The State of Cybersecurity: 
Best Practices for Securing Critical Infrastructure for State & Local Governments
Table of contents

Summary: 3
The Scenario 3
Government Agencies are Highly Vulnerable 4
Why Cyber Security is Critical for Government 4
Election Security – Points of Vulnerability and Solutions 5
10 Best Cybersecurity Practices for Government Entities 6

Summary:
Government agencies are increasingly finding themselves as targets for cyberattacks. In this whitepaper, we summarize some of the best practices these agencies can use to stay secure and highlight some of the possible consequences to having vulnerabilities. Our elections systems have been a strong focus in recent years; we are drawing upon lessons learned in that realm and extending them across the government IT infrastructure. Above all, this paper is meant to provide a reference architecture for Security Officers and CIOs, for all government entities and departments.

The Scenario
Today’s world is dramatically different than just five years ago. Ransomware attacks used to make global headlines. Now, they are commonplace. Cybercriminals have historically targeted large enterprises. Now, almost every day, we learn that a new city, county or state government entity has been attacked.

“In island hopping” attacks are also becoming more frequent, meaning that attacks are proliferating to suppliers and customers and becoming harder to stop.

Newer, sophisticated cyberattacks are bypassing traditional, signature-based antivirus solutions at an alarming rate. More than 60% of attacks are not malware based. Even malware is much more sophisticated than ever before, and phishing attacks that used to be laughably detectable by misspellings and incorrect graphics are now quite convincing.

In recent months, we’ve seen high-profile attacks against major U.S. cities. These attacks have included ransomware variants and permanent data loss. The damages have totaled in the millions of dollars. Some cities are still recovering from these attacks and the lessons learned have been sobering.

Attackers will often introduce an attack via a spear phishing email, which is opened by a city employee, exposing the entire infrastructure to an attack. In some examples, ransomware has been able to encrypt all city data, computers, workstations, phones, and dispatch systems for first responders.

For example, the City of Pensacola, Florida was hit with a ransomware attack in early December, 2019. The Maze ransomware variant was used, and the hackers threatened to release data if $1M in ransom was not paid. True to their word, they did release a small percentage of the data to prove they could. Making this especially damaging – this occurred days after a shooting at a nearby Naval Base. Experts estimate that it may take six months to a year for the city, which was mostly shut down, to recover from this hack. No one knows if the city paid the hackers or not, but we do know they paid the consulting firm Deloitte upwards of $140K to fix the issue.

Other cities in the news for December attacks include New Orleans, the city of Galt, CA near Sacramento, and St Lucie, Florida. All attacks are costly in terms of productivity, city image, and potential privacy concerns.

These types of attacks are not new, per se. What is “new” is how often attackers are taking advantage of smaller, more vulnerable entities. We continue to see new attacks on state, city, county and local governments, which sheds light on the need for more comprehensive cybersecurity protection and awareness.
Government Agencies are Highly Vulnerable

After the widely publicized Target attack of 2013, many enterprises and retail businesses saw the importance of moving away from outdated security solutions and realized the potential cost of a breach. They put into place more sophisticated solutions to stop attackers. In many cases, government entities did not follow suit; they were often hampered by limited budgets and a lack of solid security staff.

Some data to ponder:
The International City/County Management Association, better known as ICMA, released the results of a survey conducted in 2018 and found that municipalities cited the following as severe barriers to implementing cybersecurity in their patch:

- 58.3 percent cited the inability to pay competitive salaries for cybersecurity personnel
- 53 percent cited an insufficient number of cybersecurity staff
- 46.5 percent cited a lack of adequately trained cybersecurity personnel
- 52.3 percent cited a lack of funds for cybersecurity

In addition, more than 50% had not performed any cybersecurity training for personnel.

Government agencies are adding Internet-connected services and technology at a rapid rate, often without securing that new technology. This provides new and attack surfaces for cyber criminals and nefarious nation-state actors. The risk of an increased attack surface is compounded by the reality that organized crime groups have adopted cybercrime as an emerging business model with help from the dark web.

