CASE STUDY

Helping a Major U.S. Airport Outmaneuver Cybercriminals

Black Box engineers hampered a ransomware attack and ensured public confidence

INDUSTRY

Transportation (Airline).

SUMMARY

A large, U.S., international airport was the victim of a ransomware attack affecting the business side of the operation. The malware entered the airport's information systems via a phishing scam. As it took hold, the infection locked down email, payroll, and digital records - including flight and baggage information screens - which went ominously dark and had the potential to shake public confidence.

Wisely refusing the pay the ransom, but unsure what to do next, airport personnel called Black Box, a trusted airport contractor, for help. Quickly, our technical team was on-site to provide expertise and reassurance.

In two phases, Black Box engineers isolated the infection, secured the network against further attacks, and restored data information systems. Then they set about the larger task of optimizing the network by designing an upgraded data center environment, including servers and switches.

While confidential, the resulting value (visible and hidden) was significant. More importantly, the network continues to be resilient to a barrage of additional attacks since the initial assault.

CHALLENGE

Secure the network quickly and rebuild optimally

Panicked by a network that was running smoothly one moment and shut down the next, airport IT personnel lacked the resources to navigate a ransomware assault on their own. They needed technical know-how from experts who were not intimidated by cybercriminals and could not only solve the problem fast, before it became a media story, but also ensure it didn't happen again. Complicating this challenging scenario, which initially occurred near a major holiday, was the need to comply with government procurement procedures and be mindful of public relations.

CHALLENGE

- Defeat a ransomware attack and restore business functions at a major international airport before consequential impact on travel or safety

SOLUTION

- Isolated malware infection and secured airport's network from additional attacks
- Restored front- and back-office data
- Enhanced network for greater bandwidth, capacity, security, performance, and more
- Provided integrated, secure network expertise and products (IPS and cloud security and analytics)

RESULTS

- Resolved malware attack in record time
- Safeguarded network from additional hacks (short-term)
- Repopulated airport screens with flight and baggage data expeditiously
- Designed and deployed highly resilient network (long-term)

VALUE

- Fortified network against future attacks and minimized business interruption costs
- Lessened impact on airport's and city's brand Heightened awareness about prioritizing infrastructure upgrades against vulnerabilities

SOLUTION

Build resiliency against the bad actors

Shortly after the ransomware attack began wreaking havoc on the airport's data center, airport IT personnel called the Black Box help desk. A team of specialists was quickly onsite securing the network from further attack and working to get customer-facing digital information back online.

This act alone helped to reassure passengers, most of whom do not have a clear understanding of the difference between the airport's highly secure, federally regulated operation and the separate business operation. It also greatly reduced the stress level of airport and city executives who could now shift their focus from fear to confidence as they worked with Black Box to transform data operations.

Once the network was clean and secure - a process that took just days - our engineers began working with one of our trusted partners to design and implement a more resilient system.

OUTCOMES

Secure operations, strong public confidence and heightened awareness

When you consider the unspoken, but significant expense of a business interruption, the airport's network transformation brought significant value to their secure operations and daily maintenance. This is especially true when you consider that public-sector victims of ransomware who choose to pay, do so at a cost almost 10 times greater than their private-sector counterparts.

Equally important was the impact on the airport and local government's brand images and public confidence, which remain strong.

The malware incident also illustrated the vulnerabilities of state and local governments' IT infrastructure and the need for investment to safeguard, modernize, and optimize networks that are critical to the smooth operation of day-to-day business.

1/3

Major IT systems used by state government agencies that were deemed "woefully inadequate."[1]

81%

Percentage of ransomware victims who pay the ransom - but don't receive their files back.[2]

Every 11 Seconds

Estimated time that businesses will fall victim to a ransomware attack in 2021.[3]

$20B

Estimated cost of ransomware to businesses in 2021[4]

$6 trillion

Amount of global damages related to cybercrime in 2021[5]

ABOUT BLACK BOX

Black Box® is the trusted global solutions integrator and digital partner. With more than 45 years of experience connecting people and devices, we are an organization of top technical professionals dedicated to delivering solutions and services that help organizations design, build, manage, and secure their communications and IT infrastructure and networks. Technologies include Edge Networking, 5G/OnGo, Connected Buildings, Digital Workplace, Multisite Deployments, Data Centers, and IoT. We also design and manufacture award-winning products for Pro AV, KVM, cabling, and networking known for their advanced functionality, flawless performance, outstanding reliability, and fail-safe security.

1. https://ceriumnetworks.com/government-network-modernization
2. https://www.forbes.com/sites/leemathews/2018/03/09/why-you-should-never-pay-a-ransomware-ransom/?sh=475625051753
3. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
4. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion
5. https://www.natlawreview.com/article/ransomware-attacks-predicted-to-occur-every-11-seconds-2021-cost-20-billion

AGC Accelerating Business | BLACK BOX