Mitigate threats from insider

People usually focus on how to prevent attacks from outsiders. However, research showed that insider cases comprise 70% of security issues(Jouini, M., Rabai, L.B.A. and Aissa, A.B., 2014). Any system could be breached and face damage or critical data stolen due to people using it improperly or unwittingly. For example, a vital private key could be sent to an email with a misspelling or upload sensitive data to the internet. To prevent these cases, people should have a clean and consistently enforced security **policy** to guide all employees in their daily job.

Monitoring can be considered a way to approach taking against inside threats. Real-time monitoring could detect abnormal signs from inside activities and be a risk indicator (www.cisa.gov, n.d). For example, many modern monitoring tools can set the alarm to events of an uncommon data transfer outside or an intensive uploading event that happened in a short time, or the behaviour patterns don't match learning results from training data.

However, many suspected actions could be detected the first time, and to resolve these security issues, people can take the **audit** method to complete inside threat detection. Recently security flaw in the software supply chain was exposed in this way. Someone could think it may be too late to find out the problem at the time of the audit, but making an audit regular could mitigate it.

If a critical system was designed without considering internal threats, the fixing and maintenance costs could be too high for an enterprise. Initially, a **requirement** to prevent internal threats should be an ideal practice to improve the security of a system. Because in the subsequent development and testing phase, all participants could take various intent actions to achieve this target.

Access Control could be considered an essential measure to verify a system's security quality and can significantly impact threats from outsiders and insiders. Proper access control means all data/info/behaviour has been assigned an appropriate access level to each role. It reduces security breach risk to minimal but does not guarantee zero chances. On the other hand, some components without careful permission could have a growing misusing possibility as more people can get touching.

Security takes parts heavier as a quality criterion of a software system, and there could never be a zero-risk system in the world. However, if people follow a systematic security guide, they can significently gain reducing a security risk to a relatively lower level.

Reference

Jouini, M., Rabai, L.B.A. and Aissa, A.B., 2014. Classification of security threats in information systems. Procedia Computer Science, 32, pp.489-496.

www.cisa.gov. (n.d.). *Detecting and Identifying Insider Threats | CISA*. [online] Available at: https://www.cisa.gov/detecting-and-identifying-insider-threats.