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.

July 28, 2016

Both IVRS and POVA fully functional.

Security Enhancements

We concluded from the analysis of the attack that we could reasonably expect that various IVRS passwords were compromised. These passwords included those of election authorities, their staffs, internal SBE users, vendors, and web services.

In order to ensure that attackers could not access any portion of the system with stolen passwords, we took the following steps:

1. Reset all IVRS passwords in order to force users to change their password at next login.
2. Introduced enhanced password complexity requirements (length, special characters, numbers, etc.).
3. Mandated two-factor token login for all IVRS users. (Election authorities had previously been able to disable it for their staffs.)
4. Added password encryption to the IVRS database so that stored passwords can no longer be deciphered, even by SBE employees.
5. Reset and encrypted passwords used by vendors and automated web services. Ensuring that these processes continued to work was a lengthy and complex process that significantly contributed to system downtime.

As a further precaution, SBE staff added code to encrypt URL transmissions as an additional layer of security against attacks of this nature.

Finally, additional internal mechanisms were added for reviewing these and future attacks, including monitoring web server logs on a daily basis for evidence of attacks as well as monitoring firewall logs for traffic from malicious sources.

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 to determine who was responsible for the attack and to prosecute the offender(s).

The Illinois Department of Innovation and Technology (DoIT) has been very 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 is no ongoing malicious activity on any of SBE's systems. We have provided DHS with the log files that we obtained from DoIT.

PIPA

The State Board of Elections has remained fully compliant with the Illinois Personal Information Protection Act (PIPA). We fulfilled our obligation to inform the Illinois General Assembly within 5 business days of the breach.

We have determined that a number of individuals' personal information was compromised. Due to the ambiguous nature of the attack we may never know the exact number of affected voters. We can confirm that no voting history information and no voter signature images were captured.

We are continuing to analyze the extent of the breach in order to determine the individuals to be contacted and will be working with the Attorney General's office to determine the method of contact in order to comply with PIPA.

Current Status

State Board of Elections staff continues to work to improve application and database security as well as determine the scope of the breach.

The attackers continued to hit SBE IP addresses 5 times per second until August 12th when attacks abruptly ceased. We are highly confident that no data in the IVRS database was added, changed, or deleted, although the investigation is not yet complete.