cloudastructure

CASE STUDY | **Beating City Hall**

When a Ransomware Attack Occurs, GearBox Shores Up Defenses

THE CLIENT | State and Local Government

A well-known city's Convention Center and Visitors Bureau is the official destination and marketing organization for the city, charged with marketing and selling the city as a meeting, sports and leisure, and tourist destination. The department also manages a convention center, a business/tradeshow meeting center, a community market, as well as multiple parking facilities, all of which are primarily funded by hotel, motel, and restaurant taxes.

THE CHALLENGE

After refusing to pay the ransom after a Ransomware attack, a Visitor's Bureau was unable to recover critical data. Most notably, the accounting infrastructure was destroyed. Even provided they could find an expensive cybersecurity and database expert to rebuild the architecture, how were they going to ensure the hackers didn't simply do it again? Seeing as they had no idea how they got in in the first place?

THE SOLUTION

IoT devices are second only to phishing schemes as a secret hatch for hackers. In the absence of a visible phishing mistake, the Visitor's Bureau decided a scan by Cloudastructure's GearBox was an economical and logical first step to identifying problems. With a push button deployment, GearBox got to work scanning and inventorying all connected devices.

Of particular importance was the interrogation of community-facing technology access. Assessments were also performed on the parking garage metering system, the security surveillance system, and external penetration tests were performed against the organization's firewall, switching, router infrastructure, and key web applications.

GearBox also performed extensive testing to define and document the public Wi-Fi infrastructure, to ensure that it was securely deployed and that appropriate policies were in place for public utilization of the Wi-Fi provided at the various managed venues of the organization.

THE RESULT

GearBox identified various areas of risk such as default passwords from a lightly configured security camera infrastructure, a lack of appropriate network segmentation between operational technology and information technology networks and non-compliance of regulatory requirements, due to faulty implementations from previous deployment projects.

GearBox's remediation roadmap informed them of the architectural, compliance-based and cybersecurity based remediations that needed to be performed if they wished to harden their infrastructure and reduce the likelihood of more attacks. The roadmap ranked each task in terms of both priority and level of difficulty, so pricey, lower-ranked remediations could occur over time.

The Visitor's Bureau decided to use GearBox in a persistent manner, to protect against future IoT vulnerabilities and has since utilized the remediation roadmap to prioritize proactive projects to meet compliance and regulatory requirements, and they have since operated without a repeat attack.

Fast Facts

- **Department of a state government suffered Ransomware attack**
- **Needed to identify IoT inventory and possible points of hacker access**
- **Scanned the public Wi-Fi, garage metering, surveillance system, and more**
- **Results turned up enough vulnerabilities that GearBox was installed as a persistent service**

Advanced. Powerful. Affordable.

Learn more at **www.cloudastructure.com**