Supply Chain Security
Shift Left

March 03, 2020
Moderator

Michael Angelo - CRISC, CISSP
Chief Security Architect, Micro Focus

Michael F. Angelo is an ISSA Fellow and is named on the ISSA Hall of Fame. He has over 30 years of cyber security experience. Michael holds 66 patents, with the majority being in the area of Cyber Security. Michael has served as a trusted security advisor and architect with leading corporations. He has worked in the development of national and international standards. Currently he chairs the ISSA International Webinar committee. His current day job requires him to define, track, and drive the Cyber Posture for numerous products.
Supply Chain Analysis

Michael F. Angelo – CRISC, CISSP
Chief Security Architect
Micro Focus@mfa0007
Supply Chain Problem
When checking the Supply Chain

Good Water

Nutrition Facts
Serving Size 8oz Container Size (8oz) Servings Per Container 2

<table>
<thead>
<tr>
<th>Amount Per Serving</th>
<th>Calories from Fat 0%</th>
</tr>
</thead>
<tbody>
<tr>
<td>Calories 0</td>
<td>0%</td>
</tr>
<tr>
<td>Total Fat 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Saturated Fat 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Cholesterol 0mg</td>
<td>0%</td>
</tr>
<tr>
<td>Sodium 0mg</td>
<td>0%</td>
</tr>
<tr>
<td>Total Carbohydrates 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Dietary Fiber 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Sugars 0g</td>
<td>0%</td>
</tr>
<tr>
<td>Protein 0g</td>
<td>0%</td>
</tr>
</tbody>
</table>

Percent Daily Values are based on a 2,000 calorie diet.

Values are highlighted.
But.... What About the Container?

• Plastic Bottles?
• Can the plastic leach toxins?
• If so, can it cause:
  ❑ Medical Issues
  ❑ Weight Gain
• Does it get worse if you reuse them?
And Where Did It Come From?

Does It Matter
Supply Chain – The Real Picture

{ Your Environment }
How is this Relevant?

• Our Cyber Supply Chain contains much more than just the software.

• It Includes
  - Software
  - Hardware
  - People
  - Facilities
  - and Infrastructure
Thomas has over 30 years of experience in the IT industry ranging from software development to infrastructure & network operations and architecture to settle in information security. He has an extensive security background covering roles from incident responder to security architect at fortune 500 companies, vendors and consulting organisations. He is currently security advocate and threat researcher focused on advising companies on understanding their data protection activities against malicious parties not just for external threats but also compliance instigated.

Thomas is also an active participant in the InfoSec community not only as a member but also as director of Security BSides London and speaker at events like Securi-Tay, hack.lu, Troopers, DeepSec, Shmoocon, and various BSides events.
Supply Chain Risks are Seen thru History
Adapting and Changing Risk Footprint
Adapting and Changing Risk Footprint
Protecting Supply Chain

A convoy of merchant ships preparing to sail to Britain from Halifax, Nova Scotia
(Image courtesy of merchantships.tripod.com)
Cyber Security Supply Chain Attacks are Real
Service Providers

- Implicit trust levels
- Different Security Practices
- Miscommunications
- Introducing compromised software or hardware
- Data storage or aggregation
- Backdoor into your Environment

Examples
- Target hacked thru HVAC provider
- Political parties and mobile Apps
- 13 MSPs used to push RATs (report from Armor)
- Physical access controls (e.g. CCTV) providers connecting infrastructure to your network
Software Supply Chain

➢ Purpose is to provide software for the organisation
  ❑ Function as intended
  ❑ Reliable, safe and secure

➢ Risk is software will not function as intended
  ❑ Coding defects by the supplier
  ❑ Inadequate security controls
  ❑ Defects and issues in the product not addressed in a timely manner
  ❑ Operational issues over time (e.g. technical debt)
  ❑ Open source is not secure
Software Supply Chain

Software Supply Chain

Example 1

➢ British Airways suffered a data breach in 2018

➢ Javascript library compromise on payment site

➢ Affected main website and mobile app

➢ Campaign against BA ran from 22:58 BST August 21, 2018, until 21:45 BST September 5, 2018

