THREAT INTELLIGENCE SHARING & ELECTION SECURITY:

3 CYBERSECURITY STRATEGIES TO PROTECT U.S. ELECTION INTEGRITY

No matter what side of the political divide on which one falls, everyone agrees that the security and integrity of elections are critical. Throughout history, foreign adversaries have attempted to influence election outcomes to their benefit and, in 2016, the efforts escalated to cyberattacks. For this reason, the security of US elections and election infrastructure remains a top national concern, and in early 2017, the government designated the election system as one of our critical infrastructures.[1] With the number of cyberattacks growing every day, improving cybersecurity is a mandatory component in preserving our political process.

The US Department of Homeland Security (DHS) confirmed that at least 21 states have had their networks scanned by Russian adversaries.[2] Scanning is the cyber equivalent of checking for holes in a fence, an unlocked door, or an open window. There are also confirmed reports of a few specific intrusions into government-owned voter registration databases.[3]

FBI indictments in 2017 validated an organized cyberattack campaign that targeted political organizations, specifically the Democratic Congressional Campaign Committee and the Democratic National Committee.[4]

As disclosed in the Mueller Report and recently confirmed by Florida Governor Ron DeSantis, two anonymous Florida counties' voter registration databases were accessed by Russian hackers in 2016.[5]

Not surprisingly, both attacks began with spear phishing, and resulted in network access, the planting of malware, lateral movement, and the exfiltration of sensitive data. Federal, state, and local governments are responding with initiatives to improve the security of election infrastructure.

Earlier this year, the federal government approved $380 million to be used by the states to improve election security.[6] The funds are being used to improve voter registration databases, election management systems, electronic voting machines, and election night reporting systems. As reported in April 2019, states and local governments spent just 8.1% of these funds in the first 6 months of receiving access to them.[7] Crucially, states are now on track to spend the majority of the money before the 2020 elections.[8]

> **"I recently met with the FBI concerning the election issue mentioned in the Mueller report...**
>
> **Two Florida counties experienced intrusion into the supervisor of election networks. There was no manipulation."**
>
> Florida Governor Ron DeSantis in a Press Conference, May 14, 2019

BANDURA CYBER

3 WAYS TO IMPROVE ELECTION INFRASTRUCTURE SECURITY

Election infrastructure is a complex web of systems and networks that involves more than 8,000 entities with resources distributed across both state and local governments. Notably, election infrastructure is not just the systems that support the actual election process but also includes the operations of candidates and campaigns. Improving election infrastructure security requires a combination of a renewed focus on basic cyber hygiene, as well as the strategic use of advanced security technologies, threat intelligence, and information sharing.

1. REVISITING BASIC CYBER HYGIENE

Whether we are talking about election infrastructure or corporate IT infrastructure, organizations often don't focus enough on cyber hygiene. Just focusing on—or reviewing—the very basics can strengthen security posture:

- Hardening systems
- Ensuring proper access controls
- Conducting security awareness training to mitigate the risk of users clicking on malicious links (such as in spear phishing campaigns)

State and local governments can take advantage of complimentary DHS services (dhs.gov/topic/election-security) when testing their election infrastructure, which include cyber hygiene scans on Internet-facing systems and risk and vulnerability assessments.[9]

2. DEPLOYING NEXT-GENERATION CYBER TECHNOLOGIES

Cybersecurity is an ongoing race between attackers and defenders. Therefore, it's critical that organizations incorporate more contemporary and advanced security technologies into cyber defense efforts.

Current systems are overwhelmed, and hackers have been able to fly under the radar through encrypted communications such as Secure Sockets Layer. Utilizing next-generation security solutions is another way to increase election infrastructure security. It is no longer good enough to solely rely on firewalls and intrusion detection and prevention systems to protect our political system.

U.S. states & territories spent 8.1% of $380 million designated by DHS to upgrade election security in first 6 months of the funds becoming available.

3. USING AND SHARING THREAT INTELLIGENCE

In the specific case of spear phishing, even the keenest eyed among us may not be able to identify all phishing attempts. This means that additional cybersecurity protections that provide prevention are required to guard against human vulnerabilities by blocking spear-phishing attempts from even reaching a person. Utilizing threat intelligence and threat intelligence sharing is a great way to prevent phishing and other malicious attack.

Beyond the specific use case of spear phishing, threat intelligence and information sharing has become a critical element of cyber frameworks like the NIST Cybersecurity Framework.[10] With election infrastructure spread across federal, state, and local government, it is imperative that these organizations not only use but also share threat intelligence.

The good news is there is a significant amount of organized threat intelligence and intelligence-sharing efforts that can be leveraged to improve election infrastructure security. Organizations such as DHS and the FBI are valuable partners in these efforts.[11]

There is also the Multi-State Information Sharing & Analysis Center (MS-ISAC), whose stated mission is "to improve the overall cybersecurity posture of the nation's state, local, tribal and territorial governments through focused cyber prevention, protection, response, and recovery."[12] MS-ISAC serves as a central hub for members to access, contribute, and exchange threat intelligence. Earlier this year, MS-ISAC formed the Elections Infrastructure ISAC (EI-ISAC) to specifically support the needs of election infrastructure.[13] EI-ISAC provides members sector-specific threat intelligence products, incident response and remediation, threat and vulnerability monitoring, cybersecurity awareness, and training products.

