Agenda

NTT Security Background

Back to Basics

• Patching
• System Configuration
• Passwords
• Data Retention
• Encryption

Texas Cybersecurity Framework Assessments

Common Security Issues

Q&A
Formation of NTT Security - A specialized security company
Managed Security Services (MSS)

- 24/7 security analyst and proprietary advanced security information analysis platform enable real-time threat detection and validation, severity determination, reporting, remediation advisory and immediate isolation & protection.
- Additionally NTT Security provides secure IT lifecycle management with continuous vulnerability testing, patch management, advisory and compliance reporting.
- Managed Operations, Network, Endpoint, Identity, Incident Management, Asset, Threat Assessment

Professional Security Services (PSS)

- Technical support and advisories based on security specialized expertise that enables organization’s security risk identification, implementation of the right controls, appropriate incident response and forensics.
- GRC, Architecture/Design, Deployment, Integration, Threat Services, Assessments, and Advisory Consulting
2016-2020 Texas State Strategic Plan for Information Resources Management

- Strategic Goal 1: Reliable & Secure Services
- Strategic Goal 2: Mature IT Resources Management
- Strategic Goal 3: Cost-Effective & Collaborative Solutions
- Strategic Goal 4: Data Utility
- Strategic Goal 5: Mobile & Digital Services
Back to Basics
Difficulty of Breaching an Organization

ALL ORGS

- 31% Intermediate
- 63% Simple and Cheap
- 3% Difficult and Expensive
- 3% Unknown

LARGE ORGS

- 40% Simple and Cheap
- 55% Intermediate
- 5% Difficult and Expensive
<table>
<thead>
<tr>
<th>Section</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Patching</td>
<td>Chronically behind</td>
</tr>
<tr>
<td></td>
<td>Legacy systems “can’t be patched”</td>
</tr>
<tr>
<td>System Configs</td>
<td>Default and insecure</td>
</tr>
<tr>
<td></td>
<td>Infrastructure devices</td>
</tr>
<tr>
<td>Passwords</td>
<td>Blank, default, and weak</td>
</tr>
<tr>
<td></td>
<td>Reuse</td>
</tr>
<tr>
<td>Security Basics – Part 2</td>
<td></td>
</tr>
<tr>
<td>--------------------------</td>
<td></td>
</tr>
<tr>
<td><strong>Data Retention</strong></td>
<td></td>
</tr>
<tr>
<td>Storing unnecessary data</td>
<td></td>
</tr>
<tr>
<td>Storing data longer than necessary</td>
<td></td>
</tr>
<tr>
<td><strong>Encryption</strong></td>
<td></td>
</tr>
<tr>
<td>Using weak or no encryption</td>
<td></td>
</tr>
<tr>
<td>Not managing keys and certificates</td>
<td></td>
</tr>
</tbody>
</table>
Business as Usual

Formal processes

- Patching
- Hardening
- Testing

Before deployment and in production

Base on industry standards (NIST, CIS, etc.)

Update process to address new vulnerabilities
Patching

50% of vulnerabilities identified in scan data for 2013 were first discovered between 2004 and 2011
Common Vulnerability Types

Information Leakage
- Attacker gets info that may lead to any of the conditions below

Denial of Service
- Nobody can use your system

Remote Code Execution
- Attacker gains control over your software

Privilege Escalation
- Attacker with low level access gains higher level access
Attack Vectors

Remote Exploit
- Vulnerable service exposed to Internet

Drive By
- Vulnerable client software opens malicious site or file

Local Exploit
- Exploit vulnerabilities not exposed to the network
Configurations

Through 2020, 99% of firewall breaches will be caused by misconfigurations, not security flaws. – Gartner research
Reduce the Attack Surface

- Remove unnecessary software
- Disable unnecessary services
- Disable unnecessary backwards compatibility
- Disable unnecessary features
- Remove or change default accounts and credentials
- Set all security options as tight as you can

Applies to operating system and every piece of software on top of it
Passwords

76% of network intrusions exploited weak or stolen credentials. Strict policies are required to reduce this easily preventable risk.
# Strong Password Policy

## Enforce password requirements

<table>
<thead>
<tr>
<th>Change &lt;90 days</th>
<th>12+ characters</th>
<th>All character types</th>
<th>Prohibit re-use</th>
<th>Pattern checks?</th>
</tr>
</thead>
</table>

## Support

| Crack your own passwords | Awareness of phishing and re-use |
When it really needs to be secure – multi-factor

Something You Know
- PIN
- Password

Something You Have
- Token Card
- Certificate File
Common Issues

- Broken authentication and session management
- Password reset procedures
- Leaking plaintext passwords
- Users with the same password on every site
- Users who fall for phishing
- Malware and keyloggers
Many of the hacks that make the news can be attributed to weak or -- even worse -- nonexistent encryption. – Bruce Schneier
Untrusted Networks

Encrypt your data!

Or keep it out completely.

