1200 words

Rauf Bolden, Orange Beach

August 4, 2018

Municipalities, Ransomware and the Cloud-Based Browser

You could almost hear people gnash their teeth, wondering about ransomware attacks on municipalities in New Mexico and Georgia.

"The city of Farmington continues to recover from the ransomware attack that shut down computer systems throughout the city in early January [2018]," according to a report by Hannah Grover in the Farmington Daily Times.

"Six days after a ransomware cyberattack (March 22, 2018), Atlanta officials are [still] filling out forms by hand," according to a report by Kimberly Hutcherson of CNN.

The proliferation of online services to improve urban life, branded "Smart Cities", as municipalities adopt interactive technologies, allowing cities to connect with their citizens has a downside, opening up the city and its residents to ransomware attacks.

Governments know they have responsibilities, keeping residents' data safe, because malware can jump from one host to another, usually through the local browser, emailing the address book when malicious code infects a city's computer system.

In spite of the dangers, local governments continue to offer online services, supporting residents, service providers, and vendors through the local browser, but City IT systems must have a minimum-security plan. Off-site backups, and cloud-based servers are a good start, limiting the damage from browser-based attacks.

Today, cloud-based browsers provide an easy to use encrypted solution, protecting networks, ensuring the municipal-employee experience is fast and secure, while communicating effectively with residents.

Cloud-based browsers have unique features. No web-native code like HTML, PHP or JavaScript is executed on the local machine, protecting municipal networks from ransomware, malware, spyware or other malicious scripting.

Admins can disable the clipboard for copy and paste, simultaneously setting up content-access filtering, locking your network down to one browser, controlling every machine, and permission, but still giving people a fast, working experience.

Acknowledging your browser is the weak link in the security plan is vital.

"I've spent a lot of time cleaning up and preventing the influx of Ransomware and Spyware on hundreds of computers. Cleanup success was never 100%, and it was a slog to find where each flavor or variant would hide the logs or encryption keys. I had these sorts of problems everywhere I went, from home PC's to Police equipment," wrote Tanner Bonner, formerly with the City of Fairhope, presently IT Administrator, OWA Amusement & Entertainment Destination, Foley, Alabama.

"We continually strive to keep this issue [browser security] before our employees. We have watched as several surrounding jurisdictions have suffered through ransomware

attacks that were let in through browser related issues," wrote Jeff Moon, City Manager, City of Woodstock, Georgia.

”We set up the browser [Chrome] in incognito mode and enable the setting of 'Do Not Track' with browsing traffic," emailed Meagan Bing, MLIS, IT/Technical Services Librarian, Orange Beach Public Library, Orange Beach, Alabama.

“I am not one to allow my browser to remember me or my password. As annoying as it might be to have to provide credentials to Sign-On over and over to the same sites, I avoid saving my credentials to avoid the possibility of someone gaining access to a site/service. I'm surprised by how many folks I encounter that don't give this any thought, even on a shared device,” said Mark Pearson, IT Director, City of Mobile, Alabama, discussing his personal-browser strategy.

“We pride ourselves on being ahead of the curve in security, and we have not been affected [by ransomware],” wrote Shana Edmond, IT Systems Supervisor, City of Gulf Shores, Gulf Shores, Alabama.

The cities in Baldwin and Mobile Counties have talented IT personnel, getting buy-in from management for a migration policy is key. Cloud browsers require funding, and a small amount of configuration; having login credentials and pin codes, possibly text-to-phone confirmation, enabling 2-part authentication.

“We use a turn-key tech service that includes private cloud servers. They do a really good job of protecting us and stopping intruders,” said Herb Malone, President, Gulf Shores & Orange Beach Tourism, Orange Beach, Alabama.

There is a cheaper way to do things: ”85,000 employees [at Google] have managed to go more than a year without getting phished because of mandated security devices [USB authentication],” according to a report by Rhett Jones in Gizmodo, a tech web site.

Cloud-based browsers provide a secure alternative to USB sticks (Whoops! I left mine at home), making the jump from the browser to the local network impossible, because there is no physical connection.

New ideas will always find resistance, but there are worries.

"Downtime. This may be one of the worst disadvantages of cloud computing. No cloud provider, even the very best, would claim immunity to service outages. Cloud computing systems are Internet based, which means your access is fully dependent on your Internet connection," according to a report by Andrew Larkin in Cloud Academy’s Blog.

Weighing a technology’s upside potential versus its downside risk is what managers do. Given the operational downside, possibly opting for network-integrated hardware with several competent staff over the cloud.

“We do port based security on our firewalls in order to control the flow of traffic [on local browsers]. The most important piece to this security would be the staff that we have to manage the day to day business of the county infrastructure,” wrote Brian Peacock, IT Director, Baldwin County Commission, Baldwin County, Alabama.

Local governments get it, desperately needing to leave malware defeats in the rear-view mirror, keeping residents’ data safe, reducing the pressure on IT personnel, letting technology take the place of employee vigilance.

Privacy and security are not in conflict; they are bound together by the same thread, ultimately realizing the era of government-enforced regulation is over.

On March 23, 2018 Congress passed a law dismantling Internet Privacy Rules (Senate Joint Resolution 34 (S.J.Res.34)). On April 3, 2018 President Trump quietly signed the bill into law, arguing privacy regulations are burdensome.

ISPs (Internet-Service Providers) are no longer required to get explicit permission before collecting any customer's data and re-selling it, being something a City or County Administrator will have to explain to his or her Elected Officials, possibly amending the present contract.

"While everyone was focused on the latest headline crisis coming out of the White House, Congress was able to roll back privacy," said former Federal Communications Commission chairman Tom Wheeler, according to a report in the Washington Post.

Cloud-based browsers let admins sleep as soundly as a millennial after "Burning Man", knowing his or her municipality's Internet browsing is private, and the residents' data is safe, because the proprietary encryption keys are locked in the boss' safe.

An aura of technological swagger surrounds the cloud browser. You can try several flavors by googling: cloud-based browsers, joining the fray to end municipal ransomware.

ENDS.