ZIMPERIUM®

Where's the Sec in Mobile DevOps?

Mobile applications are becoming an indispensable platform for organizations, but if left unchecked they can provide an easy attack surface for malicious actors. What steps can businesses take to ensure they don't end up in the headlines?

Rela8 recently hosted roundtables, sponsored by Zimperium, that brought together a group of cloud architects, IT, software engineering, information security, intellectual property, and process & innovation professionals to take a deeper look at:

- Considering a mobile app as a digital platform
- "Baking security" into Mobile DevOps
- Why security should be a top priority at the initial app development phase
- The digital shifts in mobile app security during the last five years

Rela8 Group's Technology Leaders Club roundtables are held under the Chatham House Rule. Names, organizations, and some anecdotes have been withheld to protect privacy.

Mobile security: apps vs devices

One of the biggest challenges culturally, is that organizations don't understand mobile. They don't understand what is different about mobile platforms, or mobile apps. So organizations have to be educated about what makes mobile different from traditional software and platforms.

There are two definite areas of security risk in mobile technology: devices and apps, and there are obstacles to building security into both. For example, security can affect the performance of an app, making it slow and cumbersome. In some cases, that means security teams have become enablers, allowing security issues to continue so an app can function at maximum capacity, providing the best possible customer experience.

Additionally, companies cannot protect any device that their app is uploaded to, so many are now taking the approach that there has to be a certain standard of security on the device before their app can be accessed.

While apps used inside a company often have a high level of security, consumer apps are another story. Customers don't care about business security requirements. They care about their experience and new releases. This is where automation can help with both speed and security – developers commit codes during the day and tests run throughout the night in test environments. The next day when the developers return, they see the results and that an automatic bug ticket has been activated. In this way, a new commit is done, the bug is fixed, and another test run commenced.

Mobile apps are not traditional software

The traditional software development model has, for the most part, taken place in the safety of an organization. New code is written and run behind the shelter of an organization's firewalls. Mobile apps, however, are different. They're running on end-user devices, which means security has to be part of the development process, something that doesn't always happen.

When building mobile apps, developers are effectively clicking together building bricks, often without realizing what risks they are bringing into the app with them.

Once that app is in a public app store, threat actors have all the time in the world to reverse engineer the app, clone it, or build something bad into it. Apps could end up running in a hostile environment on devices that are never updated or connected to bad wifi networks.

Organizations need to look closely at how they can minimize the friction between development deadlines and security requirements, with tighter controls from the beginning of the mobile development phase. This can be achieved by utilizing the best practices in app security and learning from the experiences of other professionals, by looking at how they overcame their own mobile app security challenges.

DevSecOps: Balancing development and security

When companies want to produce a mobile app quickly and add in a security element, costs can escalate and the timeframe can elongate. But if organizations do not follow at least the minimum-security requirements, they can find themselves in a dire position. For example, manufacturing may grind to a halt because of a breach in an app. The company may have tried to save a few thousand dollars on security when developing the app, but now the breach may end up costing millions of dollars to fix.

If security isn't built into the development process, problems can be built into an app instead. This is why it's critical to have a DevSecOps mindset; security should be part of the process right at the beginning of development — not at the end when fixing problems will cost more and take longer.

Unfortunately, many organizations struggle when it comes to getting security buy-in for business requirements at an early stage. Quite often apps are built by developers around their perception of what security should look like, not by people with a security mindset. Security should be baked into DevOps from the very start of the process when the company is creating business requirements for the project. This will ensure that the business doesn't run away with just delivering something quickly without a security mindset.

All development teams should include a security expert who can help define requirements, assess risk for the entire project, and analyze risk at every stage of development. The security expert should also know how to work with automated CI/CD pipelines to remove manual errors and provide standardized feedback loops to developers. A team's security expert should essentially be able to advise on security as the product is being built.

In other words, security should be a guide dog for the development process, not a guard dog.

How DevSecOps will benefit mobile apps in the future

Companies want to get a mobile app to market as quickly as possible, but they also don't want to pay millions of dollars to fix a security breach on a mobile app.

Moving forward, accountability must be built into the product. As part of this, security architecture must move beyond the pen test; getting baked into the process from the very beginning.

Yes, there is a cost for security, but businesses need to recognize that there is also a security cost if an app's launch is delayed. There is a cost if the speed of development is compromised, and of course, there is a much greater cost to fix a security problem after launch.

Applying a product mindset to new app development with a product team, including a security person, ensures security is part of the process and any problems along the way are solved by the product team and security in unison.

About Zimperium

The Zimperium Mobile Application Protection Suite (MAPS) is the only solution with centralized real-time visibility and on-device response actions, unifying app development, and run-time security. MAPS continuously assess vulnerabilities, secures keys, protects IP, and provides threat visibility with on-device machine learning.

To learn more about protecting your mobile apps, contact us and talk to one of our security experts.