Sri Lanka Institute of Information Technology

Policy development on installing third party software in company PCs

Information Security Policy and Management - IE3072

B.Sc. (Hons) in Information Technology
specializing Cyber Security

Students Details

Student ID	Student Name
IT19991290	A.D. Jaliya
IT19961118	W.M.J.P. Wijesekara
IT19952376	S.A.D.H. Vishwajith
IT19961040	K.P.D.S. Madhushanka
IT19014050	B.D.T.S.P. Ariyarathna

Contents

Abstraction

Third-party software is installed on devices on a regular basis and has access to user data. It is critical to consider the risks that these applications pose to your devices and data. This information will assist risk owners and administrators in developing organizational policies for the use of third-party applications. App Locker and Windows Defender Application Control can be used to ensure that only trusted apps run. You can also rely on ‘reputation assessments' to ensure the security of third-party apps.

If your policy requires a current assessment of an application before approving a new version, you must consider how you will handle security vulnerabilities. You should try to limit the amount of sensitive data that an application has access to. Apps from large, well-known developers are less likely to be malicious than apps from unknown developers. Consider using security apps or antivirus to reduce the risk of malicious code execution. Mobile Device Management software allows you to specify which users are permitted to install and use an application.

If you consider some applications to be risky, but some users have a strong business need for them, you can consider restricting access to these users only. These areas are frequently included as part of a platform's bring your own device (BYOD) features. You should weigh your assessment against the needs of users in terms of productivity. Incorporate this procedure into your standard software asset management routine and run assessments concurrently. Allowing third-party apps to access work data is only permissible if they are performing a work-related function. For applications that may pose unacceptable levels of risk, use architectural approaches to limit risk.

Introduction

The reusable software component is a third-party software component created for free distribution or marketing by an entity other than the original developer platform provider. The financial benefit of utilizing third-party code in your program is the cost reduction. Developing software in-house by your team is more expensive than buying off-the-shelf solutions from third-party suppliers. It takes a long time to create new tools and software. Developers are often working under tight timelines to enhance their products and add new features for fast turnarounds. You don't have to reinvent the wheel for each and every issue. It’s Reduced development time. Most likely, it is time-tested code that was put through the wringer and most problems have been resolved or discovered. Third-party app stores may include a plethora of secure apps. However, there is a greater possibility that they may provide hazardous ones. And these applications have the potential to infect your company's computers with dangerous malware such as ransomware and adware.

An information security policy (ISP) is a collection of guidelines for those who interact with IT assets. To guarantee that your employees and other users follow security rules and processes, your business may develop an information security policy. The goal of IT security policies is to address security risks and adopt methods to minimize IT security vulnerabilities, as well as to specify what to do in the case of a network assault and how to recover. Furthermore, the regulations outline what employees should and should not do in certain situations. [1]

A thorough self-assessment questionnaire should be completed by all vendors as part of a third-party software compliance policy. While this questionnaire cannot be completely trusted, it will give vendors an idea of how concerned you are about security; the Shared Assessments SIG or AUP offer a standardized form of this questionnaire that the majority of vendors are accustomed to completing. Individual development teams expanding to third-party solutions or open-source code without engaging their security teams is not commonplace as businesses have grown. Many CISOs are shocked at how much code is outsourced in their organizations. Once suppliers understand and agree on an enterprise's security strategy, and CISOs realize how much third-party code they are working with, the next step is to enlist help.

After all, third-party software suppliers must be verified on a regular basis to verify they are fulfilling the criteria outlined in their evaluations. Find an independent application security testing vendor with the expertise needed to create a process that secures all elements of the network architecture, including remote third-party installs. The top security providers can offer a variety of deep code scanning services, guaranteeing that code is clear of typical vulnerabilities even if business constraints prohibit the organization from working directly with source code. If a solution is provided on a scalable, cloud-based platform, it can be quickly extended to include all incoming code and apps, providing optimum security with minimum corporate effort. Third-party software is rapidly becoming a significant source of concern for many CISOs, but it doesn't have to be for you. You may avoid the humiliating and expensive problems that are often associated with insecure outsourced code by prioritizing the creation of a third-party compliance policy. [2]

Significance of the Topic

Are you aware...? 75% of attacks are caused by vulnerabilities in third-party software. The majority of people in the world uses third-party software. And that software is susceptible to attack at any time. As a single person, this will pose no difficulty. However, if we consider a large organization, installing third-party software on company PCs can be a significant issue. Due to the numerous benefits of third-party software, we are unable to stop using it. However, we can use them under certain circumstances. That is why we should establish policies regarding the installation of third-party software on company computers.

