PUBLICATION

Power Outage Shows Unique Risks for Airport Cybersecurity

Authors: Thomas H. Barnard
June 22, 2017

On May 27, 2017, thousands of British Airways passengers across the globe were stranded when a simple power failure took down critical systems, including those used to check in passengers. As images of crowded terminals and angry complaints spread across social media, British Airways CEO Alex Cruz released a video apology in an effort to manage the harm to his company's reputation as his airline was forced to cancel flights and refund millions of dollars in erstwhile revenue. British Airways assured the public that at no point were any passengers in harm's way, nor was there any evidence of any malicious activity. The story faded from the public discourse after less than a week. This follows similar issues for several U.S. based airlines over the last year.

What this demonstrates, however, is how wide-reaching the impact can be of what turned out to be nothing more than either the failure of a power supply or a simple human error. This should be cause for alarm and inspire every company to take a long, hard look at their infrastructure. While the cause of the power system failure that struck British Airways was seemingly innocuous, control systems are often the weakest link in a company's security plan, and they are particularly vulnerable to malicious cyber-attacks. In an airport setting, the impact of such an attack targeting something as simple as a power supply can be catastrophic.

It is impossible to imagine British Airways or any other company with a global footprint operating without utilizing the Internet as a part of its infrastructure. The challenges to operate across distances without it are insurmountable. However, it is of vital importance to know in what ways leaving control systems open to remote access can create vulnerability to cyber-attack.

Most control systems employed not only by companies but by governments and public utilities are now organized within an architectural framework called Supervisory Control and Data Acquisition (SCADA). SCADA can simply be thought of as a way of organizing infrastructure control such that there is one central management point, often accessible via the Internet, that can remotely control a variety of networked modules, often from different manufacturers and controlling a wide array of different systems. While there are numerous benefits conferred by this approach, the SCADA approach is also unfortunately a prime target for a cyber-attack.

The risk of these SCADA systems is that their centralized nature multiplies the potential risk of a cyber intrusion. While there are steps that can be taken to improve security, (limiting access via VPN, for example), the central fact of the single failure point is unavoidable as it is intrinsic to the approach.

This may seem like a non-traditional form of cybersecurity risk. However, it is not hard to imagine how an attack to control the availability of power to an airport may be used in combination with ransomware to make demands from its executives or government agencies. This was a contemplated risk as early as 1990, when the action thriller *Die Hard 2* was released with a similar threat. Frighteningly, innovations in the capabilities of cyber-attacks suggest that the most dated aspect of that movie's plot is that such a scheme could now be attempted without an armed invasion force.

Traditional cybersecurity efforts are often focused only on data, and those efforts are obviously critical, but cybersecurity event planning cannot end there. SCADA attacks are far from an abstract concept or something to start worrying about in the future. Such attacks were already able to successfully set back Iran's nuclear research program by years, and the world's militaries consider such attacks so critical to overall mission support that they have created rules of war specifically addressing their usage.

While the power supply failure which impacted British Airways in May was not the result of a cyber-attack, such an attack is entirely plausible. If your airport is not already including its control systems and those of its vendors in its overall cybersecurity planning, you must commence such planning immediately. It is well within the capabilities of many potential malicious actors to directly attack power infrastructure in ways that can have devastating consequences. As British Airways learned, the failure of one simple power supply can lead to millions of dollars in lost revenue. It should be clear to us all that the importance of such planning cannot be overstated.

The American Association of Airport Executives is hosting an innovation and cybersecurity discussion on July 12 – 14 in Seattle, Washington. These and other topics unique to the utilization of technology at airports will be discussed by numerous experts. Additional information can be found on the association's website at www.aaae.org. Readers can take advantage of a discount code for $100 off current registration rates by entering the promo code CYBER2017.

If you have any questions regarding the content of this alert, please reach out to Thomas Barnard or any member of the Firm's Data Protection, Privacy and Cybersecurity Group.