UNISYS | Securing Your Tomorrow®

A HOLISTIC APPROACH TO AIRPORT SECURITY

ABOUT THE AUTHORS

Ashwin Pal: *Ashwin has over 20 years' experience in the IT security industry in Asia Pacific. He is passionate about cybersecurity and is a sought after cybersecurity expert.*

Venkatasubramanian Viswanathan: *Venkat is a senior airport applications SME with Unisys, Singapore. Venkat has been developing and delivering solutions for multiple airport/airline industry customers across APAC.*

Ajay Prabhakar: *Ajay is the Industry Manager and SME for Airports Passenger Facilitation in Unisys APAC. He is responsible for developing new solutions for passengers and is a blogger and a thought leader in airports passenger domain.*

More travelers than ever rely on air travel to reach their destinations. To meet growing demand, airports are evolving their operations to increase efficiencies and provide a top-notch passenger experience. Airports are integrating growing numbers and types of diverse systems into their networks to address operational challenges and streamline internal operations. They are also adopting ever more passenger-facing systems to streamline and improve the passenger experience. These solutions are a complex combination of heterogeneous physical, IT and OT systems from many vendors that increasingly span both on-premises and the cloud.

The complexity of today's airport systems opens up ever-increasing security vulnerabilities. One stolen password or colluding insider can give a bad actor unauthorized access to systems across the network or a restricted zone in the airport. Converged IT/OT systems open up still more entry points. Coexisting automated and manual processes within the same airport facility can lead to different handling procedures that cause security gaps. At the same time, airports must provide airport staff, baggage handlers, caterers and other partners different levels of access to airport systems to perform their jobs; security challenges can result when these levels are not clearly defined and implemented.

When security attacks strike at these vulnerabilities, hackers can steal sensitive data, disrupt airport systems or delay flights. Impacts can even reach beyond airport boundaries with severe security breaches having the potential to affect national security.

Gaps in Existing Security Solutions

Today, airport security is typically unable to address security vulnerabilities that arise from all this complexity in a comprehensive manner. Airports often rely on a vast array of discrete security solutions to protect their physical, IT and OT systems. Agencies provide security personnel. Point solutions secure individual IT solutions and manufacturers provide patches for OT systems. Use of these discrete security solutions leaves openings that malicious insiders or outsiders can exploit.

Disparate, disjointed security solutions put the odds squarely in the malicious actors' favor. Hackers simply need to find one opening in one forgotten corner of the network to slip into airport systems while airports must get security right every time. Once an attacker has successfully achieved entry, they can move across the network, gaining unauthorized access to any number of secure physical areas or to IT and OT systems.

The Need for a Comprehensive Airport Security Solution

What airports need to close the gaps and minimize vulnerabilities is a holistic, end-to-end approach to security IT, OT and physical systems in airports. Such a comprehensive approach starts with a thorough understanding of the IT, OT and physical systems the airport employs and the vulnerabilities they are likely to contain.

A suggested approach for securing airport systems in a comprehensive manner is for airports to prepare for the entire predict-protect-detect-response cycle.

To comprehend the IT landscape, airports must survey and map out exactly what IT systems they have in their environment. This includes identifying any, and all software applications, network infrastructure (including servers, firewalls, gateways and routers), IoT devices, user devices such as barcode scanners, smartphones, and more. Airports must then identify what security solutions are already in place and evaluate how secure the environment is and where vulnerabilities exist.

OT systems are largely designed by engineers with no background in IT. They typically do not incorporate as many security measures as IT solutions nor is OT patching as robust. Moreover, because many OT systems are proprietary, they cannot support standard IT security measures, such as anti-virus software. As OT systems proliferate, airports must ensure the same level of security for these solutions as they do for their IT systems. This means keeping up to date on patches and ensuring that appropriate identity and access management controls—including authentication, authorization, access control and so on are applied to OT environments.

While physical systems such as cameras, physical access control systems, body scanners and ID cards were once strictly analog, they are now converging with IT. For example, not only do surveillance systems include cameras, they might also include facial recognition, unidentified baggage detection or crowd detection while access is now controlled by electronic cards and badges run by IT. That means instead of breaking a lock with a hammer, criminals can break into an IT system to get a badge and then use it to access the baggage area where they can slip a bomb into someone's luggage. With all of these physical systems running on IT networks, airports now need to be able to secure, patch and ensure that vulnerabilities from physical systems are not propagating into other connected networks.

The Way Forward

A suggested approach for securing airport systems in a comprehensive manner is for airports to prepare for the entire predict-protect-detect-response cycle. In essence, this approach comprises of the following four steps:

- Predict – systems, tools, policies and procedures which help detect vulnerabilities and predict potential avenues of attack.
- Prevent – systems, tools, policies and procedures that prevent threats affecting your systems, for example, the corporate firewall.
- Detect – systems, tools, policies and procedures that enable you to detect threats that may be affecting your system such as the Intrusion Detection System.
- Respond – systems, tools, policies and procedures that allow you to respond to threats and contain/eradicate them. An example would be the corporate Incident Response Plan and associated tools such as a Security Information and Event Management (SIEM) system.

This simple methodology helps drive airport security in many ways. To begin with, once we start to understand who is trying to attack us based on threat intelligence and how, based on an attack methodology, we can start to add the necessary context to the security investments required. This will aid in prioritizing and justifying the investments.

No two airports are alike, and no single security solution will fit them all. To understand how to implement the predict-protect-detect-response cycle in their own IT, OT and physical environments, airports need the right partner who demonstrates deep expertise all the relevant technologies and has a depth of airport and aviation domain expertise and the unique insights that entails.

With an understanding of security priorities, airports can protect their most vulnerable systems, and then extend these safeguards across the network. The aim is to reduce the attack surface across all IT, OT, and physical systems both on-premises and in the cloud, stop attacks on unpatched OT/IT systems, establish and enforce the identity of all staff and their devices as well as guard devices from malware attacks.

Of course, in the real world, attacks are bound to occur despite an airport's best-laid cybersecurity plans. To be truly cyber resilient in the face of an actual attack, airports need to be able to detect any attacks, and then isolate critical data, systems and rogue users to reduce exposure and threat impact.

Finally, airports must then be prepared to minimize the operational impact of attacks by reducing response time. They can accomplish that objective by continually assessing the threat environment to identify new risks and improve security posture. They should also automatically adapt policies to contain damage and protect critical systems and data.

Conclusion

No two airports are alike, and no single security solution will fit them all. To understand how to implement the predict-protect-detect-response cycle in their own IT, OT and physical environments, airports need the right partner who demonstrates deep expertise all the relevant technologies and has a depth of airport and aviation domain expertise and the unique insights that entails. Such a partner can understand the threats and vulnerabilities the airport faces, and work with the airport to secure them. The partner must then support the airport as it performs everything from developing the architecture and strategy to implementing and configuring the security technology to managing and supporting all applicable systems, truly enabling an airport to realize the vision of smart and secure airports for the modern traveler.

Ready for the next step towards securing your airport from the physical and cyber threats of today? Visit www.unisys.com/smartsecureairports to explore assessments and additional content or connect with Unisys at unisysapac@unisys.com to take this conversation forward.

For more information visit www.unisys.com