9 Urgent Security Protections Every Municipality Should Have in Place Now

COVID-19 UPDATE 2020

Cybercrime is at an all-time high, and hackers are setting their sights on Municipalities of every size who are seen as “low hanging fruit.”

With many administrations no longer accepting in person meetings, and handling citizen requests in a remote work fashion, the risk of a breach of confidential and critical data is more than imminent. Finally, any disruption of mission critical services by cyber theifs could cost citizens their lives.

Do not be their next victim!

This report will get you started in protecting everything you have worked so hard to build.

{e}mazzanti® technologies

WBE/SBE CERTIFIED

TECHNOLOGY STRATEGIES FOR STATE AND LOCAL GOVERNMENTS

1-866-EMAZZANTI info@emazzanti.net emazzanti.net

Are You A Sitting Duck?

Imagine you are the proud, recently elected official. After a hard fought campaign, you finally have the office you dreamed of, and the ability to make a real impact in your community.

The first message that comes across your desk is a communication from a suspicious source demanding money and then you and your team no longer have any access to your systems.

With Covid-19, your administration is working harder than ever. Covid is impacting first responders and the communications staff of your administration. Eyes are on you. New Cyber threats are presenting themselves daily and looking to attack your systems in your building and the communications that are critical to sharing information with your work from home administration. It is best to be prepared for 2021.

In 2019, more than 45 municipalities were hacked. Some as small as 5000 citizens in population size. The typical currency for payment is Bitcoin. Just ask the FBI, Bicoin is virtually untraceable. Imagine your community impacted, emergency response services down, library books can't get checked out, and you don't have a line item in your budget titled "Ransom payment." What do you do?

Although many Municipalities are refusing to pay, the Hackers are relentless with significant expense and catastrophic results.

The New York Times quotes “Beyond the disruptions at local city halls and public libraries, the attacks have serious consequences, with recovery costing millions of dollars. And even when the information is again accessible and the networks restored, there is a loss of confidence in the integrity of systems that handle basic services like water, power, emergency communications and vote counting.”

Urgent phishing attacks are on the rise with Covid-19. Spoofing, ghosting and seemingly innocent emails are threats your team has to be prepared for.

Benjamin Franklin stated that, “an ounce of prevention is worth a pound of cure.” This still applies today with protecting local government entities. A Municipality with well-funded Cyber Security initiatives shows its citizens that it takes their personal information seriously and is willing to invest in protecting their best interests, even if an attack occurs. In addition, there is a legal obligation by public entities to protect sensitive data. Is your team doing its due diligence?

> **“We are seeing more ransom ware attacks because they work,” said Eli Sugarman, who directs the Hewlett Foundation’s Cyber Security program.”**

Eli Sugerman, director of the Hewlett Foundation’s cyber security program, comments to the New York Times, “We are seeing more ransomware attacks because they work. Cities are struggling to secure their complex and often outdated systems. Then, when attacked, some choose to pay.” And, he noted, there is notoriety that comes from each successful attack.

Today’s cyber wins are now funding more research into making attacks more precise and effective. Some municipalities are investing in Cyber insurance as way to protect the perceived eventual economic disaster but that, in fact, may shine a light on antiquated systems so hackers can then identify a place where a better payoff may occur.

Cyber insurance is not a deterrent or preventative control, but rather a recovery methodology more focused on the balance sheet of the Municipality than anything else. This situation isn’t easy to address but with best practices in place and a smart technology partner, you will fare better than many. Know that 90% of all data breaches are from internal sources.

Take the time to source and use the below 9 steps as a guide to build the fortress you'll need to help ward off cybercrimes in your district or township.

1. Train all Municipal Employees On Security Best Practices whether in Office or Remote.

The #1 vulnerability for every IT network is the staff that uses them. Infosec awareness training is important to mitigate the insider threat! It's extremely common for an employee to infect an entire network by opening and clicking a phishing e-mail (that's an e-mail cleverly designed to look like a legitimate e-mail from a web site or vendor you trust). If they don't know how to spot infected e-mails or online scams, they could compromise your entire network. Regular education regarding any potential email that could infiltrate your network needs to be mandatory for all staff. If the IT department does not have the resources to schedule and conduct this training, engage a third party resources who can Certify this training has been completed and the staff that have taken it.

