I-TEAM

How the Russians penetrated Illinois election computers

SQL, an acronym for Structured Query Language, is a database programming language. An "SQL injection" is a common piece of cyber-trickery used to illegally gain access to government, financial, business and private computers. Experts estimate that 8 of every 10 data breaches occur as a result of SQL injection.

The favored tactic of hackers usually begins with certain commands typed on a public web form and ends with broad access to the site's server. In the case of Illinois, after hackers typed a specially-crafted code into the election database search box, records were stolen and the board had to shut down registration for ten days.

"Processor usage had spiked to 100% with no explanation" state investigators determined. "Analysis of server logs revealed that the heavy load was a result of rapidly repeated database queries on the application status page of the Paperless Online Voter Application (POVA) web site" they said.
Assess Risk and Consequences

Six days after a ransomware cyberattack, Atlanta officials are filling out forms by hand

By Kimberly Hutcherson, CNN
Updated 3:00 PM ET, Wed March 28, 2018

City of Atlanta Needs $9.5 Million More for Ransomware Recovery

According to multiple sources, the City of Atlanta will need to find another $9.5 million to recover from the "SamSam" ransomware attack which brought their city government to a grinding halt. The number of applications and government services impacted by the attack has been revealed to be far greater than originally estimated, with the attack even affecting applications of the city police department and court system.
RANSOMWARE THUGS EXTORT INDIANA COUNTY FOR OVER $130,000 IN BITCOIN

By Mark Brown / 12/07/2019 / 3 Min read / In Bitcoin Crime, Cryptocurrency News, News
North Carolina's elections board provided this image to state lawmakers in a December 2017 presentation. - State Board of Elections and Ethics Enforcement

---

CISA
Cyber Infrastructural Protection
FARMER SHOOTS 23-LB. GRASSHOPPER!

Fed-up fatties kill aerobics instructor!

Thousands of gals want to marry Mr. Fuzzy-wuzzy!

Giant bug is 4 feet long!
Threats to Election Infrastructure

Potential Adversaries:
- Nation-state actors
- Black Hat Hackers
- Criminals
- Politically Motivated Groups
- Insiders
- Terrorists

Possible Motivations:
- Undermine Trust in Democracy
- Foreign Policy Goals
- Sow Social Division
- Financial Gain
- Subvert Political Opposition
- Fame and Reputation
- Foment Chaos/Anarchy
- Retribution for Perceived Grievances

Potential Targets:
- Voter registration databases
- Voting systems
- Election reporting systems
- Storage facilities and polling places
- Public confidence in the integrity of the election
- Election officials and their families
With so many factors...

- Things that matter
- Things you can control

Where you should focus!
**Mission Statement:** To ensure the Election Stakeholder Community – infrastructure owners and operators, partisan organizations, and the electorate – has the necessary information to adequately assess risks and protect, detect, and recover from those risks.

The 2017 designation of election infrastructure as critical infrastructure provides a basis for the Department of Homeland Security and other federal agencies to:

- Recognize the importance of these systems;
- Prioritize services and support to enhancing security for election infrastructure;
- Provide the elections community with the opportunity to work with each other, the Federal Government, and through the Coordinating Councils;
- Hold anyone who attacks these systems responsible for violating international norms.
Vulnerability Scanning

§ A scanning of internet-accessible systems for known vulnerabilities on a continual basis. As potential issues are identified, DHS notifies impacted customers so they may proactively mitigate risks to their systems prior to exploitation. Conducted remotely and fully automated.

Remote Penetration Testing

§ Utilizes a dedicated remote team to assess and identify vulnerabilities and work with customers to eliminate exploitable pathways. The assessment simulates the tactics and techniques of malicious adversaries and tests centralized data repositories, externally accessible assets, and web applications.

Phishing Campaign Assessment

§ Measures the susceptibility of an organization’s staff to social engineering attacks, specifically email phishing attacks. The assessment takes place during a six-week period. An assessment report is provided two weeks after its conclusion. The assessment report provides guidance, measures effectiveness, and justifies resources needed to defend against and increase staff training and awareness of generic phishing and spear-phishing attacks.
Join the Election Infrastructure ISAC

The EI-ISAC is a dedicated resource that gathers, analyzes, and shares information on critical infrastructure and facilitates two-way cybersecurity threat information sharing between the public and the private sectors.

