**Six Ways to Combat Security Vulnerability using DevOps**

With increased requirements of quick app deployment from stakeholders, businesses now need to look into DevOps for ensuring collaboration between development and operations during development lifecycle.

A recent survey by BMC/Forbes revealed that 60 percent of executives believe their security and IT teams to have very little know-how how of the requirements of each other. In addition to that, they also have goals that do not synchronize with each other. This is a complication that results in businesses taking months to fix security vulnerabilities, and in the process face a number of potential security breaches.

Following are some tips that can help businesses secure their app development lifecycle against security vulnerabilities:

1. **Standardize on a DevOps Platform**

To minimize risks associated with security vulnerabilities, the starting point is to standardize on a DevOps Platform, as it serves an important role in defense against data breach regardless of your app development being in-house or being done by third-party developers.

With a standardized DevOps platform you can practice good developer hygiene, ensuring that only authorized individuals can make changes in source code. It also enables a check and balance for developers, project managers and stakeholders and provides one security path for everyone.

1. **Role of Project Managers and Stakeholders**

Apart from their regular job roles, stakeholders and project managers of a development team have additional responsibilities to ensure security during the app development process. They also need to ensure the placement of all modules needed by developers and ensure that data is locally encrypted on the device.

Project managers and stakeholders also need to audit all tools and assets currently in use, define protocol settings, provide training to developers for practicing check-in, check-out and administrator practices, review code repository location and ensure that end-to-end process flow should be in place.

1. **Standardize Authentication Methods**

App functionality and security go hand in hand but security should not come as a barrier in providing a great user experience. The good news is that mobile devices now offer strong authentication in addition to basic password setting features such as biometrics data, enabling users to maintain strong security.

1. **Develop pre-built Modules for Developers**

This is another best practice to ensure protection against security vulnerabilities. Pre-built modules are optimized and consist of the best possible code. Instead of developing code from the scratch, developers can make use of pre-built modules and then put them in place together according to their requirements.

1. **Implement Security in your Versioning Control**

Security needs to be a part of your versioning control. The DevOps platform should provide security controls and label security issues according to:

* Severity 1
* Severity 2
* Severity 3
* By SLA

1. **Create an Enterprise App Store**

Mobile Application Management (MAM), which is a part of Enterprise Mobility Management (EMM) solution, allows you to push all updates in apps to corporate devices and BYOD devices registered on your organization’s network. This also enables your DevOps platform to notify all users registered on the network about a severity 2 or 3 issue and download app updates in case of severity 1 issue.

As businesses enter the next digital era, developing and implementing a security application development lifecycle will become a necessity. Developing a framework will ease implementation and also organize security updates, fix vulnerabilities and provide collaboration across DevOps teams.