation industry has benefited from digital modernization technologies across the airport to ensure that travel is safe and efficient for all passengers. Security checkpoints have continued to evolve over the past two decades as new threats arise, and as operational efficiency and throughput requirements change. Computed tomography (CT), artificial intelligence (AI) and facial recognition are examples of emerging technology investments we will see from airports in the coming years.

However, keeping up with the latest technology isn't enough; airports also have a growing need to integrate disparate solutions across the entire checkpoint to gain access to actionable operational data. This risk-based approach to security operations includes x-ray screening devices and other integrated checkpoint technologies that enable data analysis from multiple sources. With the addition of AI-based algorithms and predictive analysis, airports will have a more comprehensive understanding of emerging threats and the best ways to prevent them. Incorporating biometrics – facial recognition, for example – and correlating passengers' belongings have powerful implications. Accomplishing this while being mindful of passengers' rights with respect to privacy is a challenge.

The aviation market, with its network of vendors, suppliers and partners, is frequently targeted by cyber intruders. In fact, a study conducted by the European Aviation Security Agency (EASA) found that an average of 1,000 airport cyberattacks occur every month. The shift to integrated, enterprise solutions will add more challenges for airports when managing cybersecurity vulnerabilities.

Typically powered by open architecture web services, these risk-based security solutions often involve multiple third-party entities sharing operational data components in a single integrated system. As such, airports will be relying on each entity to manage cybersecurity vulnerabilities, as a breach in one component could compromise the entire integrated system.

Airports must partner with third parties that invest in and maintain core technical capabilities, ensuring the solutions provided can meet market demands and solve common technology challenges, while also protecting privacy and data. This is true regardless of the system in question – ticketing, point-of-sale terminals, parking systems, security checkpoints, baggage handling, wi-fi, etc. It is vital that these critical functions have cybersecurity as a core capability within the solution's overall infrastructure. Innovation and cybersecurity go hand in hand.

As cybersecurity is more important, and more complex, than ever, full-spectrum cyber will soon become critical to effective business operations. Full-spectrum cyber combines offense, defense and cyber-physical systems that are adaptive and capable of sustaining threat protection to effectively outpace adversaries. Advanced analytics, AI and machine-learning techniques are essential to this approach to dramatically reduce the time it takes to detect a breach, enhance decision making, and better predict and prevent events before they occur.

At Leidos, technical excellence, cyber operations, digital modernization, and integrated and mission software systems are critical to the business and the work the company does daily to help its aviation customers meet their business needs.

Passenger Terminal EXPO 2022 EXHIBITOR BOOTH Z2.4060

Mosaic, an enterprise network solution that adheres to Leidos's strict privacy and data security policies, as well as international standards, provides a holistic checkpoint by integrating all security components into a single system. It leverages an open architecture of plug-and-play integration, supports the integration of third-party technologies when additional security layers are needed, has remote screening options, and is cloud ready with containerized management and enterprise scalability.

With real-time data being available to decision makers throughout the passenger experience, Mosaic's modular design provides a scalable approach to high-security checkpoint facilities of any size. Airports can eliminate manual data aggregation across multiple pieces of equipment, as Mosaic does this automatically through detailed insights and analytics around both the people and baggage screening processes. Centralized data storage, operator actions, training data and profiles, along with other business intelligence data, help airports improve public safety and increase throughput and efficiency, while providing a seamless travel experience from curb to gate. ■

Leidos
READER INQUIRY 102