M3AAWG Messaging Malware Mobile Anti-Abuse Working Group

Messaging, Malware and Mobile Anti-Abuse Working Group

M3AAWG Summary Guidance: Essential Cybersecurity for Election Officials

February 2020

Executive Summary

Democracy depends on free and fair elections. The digitization of voting machines and the general reliance on digital communications have introduced new digital threats complicating the election landscape. With the advent of the internet, digital communications have increased across all sectors creating a host of new vulnerabilities. Most major data breaches begin with social engineering designed to steal one's login credentials, generally executed through email. Compromises using these credentials then circumvent many of the walls designed to keep attackers out because the credentials are in fact legitimate. Elections security in today's context is so much more than the security of the voting systems—everyone involved in elections must now be equally engaged in Cybersecurity.

The Messaging, Malware and Mobile Anti-Abuse Working Group (M3AAWG) has spent over a decade dealing with problems related to messaging abuse. M3AAWG has brought together a community of experts and organizations that include the largest mailbox providers on the planet, social networks, cybersecurity professionals, vendors, law enforcement, policy makers and a cadre of highly dedicated individuals donating their time and expertise to finding solutions to problems on a global scale. Over the years M3AAWG's mission has continued to expand to cover other abuse vectors, many directly relevant to securing election systems.

Numerous agencies have created best practices documents based on their unique expertise and focus. These documents span a wide variety of disciplines and address everything from the physical hardware used to cast votes to encryption methodologies and best practices for polling places.

Amongst the various guidance, there are technologies that are consistently recommended that make a significant impact on preventing abuse and compromise of elections systems, key amongst them are the use and application of Multi-Factor Authentication (MFA), email authentication, and encryption. If there are two things elections officials, or their designates can do to secure the upcoming 2020 general election in the United States, and those abroad they should consider doing the following:

1. Mitigate the impact of stolen access credentials by using MFA across all of their systems and accounts related to elections work. MFA should also be deployed across personal, social, and communications accounts to ensure that a compromise of a personal account could not be used in a social engineering effort to dupe a colleague in hopes of gaining further access to more sensitive and protected systems.

2. Mitigate spear phishing and eavesdropping by securing email communications through signing and publishing email authentication records and enabling encryption in transit. Our society, both the private and public sector, relies heavily on email as a means of communicating and coordinating businesses operations. Studies have shown that a vast number of data breaches start by

> compromising insecure emailing domains and systems and then obtaining credentials to more sensitive systems. Email security should be on top of the minds of elections officials. To that end they should consider deploying Sender Policy Framework (SPF) records, Domain Keys Identified Mail (DKIM) records, publishing a Domain Messaging and Reporting Conformance policy (DMARC) that rejects mail that fails a SPF or DKIM check to secure their email communications, and enabling STARTTLS.

This guide is a distillation of these various documents, M3AAWG best common practices (https://www.m3aawg.org/published-documents), and relevant news and research, intended to help election officials understand the need for these technologies in a manner that is digestible and actionable. This guide covers topics relevant to elections officials including:

1. Benefits of Multi-Factor Authentication (MFA)

2. Securing Email Communications

3. Web and General Security Guidance

The guide attempts to use plain language for election officials who may not be cybersecurity experts. Specific, actionable steps are included with a level of technical detail suitable to pass on as guiding details in the hopes of informing if not the reader, then those parties that can take decisive action to prevent and avoid certain threats and attacks.

Benefits of Multi-Factor Authentication (MFA)

Multi-Factor Authentication (MFA) is most likely a part of your daily life. If you've ever been asked to use your phone as a secondary means of confirming your access to your bank account, social media or email account, then you're actively using MFA to protect that account from compromise. MFA is becoming mainstream as software and applications leverage MFA technology to secure user access.

M3AAWG best practices recommend that MFA be used for "any commonly targeted user," of which election officials qualify. Election officials should use MFA on accounts that include personal and business email, social media accounts and voting systems as a first step in creating a robust security posture. Having MFA in place will prevent most attackers from successfully using stolen credentials to gain access to systems. **Election officials should strive to require MFA for all users, devices and platforms**.

Recent research by both Google and Microsoft has shown that using MFA showed a significant reduction in account takeovers — and MFA was 99.9% effective in protecting against bot and phishing attacks during the scope of their studies.