➢ Magecart group responsible
Example 2

- Huge data breach at Equifax

- Unpatched open source software to blame

- Failure in security controls
  - Scan for vulnerable systems failure

- Critical flaw in Apache Struts2
The Hidden Supply Chain
96% of applications have open source components

57% to 78% of codebase is open source based (2018)

Average number of open source components keeps growing
- 298 in 2018 versus 257 in 2017

60% of open source components had vulnerabilities
- “National Vulnerability Database (NVD) listed more than 16,500 new vulnerabilities in 2018—7,393 of them in open source products”

43% of those older than 10 years
Managing the Risk of Open Source Components

➢ Vetting of open source components
Open Source Code in Proprietary Software

➢ Vetting of open source components

➢ Scan your existing projects
Open Source Code in Proprietary Software

➢ Vetting of open source components

➢ Scan your existing projects

➢ Manage existing vulnerabilities and established remediation plans
Open Source Code in Proprietary Software

➢ Vetting of open source components

➢ Scan your existing projects

➢ Manage existing vulnerabilities and established remediation plans

➢ Build a Third Party Component repository
Open Source Code in Proprietary Software

➢ Vetting of open source components

➢ Scan your existing projects

➢ Manage existing vulnerabilities and established remediation plans

➢ Build a Third Party Component repository

➢ Understand the vulnerabilities versus impact and cost
4 Principals of Supply Chain Security

➢ Understand the risks

➢ Establish control

➢ Check your arrangements

➢ Continuous improvement
Build a Continuous Improvement Program

➢ Establish a third party component asset library

➢ Review agreements, component ageing and maintenance

➢ Vulnerabilities change over time; establish a continuous scanning and remediation

➢ Build this into your DevOps process
James McQuiggan, CISSP, is a 20 year security veteran and Security Awareness Advocate for KnowBe4. James is also a part time faculty professor at Valencia College in the Engineering, Computer Programming & Technology Division. Within the Central Florida community, he is the President of the Central Florida (ISC)2 Chapter and a Trustee Board member with the Center for Cyber Safety and Education. James has worked as a Product & Solution Security Officer, Information Security analyst and a network security engineer. He consulted and supported various corporate divisions on cybersecurity standards, information security awareness and securing product networks.
“The Supply chain stuff is really tricky”

Elon Musk
CEO of Tesla & SpaceX
The Good, the bad & the ugly

- 59% of companies experienced a third-party data breach
- 16% effectively mitigate third-party risks
- 34% track inventory with third-parties
- 36% avoided a breach from a third-party
Third Party Products

Cost Reductions
Resources
Equipment
  ❑ Hardware
  ❑ Software
Remote access
  ❑ Machine to machine communication
  ❑ Interactive User

Vulnerable Gigabyte driver allowed RobbinHood ransomware infections
By Jitendra Soni, 21 hours ago
Gigabyte did not accept the flaw initially nor did it offer a fix

A serious security flaw in Gigabyte drivers may have allowed hackers to take over entire computer systems, experts have warned.
Supply Chain

Source: SANS Cyber Risks Supply
Supply Chain – Hardware attack

- Concern over Supermicro motherboards had a secret tiny chip onboard
- Used to collect information and send back to Chinese Hackers
- Untrue... but possible
Criminals gain access to an email account and monitor incoming and outgoing emails.

When the person with the compromised email account sends an invoice to a client via email, the attackers immediately send a duplicate, fraudulent invoice from the same email address, telling the client they made a mistake and to wire money to the account in the revised invoice.

Attackers may also just generate fake invoices and send them to clients, which they are able to identify from previous email conversations.
Two Unnamed US Companies Falls Victim to $100 Million CEO Email Fraud

This scam only surfaced as the U.S. government filed a civil forfeiture lawsuit in federal court in Manhattan seeking to recover tens of millions held in at least 20 bank accounts around the world.

The scammer, a 48-year old Lithuanian managed to trick two American technology companies into wiring him $100 million.

