Is Your Rapidly Deployed Mobile Application Secure?

Social and business interaction is dramatically changing. Service-based organisations will need to find a way of operating and keeping employees and customers at a safe distance. Mobile applications will play a big part in this but security must not be lost in favour of functionality, rushed development, or inadequate security processes.

The need for social distancing has seen organisations rapidly extend their corporate network and resources into the homes of virtually every employee. The speed and resourcefulness of IT teams across the globe have been breath-taking. As we gaze into the post lockdown future, that same resourceful, rapid approach will likely be sought by software development teams to create mobile device apps that reduce direct interaction between employees and customers.

Mobile apps are already being used in the service sector. Self-service in restaurants and mobile payments reduce queues at busy till points and improve wait times. This trend is only going to rise and hackers are keen to exploit any vulnerabilities in a rushed mobile app that hasn't met strong mobile application security principles.

When exploited, corporate mobile apps can expose personal, financial and corporate information. They can even provide an entry point into your organisations network and resources.

Attackers are persistent and creative but they needn't win the battle. Mitigating your risk and being one step ahead can produce overall company welfare amidst the current Coronavirus chaos.

In an understandable rush to deploy mobile apps; essential security principles are often missed or skipped in favour of early release times. Without adequate training, functionality can be prioritised over security. Regardless of the reason, mobile apps that don't follow strong development and release principles can compromise your organisation and hinder your business objectives.

How can you recognise whether your organisation is following secure application development practices? Your answers to the below can provide an early indication:

- Does your application development project start with a defined plan that stipulates the use of secure development practices from the design stage through to release and deployment?
- Is your software development team or development partner trained in secure coding techniques?
- Are code quality and security assessments undertaken by experienced and impartial

testers at the various stages of application development?

- Do development teams follow strict development protocols including regular code reviews?

Are code or deployments provided by third-parties tested for vulnerabilities?

The key to protecting your mobile application lies in out-manoeuvring hackers by understanding and preventing avoidable risk from the outset.

About Cortida

Cortida is the home of information and cybersecurity risk management. We favour ‘appropriate’ security measures over their costly, convoluted alternatives. Learning and understanding your business, its objectives and your attitudes and appetite for risk mean that we can better protect them. We measure how data supports or threatens your objectives and dismiss any unnecessary and costly audits of your security. Our focus is reliability, technical expertise, a personable partnership approach and delivering tangible value to your organisation. This allows us to identify, understand, reduce and manage your security risk.

The Cortida partnership approach:

- Establishes an understanding of your organisation’s objectives and attitudes towards risk
- Assesses your organisations data to determine its importance and value and need for protection
- Includes a reasoned assessment of the risk, based on probability and likelihood of loss or incident
- Formally identifies an appropriate security benchmark along with any gaps between the in-place measures and the target
- Provides a clear understanding of what needs to be done and in what priority

To arrange an application security assessment for your mobile application, please get in touch :

info@cortida.com