Types of MFA

Multi-factor authentication strengthens account security by combining two or more of:

- something the user knows (a password, passphrase or PIN)
- something the user has (such as a hard token or a registered smartphone)
- something the user is (a fingerprint, iris or retinal scan or other biometric factor)

Using a single factor listed above multiple times does not meet the necessary conditions. For example, just requiring two points "the user knows," like a birthplace and a pet's name, does not qualify as multi-factor authentication.

Election officials looking to implement MFA will see two general forms of MFA solutions: hardware keys and software. Both solutions utilize time-based one-time passwords (TOTP) that are generated by the device itself, and do not need to be online to do so.

Hardware based MFA is the more secure method of preventing account and system compromise, yet it bears higher implementation costs as it requires purchasing physical security tokens or keys. The Google research referenced earlier shows that during the scope of their studies hardware MFA was 100% effective in preventing bots, phishing and even targeted attacks. New threats will certainly reduce this effectiveness over time, but today hardware MFA is the most effective means of preventing unauthorized usage of compromised credentials.

Software MFA is a less costly alternative and is also highly effective. Less reliable methods include SMS or text to receive verification codes that do not require the user to install an app on their mobile device. SMS or text message based MFA is a less effective form of MFA, as it is more susceptible to targeted attacks, like simjacking, but is still superior to not having MFA at all.

Practical Applications and Uses of MFA

There is no silver bullet that can prevent all forms of attacks; however, MFA will prevent most attacks, and may sometimes help provide awareness of an attack in progress.

Where supported, MFA can be used to improve the security of: polling place information, email accounts of polling officials and volunteers and voting machines. Election officials should encourage staff and volunteers to secure their personal email accounts and social media accounts using MFA. Attackers can target and compromise a personal email account, leveraging that to gain access to more sensitive systems (such as vote tallying or reporting systems). The use of MFA can deter these kinds of attacks and protect election workers to ensure democratic elections can proceed freely and fairly.

Please note that not all MFA authentication is equally strong, and some types of MFA are not infallible. The National Institute of Standards and Technology (NIST) published June 2017 a comprehensive review in 8.1 Authenticator Threats.

Securing Email Communications

Email is the primary attack vector in large scale data breaches. Compromise of personal email accounts have led to the exposure of sensitive information. According to the 2018 Verizon Data Breach Report, 96% of cyber attacks began from email. Research from Phishme shows a similar statistic, 91% of the time, phishing emails are behind successful cyber attacks. Election officials should become familiar with email-specific attacks and the technologies and processes to effectively mitigate them.

Types of Email Attacks

There are two primary forms of email attacks election officials should become familiar with:

1. **Phishing** emails are designed to impersonate a legitimate brand, vendor, government office, or other good actors. Although the email looks as if it is from a legitimate source it's actually being sent by a bad actor to elicit a fear response from the recipient and convince them to surrender valuable information such as a password. Phishing often casts a wide net in order to compromise as many recipients as possible.
2. **Spear Phishing** is a more targeted and socially engineered form of phishing where the attackers choose their targets carefully and craft messages that are specific and highly recognizable to the recipient. Examples of spear phishing in the commercial sector include emails to the CFO of a company purporting to be from the CEO authorizing a payment to an overseas entity. In an elections context, spear phishing could look like an email from your vendor with an updated

firmware to download and install on a voting machine. The basic rule of thumb when it comes to spear phishing is if it seems suspicious, the best practice recommendation would be to verify the requested action (e.g., face to face or over the phone).

Government and Email

Due to the pervasive nature of phishing, governments have begun to mandate minimum email security standards at the federal level. These standards are an important development in election security by closing the email channel as a primary threat vector.

- The UK government was the first to do this in 2016 https://www.gov.uk/guidance/securing-government-email
- The US government followed in 2017
- The US DHS/CISA minimum standards for email security are in BOD 18-01 https://cyber.dhs.gov/bod/18-01/

Securing Email In Transit

Email is sometimes sent unencrypted or "in the clear," and there was no broadly adopted or systematic way to utilize encryption until the introduction of STARTTLS.

STARTTLS, in its most basic form, allows for a sending mail server to connect to a receiving mail server using *transport layer security (TLS)*. STARTTLS allows one mail system to tell another to use TLS to communicate if supported. Email sent through TLS connected servers is sent in a manner that helps prevent eavesdropping; essentially sending mail securely from one server to the next, even if not end-to-end. M3AAWG best practice recommends using TLS for all mail communications as a starting point. Realizing this does not guard against more advanced Man-in-the-Middle (MITM) attacks, M3AAWG provides additional guidance for helping to address these scenarios.

