NXTKey

# White Paper on

# Mobile Application &Device Cyber Security Services

PROACTIVE SECURITY
CYBER MANAGEMENT SERVICES
SECURITY OPERATIONS CENTER (SOC)
SECURITY ARCHITECTURE & ENGINEERING

www.nxtkey.com

With more people using mobile devices every day for both business and personal use, hackers have numerous avenues available for "breaking into" them. In fact today, with the proper equipment - which incidentally is not at all expensive for hackers to purchase - cyber criminals are able to gain access to nearly any device within mere seconds.

In doing so, hackers can either mirror the device in order to see all of the information on it, and / or install malware, which will enable the criminal to essentially siphon data from the device - oftentimes without being detected for days, weeks, or possibly even months (or longer).

**5 Key Security Risks of Mobile Devices**

The threat and attack vectors with regard to mobile devices are primarily made up of retargeted versions of attacks that are aimed at other endpoint devices. With that in mind, such risks can be categorized into the following areas:

1) Malicious Code - Just like with PC users, mobile devices can also be at risk of malware threats. For example, mobile malware Trojans are designed for stealing data, and are able to operate over a mobile phone network, as well as any connected Wi-Fi network.

Oftentimes, these Trojans are sent through text messages, whereby if the user clicks on a link within the message, the malware is delivered by way of an application. Mobile malware is also increasingly being delivered via "malvertising," a concept where the victim is enticed to click on an advertising link on social media sites such as Facebook.

2) Targeted Attacks - Attacks that are targeted at a mobile device itself are also a key threat. Here, the attack itself is similar to attacks on PCs, where it is designed for either gaining control of the mobile device and accessing data, and / or attempting a DDoS (distributed denial of service).

3) Intercepted Communication - Just as a laptop user is susceptible to Wi-Fi related attacks, so are the users of mobile devices. Today, the technology that is used for hacking into wireless networks is widely available - and much of it is easily accessible online. This can make both Wi-Fi hacking, as well as MITM (man in the middle) attacks, easy for a cyber criminal to perform.

Likewise, hackers can also easily intercept and decrypt cellular data transmission, in turn exploiting weakness in Wi-Fi and / or cellular data protocols. In doing so, criminals are better able to hijack users' sessions for online services - including web-based email - as well as to eavesdrop on the transmission of data.

4) Threats from Business Insiders - In business situations, mobile devices may also be used in facilitating threats from employees, contractors, and other company "insiders." For instance,

the misuse of personal cloud services via mobile applications is one key issue, as is the downloading of applications by unsuspecting employees.

5) Physical Access - While mobile devices such as smart phones and tablets are small, compact, and therefore easy to take nearly anywhere, their smaller size can also make these devices much easier for hackers to steal and / or for their owners to unintentionally leave behind in a public place. In either case, losing physical access to one's mobile device can put personal and sensitive information at risk.

This, too, doesn't just pertain to personal mobile devices. In fact, due in large part to the growing prevalence of bring your own device (or BYOD) in the business world, the wide range of devices that contain sensitive data that relates to both individuals and companies can provide a wide array of tempting targets for cyber criminals.

In fact, adopting mobile devices without first taking into consideration the necessary policies, and / or without putting the proper management infrastructure in place, can easily increase the opportunity for hackers to breach important data.

For example, once a hacker has possession of such a mobile device, circumventing a lock or password can be a trivial task for a seasoned cyber criminal. And, while mobile device owners may think that they are able to remove sensitive data and protect themselves through a factory reset on the device, the reality is that full removal of data is actually not possible via a reset, or even by re-flashing the device's operating system.

Further, forensic data retrieval software (which is fairly easy to attain by criminals) can allow data recovery by the hacker - even from devices that have had such information deleted manually and / or have undergone a reset.

Given all of these (and other) mobile device threats, what is the most appropriate approach for the assessment of such key risks, as well as to reducing - or even eliminating - certain vulnerabilities?

One way that businesses and organizations can ensure more secure mobile solutions - particularly with regard to an expanding BYOD workforce - is via mobile device management software.

**Mobile Cyber Security and Device Management**

Mobile device management (or MDM) refers to a type of security software that is used by IT departments in order to monitor, manage, and secure mobile devices - typically those of a company's employees - that are deployed across multiple mobile service providers, as well as across multiple mobile operating systems, that are being used in an organization. (Note that MDM can also refer to master data management).

Most of today's MDM solutions provide entities with end-to-end security, which means that mobile apps, network and data that is used by the mobile device (in addition to the mobile device itself) are managed by the organization's IT department with a single mobile device software product.

With some enterprise MDM solutions, both the mobile security and the expense management functions will be combined in just one single product. However, based on the particular vendor, as well as the specific features that it supports, most MDM software will contain some, or even all, of the following features:

- Management and support of mobile applications
- Mobile policy management
- Inventory management
- Security management
- Telecom service management

**Tools Utilized with Device Cyber Security Services**

In response to the growing threat of hackers and mobile devices, a new market segment has emerged within the cyber security field which involves detecting and mitigating attacks via the scanning of risky apps and vulnerable Wi-Fi networks. Just some of the tools that are being used to deter such threats include the following:

*Lookout*

Lookout provides mobile security, identity protection, data backup, and theft prevention in just one, single application. This tool helps to prevent smart phones and other mobile devices against threats such as malware, adware, and phishing - before they can do harm.