All current personal computers are capable of running third-party programs. Most also provide an online marketplace for installing them. Allowing your users and devices to access a diverse set of applications has obvious benefits. However, it's critical to consider the threats these applications pose to your devices and data. [3]

Third-party software is often installed on devices and has the ability to access and change the user's data stored on that device. Third-party software may potentially have access to your organization's data in certain circumstances. Once a third-party software has gained access to data, it is very difficult to determine what was done with it. While certain industrial software-related services will sync your local data to cloud services, some may handle it insecurely, while others may include third-party libraries that introduce their own security concerns.

You'll be able to better control the risks involved with executing third-party code if you create a proper organizational policy that specifies the sorts of applications that are allowed. By implementing proper policies on installing third party software in company PCs your organization will be able to take advantages of the productivity benefits provided by the third-part software. [4]

Developing their own tools or new software to meet organizational requirements is a time-consuming and expensive process. The cost of developing new software in-house is higher than the cost of purchasing software or tools from third-party providers. Even developing new tools or software for the organization is insufficient because the developed software or tool must be properly maintained over time through the providing of updates and security patches. This is also an extremely expensive and time-consuming process. This procedure has a direct impact on the organization's primary objective and results in a decrease in the organization's productivity.

As a company, their primary objective is to maximize organizational productivity and provide superior customer service. To accomplish those tasks, the business must install third-party software on its computers. However, utilizing third-party applications and software can be risky at times. The company's reputation and trustworthiness can be compromised if those vulnerabilities are exploited. As a result, the organization should have an effective policy enforcement mechanism in place for third-party software or applications that are installed on organizational personal computers. [5]

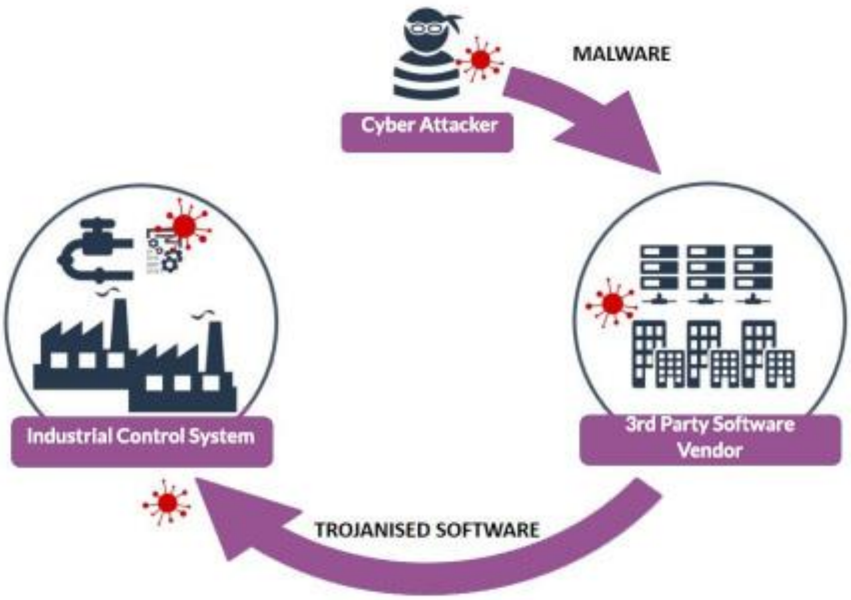
Critical Evaluation of the Topic

Nowadays, it is almost certain that any organization will use third-party software to assist in the delivery of products, systems, and services. While third-party software is critical to a business's operation, it provides numerous benefits and conveniences, it typically means that third-party personnel will need access to your organization's systems and data. If not handled properly, this immediately becomes a security issue.

