Building an Effective Supply Chain Security Program

Dave Shackleford
Sr. Faculty and Analyst
SANS
@daveshackleford
Supply chain security is a program that focuses on the potential risks associated with an organization’s suppliers of goods and services.

- Attackers are focusing on this!

There are many ways that a supply chain breach could occur:

- Software compromise, credential theft, and more are becoming common scenarios.
Supply Chain Breach Example: Target

- Target experienced a significant breach of roughly 110 million customers’ data, with at least 40 million payment cards stolen.

- During the course of the investigation, it was found that Target was initially breached through a connection established by one of their vendors, HVAC vendor Fazio Mechanical Services.
Home Depot, another large retailer, also claims that its credit card breach in 2014 was initially due to stolen credentials from a third-party vendor.

In many of the most public cases we have seen, the attackers have targeted personal data, health care information and financial data, such as debit and credit card details.
Supply Chain Breach Example: OPM

- In 2015, the U.S. Office of Personnel Management (OPM) revealed a significant breach of 22 million records including sensitive data tied to numerous federal employees, contractors and military personnel.

- This breach, like many others, seems to have originated with stolen credentials from a background check provider that worked with OPM, KeyPoint Government Solutions.
Getting a Handle on Vendor Management
Current State

Phases

- **Not Defined**
  - No Process Defined
  - Ad Hoc and Inconsistent Approach

- **Defined & Implemented**
  - Consistent but Unstructured Approach
  - Documented and Detailed but not Measured or Enforced

- **Continuous Improvement**
  - Monitoring, Measuring, and Process Improvements
  - Best Practices for Risk Management and Automation
Define Important Vendors

“Important” vendors can mean many things

These are vendors that:

- Are critical to business operations
- Maintain unique or legacy components of importance
- Provide critical services
Vendor Management: Specify Primary Contacts

• Specify primary contacts
  • Coordinate due diligence on vendors and report to senior leadership using a risk-based approach
  • Maintain knowledge of, and compliance with, policies and reporting requirements.
  • File documentation and paperwork with the legal and contracting teams to ensure there is a central repository and audit trail.
  • Coordinate broad communication with those who can add value in vendor oversight
Vendor Management: Establish Guidelines and Controls

- **Policies should include:**
  - Requiring the right to audit and test the security controls of vendors and service providers annually, upon significant changes to the relationship and in response to audit requests or events
  - Requiring vendors to adhere to security monitoring requirements
  - Requiring periodic reports from the vendors and service providers demonstrating service level attainment and performance management
  - Requiring vendors and service providers to provide timely notification pursuant to any security breaches or incidents that may cause impact to the organization
Vendor Management: Integrate with Organization’s Practices

• With the pieces in place, a vendor management program can now start to integrate with the organization’s assessment and audit practices

• Depending on the industry, organization, and culture, these practices will vary widely
Supply Chain Security Best Practices
People, Process and Technology
Best Practices: People

• These should be in place at supply chain companies

• HR Teams: Background checks should be performed on a regular basis for both new and existing employees and contractors
  • Every 6-12 months is ideal

• Monitor all staff that work with your organization’s data and systems for changes to job status and requirements
  • Access to critical systems should be monitored, and all third-party access should be revoked after a defined period of inactivity
Best Practices: Employment Agreements

• HR and security teams should verify that security requirements are clearly spelled out in contracts for supply chain personnel

• Acceptable use provisions should be in place for supply chain organization employees through their employment agreements
Best Practices: Process

- Create a supply chain assessment questionnaire and checklists:
  - Application security
  - Audit and compliance
  - Business continuity and disaster recovery capabilities
  - Change and configuration management
  - Data security and data life cycle management
  - Physical (data center) security
  - Encryption and key management
  - Governance and risk management
  - Identity and access management (IAM)
  - Infrastructure and IT operations security
  - Threat and vulnerability management
Best Practices: Process

- Supply chain review should follow these guidelines:
  - Decide on a list of controls with which supply chain organizations need to demonstrate compliance
  - Determine the frequency of security reviews for internal and regulatory compliance needs
  - Define a remediation and arbitration process for handling supply chain organizations that are not currently meeting security requirements
Process Best Practices: Code Review

• Code analysis of software should ideally be done for supply chain partners

• Having the code reviewed should ideally be the responsibility of the vendors, and they should attest to software security via a report issued prior to installation or updates
  • Contracts should require this!

• Pen testing of software should also be allowed in contracts
Process Best Practices: Vulnerability Mgmt

• Supply chain vendors should have to provide patches to their products in a timely fashion
  • Heartbleed, Shellshock, and others have affected us significantly
  • SLAs should be in place for patch creation

• Supply chain partners should be required to notify you of data breaches that may materially impact you
  • Incidents should be communicated, too...could you be the next target?
Best Practices: Technology

• The first, and perhaps simplest, change is to begin using technology services that offer supplier risk ratings or rankings compared to other industry organizations.

• Monitoring the overall risk ratings of supply chain participants from other organizations working with them provides information on industry perceptions of security posture.

<table>
<thead>
<tr>
<th>Priority</th>
<th>Description</th>
<th>Risk Score</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Urgent action – (Risk no 15 – 25)</td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>High Priority – (Risk no 10 – 12)</td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Medium Priority – (Risk no 5 – 9)</td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Low Priority – Risk no (2 – 4)</td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Very Low Priority– No Action reqd (Risk no 1)</td>
<td></td>
</tr>
</tbody>
</table>
Vendors and partners with privileges should be controlled:

- Enforce separation of duties and least privilege for accounts
- Implement strict password and account-management policies and practices
- Log, monitor, and audit all vendor/partner online actions
- Consider a “sandboxed” approach for remote access

Most importantly, all organizations need a policy and approach to managing and monitoring privileged users
Technology Best Practices: Network Isolation

• Network isolation and segmentation changes can help with improving supply chain security

• Remote attacks through supply chain access should be limited
  • Careful zoning and network isolation with strategic access controls can help prevent this
  • Multiple authentication points (while annoying) can be useful

• Logs and events from remote access systems (VPNs, etc.) should be carefully monitored

• Jump boxes and “thin client” approaches are also valuable
Many organizations use or plan to use security analytics tools and threat intelligence to help identify and combat advanced attacks.

Analytics platforms provide:
- Deep data sets
- Pattern recognition
- Machine learning

Threat intelligence can help to correlate information gleaned from internal sources with indicators of compromise spotted by other organizations.
Technology Best Practices: Exfiltration Monitoring

• Monitoring egress points from the internal network is another way to improve security within the supply chain today

• Some of the most common protocols and standards used for data exfiltration or command and control include HTTP/HTTPS, FTP/FTPS/SFTP, SSH, IRC, Email, P2P, and DNS or ICMP for covert channels

• Monitor at NGFW, IDS/IPS, Proxy, and in DNS
Wrapping Up
Next week you should:
- Review your existing vendor management/procurement capabilities

In the first three months following this presentation you should:
- Update product and vendor inventories
- Define appropriate controls for different vendor types (check best practices discussed earlier)

Within six months you should:
- Update risk assessment processes for vendor review
- Ensure all **critical** vendors have complete reviews & documentation