2. Create An Acceptable Use Policy (AUP) – And Enforce It!

An "acceptable use policy" or AUP outlines how employees are permitted to use municipal-owned PC's, cell phones, software, internet access and e-mail. An AUP policy is not a Cyber Security policy per sé, but rather a Cyber Security policy should have a component that outlines AUP of Municipal Assets.

We strongly recommend putting a policy in place, then follow up with the appropriate technology controls that will limit not only the websites that employee's can access, but also that prevent malicious incoming emails that look legitimate. For remote staff, securing in home Wi-Fi or creating VPN tunnels to securely connect to your network is a must. Further, you will have to enforce your policy with content-filtering software and firewalls. Permissions should be set up along with rules that will regulate what web sites your employee's access and what they do online during company hours and with company-owned devices, giving certain users more "freedom" than others. The AUP should include steps that need to be taken immediately if the device is lost or stolen. For cell phones there should be clauses regarding the in abilty to root or jailbreak the device that is owned by you.

What if you provide access to certain systems from an employee's personal device like a cell phone or a personal laptop? Although this is strongly discouraged for a variety of reasons, the trade off is the capital expense to require all staff to have Municipal devices. In addition, you'll need the ability to enforce security policies and monitor "Bring Your Own Devices (BYOD)" assets beyond the logical perimeter of your trusted network. If that employee is checking unregulated, personal e-mail on their own laptop that infects that laptop, it can be a gateway for a hacker to enter your network.

Next how should employees who have BYOD devices or guests in the Municipality access the internet? Secure your Wi-fi with a separation of private and public networks. All should be password protected and specifically best practices dictate the private network shares a 2-factor authentication model.

Lastly, what happens when an employee leaves the municipality. If the phone is lost or stolen, are you permitted to remotely wipe the device – which would delete all of that employee's photos,

videos, texts, etc. – to ensure YOUR Municipality's information isn't compromised? Think through all of these situations carefully, consult your legal counsel, and implement a robust training plan to educate all your staff.

3. Have a Strong Password Control Strategy.

All end users today have too many passwords to remember and manage. We all know that every account should have its own unique password for protection. But according to recent information published by Last Pass, a leading password and authentication authority, the average employee has around 191 different accounts active at one time. The likelihood that the same password is used multiple times and also standard passwords like 12345 are used way too often.

Through the addition of Multi Factor Authentication, the security of the traditional username and password login is supplemented by an additional measure. With MFA, a TOTP (time-based one–time password) or Token, is generated from a smartphone or other device that is required for access. This user now needs two pieces of information to access their IT resource making it more difficult for hackers to find their way in.

4. Keep Your Network Up-To-Date.

A well defined configuration and patch management strategy is necessary. New vulnerabilities are frequently found in common software programs such as Microsoft Office; therefore it is critical that you patch and update your systems frequently. If you are operating on-premise, in a hybrid configuration or a full cloud infrastructure, patching your servers, access points, desktops and laptops can keep them safe from easy intruders that are looking for opportunities in older hardware and software versions. Patching and updating is a change to your IT infrastructure and should be treated as such, with appropriate planning, testing and fall back. If you don’t have the processes or staff in house, qualified third parties are adept at helping in this area. The expense is often nominal at the cost of security, so consider using a local provider to be there when you need them.

5. Back up and Recovery Controls

The importance of proper monitoring, validation and testing of data recovery systems is mandatory to protect your sensitive data. Having a well-oiled backup and recovery plan can foil the most aggressive ransomware attacks where a hacker locks up your data/ files and holds them ransom until you pay a fee. Consistent and frequent backups are important as they remove the inherent threat from Hackers. Outside threats are not the only ones. A good back up strategy implemented well, can also protect you against an employee accidentally or intentionally deleting or overwriting files!