With the growth of the organization's personal computers and the third-party software that runs on those PCs, it becomes increasingly difficult and complex to manage security at all levels and ensure that all third-party software providers are sufficiently secure. Vulnerabilities can manifest themselves in any third-party software installed on company computers which risking your organization's security. Cybercriminals are well aware that poorly secured third-party software can provide an easy backdoor to sensitive data and systems, and they will seize the opportunity to exploit these vulnerabilities. [6]

When downloaded or purchased from the developers' websites, third-party software would install malware alongside legal third-party software. Additional remote access capabilities may be added to the malware, which can be used to take control of the computers on which it was installed.

Compromise third-party software is very difficult to detect if it was changed at the source, since the target company has no reason to believe it was not genuine. This puts a high degree of dependence on the program creator since it is impractical to examine every piece of hardware or software in detail in order to detect this kind of attack.



Typical attack vectors that occurred as a result of third-party software installation on corporate computers.

- **Software Manufacturers Third-Party**
  Through vendors, compromise software at the source. Malware may be inserted into update files and then installed by the business, spreading the infection to other IT systems and software users on the internal network.

- **Apps & Website**
  Hackers may inject malicious code into applications during development or attack fundamental scripts of website builders, redirecting visitors away from the genuine site and onto the hacker's malicious one.

- **Data storage facilities provided by other parties**
  Outsourcing sensitive data and granting access to other businesses risks the data getting into the wrong hands. The network may then be accessed using the stolen credentials.

Common threats

The risk of cyber safety includes the possibility for cyber-attacks, violations by third parties or other forms of system exposure that may damage an undertaking's technical infrastructure or operations. The growing reliance on safe remote third-party access to business networks and worldwide network has rendered firms even more vulnerable to cyber assaults. Common dangers were caused by third-party software installation on PCs. [7]

- Hacking
- Malware
- Pharming
- Phishing
- Ransomware
- Spam

Effects on this matter

These types of attacks have a significant financial impact on a company. While tarnishing the company's image. Customer dissatisfaction has a negative impact on the business. Users' personal information and the company's business strategy could be compromised. These factors can be harmful to the organization's success. As a result, the company will have to deal with legal issues, unanticipated financial losses, and a lack of risk management. The organization will eventually be unable to meet its long-term achievements.

Preventions of exploiting vulnerabilities on third-party software

Businesses of all sizes increasingly rely on third-party software vendors to boost profitability and efficiency, cut costs, and gain a competitive edge. Globalization increases vulnerability to data breaches and cyberattacks by third parties, emphasizing the importance of remote access solutions.

Nevertheless, many businesses lack an effective risk management program or are unaware of how to mitigate risks associated with the installation of third-party software on company computers.

With vendor remote access becoming more critical to business performance, it's critical for businesses to understand where risks originate and how to avoid future third-party data breaches. Securing sensitive data enables firms to plan ahead and keep ahead of potential cyberthreats. [8]

There are several ways to manage those kinds of risks.

- Run regular vulnerability scans.
- Patch software regularly.
- Minimize local administrator privileges.
- Configure systems securely.
- Practice secure network engineering.
- Enforce a password policy and require two-factor authentication when available.
- Change default passwords on all application and appliances.
- Ensure all devices have unique local administrator passwords.
- Use secure software development practices.
- Make sure to have working and tested backups of key systems / data.

We can mitigate and manage risk by applying these methods. However, if we had implemented security policies properly regarding the installation of third-party applications on company computers. We can mitigate the risks mentioned above prior to their exploitation.

What kinds of third-party software on company computers can exist?

Maintain a list of required third-party software within the policy. Complement that list with specific titles and their variants. The policy should specify who is ultimately responsible for the use of third-party software. In many circumstances, this will be a team comprised of members from other departments other than the IT department. While user input is more important than IT feedback in some software circumstances, it should be balanced with IT feedback in others.

