CASE STUDY

Working for the People

Even as the internet has driven innovation and efficiency in government, it's also opened the public sector to untold risks. Governments of every size are especially valuable to cybercriminals due to the trove of data collected from citizens that enable services such as e-payment of parking tickets and taxes. What's more, many public entities still suffer the aftereffects of decades of underinvestment in IT infrastructure. This leaves them particularly vulnerable to network security and software patching problems, along with rampant malware infections.

Trustwave®

Client Spotlight

Home to pristine beaches, age-old ruins, and contemporary restaurants, this Latin American state is a world-famous tourist destination. But the history-rich region is also home to more than two million full-time residents, who rely on 6,000 government employees to make sure their daily lives—and municipal websites—run smoothly.

The Challenge

The government of a Latin American state was, frankly, overwhelmed: It hosts more than 60 externally-facing websites to let residents pay for taxes and other municipal fees, schedule appointments, process vehicle registrations, and so forth. The state, like governments of all sizes, was coming under increasing attack from malicious actors eager to strip confidential information from its databases; 40 percent of inbound activity to its sites was attributed to hacking. As the government's web services—and the sensitive data it stores—increased exponentially in recent years, the tiny IT staff suffered two breaches. It was time, everyone agreed, to massively overhaul security protocol—but one-size-fits-all solutions didn't cut it. The government's original web application security solution lacked the flexibility and sophistication required to address log searches and apply patches. The small team needed a more effective, efficient way to monitor threats, block attacks, and determine the roots of code errors that introduced vulnerabilities.

> *"Prior to Trustwave Web Application Firewall, our web server supporting all our external websites had less than 90 percent uptime. Now, with Trustwave, we're experiencing 99 percent uptime."*
>
> – Government data service administrator

The Solution

The government implemented Trustwave Web Application Firewall, which led to zero new breaches and 99 percent server uptime. The firewall was so robust, in fact, that the IT administrators learned that some of its developers were uploading SQL tools with insufficient password protection, which inadvertently left entire databases exposed. With the new system in place, the state's security team is immediately alerted when new code has weakness, so it can be fixed before the site changes go live. As a result, the state's risk exposure has plummeted.

Industry Threat

Local and state governments are routinely hit by attacks, from "defacement" campaigns posting pro-terrorist messages to ransomware efforts that encrypt municipal sites' data, paralyzing them until money is paid. One U.S. state's Department of Revenue was hit by Eastern European hackers after an employee inadvertently opened a phishing link. By the time the state discovered and fixed the breach months later, some 3.8 million Social Security numbers and nearly 400,000 credit card numbers had been stolen.

Many of these public entities lack the resources and staff to address the growing threat. A scarcity of qualified security professional remains a particular problem in local government, where salaries lag those in the private sector. According to the Washington, D.C.-based Municipal Research and Services Center, many governments serving smaller communities have zero IT staff members and minimal or no funding.

> *"What used to take us days or weeks to manage website security now is either fully automated or takes mere minutes."*
>
> – Government data service administrator

Trustwave®

©2018 Trustwave Holdings, Inc

CS-LACGOV-0218