Why Cyber Security is Critical for Government

The above is very concerning when considering all the points of vulnerability in government and the potential impact to the public at large. Criminals and domestic and international terrorists can now manifest an asymmetrical cyberattack in the following ways:

- **Municipal Airports** can have critical safety interruptions, which would create chaos and provide a way for malicious nation-state actors or hacktivists to cause accidents in a new form of warfare.
- **Smart city controls** could be compromised or shut down, with chaos ensuing in the form of missed snow plowing, parking garages shut down, court houses and DMV centers with no compute power, and widespread smart meter malfunctions.
- **Court house records** could be exposed or altered.
- Critical patient data from **public hospitals** could be exposed or altered. One such case involved the deletion of a patient allergy from a chart, and the patient died on the operating table.
- **Prison inmate data** could be hacked and/or changed.
- **911 systems** could be brought down during major emergencies.
- **Government contract award data** could be compromised.
- **Key governmental communications** could be altered or changed.
- **Sealed juvenile arrest records** could be reached and exposed, or altered and exposed.
- **DMV records** could be altered, used for identity theft, and/or exposed.

Given the heterogeneous architectures of state and local systems (and the stark reality that many of these systems are older and unmanaged), it is imperative that we learn from the security exposures of another critical infrastructure. The most visible use case study is election security. A great deal of study has been done in this area. It pays to review lessons learned as well as the types of attacks and vulnerabilities so that this knowledge can be applied to the above scenarios and help to keep our cities, towns, counties and states safe as well as our elections fair.
Election Security – Points of Vulnerability and Solutions

The importance of cybersecurity in the context of the democratic process has become undeniable in recent years, with nation-state hackers setting their sights on elections as effective vehicles for attack, disruption, and social unrest.

On October 30 2019, Christopher Wray, the Director of the FBI, testified to Congress regarding China and Iran: “All of those countries in different ways are clearly interested in engaging in malign foreign influence.”

As for Russia, he said, the U.S. expects they “already have continued to up their game from what they did in 2016.” We can expect that the 2020 elections will once again be a major target for U.S. adversaries who seek to do damage to the country and reduce faith in the election process. “Malign foreign influence” will take many forms with regard to election hacking, namely:

1. **Voter disenfranchisement:**
   Voter registration systems and databases are managed on a state to state basis, and are often built on unsecure technology. These systems are a prime target for would be hackers, as was the case when Russian hackers probed and penetrated voting systems throughout the 2016 election process.

   There are two ways to manipulate the results:
   a. Change the results via database manipulation, particularly in swing states like Florida, Pennsylvania, Ohio and Michigan.
   b. Alter the integrity of voter records from one party. Specifically, altering name or address spelling, this effectively suppresses the voter from voting at the polls.

2. **State Website site defacement:**
   Election systems typically have a state website that tallies and posts results as they come in, with servers that can be manipulated if not adequately protected. While such tallies do not represent official counts and are not directly tied to vote tallying systems, these live counters can show false values, creating confusion, frustration, and distrust amongst the voting populace. If voters believe their candidate is winning or losing in a runaway, for instance, they may choose to not vote.

3. **Media Island-hopping:**
   Major media outlets (typically the ones that lean more left or right politically) can be targeted and their social channels may be manipulated. Hackers and disinformation artists in the 2016 election showed their proclivity for targeting media at the more extreme ends of the political spectrum as they discerned it was easier to manipulate them by confirming their biases. We can expect a similar pattern of activity to emerge in the 2020 elections, given how effective the tactics proved to be in 2016. Additionally, the social presence of these media channels may be used as a vehicle for manipulation as well, both through disinformation in the form of sock puppet accounts that drive a specific narrative, and through the datamining of these channel’s followers as rife sources for lists of and information on potential individual targets.

