Securing City Governments

The Imperative of Automated Pentesting Amid Rising Cybersecurity Threats

RIDGE SECURITY

Government organizations within small cities typically operate with limited security personnel to manage and oversee their digital assets and data. This limitation underscores the critical need to address security challenges efficiently. Penetration testing and security validation are indispensable in safeguarding data and infrastructure, highlighting their essential role in ensuring robust protection.

A recent study revealed the following state and local government cybersecurity challenges

In 2023, cyberattacks on U.S. cities and local governments increased significantly. They included a 148% increase in malware attacks, a 51% increase in ransomware incidents, and a 313% increase in endpoint security services incidents - including data breaches, unauthorized access, and insider threats.

- The rate of data encryption is at its highest in three years, with 76% of ransomware attacks in state and local government organizations resulting in encrypted data.
- The percentage of attacks stopped before data was encrypted continues to decrease, with just 19% stopped before encryption.
- State and local government organizations reported the highest rate of attacks (48%) where stolen encrypted data.
- Exploited vulnerabilities (38%) and compromised credentials (30%) were the two most common root causes of the most significant ransomware attacks in the state and local government sector.
- Malicious emails or phishing were the starting points for 25% in this sector.

Organizational Context

Even with today's heightened awareness of the risks associated with cybersecurity, it's still rare to find employees with titles such as Cybersecurity Director or Manager within city government organizations. This is also reflective of the fact that small city governments, in general, have limited budgets and staff. Unfortunately, it can be even more challenging to find talent with the right skill sets, which, for a small city, may require an individual to have technical security skills and business savvy to understand compliance, implement policies, and administer and manage cybersecurity technology controls. A small city in California with approximately 300 employees is overcoming its cybersecurity challenges by leveraging technology and automated security solutions. Automated penetration testing has proved invaluable as part of the city's security operations, encompassing a multi-layered security stack, each layer having its own set of controls.

Challenges

The city is responsible for its internal infrastructure and data. It also protects and stores sensitive data and Personally Identifiable Information (PII) on the many organizations and citizens that work with and rely upon it for its many services.

The data is sourced from the city's many services: waste collection, licensing, park and recreation facilities, permitting, social and family services, transportation, public utilities, police and fire departments, and environmental programs.

Because the city's cybersecurity is managed by literally a team of one individual, managing operational and technical matters requires automated technical solutions that find, report on, and help prioritize found security vulnerabilities.

The Solution

"We faced a dilemma without the technical ability to prioritize vulnerabilities based on their risk to our particular organization. To address this, we're using automated pentesting and its ability to prioritize each vulnerability based on its level of risk. This allowed us to proactively manage our devices and applications, with an understanding of which are susceptible to potential exploits with clear high-risk indicators,"

said the city's cybersecurity manager.

Automation greatly simplifies the penetration testing process and user experience, allowing the city to frequently test whenever there is an upgrade, patch, configuration change, new device and application, etc.

Areas of pentesting focus

Over the past year, security solutions, including pentesting, have been integrated into new networks and telecommunications systems the city has rolled out. As systems are brought in, the new infrastructure devices are tested to uncover any vulnerabilities that could be exploited. Internet connections, wireless connectivity, and application access are all tested for vulnerabilities.

In addition to on-premises infrastructure and applications already completed, the city will soon begin pentesting third-party software hosted by SaaS providers that will be part of the city's supply chain and risk management program.

With today's threats, automated pentesting is no longer just a nice option. It is now table stakes. There is a difference between manual and automated pentesting. Human or manual testing is limited by the capabilities and toolsets they bring. They take a broad approach and narrow the testing based on the organization. Automated pentesting limitations lie within the restriction of their technology approach, which can be more canned. However, automation becomes very attractive for a city with tight budgets and resources.

The RidgeBot advantage

According to the city's cybersecurity manager, ***"RidgeBot has the most complete set of pentesting capabilities I've seen. The technology is much broader, even human-like, in the expansiveness of its approach. Rather than being canned, it is a more elaborate reconnaissance-***

based approach. RidgeBot picks up detailed information on devices with more methodologies for identifying and reporting vulnerabilities by leveraging its comprehensive library with more than 36,000 plug-ins. Each plug-in contains multiple pre-packaged vulnerabilities, or CVEs, against which RidgeBot conducts tests and attack simulations."

"The other significant advantage is in the reports RidgeBot provides. While other vendor reports are more limited and have a truncated view of the risks, RidgeBot reports are much more comprehensive, providing detailed reporting and validation."

RidgeBot provides clear visibility and fast remediation for risks like exposed PII, broken access and authorization, account takeover, data and session hijacking, and code disclosure. RidgeBot identifies whether a device or application can be exploited due to vulnerabilities or other practices.

This clarifies a city's level of exposure and risk based on an exploit. It gathers information on the potential impact of an exploit, such as lateral movement, identity spoofing, and data breaches. As cyberattacks on cities and local governments surge, they are increasingly vulnerable due to limited budgets. Despite heightened awareness, organizations often lack dedicated cybersecurity resources and face challenges acquiring the necessary talent. Automated pentesting and security validation have proven valuable in managing and prioritizing vulnerabilities, especially given tight budgets and limited resources. RidgeBot's comprehensive testing, verification, and detailed reporting help cities proactively manage their cybersecurity risks.

About Ridge Security

Ridge Security is a leader in exposure management, dedicated to developing innovative cybersecurity products that benefit CISOs and security teams by reducing risk through validation and using automation to improve efficiencies. Ridge Security's products incorporate advanced artificial intelligence to deliver comprehensive security validation, powerful workload protection, and cloud security monitoring.

Request a Demo

RIDGE SECURITY