Mobile Security – Beware or Be Sorry

Smartphones, Tablets and Other Mobile Devices May be at Risk

It's time for a reality check. The first step to mitigating the threat that mobile security poses for businesses is to understand the situation. Unfortunately, the picture is rather bleak. Here are some recent facts and statistics from Ponemon Institute, an IT security research firm, and McAfee:

- 76% of respondents who use mobile devices in the workplace say that they believe these devices introduce serious security risks.
- Only 39% say they have mitigating security controls in place, even though they are aware of the risks.
- 59% say they have seen an increase in malware infections over the past 12 months due to insecure smartphones, tablets and other mobile devices. Almost a third of them said the increase was over 50%.
- Google Android OS is most at risk, with malware volume of 63%. Apple was best, not even making the list.
- 51% of organizations experienced data breaches due to insecure devices, which may be low, since 23% are unsure if a breach occurred.
- 38% reported theft or loss of information or other resources. 31% experienced disclosure of confidential information. 10% experienced interruption of service.
- 55% said that their organizations don't have a policy that states the acceptable use mobile devices. Of the 45% that do have a policy, less than half said it is enforced.
- 49% of organizations require device-level security settings, but only 6% of them said their employees are compliant. 15% were unsure.
- 59% of organizations said their employees disengage security features like key locks and passwords.

It's not a pretty picture, but it is important to remember that mobile security is an issue that has not yet received adequate attention in the industry. There are steps to be taken that can greatly reduce the threat.

TOP THREATS

Following are some of the biggest concerns:

- Drive-by exploits – the injection of malicious code by the HTML of websites that exploit vulnerabilities in web browsers
- Worms/Trojans – malware that hides in the device and spreads to others
- Code Injection – designed to steal credentials such as logins
- Exploit Kits – a streamlined methodology of distributing malware
- Botnets – malware that runs automatically once installed

GRUDI ASSOCIATES
Innovative Solutions
Simplified Telecommunications

1044 East Main Street, P.O. Box 626,Palmyra, PA 17078 ▪ Office: 717.838.5022 ▪ Fax: 717.838.5086
www.grudiassociates.com

- Denial of Service – creates a flood of traffic so legitimate traffic cannot be processed
- Phishing – fraudulently obtain financial or other information by impersonating a legitimate organization
- Compromising Confidential Information
- Rogueware/Scareware – designed to force users to pay for fake anti-virus or other software
- Spam – many spam messages have corrupted links and attachments
- Targeted Attacks
- Physical Theft/Loss/Damage
- Identity Theft
- Abuse of Information Leakage
- Search Engine Poisoning – manipulate search engines to display search results that contain references to malware-delivering websites
- Rogue Certificates – enables malicious users to impersonate any Web site
- Jailbreaking – a hack allowing access to phone/tablet file system/root directory
- Bluesnarfing – the theft of information from a wireless device through an unsecured Bluetooth connection (mostly older devices, newer ones are not as vulnerable)
- Data Exposure – unsecured devices and pathways (DropBox)
- Open WiFi Networks – those not requiring password entry leave users totally vulnerable

BYOD

BYOD stands for Bring Your Own Device (to work). It is the growing practice of businesses allowing – or requiring in some cases – employees to use their own smartphones, tablets and other mobile devices. While BYOD in itself does not directly do harm, it can create a significant security risk by exposing the organization to the threats outlined above and other concerns. Read more in Grudi Associates' article: BYOD ASAP? Not So Fast.

SYMPTOMS

Most people, including many in the telecom industry, are unaware of the magnitude and significance of these threats to mobile devices. One reason is because they are not familiar with the symptoms. They often attribute the effects of malware to other issues by mistake. Watch for these key symptoms:

- Slow device response
- Programs running in the background – in most devices, this is indicated somewhere in the settings menu under apps, usage or similar locations
- Pop-Ups & unwanted notifications
- New apps appearing that were not knowingly downloaded

- Web sessions abruptly disconnected
- Unusual battery drainage
- GPS or Bluetooth usage not initiated by the user
- Unauthorized phone bill or credit card charges
- Applications using large amounts of memory storage or RAM

PRECAUTIONS & FIXES

Businesses should take threats to mobile devices as seriously as they do to their other IT and communication systems. The dramatic increases in mobile data capabilities that are providing many benefits are also creating a high-risk entry point into enterprise networks and data sources for hackers and data criminals. Following are some specific actions that can be taken to help mitigate that risk:

- Device-level encryption
- End-point security solutions – protection for file servers, desktops, laptops, and mobile devices
- Identity and Access Management (IAM) solutions
- Device locking and control requirements
- Anti-virus and Anti-malware – following are several currently available options:
  - Android
    - Verizon Mobile Security (Info & FAQ)
    - Kapersky Mobile Security
    - AVG! Mobile Security Antivirus
    - NetQin Mobile Security
    - Lookout Mobile Security
    - McAfee Antivirus
    - Eset Mobile Security
    - Zoner Antivirus
    - Bitdefender Mobile Security
  - Blackberry
    - Junos Pulse
    - NetQin Antivirus
    - Lookout Mobile Security
    - SMobile VirusGuard
    - BullGuard
  - Apple
    - Lookout Mobile Security
    - Trend Micro Mobile Security
    - Inego VirusBarrier
    - McAfee WaveSecure Antivirus
    - GadgetTrak Antivirus

Some specific things every user can do are:

- Immediately report a lost or stolen device to the carrier and suspend their operation.
- Set a password or pattern screen lock – before selecting facial recognition options be aware of the limitations and issues.
- Download a security application that can track the device location, photograph a user who enters an incorrect password, sound an alarm, lock the device and more.
- Ensure that any computer the device synch to is also malware-free – you can infect your own phone or tablet.
- Never transfer personal or sensitive information on public or unsecured WiFi networks.
- Request that corporate IT sets the server to require a password for email access.

IT and executive leadership should consider putting the following in place:

- Create a comprehensive mobiles devices security policy and plan.
- Strictly implement an enforcement policy.
- Leverage mobile device management solutions.
- Implement security access controls.
- Utilize cloud-based services for better access control and security.

Addressing all of these initiatives can be a complex and daunting task for businesses that do not have adequate in-house resources and expertise.

Enlisting the help of telecom and IT professionals can produce better results.

SUMMARY

If the statistics listed at the beginning of this article are alarming, they should be. Businesses without adequate mobile device security systems in place are exposed to an insidious menu of malware and criminal activities. Take action now, because hackers are on the move.