Supporting end-to-end encryption and digital signatures will provide a greater level of privacy and confidence that a message: 1) really comes from who it purports to come from, and 2) hasn't been altered in transit.

Enabling STARTTLS is generally made through a simple configuration change of your mail system. We urge election officials to consult with IT personnel and ensure that any and all email communications are sent through emailing servers with STARTTLS enabled.

Email Authentication

When email was first created there were no email specific compromises, phishing or other forms of email abuse. Email's architects couldn't foresee how email would grow and connect today's internet users. As a result, email was originally implemented with few security and privacy features.

In response to the growing abuses of email, and the openness of the platform, email authentication technologies were created to help prove the identity and authenticity of delivered email.

Email authentication helps to prevent the spoofing and other misuse of domains that you control. M3AAWG best practice documents recommend publishing appropriate email authentication records in the Domain Name System (DNS). Email authentication records can protect critical communications and ensure that election related domains and emails are significantly less likely to be spoofed and used as part of a phishing attack.

Forms of Email Authentication

Sender Policy Framework (SPF) — SPF was the first email authentication standard to be created. SPF is a simple text record residing in DNS which associates the sending domain used in email with a whitelist of IP addresses authorized to send from that domain. (For example, there's no reason why a laptop in a South American cyber cafe should be able to send email purporting to be from your state department of elections.)

SPF by itself can not fend off email borne attacks, yet SPF is an additional data point that can help determine the origin of email and whether it originated from an authorized source.

Domain Keys Identified Mail (DKIM) — DKIM is a cryptographic solution that uses a public/private key pair to associate an email with a unique identifier. A benefit of DKIM is the ability to determine if email has been manipulated in transit. Again, DKIM alone can not completely stem the tide of phishing or other forms of email abuse, yet it is a strong signal of legitimacy and, as with SPF, can help.

Domain Messaging and Reporting Conformance (DMARC) — DMARC makes sure that an email is both authenticated (using SPF or DKIM) and aligned, meaning the authenticated domain must match what is displayed to a user. By tying authentication to what a user is shown, DMARC has proven effective at preventing fraud. This is accomplished by allowing the senders of email to create a policy instructing the receiver of the email what to do with the message if it doesn't authenticate via SPF or DKIM in an aligned manner. Email failing the DMARC checks may be discarded and not delivered: this is called DMARC at enforcement and is the industry best practice for defending legitimate senders and their domains from abuse. An additional benefit of DMARC is that it can also be used to provide a heads up through its reporting mechanism about abusive use of your domain.

Properly setting up email authentication requires expertise to configure, publish and align email records. Depending upon the complexity of your organization, this may incur additional costs, but there are do-it-yourself guides and numerous tools available. The potential costs of implementation are nothing compared to the costs associated with phishing attacks: the FBI's internet crime complaint center reported $26.2 billion dollars in losses due to spear phishing (quantified as Business Email Compromise, or BEC, in the report) between June 2016 and July 2019. While breaches can result in millions of dollars in financial losses to businesses, breaches to election systems can result in compromised elections and a loss of public trust.

Email filtering

Election officials should consider email filtering as an additional security layer to protect recipients from malware, ransomware, viruses, malicious links and phishing. Email filtering can be deployed using purchased software packages or by public/private cloud providers as part of their overall services. There are numerous companies and products, called Secure Email Gateways, that specialize in email based filtering to prevent the delivery of unwanted and malicious messages.

Web and General Security Guidance

An overall proactive approach is needed to create good web security.

HTTPS everywhere

The Department of Homeland Security Binding Operational Directive (BOD 18-01) that set forth the minimal email security standards that brought the US federal government's email communications into enforcement also set forth the requirement that HTTPS be required for all government web presences. This ensures that all communication with government web services is done securely, and cannot easily be intercepted and read or altered by a third party in transit.

HTTPS is often associated with the little lock icon google.com visible in a browser to denote a secure connection. Ensuring that your websites are using HTTPS will prevent a number of compromises.

Strong Passwords

It is common knowledge that strong passwords are a good practice. Enforcing the use of strong passwords in conjunction with multi-factor authentication will harden user accounts and systems. M3AAWG has best practices providing specific guidelines for the use of strong passwords, as does The National Institute for Standards and Technology (NIST). To ensure such strong passwords and make for ease of generation and usage, election officials should strongly consider the usage of password managers.

