Cybersecurity Tips for Local Governments

The following list will help ensure better security for your government, especially if you notice unusual activity or if you want to prevent such activity.

1. If you see something on your network that looks like ransomware, start severing/unplugging all Internet-based connections asap! Do not try to stay up and "functional", as it will allow for rapid, catastrophic proliferation across your networks and into any interconnections you might have with neighboring entities.

2. Do not try to stand your environment, whole or in part, until you are certain that it is clean. Re-infection and possible expansion of the infection is highly probable if you have not properly contained and cleaned your environment.

3. Assess and restrict any public facing remote access ports (RDP, SSH, telnet, FTP) to a whitelist of absolutely required addresses. Block traffic to any of those ports not critical to business.

4. Do not allow vendors to have open tunnels into your environment for remote support. They need to follow best practices, such as requesting access via a help desk system, then after work is completed, the access should be terminated. Ask the hard questions to require all external connection requests to determine the minimal level of access needed to perform work instead of what is easiest for those external requestors, which is usually the least secure option.

5. Do not use the same credentials for domain administrator and your local administrator accounts. Many of the recent breaches have involved compromised domain administrator credentials, which often are found to be the same as cached local administrator credentials.

6. Start planning now for immutable backups that are stored physically and virtually apart from the network. After attacking the domain controller(s), most current variants go straight to encrypting your backups.

7. Engage in user education for phishing messages and aggressive response to mitigate anyone who falls for phishing. Exposed credentials and malware downloads are part of the problem and can be limited with proper education.

8. Create a Continuity of Operations plan for your entity and drill it to make sure it works for your team! If you have not experienced a ransomware event, this will be invaluable—nothing generates stress like trying to figure out how to run payroll three days after you get hit.