ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (13-17), Month: October - December 2020, Available at: www.researchpublish.com

Demystifying Third Party Software Endorsement

[1]Johara Aljarri, [2]Reema Alomar, [3]Mohammed Omani

Saudi Aramco, Dhahran, Saudi Arabia

Abstract: **Introducing a new third-party software to an enterprise environment is often overlooked task. When it comes to adding new software to environment, an assurance of its compliance with the enterprise security posture and operational standard is a must; and the software reputation must be also verified. The software endorsement process will ensure full assessment of the third-party software at the initial stage, and a maximum utilization of IT software solutions. Moreover, it will also help to avoid duplication in software solutions within the enterprise environment. This paper will explore an overall endorsement practice and cybersecurity methodology that can help an organization to endorse new third-party software, from cybersecurity and licensing perspectives.**

Keywords: **software, license, security, endorsement, cybersecurity, third-party software, enterprise.**

I. INTRODUCTION

Companies are increasing the use of third-party software since it is convenient and easy to access. Also, it has other advantages, including low comparative cost, easy installation and use, diverse software options, and trial version testing. Such software can have security vulnerabilities, doesn't meet user requirements and limited customer support. Companies cannot assume that a third-party software is properly secured. It's crucial that a company's IT support assess the security of the software before it gets connected to the network. Moreover, there are many different types of software licenses, so the software might also cause a legal issue if it is not licensed or not intended to be used for commercial or business use. Therefore, to avoid penalties of license incompliance or security threats, any third-party software must be assessed, even in earlier stages, before contracting and purchasing.

From a security perspective, the assessment for the software is fairly straight forward if the software already installed in the environment through vulnerability scans, penetration testing activities, or binary analysis of the software. Assessing a software that is not installed or purchased is a challenging process due to lack of information about the software design and underlying technology used for developing this software. Furthermore, software developers do not follow a secure development life cycle (SDLC). Therefore, it imperative that software developers might not follow a development security testing standard to test all software components, such as Open Web Application Security Project (OWSAP) top 10[1]

In this paper, an end-to-end process has been developed to measure the risk of getting the software on the company's network, before any engagement with the software provider.

II. PROCESS

The process of conducting software endorsement starts with collecting any needed information about the software. Then a thorough review of the information from security and licensing perspective in parallel. Finally evaluate the risk of having the software introduced to the corporate network based on the provided information.

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (13-17), Month: October - December 2020, Available at: www.researchpublish.com

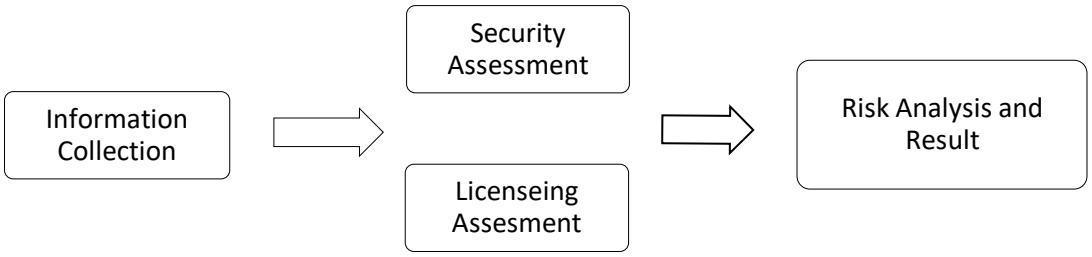

Figure 1: Process Diagram

III. PROCESS DETAILS

A. Information Collection

To conduct security and licensing assessment on a software, information about its vendor and the software itself is crucial. There are two main sources for this information:

Online Search

An online search provides full cybersecurity information about a given software. The online search is the initial step in the information collection. Vulnerability database websites may provide a history of the software security state. It important to note that if a software contains a vulnerability, it doesn't mean the software is not secure. Knowing that the vendor is releasing software patches frequently and in a timely manner after vulnerability discourse is a good sign about the vendor support. As for the licensing terms and details, each software has an end-user licensing agreement (EULA), which can be also obtained from the official software website or by request. It is very important to go through the licensing terms and conditions, and get to know the licensing model and type, before purchasing the license.

