Osterman Research
WHITE PAPER

White Paper by Osterman Research
Published **December 2019**
Sponsored by **Zix**

Cyber Security in Government

Executive Summary

State and local governments, municipalities, city councils, local law enforcement agencies, federal government agencies, and other government entities – collectively the government sector – are under attack from cyber criminals and nation-states. Threats from ransomware, business email compromise, phishing and other security threats are relentless, and 2019 has been a banner year for various types of attacks against government.

This white paper explores the current state of security threats in the government sector today and offers direction for government decision makers and influencers wanting to increase the effectiveness of their security capabilities.

KEY TAKEAWAYS

- The threats are real and growing because they continue to be successful. For example, numerous government entities have been compromised by ransomware in the past year, leading some to pay millions to clean up and recover from the attack. Others have opted for the easier path of paying the ransom demand, usually covered by their cyber security insurance policy (which was already in place).

- There are several basic security defenses that must be activated for all government entities to drive back security threats. Stronger authentication methods including the use of strong multi-factor authentication is an essential step, as is keeping systems patched and up-to-date. The latter benefits from clear visibility into vulnerabilities across all connected devices.

- There are many advanced solutions and capabilities available that should be investigated for applicability, in light of a risk profile for each government entity.

- Technology solutions alone will not solve the cyber security threats facing the government sector. People play an equally important role, and significantly increasing the awareness of security threats, social engineering attacks, and other common risk situations must go hand-in-glove with technology and process changes.

- There are early warning signs that what's started as a financial annoyance with ransomware will escalate to cyber warfare. The NotPetya attack[i] in 2017 had devastating effects in the Ukraine (and beyond), and the vulnerabilities easily exploited for financial gain could just as easily be exploited to create destruction across large-scale transportation, energy, and telecommunications infrastructure.

Attacks on the government sector are many and varied.

ABOUT THIS WHITE PAPER

This white paper was sponsored by Zix; information about the company is provided at the end of this paper.

Cyber Security Threats in Government: A Snapshot

From small municipalities in the United States, a tram system in Ireland, and city councils in the United Kingdom, the attacks on the government sector are many and varied. Attacks include (this is a non-exhaustive list):

- **Ransomware**
  Numerous ransomware attacks in 2019[ii] have affected entities in the government sector, inflicting significant cost through either emergency remediation or payment of the ransom demand. Successful attacks hit four municipalities in the state of Florida (April and June)[iii], more than 20 local government organizations

in the State of Texas (August)[iv], and two power utilities in India (August)[v]. Several recent market research studies have also noted the high attack rate in the government sector. For example, a report from a leading security provider highlighted that two-thirds of more than 70 ransomware attacks in the United States in the first half of 2019[vi] had local and state government organizations in the crosshairs.

- **Phishing**
  Nine out of ten attacks start with phishing. While successful ransomware attacks capture the headlines, it's the relentless phishing campaigns that underlie the vast majority of ransomware deliveries and compromised account credentials that provide system access to cyber criminals. The general consensus is many ransomware attacks start with a phishing campaign – either broad-based or highly targeted (spear-phishing). In response to its Freedom of Information requests, an insurance company in the United Kingdom found that local councils were subject to almost 800 cyber-attacks per hour[vii], which in aggregate swells to more than 250 million individual attack attempts over six months; many of these attacks were phishing or spear-phishing attempts. In the face of such relentless attack attempts, it is almost guaranteed that phishing messages will successfully route into a user's inbox. In the United States, the City of Naples in Florida was the victim of a spear-phishing attack in July 2019[viii] that netted a cool $700,000 for the cybercriminal; this occurred after the wider Collier County suffered a similar attack in December 2018 that netted $184,000[ix]. Phishing – rather than malware – is increasingly the attack vector of choice because it is so lucrative and successful.

- **Multi-Factor Authentication (MFA)-Resistant Phishing**
  Over the past year cyber criminals have designed phishing attacks that circumvent certain types of multi-factor authentication protections. Carefully created phishing campaigns linking to fake-but-realistic destination login sites have been able to bypass both short message service (SMS)-based and authenticator-app based second factor approaches, enabling successful account credential compromise. Amnesty International noted the use of MFA-resistant phishing attacks on journalists and activists in the Middle East and North Africa. Several security experts have demonstrated similar attack methods.

The government sector is one of the top three sources of breached records.

