STATE BOARD OF ELECTIONS

ELECTION NEWS ELECTION NEWS ELECTION NEWS

100 W. Randolph Street
Suite 14-100
Chicago, Illinois 60601
312-814-6440

2329 S. MacArthur Blvd.
Springfield, Illinois 62704
217-782-4141
www.elections.il.gov

FOR IMMEDIATE RELEASE

CONTACT: MATT DIETRICH
(217) 558-1955 mdietrich@elections.il.gov

Feb. 28, 2018

2016 VOTER DATA BREACH LEADS TO ENHANCED SECURITY MEASURES

SPRINGFIELD, Ill. – In July 2016, the electronic voter registration database maintained by the Illinois State Board of Elections was breached in a cyberattack. The breach was detected and closed by SBE information technology staff, who later notified some 76,000 voters whose data may have been viewed in the intrusion.

What follows is a report filed in August 2016 detailing the data breach and an addendum listing steps that have been taken in its aftermath to avoid another such incident.

Illinois Voter Registration System
Database Breach Report
August 26, 2016

The Illinois State Board of Elections was the victim of a malicious cyber -attack of unknown origin against the Illinois Voter Registration System database (IVRS) beginning June 23, 2016. SBE staff became aware of a breach on July 12 and immediately took measures to stop the intrusion. In the following weeks, SBE staff has worked to determine the scope of the intrusion, secure databases and web applications, comply with state law regarding personal information loss, and assist law enforcement in their investigation of the attack.

Timeline

July 12, 2016

- State Board of Elections IT staff was made aware of performance issues with the IVRS database server.
- Processor usage had spiked to 100% with no explanation.
- 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.
- Additionally, the server logs showed the database queries were malicious in nature – a form of cyber-attack known as SQL Injection. SQL Injections are essentially unauthorized, malicious database queries entered in a data field in a web application.
- SBE programmers immediately introduced code changes to eliminate the vulnerability.

July 13, 2016

- SBE IT took the web site and IVRS database offline to protect against further attack.
- Analysis of the web server logs showed that malicious SQL queries began on June 23, 2016.
- SBE staff maintained the ability to log and view all site access attempts.

- Malicious traffic from the IP addresses continued, though it was blocked at the firewall level.
- Firewall monitoring indicated that the attackers were hitting SBE IP addresses 5 times per second, 24 hours per day.
- SBE staff began working on determining the extent of the breach, analyzing the integrity of the IVRS database, and introducing security enhancements to the IVRS web servers and database.

July 19, 2016

- We notified the Illinois General Assembly of the security breach in accordance with the Personal
- Information Protection Act (PIPA).
- In addition, we notified the Illinois Attorney General's office.

July 21, 2016

- SBE IT completed security enhancements and began bringing IVRS back online.

ADDENDUM, February 2018

In the aftermath of the 2016 cyberattack, SBE has taken numerous steps to bolster the security of its electronic database. These include:

- Since October 2016, the U.S. Department of Homeland Security has performed weekly "hygiene scans" to detect potential vulnerabilities in our systems. None have been identified to date.
- Scheduling a "Risk and Vulnerability Assessment" with DHS, the most stringent cybersecurity analysis the agency offers
- Participation in numerous groups and associations dedicated to sharing cybersecurity intel and analysis, including the Multi-State Information Sharing & Analysis Center
- Working with state and federal law enforcement and intelligence agencies to facilitate information sharing from the Federal level all the way down to the local level
- Continued partnering with the Illinois Department of Innovation and Technology to leverage their cybersecurity services
- Purchased specialized hardware designed to further protect us from attacks
- Executive Director Steve Sandvoss obtained security clearance to attend national briefing with DHS in Washington, D.C., on cybersecurity and election integrity efforts on Feb. 18, 2018. SBE Director of Voting and Registration Systems Kyle Thomas and Legislative Liaison Cris Cray also attended the briefing.

###