Since many Municipalities have moved email platforms to Microsoft 365, it is important to note that there is no back up plan included in the M365 mailbox license. A good technology consultant like eMazzanti, can advise you of the most cost effective strategy to make sure your important data is retained and backed up for the length of time you need as part of your data retention policy.

Additional disasters can be either natural like fires and water damage or electrical, such as fires. Backups should be automated and restorations should be tested and flawless.

6. Don’t allow employees to download unauthorized software or files.

One of the fastest ways Cybercriminals access networks is by duping unsuspecting users to willfully download malicious software by embedding it within downloadable files, games or other “innocent”-looking apps. Policies should be put in effect to block certain executable file types that can transport malicious code.

7. Upgrade to a Next Generation Firewall with full Unified Threat Management capabilities.

A firewall acts as the frontline defense against Hackers blocking everything you haven’t specially allowed to enter or (leave) your internal network.

All firewalls need monitoring and with a Next Generation Firewall there are enhanced administration capabilities which includes deeper awareness and control of individual applications and the inspection thereof.

Firewall restrictions should block international access as well as potential public domain access. Preventing these threats does take away the opportunity for overseas Hackers. Keep vigilant in your firewall management and alerts and always double check Firewall policies to keep them up to date.

8. Knowing Where the Dead Bodies Lie:

All Municipalities should do an annual network assessment and a penetration test. These two items should be reoccurring investments in the municipal budget on an annual basis. The performance or execution of these two items will allow IT services to understand who has what assets and where, as well as determine what opportunities exist for Hackers to break into the Township. A certified statement from a third party source, allows the Municipality to show that they have done all that they can to confirm that the data on the network is safe and secure. With the penetration test, there are often recommnetations that the Municipality will have to take into consideration to to secure the data. This beomes a worthy exercise in preventative maintence for all to be secure.

9. Keeping your Municipalities Infrastructure Safe During Covid 19- this includes mission critical services.

As we contemplate our journey over the last several months with Covid, we must not rest on our laurels and consider that we are safe in this journey. Not only can the pandemic hit a second wave, but it can also continue to selective cause stress on mission critical services that municipalities have to offer and leave citizens at risk. At Cisa.gov you can learn about practicing and planning for a next wave and Cyber Attack through the cybersecurity and infrastructure Security Agency.

Additionally eMazzanti Technologies can show you how to protect and monitor your infrastructure against the ever present threats for data breach and ransomeware. Late in 2019, a new cyber security threat emerged. Criminals used ransomware to attack Allied Universal. In a twist now known as double extortion, the bad actors first extracted sensitive information before encrypting company data. Then they insisted that Allied pay a stiff ransom to avoid seeing sensitive data leaked publicly.

Throughout 2020, other attackers have followed suit. To convince organizations to pay a ransom, criminals threaten to publish or sell the stolen data. To prove their point, they post samples of the data on their websites. Thus, the tactic effectively combines ransomware with data breach. And it places organizations in an extremely difficult position.

In these cases you need to work with a savvy and intelligent managed security services provide like eMazzanti Technologies to help secure your internal infrastructure while also providing critical advisement on how best to address any attack. Don't underestimate the experience of the dark web and or the capabilities of your Cyber Security insurance policy. It is important that you do not risk your citizens trust.

For more information on Cyber Security best practices for Municipalities please contact us at info@emazzanti.net.

{e}mazzanti® technologies

TECHNOLOGY STRATEGIES FOR STATE AND LOCAL GOVERNMENTS

WBE/SBE CERTIFIED

eMazzanti's team of trained, certified IT experts rapidly deliver increased revenue growth, data security, and productivity for Municipalities of all sizes. Headquartered in New Jersey, the firm offers cloud and mobile solutions, multi-site technology implementations, outsourced network management, 24 x 7 support, digital marketing services and cybersecurity assessments and protection services.

eMazzanti has received many accolades for superior service delivery and stellar growth. The firm has been included on the INC 5000 list of fastest growing privately held companies nine times - including eight consecutive years in a row, recognized by Microsoft as a 4x partner of the year and a Watchguard 5x partner of the year. NJ Biz has recognized the firm as the 2016 Small business of the year and also as a leading NJ Digital Innovator.