- **Business Email Compromise (BEC)**
  Capturing login credentials for business email accounts enables cybercriminals to attempt to defraud organizations of vast sums of money. The FBI reports that, globally, more than US$5 billion has been lost to BEC scams[x]. Over the past year in the government sector, a public school in Portland almost lost US$3 million to a successful BEC attack[xi], and a county in North Carolina was tricked into paying US$2.5 million into the wrong bank account for a contractor working on a local project (some of which it was able to recover through quick action by the bank)[xii].

- **Data Breaches**
  The government sector is one of the top three sources of breached records. Mega-breaches include the US Office of Personnel Management in mid-2015 with 21.5 million sensitive data records breached[xiii], and the US Justice Department in 2016 with a data breach exposing contact details for more than 20,000 FBI and Homeland Security employees[xiv]. A White House audit in 2015 discovered a cumulative 77,000 cyber incidents across government, with theft of data a common occurrence[xv]. In late October 2019, hackers breached the City of Johannesburg and claimed they had exfiltrated sensitive financial and personal data[xvi]. The hackers said they would publish the data if a ransom payment was not made.

- **Malware**
  Commonly used server and desktop operating systems in use in government circles suffer from known vulnerabilities, and unpatched systems of all kinds

elevate the risk of being compromised by many types of malware. The NotPetya ransomware attack in 2017 succeeded in gaining a destructive foothold across the globe due to exploits of known-but-unpatched vulnerabilities in Windows-based devices. Other malware works stealthily in the background over time to scout the infected network and spread quietly to infiltrate an ever-expanding collection of devices before turning lethal.

- **Non-Malicious Human Error**
  People make mistakes. Email mishaps happen because phishing attempts are increasingly convincing, with the easy giveaways of social engineering becoming fewer and less obvious. Type-ahead addressing in email messages makes it all too easy to accidentally send sensitive data to the wrong recipient. And public-service-minded employees can believe innocent-sounding requests that are only a cover for fraud.

- **Malicious Insiders**
  Employees with malicious intent are a leading cause of security breaches and successful attacks across all industries, and according to the Verizon Insider Threat Report of 2018[xvii], public administration services is the second highest industry affected by insider and privilege misuse. With the US government employing over two million people, even if only 0.1 percent of all employees act maliciously with respect to cyber security, that's 2,000 malicious insiders at work in the US government sector today. It is likely many are hidden and deeply embedded in the critical systems that run US government operations, and are working quietly to gain even greater powers and system access.

- **Election Interference**
  Foreign governments, cyber activists, and email hackers have interfered with the apparatus of democracy – elections – in recent years, including the presidential election in the United States in 2016, the Brexit vote in the United Kingdom in 2017, and the election of the European Parliament in 2019. Election interference is a highly political and sensitive issue for all involved, because it affects the trajectory of both countries and careers.

In summary, government entities are faced with on ongoing barrage of security threats from multiple directions. In the next section, we consider why government entities are such a highly attractive target.

Governments across the world find themselves under cyber attack.

Government is a Highly Attractive Target

Governments across the world find themselves under cyber attack. The government sector is attractive to cybercriminals for many reasons, including:

- **Hold Vital and Classified Data, Operate Critical Infrastructure**
  Government entities hold sensitive data on citizens (e.g., PII, PHI, court records, and more) and also operate the critical infrastructure and systems that run cities and states. Cyber-attacks that compromise sensitive data hand ammunition to cyber criminals for more informed profiling of potential attack victims, and attacks that compromise critical infrastructure threaten mass disruption or destruction of whole ecosystems. Although not at the extreme level of disruption, the ransomware attack in Baltimore in May 2019 halted the real estate market in the city for at least two weeks, because transactions could not be completed with city officials[xviii]. The ransomware attack on the City of Atlanta in March 2018 compromised around 150 applications, including mission critical services such as the court system and police[xix]. The Atlanta's Attorney Office lost 71 of its 77 computers and a decade worth of documents in the attack.

- **Government Employees with Intense Workloads**
  Employees working at state and local government entities face multiple competing priorities by demanding constituents, while simultaneously working through long task lists. Because of this, they are easily caught off guard by social engineering attempts creating an environment ripe with security vulnerabilities.

- **Cyber Security Is Only One Issue**
  A government ecosystem presents a complex and multi-faceted attack surface, with cyber-security being only one of the critical security threats at play. National defense, terrorism, emerging technologies that offer new ways of creating weapons, and infectious diseases, among many others, make up a conglomeration of critical issues. The US government, for example, has over 25 critical national security threats to manage. With an attack surface so wide and unwieldly, it's easy to be blind to any given threat event.

