THREATS
Election 2016: Where, when and how to vote on Nov. 8

Voters stand near a voting sign before casting ballots during early voting at the Franklin County Board of Elections in Columbus, Ohio, October 28, 2016. / REUTERS/SHANNON STAPLETON

34 Comments / Share / Tweet / Stumble / Email
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.
North Carolina’s elections board provided this image to state lawmakers in a December 2017 presentation. - State Board of Elections and Ethics Enforcement
DDoS Attack Hits Knox County, TN Results Reporting Site On Election Night

By Doug Chapin    May 7, 2018
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

By NICOLE PERLROTH  JULY 6, 2017

The Wolf Creek Nuclear power plant in Kansas in 2000. The corporation that runs the plant was targeted by hackers. David Eulitt/Capital Journal, via Associated Press
Cybersecurity – Common Attacks

• Social Engineering
  ▪ Spear-phishing

• Hacking
  ▪ SQL Injection
  ▪ Port scans
  ▪ Man in the Middle (MITM) Attacks

• Distributed Denial of Service (DDoS)

• Information Operations
  ▪ Leaking stolen information
  ▪ Spreading false or misleading information
  ▪ Amplifying divisive content
  ▪ Interrupting service to public facing online resources
Spear Phish Example 2:

Jen –

How are you? I am going to be in Cincinnati next week. Can we do lunch? I have a new project I am working on, really excited to share it with you. Check it out: https://www.somethingcool.com. I think this could be a big addon for the INBiz program.

Tell Jack hi.

Thanks,
Jeff

-----------------------
Jeff Dada, Ph.D.
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!
# Summary of DHS Services: Cybersecurity Assessments

<table>
<thead>
<tr>
<th>Needs</th>
<th>DHS Services</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>Identify and Limit Vulnerabilities</td>
<td>Cyber Hygiene Scanning</td>
<td>Broadly assess Internet-accessible systems for known vulnerabilities and configuration errors on a persistent basis. As potential issues are identified DHS works with impacted stakeholders to mitigate threats and risks to their systems prior to their exploitation.</td>
</tr>
</tbody>
</table>
|                                            | Risk and Vulnerability Assessment (RVA)   | • Penetration testing  
• Social engineering  
• Wireless access discovery  
• Database scanning  
• Operating system scanning |
|                                            | Phishing Campaign Assessment              | • Measures susceptibility to email attack  
• Delivers simulated phishing emails  
• Quantifies click-rate metrics over a 10-week period |
## Summary of DHS Services: Cybersecurity Assessments

<table>
<thead>
<tr>
<th>Needs</th>
<th>DHS Services</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>IDENTIFY</td>
<td>Cyber Resiliency Review</td>
<td>The Cyber Resilience Review (CRR) is a no-cost, voluntary, interview-based assessment to evaluate an organization’s operational resilience and cybersecurity practices.</td>
</tr>
<tr>
<td>PROTECT</td>
<td>External Dependencies Management Assessment</td>
<td>The External Dependencies Management (EDM) assessment is a no-cost, voluntary, interview-based assessment to evaluate an organization’s management of their dependencies.</td>
</tr>
<tr>
<td>DETECT</td>
<td>Cyber Infrastructure Survey</td>
<td>The Cyber Infrastructure Survey (CIS) is a no-cost, voluntary survey that evaluates the effectiveness of organizational security controls, cybersecurity preparedness, and overall resilience.</td>
</tr>
</tbody>
</table>
Cyber Security Advisors (CSA)

For more information about the CSA Program, to schedule a review or assessment, email cyberadvisor@hq.dhs.gov
• Provides cybersecurity support to SLTT governments.
• Furthers DHS efforts to secure cyberspace by distributing early warnings of cyber threats to SLTT governments.
• Shares security incident information and analysis.
• Runs a 24/7 watch and warning security operations center.
• Operates an election threat warning center, the Election Infrastructure-ISAC.
• Funded by DHS.

For more information, see https://www.cisecurity.org/ei-isac
EI-GCC Supported Resources

• Election Infrastructure Security Funding Considerations
• Election Infrastructure Communications Protocol
• Belfer Center Defending Digital Democracy Project (D3P) Playbooks
  ▪ The State and Local Election Cybersecurity Playbook
  ▪ Election Cybersecurity Incident Communication Coordination Guide
  ▪ Election Cyber Incident Communication Plan Template
  ▪ Cybersecurity Campaign Playbook
• Center for Internet Security’s A Handbook for Elections Infrastructure Security
• Private/Non-profit Resources for SLTT & Campaigns
Election Infrastructure Security – Best Practices

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