Separating Systems

Publicly accessible systems such as web servers should be segmented in an environment that is separate from core election systems. Compromised web servers should not lead directly to the compromise of elections systems. It is critical to ensure that there is distance between these systems by logically isolating them. Do not use election systems to host web pages, run web servers, mail servers or other applications that, if/when compromised, can lead to a bad actor manipulating votes, stealing voter rolls or causing other mayhem.

Utilize free/low-cost tools for elections and campaigns

Many cloud services provide enhanced security at reduced cost for elections and campaigns. Election officials could inquire with all their cloud vendors if reduced cost or enhanced services are available.

Backups

In the event of a successful ransomware attack the only way to recover and get back online is by having a good backup and recovery system in place. Ransomware attacks have crippled municipalities. According to research 15% of ransomware victims paid their attackers to recover their data and systems.

Offline daily backups could help mitigate these costs and prevent system collapse. Backing up alone isn't enough; ensure your backups are functional by testing and restoring a system on a monthly basis to ensure their viability in the event of an attack. Note that some sites may use systems designed to protect against hardware failures by mirroring content. Those systems will NOT adequately protect data against intentional corruption by malware since the mirroring technology will dutifully copy the corrupted data from the original disk to the mirror.

For more information on ransomware see the No More Ransom Project: https://www.nomoreransom.org/

Monitor and patch systems quickly

Create the necessary processes to ensure that both critical and non critical systems are patched and software running on those systems is also patched and up to date. Out of date software represents a liability and must be kept up to date in order to prevent compromise. Monitor common vulnerabilities and exposures (CVE's) and patch affected systems as soon as possible, and no later than within 15 calendar days. For critical vulnerabilities, DHS orders federal agencies to patch their systems within 10 calendar days.

Provide cybersecurity awareness training

A common refrain in most private sector companies is that cybersecurity is everyone's responsibility. Likewise, securing elections to ensure the continuity of a democracy is not only the job of private and public security experts, it is the job of election officials, their staff and volunteers. Cyber criminals are aware that there is a distinct scarcity of specialized cybersecurity expertise among the people who are on the ground running elections. Officials should provide cybersecurity training that focuses specifically on social engineering threats meant to gain access to systems as a basic and lowest common denominator to create awareness among the people conducting a country's elections. The goal is for every election worker to have a cursory knowledge of cyber threats and a heightened awareness, decreasing the likelihood of malign actors derailing a free and fair election.

Conclusion

Every election official can take steps to improve the security of election systems and procedures. Starting with MFA and email authentication alone, the cyber threat surface can be dramatically reduced. Recognize that the majority of attacks will often begin by obtaining a login and password through social engineering. Tricking someone into "letting you in the front door" is easier than hacking through a firewall. Deploying technology designed to establish control and confirmation, and employing best practices around messaging policy and password management, can further close gaps and protect elections systems and officials.

For further analysis of the threats and mitigations possible, please review the M3AAWG best practices and below resources section.

Resources for Election Officials

- United States Department of Homeland Security Binding Operational Directive instructing US agencies to use email authentication in their email communications and do so at enforcement: https://cyber.dhs.gov/bod/18-01/
- Department of Homeland Security (US Cyber Emergency Response Team) guidance:
    - https://www.us-cert.gov/ncas/tips/ST19-002
    - https://www.dhs.gov/cisa/election-security
    - https://www.us-cert.gov/ncas/tips/ST16-001
- US Election Assistance Commission security guidance: https://www.eac.gov/election-officials/election-security
- National Institute for Science and Technology (NIST) created a voting systems standard for next generation voting systems: https://www.nist.gov/itl/voting/vvsg-introduction
- Messaging, Malware and Mobile Anti-Abuse Working Group's (M3AAWG) repository of published best communication practices documents: https://www.m3aawg.org/published-documents
- The UK's National Cyber Security Center's (UK NCSC) guidance for election security: https://www.ncsc.gov.uk/guidance/election-guidance-for-local-authorities, https://www.ncsc.gov.uk/collection/10-steps-to-cyber-security/introduction-to-cyber-security/executive-summary
- Center for Internet Security guidance on combating spear phishing, a targeted form of phishing attacks: https://www.cisecurity.org/white-papers/ms-isac-security-primer-spear-phishing/
- The Global Cyber Alliance, in conjunction with the Center for Internet Security, built a Cybersecurity kit for elections: https://gcatoolkit.org/elections/