Additionally, address the manner in which the applications will exist. While this may be a more IT-specific issue, it should be addressed in the policy. That only the following kind of third-party software should exist:

- Part of a clone image or OEM image
- An IT-drafted step-by-step installation procedure identifying installation options
- A shortcut only
- An automated installation through a deployment tool
- A terminal or Citrix application
- Some other controlled and documented distribution method

By mandating third-party software to exist exclusively in this form, IT will have a much clearer picture of what should be installed on company PCs. [9]

How does the license process?

IT is aware of the importance of third-party software licensing, and the policy should handle it. Non-IT professionals may be unfamiliar with licensing concerns and associated expenditures. While the majority of third-party software is an expensive tool, it is a necessary component of running business. The policy should specify who is responsible for the payment of which third-party software licenses. According to a common paradigm, IT is responsible for the costs of the desktop operating system, productivity tools package, groupware and its associated server, network operating system, and maybe an ERP package. This paradigm would tie the expenses of specialized apps to the workgroup for which they are designed. This is entirely dependent on your organization's requirements.

How do you deal with the need for software?

A critical component of the policy's implementation is an easy approach for requesting third-party software for commercial purposes. In the majority of IT organizations, a phone call or a stroll down to the IT department will likely resolve the issue, but this is also how licensing may spiral out of hand. Today, IT organizations can establish standardized processes for resolving requirements for third-party software. IT can monitor the pattern of requests and track software installs for licensing purposes using tools such as a company intranet with a third-party software request form, call Centre third-party software packages, database macros, or even an e-mail form. This is critical because analyzing demands enables IT to make more informed decisions in the future when it comes to third-party software planning. When weighing the cost per seat versus the difficulty of installing it repeatedly, it may be advantageous to include a specific third-party software title on a "clone" image or as part of a common installation set.

How to develop security policies to prevent vulnerabilities while installing third-party software.

The organization will be able to develop an effective policy on installing third-party software in company PCs by considering bellow key areas:

- Make the policy apply to your organization directly.
- Encourage management to support the policy.
- Re-examine and revise the policy if necessary.

Make the policy apply to your organization directly.

Third-party software installation policies should be designed to your organization's unique circumstances and address common occurrences. A weak copy of another organization's policy will be deficient in substance and efficacy.

Encourage management to support the policy

A third-party software policy, like any other policy, will require management support to be enforced. Begin at the top by convincing the CEO or general manager that the IT third-party software policy must be implemented. Additionally, collaborate with human resources to assist improve the policy, and provide a paper copy of the policy as well as a briefing to employees as part of their orientation.

Management groups are concerned with third-party software installation policies on company PCs. The prospect of what can happen if policies are violated becomes a critical selling point for management's backing of the organization. Performance, property, and risk are the facts that consider before making a purchase to ensure proper management of a company's policy for third-party software installation. By considering above key factors organization will able to develop appropriate policies of installing third-party software on organizational computers.

One of the primary failings of many policies is allowing them to grow stale. IT is fortunate in that it can readily change and distribute policies via technology. A policy must be a living document with basic ideas that stay constant throughout its enforcement period. However, the policy for third-party software installation should be updated on a regular basis to reflect changes in the organization's environment. [6]

How to deal changes

With the changes of organizational environment, there should be specific plan to implement updates

- Make provisions and decide who will make adjustments to the policy.
- Specify a monthly reminder in your groupware product to ask if the policy requires changes or new situations.
- Mail the policy frequently to all users or post the updates on their intranet and notify users of updates.

The policy on third-party software aids the company in attaining its goal. The management of the company computer is a vital area for determining an IT group's success. Keeping company PCs in a regulated environment allows you to be more responsive to organizational changes. By adhering to these standards, organizations can avoid security vulnerabilities caused by installing third-party software on company PCs. [10]

Advantages and disadvantages of implementing security policy development on installing third party software in company PCs

Advantages

- Protection from malicious attacks on your network.
  Implementing these security policies on corporate computers protects the security of corporate resources and minimizes the risk of data leakage or loss.
- Deletion and/or guaranteeing malicious elements within a pre-existing network.
  If any malware or suspicious file is detected on an enterprise system, it can be removed immediately before entering the system.
- Prevents users from unauthorized access to the network.
  Provides security from outside and inside attacks that cover the company's computers and the entire network.
- Deny's programs from certain resources that could be infected.
  Due to the ability to deny requests to the company's computers, the entire system is systematically equipped with access privileges. In addition, the personal information and company confidential information of the employees involved in the company is obtained through the implementation of security policies using high security mechanisms for company PCs.

