Illinois Voter Registration System Database Breach Report

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. Because of the initial low volume nature of the attack, SBE staff did not become aware of the breach until the volume dramatically increased on July 12th. At that point, SBE IT immediately took measures to stop the intrusion. In the following weeks, SBE staff 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.

Analysis concluded that in addition to viewing multiple database tables, attackers accessed approximately 90,000 voter registration records.

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 (Structured Query Language) Injection. SQL Injections are essentially unauthorized, malicious database queries entered in a data field in a web based application. We later determined that these SQLs originated from several foreign based IP addresses.

SBE programmers immediately introduced code changes to eliminate this vulnerability.

July 13, 2016

SBE IT took the web site and IVRS database offline to investigate the severity of the attack.

Analysis of the web server logs showed that malicious SQL queries had begun 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 to determine 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.

July 28, 2016

Both the Illinois Voter Registration System and the Paperless Online Voter application became fully functional.

Ongoing

SBE IT staff continues to monitor its web server and firewall logs on a daily basis.

Outside Agency Participation

As a result of informing the Illinois Attorney General's office of the breach, the SBE was contacted by the Federal Bureau of Investigation. We have fully cooperated with the FBI in their ongoing investigation.

The Illinois Department of Innovation and Technology (which is a State-wide entity that coordinates the IT systems of the various State agencies) was helpful by providing web traffic logs and assisting with web server log analysis.

The FBI advised that we work with the Department of Homeland Security's (DHS) United States Computer Emergency Readiness Team (US-CERT) to ensure there was no ongoing malicious activity on any of SBE's systems.

PIPA Compliance

Nearly 76,000 registered voters were contacted as potential victims of the data breach.

The SBE provided these individuals information on steps to take if they felt they were the victims of identity theft. Additionally, the SBE developed an online tool to inform affected individuals of the specific information included in their voter record.

Future Concerns

Voting Equipment – One of the concerns facing our state and many others is aging voting equipment. The Help America Vote Act (HAVA) established requirements for voting equipment, but, while initial funding was made available, additional funding has not been appropriated.

In addition to future funding, HAVA restrictions on spending could be relaxed to allow spending on enhanced security across all election-related systems.

New Standards for Voting Equipment

Security Training and Guidance for State and Local Election Officials – Cyberattacks targeting end users are of particular concern. Security training funded and provided by a federal entity such as the EAC would be beneficial. In addition, any guidance or recommendations as to methods for the protection of registration and voting systems from cyber intrusions are always welcome.