- **Insufficient Supply of Cyber Security Professionals**
  There is a general shortage of cyber security professionals across all industries, with millions of unfulfilled jobs available around the world. The number of unfilled cybersecurity roles will grow from one million in 2018 to 1.5 million by the end of 2020. As of January 2019, the U.S. faced a shortfall of almost 314,000 cybersecurity professionals across all industries. With the private sector often willing to pay at the higher end of the scale for top-flight cyber security professionals, government agencies of all kinds will bear the brunt of the shortage.

- **Insufficient Funding**
  Across all industries, the general recommendation is to spend at least five percent of the IT budget on IT security. While some government entities spend at this level, many municipalities spend less than a fifth of this recommendation. Spending is directed to other competing priorities, and security gets short-changed.

- **Low Cyber Security Readiness**
  With the combination of an insufficient supply of cyber security professionals and insufficient funding directed towards IT security, it should come as no surprise that the government sector often ranks at the low end of cyber security readiness assessments. Third parties have verified in independent assessments that government is near or at the bottom in their cyber security assessments.

- **Many Smaller Cities and Agencies**
  There are thousands of small cities and agencies in the United States that can be targeted by security threats. The United Kingdom, similarly, has over 400 local city councils. Each entity carries the responsibility to protect itself from cyber security threats, and as smaller entities, will have fewer full-time cyber security professionals than the large government agencies. Lacking the people, processes and technologies for a hardened cyber security surface, smaller cities and agencies are relatively easy pickings for cyber criminals, as witnessed by the increased willingness among US municipalities to pay ransom demands rather than go through the more costly process of rectifying faltering systems.

- **Decentralized Budgets and Security Operations**
  The right of self-determination for security expenditure and security operations isolates each government entity as standalone. Non-integrated security solutions and separate instances of threat data almost entirely eliminate the ability for shared learning to flow across municipalities, local governments, and local law enforcement agencies.

- **Moving to the Cloud Without Proper Security Increases Risk**
  While agencies look to the cloud to reduce cost and increase capabilities, many private and public sector entities are seeing increased risk and threats due to the open nature of the cloud and the new shared security model. Many entities that

> ***A government ecosystem presents a complex and multi-faceted attack surface.***

have moved to cloud solutions have become subject to increased security threats without corresponding security capabilities offered by their cloud provider. This requires expertise in determining whether native cloud-based security tools or third-party tools are best suited for their specific use.

- **Outdated Equipment and Software**
  Windows 7 hits end of life in mid-January 2020, which according to StatCounter, almost 30 percent of the global installed base of Windows desktops are still running. With no security updates, patches or support available for Windows 7 after mid-January, and over 500 known vulnerabilities already documented for the operating system, continued use of Windows 7 and Windows Server 2008 and their earlier versions (e.g., Windows 2000 and Windows XP that have long been unsupported) provides an opportunity for cybercriminals to exploit any remaining unpatched vulnerabilities. Government agencies still running older, unpatched, and unsupported operating systems will continue to be highly vulnerable to malware.

While the government sector is increasingly under cyber-attack – and make perfect targets because they run essential services for constituents – it is not the only sector under attack. Most cross-industry research concludes that security threats are unleashed across all industry sectors.

Expectations of Changing Threat Dynamics

Ransomware attacks on government targets have held the headlines over the past year. But what about going forward? In light of the current state of threats – and the opportunities cybercriminals have to embrace the weaknesses in the government sector – where do we see attacks intensifying over the coming year?

> ***Ransomware attacks on government targets have held the headlines over the past year.***

PICK OFF WEAK TARGETS

Wherever the government sector is weakest, cyber criminals motivated by financial gain will do more. State and local governments, municipalities, city councils, and local law enforcement agencies lacking strong security defenses and suffering from a dearth of cyber security professionals will remain in the crosshairs. The evidence from 2019 shows some cities are willing to pay the ransom to get back to work quickly – and this only emboldens cyber criminals to attack again.

