Secure Acquisition Case Study 2: Acquisition/SCRM Project Risk Analysis

Dan Shoemaker, University of Detroit Mercy

April 2021

Secure Acquisition Case Study 2: Acquisition/SCRM Project Risk Analysis

Background

Systems are built out of components that are integrated from the lowest level of a supply chain up to a finished product. This creates a serious weakness in that malicious code, or counterfeit parts can be inserted at the bottom of the process without scrutiny and then integrated up into the end-product, as was demonstrated by the recent SolarWinds hack.

The possibility of such a thing occurring is so obvious that you would think that there have been practical efforts to address it. However, even though we've expended much time and effort to ensure robust, efficient and defect free code, we have done very little to ensure against compromises that could occur during the integration process. Thus, the aim of this project is to help the student understand the stages involved in establishing supply chain capability, as well as present a sample solution.

Case Study Overview

The student will utilize NIST 800-161 (provided) to identify and assess risks against the standard Base Practices SCRM in order to obtain an overall risk rating for each of the functions identified in case one. The risk rating can be used to prioritize the risks.

Student Instructions

There are a lot of requisite best practices. Therefore, it is necessary to employ a generic checklist as a means of identifying what risks may affect components, or participants. Hence utilize the forms taken from NIST 800-161 (provided) to obtain an overall risk rating for the organization under analysis. In order to prioritize findings by criticality, we have developed the following standard for remediation timelines: Critical = 30 days, High = 60 days, Medium = 120 days, Low = 356 days

Instructor notes

This is an individual assignment done during a live-lab session. The process steps are taken a step at a time as guided by the instructor. This is done in-class as a first of four lab projects done over the semester to illustrate an explicit process for risk mitigation in supply chains using NIST 800-161

Example solution

A checklist form is provided. The student works through the example case with the blank checklist and makes judgments about whether each function is adequately performed. A sample solution follows:

Gap Description	Additional Comments	Priority	Action	Timeline
Do you evaluate the use of multifactor authentication mechanisms	MFA configured for the mobile apps but not when users login via the web browser	Critical	Implement MFA across the board, including for users who login using the web browser	September, 2020

Do you document any applicable information-sharing arrangements between customer and supplier in contract documents - including: a. Description of the information to be shared? b. List of Recipients?	No NDA in place	High	Implement a non-disclosure agreement as well as provision a system for information sharing	November, 2020
Do you have organizational policies and contractual requirements that require SCRM awareness and training for all relevant personnel in acquirer and integrator organizations	SCRM process are already in place but there is a lack of awareness.	Medium	Develop training in place to educate business stakeholders on how to leverage the existing SCRM process	January, 2021
Do you do comprehensive awareness and training that promotes the organization's SCRM policy and procedures	SCRM process are already in place but there is a lack of awareness.	Medium	Develop training in place to educate business stakeholders on how to leverage the existing SCRM process	January, 2021
Do you require SCRM awareness training for all acquirer and integrator personnel who are involved in requirements, acquisition, and procurement activities	No required training available	Medium	Develop training to educate business stakeholders on how to leverage the existing SCRM process	January, 2021
Do you leverage industry best practice for security patches to include a list of what issues are "covered" in the patches (i.e., the nature of the issues, a severity rating such as CVSS, etc.)	Patching in general is scheduled quarterly, which is a gap for newly discovered vulnerabilities	High	Implement a patch policy to enforce monthly patching	December, 2021

Do you utilize existing vulnerability and incident management capabilities to identify potential supply chain vulnerabilities	Identified multiple supplier who are not using our existing IR & VM processes	Critical	Identify suppliers, vendors who do not follow the existing processes, especially when it comes to indecent notification and work with them to socialize and enforce the processes	October, 2020

References

Sigler, Ken, Dan Shoemaker and, Anne Kohnke, Supply Chain Risk Management: Applying Secure Acquisition Principles to Ensure a Trusted Technology Product, Auerbach Publications; (Internal Audit and IT Audit) 1st Edition, November 3, 2017

Shoemaker, Dan, and Kenneth Sigler, "Cybersecurity: Engineering a More Secure IT Organization", Cengage Learning, 2014, Chapters 5 and 7

ISO 27001 and ISO 27002 (provided as BS7799)

IEEE 1028-1997 Standard for Software Reviews

ISO/IEC 9126 – 1991 Software Product Evaluation - Quality Characteristics and Guidelines for Their Use (can be read as ISO/IEC 9126- 96)

IEEE 610 - Standard Glossary of Software Engineering Terminology
The Common Weakness Enumeration http://cwe.mitre.org/

Foreign Ownership, Influence or Control Investigations (FOCI)
http://www.dss.mil/isp/foci/foci_info.html