THINKING AHEAD

To ensure our electoral system is protected for years to come, federal, state, and local governments have significantly increased investments in election infrastructure security. While no one thing will solve this problem overnight, by revisiting basic security hygiene, deploying next-generation technologies, and using, sharing, and acting on threat intelligence, we will begin to move forward in mitigating the massive amount of cyber-risk that currently threatens our election system.

THREAT INTELLIGENCE SHARING RESOURCES FOR STATE & LOCAL GOVERNMENT AGENCIES

- **Albert Sensor IDS Program (DHS)** - cisecurity.org/services/albert-network-monitoring/
- **DHS Cyber Information Sharing and Collaboration Program (CISCP)** - dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp
- **Aviation ISAC** - a-isac.com
- **Defense Industrial Base ISAC** - dibisac.net
- **DHS Cyber Information Sharing and Collaboration Program (CISCP)** - dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp
- **Downstream Natural Gas ISAC** - dngisac.com
- **Elections Infrastructure ISAC** - cisecurity.org/ei-isac/
- **Electricity ISAC** - eisac.com
- **Emergency Management and Response ISAC** - usfa.fema.gov/operations/ops_cip_emr-isac.html
- **Energy Analytic Security Exchange (EASE)** - grfederation.org/ease
- **Financial Services ISAC** - fsisac.com
- **Health ISAC** - h-isac.org
- **Healthcare Ready ISAC** - healthcareready.org
- **Maritime ISAC** - maritimesecurity.org
- **Multi-State ISAC** - ms-isac.org
- **National Defense ISAC** - ndisac.org
- **Oil & Natural Gas ISAC** - ongisac.org
- **Research and Education Networks ISAC** – ren-isac.net
- **Surface Transportation, Public Transportation, & Over-The-Road Bus ISAC** - surfacetransportationisac.org
- **Water ISAC** - waterisac.org

BANDURA CYBER

CONTACTS:

LISA RHODES

Head of State & Local Government, Education
Bandura Cyber Threat Intelligence Gateway: Fully Automated, Actionable, Advanced Threat Intelligence

lisa.rhodes@banduracyber.com
(719) 332-7558

TODD WELLER

Chief Strategy Officer
Bandura Cyber Threat Intelligence Gateway: Fully Automated, Actionable, Advanced Threat Intelligence

todd.weller@banduracyber.com
(443) 832-8596

Read more about governmental cybersecurity and threat intelligence on the **Bandura Cyber blog** or get the whitepaper, *Phishing in State and Local Governments, and Education Environments*.

REFERENCES & ADDITIONAL READING

1. Sheridan, K. (2017, January 9). DHS Designates Election Systems As Critical Infrastructure. Retrieved from https://www.darkreading.com/risk/dhs-designates-election-systems-as-critical-infrastructure/d/d-id/1327856
2. Borchers, C. (2017, September 23). What we know about the 21 states targeted by Russian hackers. Wall Street Journal. Retrieved from https://www.washingtonpost.com/news/the-fix/wp/2017/09/23/what-we-know-about-the-21-states-targeted-by-russian-hackers/
3. McFadden, C., Arkin, W. M., Monahan, K., & Dilanian, K. (2018, February 27). U.S. intel: Russia compromised seven states prior to 2016 election. Retrieved from https://www.nbcnews.com/politics/elections/u-s-intel-russia-compromised-seven-states-prior-2016-election-n850296
4. Higgins, K. J. (2018, July 13). Mueller Probe Yields Hacking Indictments for 12 Russian Military Officers. Retrieved from https://www.darkreading.com/attacks-breaches/mueller-probe-yields-hacking-indictments-for-12-russian-military-officers/d/d-id/1332297
5. Parks, M. (2019, May 14). Florida Governor Says Russian Hackers Breached 2 Counties In 2016. Retrieved from https://www.npr.org/2019/05/14/723215498/florida-governor-says-russian-hackers-breached-two-florida-counties-in-2016
6. Congressional Report Cites States Most Vulnerable to Election Hacking. (2018, July 13). Retrieved from https://www.darkreading.com/threat-intelligence/congressional-report-cites-states-most-vulnerable-to-election-hacking/d/d-id/1332295
7. Collier, K. (2019, April 04). States slow to spend funds to enhance election security, report finds. Retrieved from https://www.cnn.com/2019/04/04/politics/election-security-states-slow-to-spend/index.html
8. Marks, J. (n.d.). The Cybersecurity 202: States spent just a fraction of $380 million in election security money before midterms. The Washington Post. Retrieved April 5, 2019, from https://www.washingtonpost.com/news/powerpost/paloma/the-cybersecurity-202/2019/04/05/the-cybersecurity-202-states-spent-just-a-fraction-of-380-million-in-election-security-money-before-midterms/5ca697b81b326b0f7f38f32b/
9. Election Security. (2019, March 05). Retrieved from https://www.dhs.gov/topic/election-security
10. Weller, T. (2018, February 27). Threat Intelligence in NIST Cybersecurity Framework. Retrieved from https://banduracyber.com/resources/blog/importance-of-threat-intelligence-increasing-in-nist-cybersecurity-framework/
11. Cyber Information Sharing and Collaboration Program (CISCP). (2019, March 06). Retrieved from https://www.dhs.gov/cisa/cyber-information-sharing-and-collaboration-program-ciscp
12. Multi-State Information Sharing and Analysis Center. (n.d.). Retrieved from https://www.cisecurity.org/ms-isac/
13. EI-ISAC. (n.d.). Retrieved from https://www.cisecurity.org/ei-isac

BANDURA CYBER