eBook

datamax®
Relevant Technology • Raving Results™

The Impact of Ransomware on Government

How State and Local Governments Can Strengthen their Security Posture

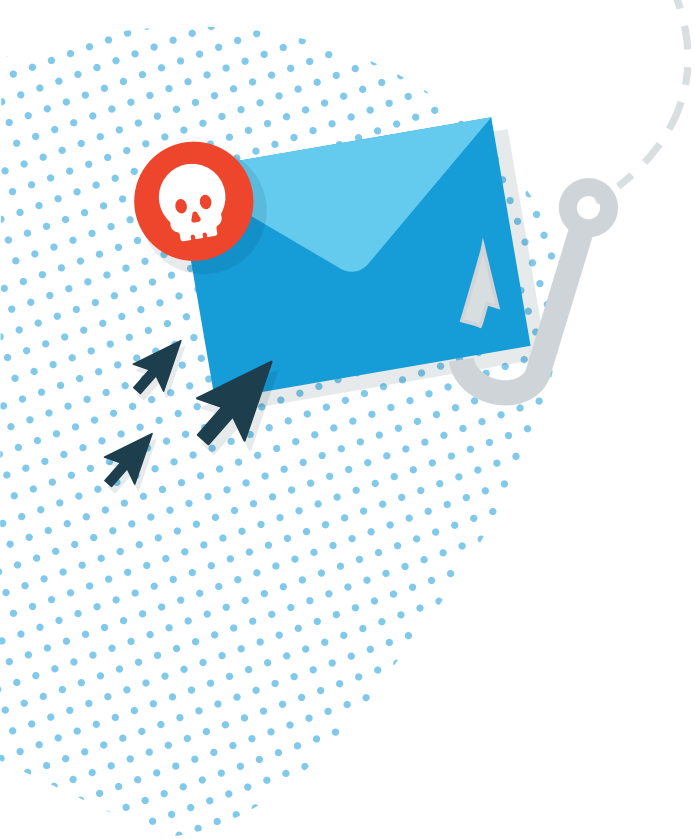
How State and Local Governments Can Strengthen their Security Posture

Cybersecurity has been a topic of discussion among IT professionals for quite some time. More recently local and state governments have faced an increasing number of cybersecurity threats and vulnerabilities. Much is at stake as breaches lead to extensive downtime and threaten the confidentiality of personal data, such as social security numbers, birth certificates, driver's licenses, voter registration, immunization history, medical records, bank accounts, and credit card numbers of people and businesses.

With the added challenge of limited budgets, legacy IT applications, and infrastructure and resource constraints, local and state government agencies have found themselves in a vulnerable, potentially dire situation when it comes to reducing security risks.

The Crippling Effect of Cybersecurity Attacks

Recent headlines offer alarming examples of the detrimental impact security breaches have on local cities. Four cities in the US were hit with ransomware infections as 2019 ended. These cities, including New Orleans and Pensacola, Florida, all had essential government services sabotaged or halted. After the ransomware attack on New Orleans, the mayor was forced to declare a state of emergency. In Pensacola, the sanitation department lost email and telephone systems, internet servers, and their online payment system. In May 2019, an encrypting ransomware attack took Baltimore's IT systems hostage, the attack froze thousands of government computers and disrupted everything from real



estate sales to water bill payments. Even with the help of the FBI, the Secret Service, and cybersecurity experts, the cost to the city is astronomical at an estimated $18 million.[1]

All too often these attacks start with targeted phishing emails. There is more to be done to proactively arm employees with the information they need to avoid these dangerous security breaches.

Targeted Phishing Attacks are a Growing Threat to State and Local Governments

Today's cybercriminals continue to leverage social engineering[2] emails as the top attack vector. According to the Anti-Phishing Work Group's[3] Q1-2019 report[4], the total number of phishing sites from Q4- 2018 to Q1-2019 increased by 30%. In addition to the rise in phishing, ProofPoint's Q1-2019 Quarterly Threat Report[5] states emails with malicious URLs exceeded those with emails containing malicious attachments by 5 to 1 and are up 180% versus Q1-2018. Users are closer than ever to be within a single click from the threat.

A single mistaken click on an email URL redirecting an unsuspecting user to a fake website will lead to executing code to exploit a vulnerability. Security professionals all agree that a comprehensive security strategy is multi-faceted, incorporating perimeter hardening, end-user education, software patch management, and disaster recovery planning. It is also becoming more complex to proactively prevent attacks from occurring. Threats, like strains of ransomware, adapt as prevention measures mature and new technologies emerge making it difficult for state and local governments, especially with limited resources, to remain ahead of the criminals. However, the problem needs to be addressed head-on.

As Gartner states, "Cybersecurity risk, if not treated appropriately, translates into business risk, reputation loss, regulatory breaches and general disruption of operations." The cost of disruption is too significant, and often orders of magnitude higher than prevention when responding to an event after it has occurred.

How to Effectively Combat Threats

The first line of defense against cyberthreats is patch management. The types of services your agency may need include: Vulnerability Assessments & Management, Patch Assessments & Management, Secure Configuration Assessments, Application Security Testing, Compliance Assessments & Management, and Business Continuity Solutions.

According to Gartner, the goal of proper patch management services is, "to mitigate the risks of security breaches or performance issues by standardizing the patch management processes across the entire organization."

Automating patch management with a reliable solution and working with an outsourced trusted solution provider who can provide you with easy-to-understand reports, brings clear visibility to the sites and devices with the highest risk so something can be done before an attack occurs. Working with us as your strategic partner. We can implement the right solutions to reduce security risks and work proactively on your behalf to prevent downtime, keep your valuable citizen data safe, and maintain your best interests.

1.Security Boulevard (2020, January 9) Cyber Attacks Against State and Local Government Surge [Blog post]. Retrieved from: https://securityboulevard.com/2020/01/cyber-attacks-against-state-and-local-governments-surge/

2. https://www.datto.com/blog/5-types-of-social-engineering-attacks

3. https://apwg.org/ 4. https://docs.apwg.org/reports/apwg_trends_report_q1_2019.pdf

5. https://www.proofpoint.com/sites/default/files/pfpt-us-tr-q119-quarterly-threat-report-0528.pdf

For more information please contact:

Justin Huffaker

Vice President, Strategic Technology

jhuffaker@datamaxinc.com

www.datamaxinc.com