CASE STUDY

Securing the Vote

From the moment a ballot is cast to when it's counted, any security fissure can shake voter confidence, impact election results and lay bare citizens' personal records. With an uptick of electronic voting technology and concerns of foreign influence in U.S. elections, voter security is firmly a part of the national conversation. In 2016, the FBI announced it had uncovered evidence that foreign hackers had successfully penetrated two state election databases, and urged state officials to shore up their own systems. Two months later, news broke that hackers may have targeted an additional 20 states. And it's not just electronic ballots that can fall prey to hacking—even paper ballot systems can be at risk.

Trustwave®

Client Spotlight

This western city is one of the 20 most populous municipalities in the U.S. and with a population of just under 700,000 residents, government employees have thousands of paper ballots to validate to ensure a fair and honest election.

The Challenge

Following a distributed denial-of-service attack on its municipal systems, one major U.S. city decided it was time to step up its IT security measures to address future crises scenarios. They chose to focus their efforts on one of the city government's most pivotal dates: Election Day. Though the city uses mail-in paper ballots rather than electronic voting, the Chief Information Security Officer was concerned with "non-air-gapped" portions of the network—the part that communicates the city's precinct totals and voter registration information to the state for ballot verification. A breach in this system could interfere with voting results or expose a wealth of private data.

> *"Trustwave has always delivered for us, and they've always found something. Elections are the first thing we came up with the money for. We also have television networks, police surveillance, building control systems — all these other networks that will need testing too. I don't have the in-house resources to cover them adequately."*
>
> – Chief Information Security Officer for major U.S. city

The Solution

With limited internal resources, the city needed to outsource the penetration testing necessary to assess their election network's vulnerabilities. Already in a long-standing relationship with Trustwave for compliance services, the city engaged Trustwave to help determine how resilient the network is to attackers through a managed security test. It was performed remotely through a virtual remote penetration test application installed on one of the municipality's workstations. It involved several days of attempting to elevate privileges and conduct a bevy of attacks on the network, including IP redirection, session hijacking, password capture, spoofing and man-in-the-middle attacks.

By delegating these security testing measures, the Chief Information Security Officer and his team were able to focus their energy on the 50-plus city and county agencies under their watch.

Industry Threat

Influencing an election can have catastrophic consequences. But that's not the only outcome hackers are after. Election databases can also be a treasure trove of personal information. When hackers breached one Midwest state's voter registration system in 2016, and downloaded personal data on up to 200,000 voters, state officials were forced to shut down the entire system for 10 days. "PCI has oriented security dollars in an organization toward credit card data," says one consultant at Trustwave. "They end up pushing a lot of their security budget over to the parts of the network that handle credit cards. The question then arises: Are they applying enough security into the other places?"

> *"The only way you're really going to know [if you're vulnerable] is with some tests."*
>
> – Chief Information Security Officer for major U.S. city

Trustwave®