4. **Manipulation of voting machines:**
   Recently, a group of white hat hackers participating in the Def Con Voting Village event proven that machines used in more than half of the U.S. States in 2018 were vulnerable to hacking, and this vulnerability remains for 2020. While there's no evidence of this directly occurring in previous elections, the possibility is very real.

   From MSSP Alert:
   "The Voting Village hackers found new way to “replicate previously published methods, of compromising every one of the devices in the room” that could change vote tallies, ballots or manipulate the machines’ software, the authors wrote. This despite the participants having no prior knowledge of the voting systems and only the hacking tools at their immediate disposal."

5. **Manipulation of servers with critical vote data and laptops/desktops that touch that data:**
   Many such servers and/or critical computers have been found to have active, direct connections to the Internet, which makes them even more vulnerable to attack. Attackers can stealthily modify files, internal server or computer memory, boot files, and binaries to change or corrupt voting data. In 2017, a server critical to Georgia elections was wiped clean by a hacker after a lawsuit was filed.

Study of these attack surfaces by white hat hackers, security experts, lawmakers, and companies such as VMware Carbon Black have led to the formulation of a set of best practices codified by the U.S. Department of Homeland Security – CISA and a questionnaire for State and Local Governments to use to determine their vulnerability, which can be found here: [https://www.us-cert.gov/ncas/tips/ST19-002](https://www.us-cert.gov/ncas/tips/ST19-002)
10 Best Cybersecurity Practices for Government Entities

1. As many government entities are using outdated security methods and products, it is critical to get a baseline on where vulnerabilities lie. A baseline “Red Team” or “Purple Team” (uses a third party plus in-house security experts) audit and/or Cyber Hunt exercise can help expose where systems are vulnerable and where increased controls need to be applied. PEN tests and general audits are also recommended.

2. Multi-factor authentication with “just in time” administration should be deployed to web servers, and servers holding key data. Websites that are accessible to the general public should be reviewed for accuracy continuously.

3. Deploy application control (whitelisting) on critical servers, ensure they do not touch the raw Internet, and place them in high enforcement and only allows approved programs to run, stops all unauthorized file or memory modifications, and has been used for many years by universities and financial institutions to protect critical data.  

4. Create a comprehensive microsegmentation strategy for your network and then execute it – flat networks are much more easily hacked and more of your critical network will be exposed during that attack. Microsegmentation is simply the practice of isolating segments of your network or data center into “enclaves” that are separate from each other. This limits the expansion and reach of an attack if one occurs. If you don’t have expertise in house for this task, money spent for a consultant will be well worth the extra expense.

5. Deploy endpoint detection and response (EDR) technology as well as non-signature based NGAV (next generation antivirus) that uses unfiltered data to detect and remediate advanced attacks (even zero day attacks.) Remember, the endpoint is the easiest attack surface for hackers.

6. Integrate your critical security systems across your network. (NOTE: VMware Carbon Black integrates with most firewalls (although firewall integration is not necessary for endpoint quarantine and isolation. Most SIEMs can be integrated with VMware Carbon Black’s RESTful APIs, and integration with cloud security providers such as NetSkope can help ensure that the cloud doesn’t become a point of ingress for bad actors.)

7. Continually work to attract, hire, and retain the best security talent in order to ensure you are not only protected, but know how to remediate if an attack happens.

8. Stay up to date on the latest attack methodologies as well as attack vehicles. VMware Carbon Black’s Threat Analysis Unit (TAU) provides customers with the latest knowledge and information. Our User Exchange also is a rich source of data and intelligence. Take time to attend conferences, and network with other government security teams.

9. Use a product that allows the integration of third party threat feeds. This way, you can stay on top of the latest innovations by bad actors.

10. EDUCATE! EDUCATE! EDUCATE! Make sure that everyone in your network, your administration, and your leadership understands the importance of cybersecurity, how not to fall for phishing attacks, and how to maintain a secure environment.