RANSOMWARE OFFERS GREAT ROI; EXPECT MORE

Cybercriminals have found great financial success in ransomware attacks, because the economics are always in favor of paying the ransom rather than doing the deeper work to recover, restore, and harden all systems. It is always cheaper to pay the ransom unless all precautions and safeguards are already in place. Two examples from the State of Georgia are insightful. When Atlanta suffered a ransomware attack in 2018 and chose to recover without paying the ransom, their clean-up bill totaled more than $18 million, a huge escalation over the initial $2.6 million estimate to clean up, and a far greater number than the ransom demand of $51,000. In 2019, however, when Jackson County was ransomed, they paid the $400,000 ransom and got back to work[xx]. As noted above, we have also seen two cities in Florida in mid-2019 go the pathway of just paying the ransom (it is unclear whether the third city did or did not pay the ransom to recover). For one of those cities in Florida – Lake City – paying the ransom did not result in a quick and full restoration, with some city data still unavailable a month after paying the ransom[xxi]. Overall, in general, while the immediate threat goes away by paying the ransom, it does nothing to prevent a ransomware attack from happening again.

It is foreseeable that cybercriminals could almost run a monthly subscription service of ransom payments against weakly secured ineffectual government agencies, much like the mob-protection payments of old. Over the coming year, we expect to see ongoing ransomware attacks; it offers easy money for cybercriminals because city governments have proven only too willing to pay.

FROM RANSOMWARE TO DESTRUCTWARE

Ransomware attacks cause financial annoyance; destructware attacks are designed to cause mass chaos through destruction of IT systems and processes for essential services. Cybercriminals don't seek financial gain through destructware, but rather economic collapse. Compromising control systems and operational technology at nuclear power plants, power transmission grids, and mass transportation systems hold the tantalizing possibility of crippling entire economies. For example:

- The NotPetya attack in 2017 was an early-warning shot in destructware, with the country of Ukraine bearing the brunt of its destructive payload.
- Several industrial plants in Saudi Arabia[xxii] were the victim of destructware attempts in recent years, with an unnamed petrochemical company narrowly avoiding a destructware disaster in August 2017.
- Destructware can also be used to enable insidious data corruption of sensitive data such as health records, drug formulations, quality control standards, and more. Over the long run, these subtle modifications to data could have deadly effects and undermine consumer confidence.

While not all cybercriminals seek such drastic outcomes – and will thus continue to focus on financial gain through ransomware – some nation state threat actors have different motivations.

Several ransomware attacks in the government sector over the past year… have flowed from compromised trusted supply chain partners.

Solutions to Consider for Improving Cyber Security in Government

There is no single solution for improving cyber security in government. The attack space is so broad and the environment so complex that a coordinated set of solutions is essential. In this section, we look at the types of solutions that all government entities should consider to improve their cyber security readiness. The solutions profiled in this section flow from five core principles:

1. **Reduce the Attack Surface**
   Be proactive about removing potential footholds where cybercriminals could start. For example, keep systems patched against known vulnerabilities, use conditional access policies to reduce the ability for credentials alone to be used for system access, and harden email systems against spoofing and impersonation through strong email authentication approaches. Use network isolation and segregation approaches to decrease the ability for a single compromised device to spread malicious payloads. Set policies on accessing personal social media accounts on government networks (because malicious links can be shared without going through a secure email gateway), and limit access to government systems from home or unmanaged devices.

2. **Audit Efficacy of Current Cyber Security Solutions**
   Assess the current efficacy of your cyber security solutions to see what is and isn't working, and where the gaps are. Visibility into what is and isn't working enables the development of a prioritized plan of action to remediate weaknesses and bolster defenses.

3. **Monitor Your Supply Chain for Security Threats**
   Several ransomware attacks in the government sector over the past year, including the August 2019 attack in Texas, have flowed from compromised

trusted supply chain partners. Audit current system access mechanisms and linkages for security threats that begin with trusted third-parties, and harden background processes to reduce the likelihood of threat-laden compromises being overlooked because they originated with a trusted partner. On a broader scale, government agencies, with the U.S. Department of Defense in the lead, are taking steps to ensure their providers are secure by moving beyond a self-attestation model to a third-party compliance model to validate authorized providers meet cybersecurity compliance requirements. Pay attention to the Cybersecurity Maturity Model Certification (CMMC) which goes into effect in June 2020.

4. **More Than Just Cyber Protections**
   Protecting against cyber threats requires more than just technology solutions; people and process protections are equally necessary. Process examples include background checks on new employees, policies on physical access to computer printouts (e.g., a clean desk policy, and how trash is managed), secure computing and cyber security awareness training and restricting access to the physical devices that hold classified data.

5. **Consider a layered cybersecurity approach on top of SaaS solutions with purpose-built products**
   Many cloud solutions offer native cybersecurity capabilities; however these are often limited and not as effective as purpose-built cybersecurity services. In addition, native cybersecurity capabilities require additional licensing costs that are more expensive than utilizing a purpose built, evolving cybersecurity product.

