SC MAGAZINE
SECURE BUSINESS INTELLIGENCE

CISO's GUIDE TO MOBILE SECURITY

"A white paper that outlines the latest mobile security issues facing enterprises and highlights best practice on balancing employee freedom to "bring your own device" (BYOD) with measures that protect mobile devices, apps and access from a rising tide of threats"

Sponsored exclusively by:

IBM

The explosion in use of smart mobile devices brings with it unparalleled opportunities, but also enormous enterprise risk. It is difficult enough to secure corporate resources when they are in the building, or at least on the company grounds. But what does a CISO do when suddenly the devices, data and applications go walkabout?

A forecast from ABI Research predicts that the number of employees using smartphones will increase at a rate of 17% a year, reaching 2.4bn employees in five years.

More employees than ever are using their personal phones and tablets for work, but the trend is putting pressure on corporate IT departments to extend bring-your-own device (BYOD) policies and highlighting issues of mobile security.

BYOD users will more than double by 2014, when 350 million employees will use their own mobile devices, reckons Juniper Research.

Current threats are familiar foes, such as spam, malware and phishing. According to a recent report by a leading vendor, 13,000 types of mobile malware have already been uncovered in 2012, a huge increase on the 2,000 discovered last year.

But mobile phones are also much more susceptible than laptops to theft and loss – a security firm recently reported that 35% of users had either misplaced their mobile device or had it stolen - and could be prey to criminal hackers seeking to target confidential data, interrupt core services or commit financial data fraud, thanks to smartphones' emerging use as payment methods.

Balancing threats with opportunities

The possibility of these kinds of threats is motivating information security chiefs to pause and consider how they might balance security with the productivity of mobile devices. Yet less than a quarter have policies to control it, according to software firm LANDesk. Of the 200 IT professionals it surveyed, only 23% had policies in place to govern the use of mobile phones or tablets and only 25% expressed confidence they could stop viruses transferring from the personal products to the corporate environment.

Each operating system - from Android and iOS to BlackBerry and Windows – presents its own set of security challenges. Vulnerabilities can be exploited in mobile apps and mobile browsers, as well as via insecure Bluetooth and WiFi hotspot usage, to spread mobile rootkits, mobile worms, mobile botnets and mutating malware that avoid mobile anti-virus detection.

And yet many employees remain ignorant of the security risks associated with mobile devices – oblivious that much of their organisation's intellectual property and data assets are sitting on their smartphone or tablet.

The trick for CISOs and their IT departments is to allow employees to work as efficiently as possible while protecting corporate assets, sensitive data, competitive IP and client contacts. Auditing and compliance regulations are just as applicable to smartphones and tablets as they are to laptops and desktop PCs.

Mobile security is about protecting an organisation's evolution into a mobile enterprise. And a comprehensive mobile security strategy will address three key issues: mobile device security, mobile app security and mobile access security.

New types of devices are entering the corporate environment and enterprises are recognising that they have little to no visibility over these new devices. These devices are being employed to connect to corporate resources and storing proprietary data. The sheer number of devices, their form factors and their usage patterns make them susceptible to being lost or stolen. These inherently consumer devices if infected with malware can become a source of threat to the enterprise network.

Organisations therefore must look to gain awareness of these devices and how their composition may influence the risk to the enterprise. A Mobile Device Management (MDM) solution is a logical starting point providing to define and enforce security policies such as encryption policies. It provides control to lock or selectively wipe data on lost, stolen or decommissioned devices. In addition it provides the infrastructure to deliver higher level security capabilities – anti-malware and device updates. Important considerations in choosing an MDM solution include mitigating costs to manage all the new endpoints and minimising specialised skills required to manage new devices.

Next, it should be noted that user experience on mobile devices increasingly centers around mobile apps. The threat vectors that affect mobile apps include extracting data they store, using them to funnel malware back into corporate systems, stealing personal information and hijacking identities. Now users may unintentionally download malicious apps that masquerade as innocuous apps or they may be using legitimate apps with inherent vulnerabilities that may go rogue with malicious code or data injection.

Incorporating security into mobile apps is most cost-effective when done during development and test phases. Instead of trying to counter every new type of exploit targeting mobile apps, organisations should focus on identifying and removing vulnerabilities through vulnerability testing. Employing a mobile application platform can help an organisation standardise its coding practices and provide developers better support to include security best practices in the app development process. When selecting technologies attention should be paid to the vendor's research into mobile vulnerabilities so the testing tools they deliver reduces the number of false positives making development more efficient and training future coding behaviors.

Regardless of whether or not an organisation begins with device security or app security, mobile access security is a prerequisite. Majority of business related apps will connect to back-end services or resources. And no matter how much data is stored on the device there will be much more information a device or app is enabled to access. In the mobile context the risk of an access attempt is governed my many fluctuating variables – location, network, time, device attributes among others. This risk can significantly impact not only the user experience but also the viability of the overall mobile solution. In addition, users may want to engage with multiple entities securely at any given point in time.

Enterprises should look to centrally manage users through a robust policy based mechanism. This would simplify app development and allow administrators to account for fluctuating risk given the dynamic nature of mobile use. The risk of an access attempt can influence the choice of the authentication scheme or even the features an app enables for a specific interaction. When evaluating secure connection technologies opt for ones that enable app-level VPN rather than just device-level VPN to allow for multitasking on the devices and prevent traffic piggybacking on secure interactions.

Given that organisations may have different starting points in building out their mobile security postures some crucial questions need to be answered. Can we demonstrate compliance? How do we

know we have coverage? How do we become proactive in reducing response time? This points to the need for mobile security intelligence. Additionally, given that the evolving threat landscape is seeing an emergence of more targeted attacks, mobile security intelligence plays a key role in aggregating security events from the device, apps, network and users to help showcase compliance, perform risk assessments and detect new threats.

Fresh mobile innovations and security challenges will continue to arise daily. However an integrated approach to addressing these three issues would give CISOs and their IT departments much greater visibility and control. A holistic mobile security intelligence solution can free up organisations to explore and pursue new business opportunities without risking trust relationships with employees, partners and clients.