Software Questionnaire

The software questionnaire will be used as an open channel with the vendor, to obtain a lot of information about the vendor reputation, software maturity, and the licensing model and type. This will be considered as the main source of information to perform the preliminary security assessment, and confirm if the licensing model is applicable to be used in the enterprise. The questionnaire will be generic to cover common software information and critical security domains.

In addition, the questionnaire can be customized if needed, based on the software function or any other aspects. OWSAP top 10[1] has identified the following security domains:

A. Access Control:

This domain includes controls that verify "who a user is" (Authentication) and "what they are permitted to do" (Authorization), and should include controls, such as credential management and Role-Based Access Controls (RBAC).

B. Session Management:

This domain should include how these sessions are generated, transmitted, cached, and validated in a secure fashion.

C. Input/Output Validation:

This domain should validate the correct formatting of input and output data.

D. Error Handling:

This domain ensures errors generated by the software do not reveal information about the underlying infrastructure and contain generic error message.

E. Logging:

Ensure a proper audit trail is maintained for the software.

This domain relates to the ability of a given system to generate appropriate logs to support operational, procedural, and security monitoring of the system.

F. Data Protection:

Ensure data is being handled securely.

G. Secure Communication

This domain relates to security controls that can be enforced to protect systems at a network level.

When it comes to gathering information about software licensing, it is very important to ensure alignment with corporate strategy. The software should comply with the enterprise regulations and specifications. Thus the following areas should be covered during this phase, to prepare for assessment:

A. Hosting environment

B. License type

C. Installation Platform

D. Documentation on current release

E. Data Privacy and legal term for cloud-based solutions

Overall, this section should capture general information about any required third-party software solution. This information is required to assist with security and licensing related decisions and risk assessment activities. Finally, we recommend also to ask the vendor to provide any supporting documentation with their answers for validation and to expedite the next stage of analysing this information. The next phase will demonstrate the actual assessment on licensing and security in parallel.

B. Security Assessment

In this stage IT support must review the answered questionnaire about the software. Reviewing the questionnaire and marking each security domain with Fulfilled, Not Fulfilled or Not Applicable. While the Not Fulfilled security domains might not pose a security risk individually, a combination of Not Fulfilled domains may increase the risk.

This a sample matrix that will help the analyst to do a thorough assessment on the software:

TABLE I: Security Assessment Questionnaire

Security domain	Question	Fulfilled	Not fulfilled	Not Applicable
Access Control	Is there any authentication controls implemented to secure the user authentication process?	☐	☐	☐
	Does the software integrate with directory services for authentication?	☐	☐	☐
Session Management	Does the software use session IDs?	☐	☐	☐
	Are there any session management controls implemented to secure the software, such as setting session timeout, disabling concurrent session?	☐	☐	☐
Input/Output Validation	Is data from the user encoded?	☐	☐	☐
	Does the software verify files to be uploaded to the software?	☐	☐	☐
Error Handling	Does the software display generic error messages to the user?	☐	☐	☐
	Are there controls placed to ensure the software recovers securely from errors?	☐	☐	☐
Logging	Does the software support collecting security audit logs?	☐	☐	☐
	Does the software support forwarding the logs to external log monitoring tools?	☐	☐	☐

ISSN 2348-1196 (print)
International Journal of Computer Science and Information Technology Research ISSN 2348-120X (online)
Vol. 8, Issue 4, pp: (13-17), Month: October - December 2020, Available at: www.researchpublish.com

Data Protection	Does the software use secure encryption and hashing algorithms such as AES 256, SHA 256?	☐	☐	☐
	Is data being protected during storage?	☐	☐	☐
Secure communications	Does the software encrypt sensitive data during transmission?	☐	☐	☐
	Does the software use secure protocols such as HTTPs or SSH?	☐	☐	☐

C. Licensing Assessment

As for the licensing assessment, the license type varies from perpetual type to subscription-based, and can be a complex license that requires further analysis, such as metric licenses. Knowing the type of license and how to manage it is crucial. The software asset manager in every enterprise should be consulted and provided with licensing details obtained from the vendor. The vendor's response to the questions in Table 2 Licensing Assessment Questionnaire will be evaluated at this stage, as part of the assessment:

TABLE II: Licensing Assessment Questionnaire

Question	Answer
Provide the Product Model number (Part Number), and the SKU number(s) for all the software components. This also indicates the version and edition.	
Specify the warranty/support period.	
Provide the End-User License Agreement (EULA)	
Specify the installation platform workstation, server or cloud.	
Is the software licensed based on a "Per Server" basis? If yes, please specify whether it is licensed base on: Devise, CPU or Core.	
Is the software licensed based on a "Per Workstation" basis? If yes, please specify whether it is licensed base on: Number of Installations, Site or Enterprise.	

All the public cloud solutions have to be fully reviewed by the enterprise lawyers to ensure its alignment with the enterprise regulations and standards, and compliance with the country's law.

D. Risk Analysis and Result

Security Assessment as mentioned previously in Table 1 the fulfillment of security domains section, a control may be marked as not fulfilled or not applicable with a valid justification. While these exempted controls may not pose a security risk individually, a combination of not fulfilled controls may compound the risk.

When performing the risk assessment, it is important to assess the cumulative impact of all the not fulfilled controls collectively rather than individually, and factor in the overall criticality of the software.

As for licensing evaluation, the licensing information provided in Table 2 must be considered in the risk assessment, which includes verifying first the EULA. Then check the data privacy and legal term for cloud-based solutions if it's acceptable, based on the company and government regulations. The regulations differ from one enterprise to another, based on their country rules and standards.

The SKU [3] is a unique number for each software and it is an important piece of information, as it allows the assessor to identify the exact software version and edition in which they can decide whether this specific type of edition is applicable for the enterprise use or not. It also provides a lot of details on the software, such as license type and use rights, which includes the right to upgrade or downgrade. Below are two different SKU as an example [3]:

- SKU: 810-03324:

Publisher= Microsoft, Product = Microsoft SQL Server 2005 Enterprise Edition Win-64Bit 1 Processor German 2 Years Software Assurance OPEN C

- SKU: 810-03537:

Publisher= Microsoft, Product = Microsoft SQL Server 2005 Enterprise Edition Win-64Bit 1 Processor German 2 Years Software Assurance OPEN NL

Security and licensing depend heavily on each other to get software approved for use in the corporate network. Failure in either security or licensing evaluation assessment means rejection of the software, unless there are compensating controls.

Responsible risk assessment entities have a defined risk tolerance. The risk tolerance needs to be considered during the assessment phase and the final result of the software endorsement.

The result whether approving or rejecting the software must be documented in the report. The report should highlight the assessment findings and the approve or reject status. It is good practice to share the findings with the software provider for improvement purposes.

IV. CONCLUSION

Third-party software is considered a significant enterprise asset, and might also present a huge risk of license misuse or security threats. Any compromise to integrity, confidentiality and availability, presents a huge risk, and is associated with unsecure software.

A full endorsement process should be conducted on the third-party software before any commitment to the software vendor. This process will highlight key software indicators that must communicated with the involved entities, to ensure alignment with enterprise regulations.

In cybersecurity, we all agree that one way to protect our corporate network is by performing significant security practices. In addition to ensuring business continuity through substantial licensing agreements. Achieving these goals requires solid techniques and mechanisms to detect and prevent any potential threats proactively. All organizations should consider conducting a thorough endorsement on the software before any engagement with the vendor. This will lead to a more secure compliant and visible organization network.

REFERENCES

[1] Owasp.org. 2020. OWASP Top Ten Web Application Security Risks | OWASP. [online] Available at: <https://owasp.org/www-project-top-ten/> [Accessed 26 August 2020].

[2] Eula.com.au. 2020. End User License Agreement – EULA — End User License Agreements Explained. [online] Available at: <https://www.eula.com.au/> [Accessed 8 September 2020].

[3] Flexera Blog. 2020. Why A SKU Is Important To Software Asset Management | Flexera Blog. [online] Available at: <https://www.flexera.com/blog/elo/why-a-sku-is-important-to-software-asset-management/> [Accessed 9 September 2020].