What makes this remarkable is the amount of money he managed to score and the industry from which he stole it. The indictment specifically describes the companies in vague terms, but Apple, Cisco, HP and Facebook come to mind.
Risk Differences

Digital Transformation introduces
Third Party Risk

Third Party Risk

Traditional Business Risk

Change Impact Complexity

RISK
Supplier Security Risk

• Supplier Risk Management Solution
• Three methods
  • Risk Management solution
  • Managed Support Services
  • Hybrid of VRM and Risk Assessment Data
• Depending on cost, time, resources
• Risk Assessments – Threats vs Vulnerabilities
• Likelihood, Opportunity leading to risk
Challenges for the Third Party / Vendor / OEM

- Global products – Embargo, processes
- Secure Configuration / Hardened – patch management, remote access available?
- Possible Multiple certifications for lines of business
- PCI, NERC, ITAR, HIPAA
- Vendors are asked for 3rd party validation to confirm their products are secure
- What is the responsibility of the customer vs the provider?
Questionnaires

YEA / NAY?
Questionnaires

• Pros vs Cons
• Self Audit vs. 3\textsuperscript{rd} party audits
• Evidence – Confidential vs Public
• Remediation strategies
• Common Questionnaires
  ❑ FICO CyberRisk Score -> Chamber of Commerce ABC Risk Score
  ❑ SIG – Standard Information Gathering
  ❑ CAIQ – Cloud Security Alliance
Identification

Monitoring

Assessment

Remediation

Analysis
GRC - Overview

<table>
<thead>
<tr>
<th>Governance</th>
<th>Provides the ability to monitor processes towards company goals</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk Management</td>
<td>Work to assess and mitigate risks (risk management)</td>
</tr>
<tr>
<td>Compliance</td>
<td>Support and comply with internal policies or laws &amp; regulations</td>
</tr>
</tbody>
</table>
# Governance

<table>
<thead>
<tr>
<th>Regulations</th>
<th>Standards</th>
<th>Policies</th>
<th>Contracts</th>
<th>Process / Procedures</th>
<th>Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Laws / Statutes</td>
<td>• ISO</td>
<td>• Organizational</td>
<td>• B2B Agreements</td>
<td>• NIST CSF</td>
<td>• Administrative</td>
</tr>
<tr>
<td></td>
<td>• NIST</td>
<td>• IT / HR</td>
<td>• IT / HR</td>
<td>• ISO</td>
<td>• Physical</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• OEM</td>
<td></td>
<td>• Technical</td>
</tr>
</tbody>
</table>
## Risk Management

<table>
<thead>
<tr>
<th>Conduct</th>
<th>Plan</th>
<th>Authorize</th>
<th>Incorporate</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Asset</td>
<td>• Business line</td>
<td>• Regulations</td>
<td>• Link to business</td>
</tr>
<tr>
<td>Management</td>
<td>• Asset Type</td>
<td>• Track &amp; implement</td>
<td>• Automate</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td>• What's the risk?</td>
</tr>
</tbody>
</table>
## Compliance

<table>
<thead>
<tr>
<th>Monitor</th>
<th>Assess</th>
<th>Audits</th>
<th>Reporting</th>
</tr>
</thead>
<tbody>
<tr>
<td>Threat Landscape</td>
<td>Systems</td>
<td>Regulatory</td>
<td>Internal (C-Suite)</td>
</tr>
<tr>
<td>Internal activity (SIEM)</td>
<td>Processes</td>
<td>Standards (ISO)</td>
<td>Regulatory</td>
</tr>
<tr>
<td>Implemented controls</td>
<td>Audit Prep work</td>
<td>Contractual (PCI, CIP, GDPR)</td>
<td>Customers / Vendors</td>
</tr>
</tbody>
</table>
Wrap-up

➢ Work with your third parties
➢ Identify the types of risk for each third-party
➢ Determine the access the third-party needs / requires
➢ Understand all connections / risk
➢ Monitor all access from all parties
➢ Collaborate with third parties on all incidents
➢ No silver bullet – it requires a machine gun
The lighter side of third party suppliers....

"We've talked it over and we've decided that you must not really be a customer."

VS

“A lot of times, people don’t know what they want until you show it to them.”
– Steve Jobs