The rapid growth of smartphones is seeing mobile applications become a prime target for hackers. At the same time, breaches are now even easier to perpetrate because cyber criminals no longer work manually: they use huge networks of 'bots' that can attack automatically.

The popular mobile operating system Android is the biggest target, but hackers are also finding ways of penetrating the more 'closed' platforms.

This was evident in September this year when Apple - which has always administered stringent checks and guidelines - saw hundreds of legitimate apps in its App Store infected with malicious code.

Increasing threats

Human error is the weakest link when it comes to security. In a business, any mistake made by employees can cause a threat. People can easily download infected applications without checking they are secure - and the results can be catastrophic.

Third party plug-ins and extensions are particularly risky, including payment systems and those that integrate with social networks including Facebook. Another error made by employees is the use of insecure passwords or sometimes, not having a password at all. It is not uncommon to see an employee type '123' or 'password' to access their mobile devices - and this opens a backdoor to your corporate systems.

Adding to the complexity, the advent of 'bring your own device' (BYOD) poses a big security risk for businesses. Allowing employees to bring their own devices to work can cut the cost of hardware, but a lost smartphone can also potentially expose your company data to criminals.

Further to BYOD, employees are also bringing their own apps into work under the trend known as 'bring your own app' (BYOA). This is seeing users find their own ways of increasing efficiency, rather than

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

relying on approved corporate software. If left uncontrolled, it is a major risk, often leading to the downloading of malicious apps or software.

Vulnerable operating systems

Some mobile operating systems (OSs) are more vulnerable than others. While Apple's iOS is generally thought to be secure, the Android system is much more vulnerable.

The risk centres on around the fact that the OS is Linux based, and its architecture is well known. Android is also said to be fairly 'open', allowing attackers to easily load malicious apps onto Google Play. This is almost impossible via Apple's App Store.(Need to be explained why)

Add to this the huge number of Android handsets in the market - according to IDC figures, the OS had an 83% share of the 341.5 million smartphones globally in quarter two 2015 - and it's no surprise it is the operating system most frequently targeted by hackers.

So which businesses are most at risk of attack? The more customers and personal, or sensitive data you hold, the more interested hackers will be. It is therefore important that large companies employ a specialist team to oversee cyber security. Firms should also make sure they are audited by an external company. Within this, organisations must examine the security of their mobile apps plus software and applications. This should be done regularly: if left unchecked, viruses can grow - and new ones are always being developed.

A secure strategy

Security is usually not the first thing taken into consideration when developing an app. But this must change: as a growing number of firms are realising, no one is unhackable.

When building an app, it's important to follow the best practice recommendations on how to handle potential problems, taking into account elements such as encryption and passwords.

When managing mobiles in the workplace, mobile device management capabilities are also useful. This includes the ability to switch off, or wipe a mobile phone if it gets into the wrong hands.

However, security often only becomes an issue once the mobile app is in use. This can be managed accordingly by continuing to audit even after the app has launched within the business.

Security must be built in at the start of app development. This is why Magora Systems undertakes a security audit from an app's inception: we make this a priority when choosing our suppliers, extensions, and APIs. Quality assurance should include security - and this must be applied to the code itself, as well as the functionality.

Top tips for mobile app security

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk

- Ask the right questions: You have to be able to rely on and trust your supplier. The only way to ensure they are right for you is to ask questions. When developing your mobile app, it's integral that you ask the company how it is managing your security. Don't ask the sales people: questions should be directed at project managers and developers.
- Estimate your own risk first: The first thing a business should consider is: how attractive is my intellectual property (IP) to criminals? If you hold sensitive data such as bank account or credit card details, your business is at a high risk of attack. If your data is attractive, you should also consider how much damage would be done if there was an attack. Taking this into account, you must calculate how much you are prepared to invest to ensure this does not happen. The cost of a breach can be huge; it's worthwhile making the investment to stay secure.
- Understand your data landscape: Security is about understanding your data. This includes being aware of how many data transactions of any kind are used in applications - and which systems are involved. This could go beyond the system: a partner, data centre or other third party can also make you vulnerable to attack. This is why Magora Systems chooses its suppliers carefully. Once companies understand their data, they can then identify their potential points of vulnerability. It's important to note that you cannot eliminate attacks - but you can minimise the chance of a breach. Part of this should include minimising data transfer between systems and within your business and core systems. Critical data should be in a proven place - both physically and logically.
- Watch what you install: Take care with what you install on your phone, tablet or system. Stay aware of non-approved and non-secure sites. Watch your step - and remember to monitor your employees.

+44 20 7183 5820

info@magora.co.uk
sales@magora.co.uk