Spring Security

Beginner to Guru

Application Security 101

Application Security 101

- Security is a very large topic
- Larger than just a technology topic
- Securing applications involves technology solutions, adopting best practices, personal, and physical security
- Security often involves analyzing the risk vector then implementing mitigating actions

2016 DNC Email Hacks

- In the 2016 US Presidential Election, Wikileaks published emails obtained from the Democratic party
  - Information revealed was very damaging
- Hacked Emails Involved 3 Distinct Areas
  - DNC (Democratic National Committee) Email Server
  - John Podesta's Gmail Account
  - Hillary Clinton's Private Email Server

DNC Email Server

- US Intelligence believes the hacked emails were obtained by Russian hackers via a cyberattack
    - What does this mean?
        - Hackers obtained access to the DNC server via the internet to copy files from the server
- Mitigating Actions
    - OS Patching to prevent known exploits - Unpatched Windows XP has about 8 minutes when exposed on the internet
    - Password Length / Complexity requirements

Mitigating Actions

- Don’t use common passwords!
- Firewalls - Only expose necessary ports to internet
- Prevent direct sign-on to super user accounts
- Use OS Level security features to restrict access
    - Read access to email data files should be highly restricted

DNC Email Server - Alternate Theory

- There is a theory that challenges the official conclusion based on file timestamps the email data files were copied to a USB drive
- What does this mean?
  - Hacker had physical access to the DNC Email Server
  - Likely an employee with a sign-on
- Plausible theory, since a lot of data breaches do happen this way

Mitigating Actions

- **Physical Security** - Place Servers in secure rooms which require badge access at a minimum
  - Limit number of people, log access to room
  - Video security
- **Personal Security** - Only people who need access to the server should have access
  - ie - an email administrator, might not need physical access to the server
- **Segregation of Duties** - People should have roles and limited access for those roles
  - ie - department managers should not have super user accounts

Podesta Emails

- March 2016, the personal Gmail account of John Podesta, Chair of Clinton’s Presidential Campaign was compromised
- Breach was done via a phishing attack
- What does this mean?
  - Podesta was tricked into giving a hacker the password for Gmail account
  - With Podesta’s password, the hacker was able to authenticate and access the Gmail account

Mitigating Actions

- End User Education about risk of phishing attacks
- 2FA - Two Factor Authentication to help confirm identity
- Don’t use Gmail for official business - corporate email systems can enforce a variety of security policies
  - Yes, Google Apps for Business can do this - its a matter of policy enforcement
- Threat scanning of incoming emails
- Password expiration policies

Clinton’s Private Email Server

- In 2009, Hillary Clinton established private email server. The Microsoft Exchange Server operated from Clinton’s home in Chappaqua, New York until 2013
- The Inspector General determined with four exceptions, all emails passing through the server were forwarded “to an unauthorized source that was a foreign entity unrelated to Russia.”
- What does this mean?
  - The Clinton server was compromised early on, likely from an external source
  - Does not rule out a malicious actor with direct access

Mitigating Actions

- #1 Mitigating Action would have been to use the State Department's email
- A 45,000 person organization will have more specialized resources
- Accounts indicate the Clinton email server was setup by a Clinton aide.
  - It is likely the aide did not have the training nor experience to configure and secure the server
- Unlikely server was patched on a regular schedule
- Unlikely network security in place
- Unlikely to have physical security or segregation of duties

Security Audit Frameworks / Certifications

- **PCS-DSS** - Payment Card Industry Data Security Standard
  - Applicable if your organization processes credit / debit cards
- **SOX** - Sarbanes-Oxley
  - For US based publicly traded companies
- **HIPAA** - Health Insurance Portability and Accountability Act
  - US Based Medical Industry
- **SSAE 16** - Statement on Standards for Attestation Engagements (SSAE) No. 16
  - CPA - authoritative guidance for reporting on service organizations

Common Terminology

- **PII** - Personally Identifiable Information - name, address, email, tax ids, etc
- **Encryption at Rest** - Sensitive data needs to be encrypted when stored (database, filesystem, backup tapes, etc)
- **Encryption in Flight** - When transmitted, sensitive data needs to be encrypted - can be protocol (https, ssh, etc)
- **Segregation of Duties** - Avoid having powerful super users in organization
- **Processes and Controls** - Be able to document compliance (source control, issue management)

PCI DSS Requirements

1. Protect System with Firewalls
2. Configure Passwords and Settings - Don’t use defaults
3. Protect Stored Cardholder Data - Use Industry accepted algorithms, don’t roll your own!
4. Encrypt Transmission of Cardholder Data across open, public networks
5. Use and update anti-virus software
6. Regularly update and patch systems
7. Restrict access to card holder data by business need to know

PCI DSS Requirements

8. Assign Unique Id to each person with computer access
9. Restrict physical access to workplace and cardholder data
10. Implement logging and log management
11. Conduct vulnerability scans and penetration tests
12. Documentation and risk assessments

Other Best Practices

- Use OS Service Accounts for Applications
  - Service accounts should have minimal access needed
- Use database Service Accounts with minimal access
  - Application account should not have access to alter or drop database tables
- Use layers of network security to protect internal systems
  - ie - should not be able to reach database server from internet edge
  - VPCs, VPNs, multiple physical networks

SPRING FRAMEWORK

GURU