Solutions for improving cyber security in government are:

STRENGTHEN IDENTITY ACCESS CONTROLS

Strong, complex, frequently changed, and unique passwords are not working. Users forget them, incrementally numerate passwords to simplifying recall, or write them down. Once credentials have been compromised – even if it's a long password or passphrase – cyber criminals still have access. Strengthen access controls through new approaches that don't rely on passwords, either by removing passwords altogether in favor of FIDO2-enabled passwordless authentication or other modern authentication mechanisms.

PROTECT DATA WHERE IT RESIDES

> ***Bad actors infiltrate agencies primarily to access valuable data.***

Bad actors infiltrate agencies primarily to access valuable data. To ensure a complete cybersecurity strategy, ensure your databases are secure, patched, vulnerabilities remediated, user rights reviewed and limited and monitored for suspicious activity. A continuous assessment and continuous protection model is recommended to ensure target data is appropriately inventoried, tested for vulnerabilities, rights management enforced for least privilege, monitored for anomalies, and alerted when incidents arise for fast response and system remediation.

Encryption solutions apply strong protections to email messages and documents that contain sensitive, confidential or other private information that should not be widely shared. Transparent encryption works through automatic policy application based on contents or other rules, and access rights define who is – and who is not – permitted access. Messages and documents that are encrypted appropriately remain inaccessible in the event of a security breach.

STRONG MULTI-FACTOR AUTHENTICATION (MFA)

Reliance on a username and password for controlling access to systems is no longer enough for any government employee—and hasn't been for several years. If access credentials can be compromised just by asking for them through a phishing campaign, an attacker can take whatever data they want when they want it, or use modular malware to extend from an initial foothold to compromising additional systems and planting malware for a subsequent more devastating attack. Approaches for MFA are available on a good-better-best continuum, with good (SMS code, email notification) and better (Authenticator app) approaches still being vulnerable to carefully designed phishing attacks. The best approach currently, which ideally would be provisioned for all government employees, is to use modern hardware security keys based on FIDO2 that use public-key cryptography. These also provide an additional promise of secure passwordless logins, which has been the holy grail for authentication. Some security keys provide multi-protocol support so that organizations can easily bridge between legacy systems and those supporting modern authentication protocols.

Any approach to MFA is better than doing nothing, but continuing with approaches that have already been compromised and expecting a different outcome is ill-advised.

DEFEND AGAINST PHISHING

Reduce the likelihood of phishing messages getting through to end-users and being used as a threat vector for stealing credentials or deploying malicious payloads on a device. Clean the flow of email messages using advanced threat protection mechanisms, such as deep analysis of links, sandbox detonation of attachments, and language profiling to highlight suspect spear-phishing emails. Harden your overall email system with SPF, DKIM and DMARC (currently not available in the E1 and E3 Office 365 packages). Get to a DMARC policy of reject so email identities cannot be used to phish internally or externally and leverage the best possible approaches to MFA to eliminate the cost of credentials compromised through human error.

VISIBILITY INTO VULNERABILITIES AND TIMELY PATCH MANAGEMENT

In principle, as above, reducing the attack surface through patching known vulnerabilities is essential. But in order to execute on the principle, complete visibility into vulnerabilities across a network and its fleet of connected devices is required. Vulnerability management solutions show where weaknesses currently exist, and use newly-issued threat intelligence to enable continuous insight into high-risk threat vectors. Vulnerability management solutions also aid with closing the gap across a heterogenous collection of security tools, showing where security holes and weaknesses remain.

In addition to threat vectors, insight into vulnerable assets in the context of surrounding network infrastructure is also key to understanding exposure to those threats. Likewise, understanding of surrounding security controls can help to create defense-in-depth and to mitigate risk.

> ***Strong cyber security operates at the intersection of people, process, and technology solutions.***

SECURITY AWARENESS TRAINING

Strong cyber security operates at the intersection of people, process, and technology solutions. On the people side, security awareness training is essential for cultivating a degree of caution and an attitude of thoughtful consideration before opening an email, clicking a link, or enabling macros in an unexpected document, among other direct threats and social engineering attempts. Simulation exercises strengthen security awareness by evaluating the efficacy of employees to identify threats and act appropriately.

CLOUD SECURITY SERVICES

Replace the era of the lone cyber security analyst fighting blind against the world with security services that operate at cloud-scale. Cloud-based security services remove the need for individual on-premises deployments at each government entity and offer threat intelligence based on observed data points and threats across a whole collection of government entities. Access to highly trained threat experts is often also available, supplementing the work of the lone cyber security analyst with a much wider team with deeper security skills. Using cloud security services and trusted security advisors offers a very practical way to address the talent shortage in cyber security.