The EI-ISAC supports the election community through:

§ 24 x 7 x 365 network monitoring
§ Election-specific threat intelligence
§ Threat and vulnerability monitoring
§ Incident response and remediation
§ Training sessions and webinars
§ Promotion of security best practices
Federal, state, and local government partners formed the Election Infrastructure Subsector GCC (EIS-GCC) and met for the first time in Atlanta in October 2017.

The formation of the EIS-GCC was a milestone in multi-level government cooperation that bolstered election infrastructure security and resilience.

**The EIS-GCC:**

- Enables partners to leverage information sharing, cybersecurity and physical security products, resources, capabilities, and collective expertise.
- Consists of 27 members, 24 of which are state and local election officials.
- Is led by a five-member Executive Committee which meets biweekly (DHS/CISA; EAC; a Secretary of State; a state Election Director; and a local Election Director).
- Adopted a Subsector Specific Plan in 2018. Subsector priorities for 2019-2020 were approved on February 1, 2019.
Private sector stakeholders formed the Election Infrastructure Subsector Coordinating Council (EISCC) and met for the first time in February 2018.

The EISCC:

- Is led by a five-member Executive Committee.
- Serves as the primary liaison between the private sector and government on election infrastructure security.
- Facilitates information and intelligence sharing.
- Coordinates with DHS and the EIS-GCC to develop, recommend, and review subsector-wide plans and procedures.
- Established an action plan complete with goals and priorities in February 2019.
Progress in the 2018 Election Cycle

Establishment of the EI-ISAC

In February 2018, the EIS-GCC established the EI-ISAC, which is now the fastest growing ISAC ever.

Funding Consideration Document

In May 2018, the EIS-GCC released a guidance document with potential short- and long-term funding considerations to support elections officials making decisions on how they could use newly available funding to help secure election infrastructure.

Communications Protocols

In July 2018, the EIS-GCC issued a set of voluntary Communications Protocols to improve the efficiency and effectiveness of information sharing between election stakeholders.

New Trainings and Assessments

Driven by feedback from election officials, DHS now offers Remote Penetration Testing as well as “The Election Official as IT Manager” online course.

National-level Election Security Tabletop Exercise

In August 2018, DHS hosted a three day tabletop exercise with 44 states, the District of Columbia, and 10 Federal agencies.

Classified Briefings

DHS partnered with the Intelligence Community to share classified information on several occasions, pushing more threat information to this subsector than ever before. The most recent classified briefing was in February 2019.

Election Day Situation Room

On Election Day, DHS hosted the National Cybersecurity Situational Awareness Room. This online portal for election officials and vendors facilitated rapid information sharing and provided election officials with virtual access to the 24/7 operational watch floor of the NCCIC.
DHS Priorities for the 2020 Election Cycle

- Increase engagement and support provided to local election officials
- Raise awareness regarding the need for regular investment in election infrastructure
- Further develop DHS’s understanding and conversations about risks to election infrastructure
- Improve communications and information sharing across the subsector
What Can Be Done

1. Develop an incident response & recovery plan
2. Assess your data risks & secure it appropriately
3. Continuous monitoring
4. Conduct trainings and exercises
5. Take advantage of all available resources
What Can Be Done

Mitigate Internet Vulnerabilities in a Timely Manner

§ Mitigate all high and critical severity level vulnerabilities to internet-accessible systems within 30 days. Vulnerabilities with lower severity levels should be reviewed and mitigated within 60 days.

Strengthen Password Policy and Auditing Processes

§ Use multi-factor authentication and perform regular audits of password policies. Password best practices include ensuring that strong passwords are required and that administrators utilize encrypted password vaults.

Implement Network Segmentation

§ Internal network architecture should protect and control access to the entity’s most sensitive systems. User workstations should be less trusted and connections to external networks should be isolated, controlled, and monitored.

Have a Plan and Implement Backups

§ Follow established enterprise network best practices for IT infrastructure. This includes implementing a strong patching methodology for operating systems and third-party products. Your organization should also create an Incident Response Plan and Continuity of Operations Plan.

Replace Unmaintainable Equipment

§ Use equipment that is maintainable with current security patching. Exceptions should be minimized and isolated.
§ Replace aging voting systems with auditable systems.
CISA Election Security 101

Matt Masterson
Senior Cybersecurity Advisor
Department of Homeland Security
Matthew.Masterson@hq.dhs.gov

Geoff Hale
Director, Election Security Initiative
Department of Homeland Security
Geoffrey.Hale@hq.dhs.gov