Disadvantages

- **Strict Regulations**
  When we considering the implementing of security policies related with installing third party software applications, each organization has different rules and regulations. After applying this security policies, employees may be disappointed and It may directly affect Employees' enthusiasm and enthusiasm for work may decrease. This can lead to problems with the productivity of the organization and retention of employees in the organization.

- **Difficult to work with for non-technical users**

  This third-party software police can indirectly reduce the time and efficiency of the organization for the people working in the company and the employees who are indirectly connected to the company.

- **Restrictive to resources**

  The above security policies related to installing third party software applications may reduce the efficiency of the company due to the time and permission available for access to valuable files and resources of certain organizations.

- **Constantly needs Patching**

  Once security policies are implemented, it is imperative that these police be updated again. If Compared to the company's profit, it can be a waste of time and money.

Conclusion

The importance of installing third party software in computers of a company is to read or modify the data within that device. These devices may contain many of the organizational confidential information and once the third-party application access to the system, the company has no mechanism to identify that does the system do with the data inside the machine. Syncing company local data to a cloud service is one major advantage of the third-party software but the company must bear the security risks of using that software.

According to the critical evaluation of the project we have identified that, there is a considerable risk to the company ICT systems from the point of purchasing the software from the suppliers as there is no way to track the negativities of the software.

Also, this software might have injected with viruses which is a nightmare to the company that destroys and interrupt the valuable information stored in the computers of the company.

Sometimes the customers are considering the security of the system as one of the second issues which might cause many negative effects to the company and some customers do not check whether a proper security system is available within the software thinking that it is definite with the system. But some security measures are not available with the package instead the customer must buy it buy paying an extra amount.

Malware software getting installed with the third-party software for the system might let hackers to hack the organizational data and they might control the company systems. Therefore, a strong security management system and policy for developing such a system is much important.

Expectation of an organization by installing a third-party application is to take its advantage and by developing an organizational policy, the company can easily manage the security risks.

As a conclusion for the case study, preparation with a strong policy when acquiring third party software will positively affect the company

Recommendations

When developing a policy for installing third party software to a computer network of a company, it must be able to balance the need of the organization with the information risk. When developing a policy, the company must consider some important points. As the first the step, the company must consider the ways of minimizing the likelihood of purchasing the insecure software applications to the computer network and as the second step the company must consider the steps to minimize the negative impact of any application.

The certainty of having an ideal application is not much practical but the company can take some preventive measures to can be taken by the organization to prevent their computer network.

As a preventive measure to reduce the likelihood of purchasing a malware to the company, the professions can conduct “allow and deny list”. [11]

There are many known malwares which can cause negative effects to the system and then the professionals can create a deny list for such applications when selecting third party software. Allow list can be created by considering the application licenses and procurement activities.

Introducing a policy for formal assessment and assurance for the applications will also help to reduce the likelihood of getting malwares as the third-party application. By undertaking a proper application assessment for the chosen list of applications the professionals can pick up the optimal application to install. The policy can be introduced to the organization by providing databases of app assessments where it includes the risk scores for relevant applications that has been undergone by the company assessment criteria. Some companies prefer a policy of up-to-date assessment of an application and the professionals of the companies using such policies must undergo an analysis of vulnerabilities occurring in the current system and the steps taken to handle the issues before moving on to install the new version of the same application. [12]

Companies using third party software can conduct a reputation assessment for the software. This method is much cost effective, and this is a risk assessment of the developer of that specific application. In here the professionals are considering the security maturity of the system developer and his historical background of the security breaches. By this mechanism the company professional can estimate the probability of the company getting affected by a security breach and can take immediate steps to avoid them.