Anything that happens over radio (WiFi, Bluetooth, Cellular)

Any wire that leaves your building (Internet, MPLS, Point-to-point)

Any network with a workstation on it (Phishing targets)

Any network with public IP addresses on it (Zero days)
Application Security

Not basic perhaps, but fundamental to supporting the organization’s mission.
**Application Vulnerabilities**

- Custom applications
- Create custom vulnerabilities
- Require custom patches

For more information:

http://www.owasp.org
Software Development Lifecycle

Use Coding standards

- OWASP
- QA for security, not just functionality

Dev/test/prod/backup environments

- Change control
- No testing in production environment
- No production data in test environment

Treat the cause, not the symptom

- Proper design can prevent vulnerabilities
- Stored procedures, standardized libraries, centralized error handling
People

Users don’t want to be insecure, they just don’t know how not to be

- Where and what are the policies?
- Demonstrate real-world threats
- Initial and ongoing training
- The highest value targets often exempt themselves from the rules
Managing Risk and Improving Security –

Texas Cybersecurity Framework
### Texas Cybersecurity Framework – 40 Security Control Categories

<table>
<thead>
<tr>
<th>Category</th>
<th>Control Category</th>
</tr>
</thead>
<tbody>
<tr>
<td>Privacy &amp; Confidentiality</td>
<td>Physical and Environmental Protection</td>
</tr>
<tr>
<td>Data Classification</td>
<td>Personnel Security</td>
</tr>
<tr>
<td>Critical Information Asset Inventory</td>
<td>Third-Party Personnel Security</td>
</tr>
<tr>
<td>Enterprise Security Policy, Standards and Guidelines</td>
<td>System Configuration Hardening &amp; Patch Management</td>
</tr>
<tr>
<td>Control Oversight and Safeguard Assurance</td>
<td>Access Control</td>
</tr>
<tr>
<td>Information Security Risk Management</td>
<td>Account Management</td>
</tr>
<tr>
<td>Security Oversight and Governance</td>
<td>Security Systems Management</td>
</tr>
<tr>
<td>Security Compliance and Regulatory Requirements Mgmt</td>
<td>Network Access and Perimeter Controls</td>
</tr>
<tr>
<td>Cloud Usage and Security</td>
<td>Internet Content Filtering</td>
</tr>
<tr>
<td>Security Assessment and Authorization/ Technology Risk Assessments</td>
<td>Data Loss Prevention</td>
</tr>
<tr>
<td>External Vendors and Third Party Providers</td>
<td>Identification &amp; Authentication</td>
</tr>
<tr>
<td>Enterprise Architecture, Roadmap &amp; Emerging Technology</td>
<td>Spam Filtering</td>
</tr>
<tr>
<td>Secure System Services, Acquisition and Development</td>
<td>Portable &amp; Remote Computing</td>
</tr>
<tr>
<td>Security Awareness and Training</td>
<td>System Communications Protection</td>
</tr>
<tr>
<td>Privacy Awareness and Training</td>
<td>Vulnerability Assessment</td>
</tr>
<tr>
<td>Cryptography</td>
<td>Malware Protection</td>
</tr>
<tr>
<td>Secure Configuration Management</td>
<td>Security Monitoring and Event Analysis</td>
</tr>
<tr>
<td>Change Management</td>
<td>Cyber-Security Incident Response</td>
</tr>
<tr>
<td>Contingency Planning</td>
<td>Privacy Incident Response</td>
</tr>
<tr>
<td>Media</td>
<td>Disaster Recovery Procedures</td>
</tr>
</tbody>
</table>
### TX CSF CMM Scoring – General

#### Maturity Levels

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>There is no evidence of the organization meeting the objective.</td>
<td>The organization has an ad hoc, inconsistent, or reactive approach to meeting the objective.</td>
<td>The organization has a consistent overall approach to meeting the objective, but it is still mostly reactive and undocumented. The organization does not routinely measure or enforce policy compliance.</td>
<td>The organization has a documented, detailed approach to meeting the objective, and regularly measures its compliance.</td>
<td>The organization uses an established risk management framework to measure and evaluate risk and integrate improvements beyond the requirements of applicable regulations.</td>
<td>The organization has refined its standards and practices focusing on ways to improve its capabilities in the most efficient and cost-effective manner.</td>
</tr>
</tbody>
</table>

#### Control Objective Maturity Indicators

| 0 | 1 | 2 | 3 | 4 | 5 |
Common Security Issues

Policy & Procedure Documentation
Asset Management
Vulnerability & Risk Management
Compliance (HIPAA, PCI...)
Logging Strategy
System Development Lifecycle

Incident Response
Configuration Standards
Perimeter Security
Change Management
Data Loss Prevention
Thank you

Joe Mancino
214-770-0162
Joseph.Mancino@nttdata.com

Jeremy Wolff
917-576-6139
Jeremy.Wolff@nttsecurity.com