DATA LOSS PROTECTION (DLP)

DLP solutions examine the contents of email messages, email attachments and stored documents for sensitive information and apply appropriate protections. DLP policies support automatic encryption, quarantining, and routing for approval before being released. DLP solutions safeguard against accidental data breaches by a careless insider and provide early warning and detection of potentially malevolent activity by a malicious insider.

VISIBILITY INTO CLOUD SERVICES USAGE AND THREATS

A Cloud Access Security Broker (CASB) provides visibility into activity and usage in connected cloud services. Analytics that run across all activity and usage logs can highlight security threats, such as compromised credentials. For example, if the same credentials are used for logging into cloud services from weird locations (outside the municipality or in foreign countries where an agency has no presence) or from multiple locations that would require impossible travel, a security alert can be raised for investigation and/or a proactive security policy initiated to limit the access granted to the login attempt. A CASB usually either integrates with or offers its own DLP solution as well, for seeking out and identifying sensitive data that is over-exposed and under-protected.

Another important consideration is visibility of the hybrid network infrastructure – connectivity between and within networks/zones. Modeling and simulating access or attacks on these environments can ensure proper segmentation is enforced at all times. Moreover, this will also shed light on all ingress and egress points and it will reveal where third-party connections may be putting an organization at risk.

RANSOMWARE-RESISTANT BACKUP SERVICES

With ransomware being an ongoing existential threat to government entities, having the appropriate precautions and safeguards in place before being the victim of a ransomware attack is essential. Access to an up-to-date backup copy of data-held-for-ransom streamlines the recovery process, as demonstrated by the Dutch parliament in 2017 after a ransomware attack. Online and offsite backup services offer one approach. Another approach is to use a network-based backup solution running on Linux, which carries less risk of being compromised through ransomware.

Because ransomware is a financially driven attack method, attackers want to achieve the best return-on-investment that they can. As such, they attackers will use and reuse vulnerabilities with known exploits to launch the attack rather than investing efforts in developing zero-day threats. As a result, correlating vulnerabilities with up-to-date threat intelligence on exploits leveraged by ransomware will help focus attention on the vulnerabilities that are most likely to be used in these attacks. Patching these vulnerabilities can help to ensure that government entities are not viewed as "low-hanging fruit" by opportunistic cyber criminals.

RISK-BASED AUTHENTICATION

Solutions for risk-based authentication or conditional access take into consideration additional factors about the user and the context of the authentication request, such as geo-location, the network they are connecting through, and the status of the device and applications they are using. For example, if the location is abnormal, the network has not been seen before, or the device is unmanaged, these additional risks are used to escalate the type of authentication request issued or to reduce the level of access granted. This could result in a request for strong multi-factor authentication, or only granting read access to a document. Risk-based authentication reduces the attack surface in line with principle 1 above, reducing the scope for inappropriate or potentially unsafe access requests.

ENDPOINT PROTECTION

As with MFA above, endpoint protection solutions cover a continuum of good-better-best. Good solutions offer protection against known and emerging threats through regular scans and continuous monitoring. Better solutions add shared visibility for

> ***Endpoint protection solutions cover a continuum of good-better-best.***

cyber security professionals of threats across all connected endpoints, along with the ability to proactively hunt for, detect and remediate vulnerabilities before and after a security breach has occurred. The best solutions proactively harden each endpoint by preventing any activities outside the parameters of a normal acceptable pattern from executing.

MODERNIZE WITHOUT MICROSOFT

Microsoft reached its original mission of "a computer on every desktop," but did so at the expense of deep security. Moving away from Windows-based endpoints immediately reduces the number of vulnerabilities that can be exploited. While no endpoint device has perfect security, replacing Windows endpoints with Linux, Chrome OS or Mac devices reduces the security attack space. Fewer malware and ransomware programs target non-Windows endpoints.

MESSAGE AND DOCUMENT ARCHIVING

Email archiving solutions allow the government sector to retain email data for long periods of time and to ensure those emails are secured. With the increase in regulation globally there is a greater emphasis on knowing what data is held, who has access to the data and how quickly the data can be found and actioned.

LEARN FROM GOVERNMENT COLLEAGUES

The Multi-State Information Sharing & Analysis Center (MS-ISAC) is a government sector-focused cyber security community, offering security operations, incident response services, cyber security advisory, and education, among other services. Membership is open to employees of U.S. state governments, local and tribal governments, and public education entities.