In addition, the Lookout tool also provides timely alerts on corporate data breaches that could affect a company or business owner. Likewise, this tool offers access to ID restoration experts 24/7, should a user's identity be compromised. And, users also have access to identity theft insurance coverage of up to $1 million to help with offsetting the costs of restoring and / or recovering their identity.

The security alerts that users have access to via Lookout include more in-depth information than many of the other security platforms that are presently available. For instance, these alerts provide highly relevant details regarding a potential threat at hand, such as the app name, the app version, the app icon, the amount of time that has elapsed since the user initially encountered the threat, and suggested remediation action(s). Plus, Lookout provides tools that can help with finding a lost or stolen device, which include email alerts with a photo and map if a thief attempts to steal it.

*MaaS360*

Another tool, MaaS360 (also known as Mobile as a Service 360), is a SaaS (Software as a Service) product that is offered through IBM. With the rapid rise of BYOD, all companies and organizations have a need to both see and control the mobile devices that are entering the business environment - regardless of whether these devices are provided by the business itself or are brought in by the employee or contractor. Using the MaaS360 mobile device management system, companies can accomplish this quickly and comprehensively.

MaaS360 allows for the management of BYOD (Bring Your Own Device), as well as enterprise-issued devices, that include smart phones, tablets, and even laptop computers. Among other things, MaaS360 can maintain catalogs of native mobile apps, and can manage the distribution of those apps to devices.

Additionally, MaaS360 simplifies MDM (Mobile Device Management) with rapid deployment, as well as comprehensive visibility and control that spans across mobile devices, applications, and documents.

MaaS360 also allows for ease of integration between the enterprise systems and mobile devices. One way it does so it by leveraging existing Active Directory / LDAP and Certificate Authorities.

It also provides a unified console for smart phones and tablets, with centralized policy and control across multiple platforms. For instance, with MaaS360, users can securely share and update content and documents, as well as configure contacts, calendar, email, Wi-Fi, and VPN profiles over the air.

Plus, if there are any issues that arise, MaaS360 can also help to streamline mobile device management support - starting with diagnosing and resolving user, app, and / or device issues in real time.

For example, locating a lost or stolen device can be made much easier, as can resetting forgotten pass codes. Device views may also be used for the diagnosis and resolving of such issues.

Presently, MaaS360 supports all mobile devices, including the iPhone and iPad, Android, Windows Phone, Blackberry, and the Kindle Fire.

**Keeping Up with Mobile Application and Device Cyber Security Requirements**

Due to the substantial increase in popularity of tablets, smart phones, and other mobile devices, the IT environment has changed drastically over the past few years - and it is likely to continue moving forward, with cyber criminals at every turn.

Due in large part to the fact that security controls have, for the most part, not kept pace with the potential security risks that may be faced, ensuring that entity-owned and employee / contractor-owned mobile devices are secure is essential.

In doing so, it is important that security is supported throughout the entire mobile device life cycle so that risk to the user - as well as to the other individuals and businesses that are networked with each user - is reduced, in turn, allowing those who are associated with the organization or entity access to needed data from nearly any location (and over any network) without taking on additional risk.

About the Author:

Shivaji Sengupta is a seasoned business management and solutions development entrepreneur who has over 24 years of experience providing solutions to customers across 17+ countries in the areas of cyber security, enterprise information management, content management and information technology.

Mr. Sengupta's company NXTKey Corporation provides cyber security solutions to key federal government agencies supporting them in maintaining their cyber defensive posture. Mr. Sengupta is also an Adjunct Professor for Cyber Security at Delaware State University. He has designed and is teaching the Applied Cyber Security Course at DSU.

About the Company:

NXTKey Corporation is an agile Small Business that places emphasis on teamwork and partnership with our clients to produce optimum contract performance. We have refined our solution from experience supporting highly complex Department of Justice (DOJ) environments such as United States Marshals Service (USMS), Justice Management Division (JMD), Office of Justice Programs (OJP) and Federal Prison Industries (FPI).

Our depth of experience allows us to provide IT security support for a wide range of IT General Support Systems (GSS) and major applications (MAs) within the Federal Enterprise and following the guidance in the Federal Enterprise Architecture (FEA) and information systems security support services in accordance with OMB Circular A-130, NIST guidelines and standards, as well as other federal policies and regulations.

We specialize in providing our clients a full range of security services specifically tailored to their requirements. These services include: Certification & Accreditation, Security Architecture, Mobile Security and Governance, Risk Analysis and Assessments, Security Policy and Processes, System Auditing, Security Control Assessment, Disaster Recovery Planning, Contingency Planning, Vulnerability Assessment, Penetration Testing, Physical Security Survey, Information Systems Security Training and Security Program Management.

More information on our website at https://www.nxtkey.com