Application store checks are another recommendation for the company to overcome the security threats arising from third party software. Majority of the application stores checks whether the application is malware before it is getting added to the store or getting updated. If a company can make a policy of acquiring third party applications through an application store, that will be a favorable measurement for the company. [13]

Installing security apps before installing a third-party software will also help the company to protect their computer network from malware.

The impact of using insecure applications can be minimized by splitting work and personal apps into different spaces. By providing a separation between the work data and personal apps by using work profiles will avoid third party applications reaching into the sensitive information of the company.

Sometimes the company must hire a third-party application for a strong business need though it is identified as risky application with many security breaches. A policy can be implemented regarding such situations to limit the applications only to the individuals who needed them, and this can be decided by using a mobile device management product. [14]

There are high privilege applications such as security products and management services and due to the privileges, the company might not much focus on the security issues. Therefore, a strong policy must introduce to check the security level of high privilege applications before installing them to the computer network.

References

[1] "Norton.com," [Online]. Available: https://us.norton.com/internetsecurity-mobile-the-risks-of-third-party-app-stores.html.

[2] "Information Security Policies," 28 10 2020. [Online]. Available: https://www.exabeam.com/information-security/information-security-policy/.

[3] "Tech Republic Tutorial," 28 03 2001. [Online]. Available: https://www.techrepublic.com/article/techrepublic-tutorial-develop-a-software-installation-policy-that-works/.

[4] "Using Third party application on devices," 21 08 2021. [Online]. Available: https://www.ncsc.gov.uk/collection/device-security-guidance/policies-and-settings/using-third-party-applications-on-devices.

[5] "Can Using Third Prty Software benefit your Company," 22 08 2021. [Online]. Available: https://www.accusoft.com/resources/blog/can-using-third-party-software-benefit-your-company/.

[6] "Develop a software installation policy that works," Tech Republic, 28 03 2001. [Online]. Available: https://www.techrepublic.com/article/techrepublic-tutorial-develop-a-software-installation-policy-that-works/.

[7] "10 Tips to Reduce Common Vulnerabilities Explioted By Cyber criminals," [Online]. Available: https://www.tylercybersecurity.com/blog/10-tips-to-reduce-common-vulnerabilities-exploited-by-cybercriminals.

[8] "Third Party Vendor Security Risk Management & Prevention," [Online]. Available: https://blog.netop.com/vendor-access-risk-management/.

[9] "Third party software providers," [Online]. Available: https://www.ncsc.gov.uk/collection/supply-chain-security/third-party-software-providers.

[10] "5 ways to protect your systems from exploits," 22 08 2021. [Online]. Available: https://www.eset.com/us/about/newsroom/corporate-blog/5-ways-to-protect-your-systems-from-exploits/ .

[11] "5 Security Tips for Using Third-Party Applications," [Online]. Available: https://www.trustwave.com/en-us/resources/blogs/trustwave-blog/5-security-tips-for-using-third-party-applications/.

[12] "How a Third-Party Compliance Policy Can Save Your Business," [Online]. Available: https://www.veracode.com/blog/2015/03/how-third-party-compliance-policy-can-save-your-business.

[13] S. Jones, "How Secure Is Your Supply Chain?," [Online]. Available: https://info.cybertecsecurity.com/how-secure-is-your-supply-chain.

[14] "“Pros and Cons of Using Third-Party Software in Your App Development,” Droids On Roids, Dec. 23, 2020," [Online]. Available: https://www.thedroidsonroids.com/blog/third-party-software-pros-and-cons#Our_recommendations_for_using_third-party_software.

Contributions

Student ID	Student Name	Contribution
IT19991290	A.D. Jaliya	Significance of the topic Critical evaluation
IT19961118	W.M.J.P. Wijesekara	Critical evaluation Abstract
IT19952376	S.A.D.H. Vishwajith	Introduction Critical evaluation
IT19961040	K.P.D.S. Madhushanka	Conclusion Recommendations
IT19014050	B.D.T.S.P. Ariyarathna	