> ***Email archiving solutions allow the government sector to retain email data for long periods of time and to ensure those emails are secured.***

ENSURING GOOD INSTEAD OF CHASING BAD

In order to create true defense in depth security posture, organizations need to layer solutions that focus on malicious code or behavior detection (e.g. AV, EDR, UEBA) with tools that focus on the opposite. Those can include system hardening, isolation/microvisualization, app control and OS behavior whitelisting tools. This combination assures better detection of both known and unknown attacks.

CYBER SECURITY INSURANCE

A cyber security insurance policy reduces the financial costs carried by a government entity in the situation that a cyber-attack is successful. Several municipalities have leveraged their cyber security insurance protection during 2019 to fund the ransom payment and get an easier exit after a ransomware attack (although there are ongoing drawbacks to taking this approach, as noted earlier). Cyber security insurance policies can also provide protection against the costs of a data breach, for example.

A SECURE ROOT OF TRUST

Of significant benefit to government employees, particularly those who are frequently out of the office, is the concept of a secure and portable "root of trust". Because employees lose devices and may want to use new ones periodically, a secure root of trust in the form of an internal (e.g., a fingerprint pad on a laptop) or external (e.g., a USB device) key enables more rapid recovery for the user when the device is lost or when they need to access a new platform.

THE CYBER SECURITY SKILLS GAP

What can government agencies do about not having enough of or the right personnel to get the most out of their current and future tools? Do they have enough of or the right staff to harden their current environment? Should they seek help from a trusted security advisor here? This is a key issue for government agencies that may not be able to offer the same level of salary as private companies, and so may suffer from an even greater problem in attracting good talent. This issue needs to be addressed, since not having sufficient skilled staff members is closely tied to misconfigurations that lead to breaches.

One way to address the cyber security skills gap is through the use of intelligent automation solutions. By offloading repeatable tasks or tasks that are too complex to be handled manually, it will help existing security teams to focus their attention on more strategic actions.

Conclusions and Next Steps

In this white paper we have looked at the state of cyber security in the government sector, reviewing current threats, the attractiveness of the sector to cyber criminals, and the profile of security threats and attacks we expect over the coming year. We have reviewed the type of cyber security solutions that entities in the government sector - municipalities, state and local governments, and local law enforcement agencies, among others - should be investigating to reduce the likelihood and severity of security threats.

We conclude with three next actions:

1. Assess cyber security readiness, threats and areas of concern. Phishing attempts, unpatched systems, and missing security solutions are likely to feature highly for most government entities.

2. Prioritize threat areas and take action. Informed by your readiness and threat profile, prioritize the current threat areas and take action. This should include the three areas of people, process and technology in order to create robust defenses.

3. Investigate solutions that offer cyber defenses beyond a single city, agency, local law enforcement unit or other government entity. Everyone in the government sector is facing the same cyber security threats and leveraging solutions that can aggregate threat intelligence from across a wider population to protect everyone in the population are to be preferred than isolated approaches.

Sponsor of This White Paper

To better meet your company's security, data protection and compliance needs, Zix can enhance your Office 365 environment with advanced threat protection, archiving and email encryption. Zix delivers a superior experience and easy-to-use solutions that have earned the trust of more than 19,000 organizations including the nation's most influential institutions in healthcare, finance and government.

To defend your company from malware, ransomware, phishing and other email threats, ZixProtect combines a multi-layer email security approach with automated traffic analysis, machine learning and real-time threat analysts. In addition, ZixProtect's business continuity feature ensures that your organization can continue to communicate if your email experiences a disruption.

ZixArchive eases email archiving and eDiscovery with automatic email collection and storage in a secure cloud. Its automatic indexing and multiple search criteria gives you and your employees convenient and rapid access to archived emails. ZixArchive also enables you to share an email hold with outside legal counsel and auditors and revoke privileges when access is no longer needed, keeping your data within your control.

To ease email encryption for you, your employees and your recipients, leverage the industry's leading solution ZixEncrypt. Automatic transparent delivery between

zix®

www.zixcorp.com

@ZixCorp

+1 866 257 4949

sales@zixcorp.com

customers and robust delivery methods for other recipients enables easy access to encrypted email for anyone, anywhere and on any device, making the user experience exceptional and compliance simpler. Proven policies and advanced reporting provide peace of mind, while customizable branding and security capabilities make email encryption fit your unique company needs.

Leveraging our more than 15 years of hosted experience, you can have confidence that Zix email security solutions integrate seamlessly with Office 365. You also benefit from the support of the ZixData Center, a state-of-the-art facility with PCI DSS 3.2 certification, SOC2 accreditation and SOC3 certification. Staffed 24/7/365, ZixData Center has a track record of consistent 99.999% availability. In addition, Zix delivers exceptional customer support 24/7/365 no matter your questions or concerns.
With reliability, experience and superior support, Zix improves email security for your Office 365 environment. To learn more about our solutions for Office 365, visit www.zixcorp.com/office365.

Osterman Research, Inc. does not provide legal advice. Nothing in this document constitutes legal advice, nor shall this document or any software product or other offering referenced herein serve as a substitute for the reader's compliance with any laws (including but not limited to any act, statute, regulation, rule, directive, administrative order, executive order, etc. (collectively, "Laws")) referenced in this document. If necessary, the reader should consult with competent legal counsel regarding any Laws referenced herein. Osterman Research, Inc. makes no representation or warranty regarding the completeness or accuracy of the information contained in this document.

THIS DOCUMENT IS PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND. ALL EXPRESS OR IMPLIED REPRESENTATIONS, CONDITIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS ARE DETERMINED TO BE ILLEGAL.

REFERENCES

[i] https://www.washingtonpost.com/world/national-security/russian-military-was-behind-notpetya-cyberattack-in-ukraine-cia-concludes/2018/01/12/048d8506-f7ca-11e7-b34a-b85626af34ef_story.html

[ii] https://www.msspalert.com/cybersecurity-breaches-and-attacks/ransomware/attack-list-cities-government-agencies/

[iii] https://www.naplesnews.com/story/news/crime/2019/08/20/7-florida-municipalities-have-fallen-prey-cyber-attacks-ryuk-ransomware-phishing/2065063001/

[iv] https://arstechnica.com/information-technology/2019/08/ransomware-strike-takes-down-23-texas-local-government-agencies/

[v] https://www.cybersecurity-insiders.com/ransomware-attack-on-telangana-and-andhra-pradesh-power-utilities/

[vi] https://www.cbsnews.com/news/ransomware-attacks-on-the-rise-and-governments-are-in-the-crosshairs/

[vii] https://www.infosecurity-magazine.com/news/uk-councils-800-cyberattacks-per/

[viii] https://www.naplesnews.com/story/news/local/2019/08/02/scammers-trick-naples-out-700-000-spear-phishing-cyber-attack/1902321001/

[ix] https://www.naplesnews.com/story/news/government/2019/08/19/collier-county-scammed-out-184-k-cyber-attack-phishing-scheme/2049019001/

[x] https://www.csoonline.com/article/3195010/bec-attacks-have-hit-thousands-top-5-billion-in-losses-globally.html

[xi] https://nakedsecurity.sophos.com/2019/08/22/quick-thinking-by-portland-public-schools-stops-29m-bec-scam/

[xii] https://www.journalnow.com/news/local/scammers-target-cabarrus-county-million-remains-missing/article_3daabb5b-3788-5a72-90c4-2c4fa0a5d078.html

[xiii] https://www.opm.gov/cybersecurity/cybersecurity-incidents/

[xiv] https://www.computerworld.com/article/3030983/hackers-breach-doj-dump-details-of-9-000-dhs-employees-plan-to-leak-20-000-from-fbi.html

[xv] https://www.reuters.com/article/us-usa-cyber/number-of-u-s-government-cyber-incidents-jumps-in-2015-idUSKCN0WN263

[xvi] https://www.dailymaverick.co.za/article/2019-10-25-attempted-hack-attack-triggers-system-shutdown-in-the-city-of-johannesburg/

[xvii] https://enterprise.verizon.com/resources/reports/DBIR_2018_Report_execsummary.pdf

[xviii] https://en.wikipedia.org/wiki/2019_Baltimore_ransomware_attack

[xix] https://en.wikipedia.org/wiki/2018_Atlanta_cyberattack

[xx] https://www.victoriaadvocate.com/counties/jackson/hackers-hold-jackson-county-computers-ransom-for-undisclosed-amount-of/article_046e6d1e-8316-11e9-97be-b70449000d28.html

[xxi] https://www.nytimes.com/2019/07/07/us/florida-ransom-hack.html

[xxii] https://www.itproportal.com/features/ransomware-attacks-one-critical-prevention-method-cisos-are-overlooking/