Smart Phone Security

Large threats comes in small packages

AISA National Conference 2010
Sydney, Australia

30 Nov 2010

Compliance, Protection & Business Confidence

Sense of Security Pty Ltd

Sydney
Level 8, 66 King Street
Sydney NSW 2000
Australia

Melbourne
Level 8, 350 Collins Street
Melbourne VIC 3000
Australia

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455

info@senseofsecurity.com.au
www.senseofsecurity.com.au
ABN: 14 098 237 908

Agenda

What are the topics we intend to discuss today?

- Introduction
- Overview of iPhone Security
- Jailbreaking the iPhone
- Other Security Concerns
- Demonstration
- Governance
- Conclusions

Introduction

Why are we discussing smart phone security?

- Push for mobile devices by staff
- Business opportunity or iFad
- Cultural changes to the workplace
- BYOD (Bring Your Own Device)
- Focus on the Apple iPhone

Overview of iPhone Security

What security mechanisms has Apple implemented?

- KISS Principle
- Application sandboxing
- Hardware encryption
- Segregation and levels of security
- Inherent issues

Jailbreaking the iPhone

Who? What? When? Where? Why?

- iOS (formerly iPhone OS)
- What is jailbreaking?
- Why do people do it?
- How is it done?
- What's the problem with that?

Other Security Concerns

What other security concerns should be considered?

- Reliance on iTunes
- Application and URL black-listing or white-listing
- Security controlled by a third-party
- Corporate applications

Demonstration

A real world example of a possible attack scenario

Please see the following URL for video recordings of the demonstration that was given during this presentation:

http://www.senseofsecurity.com.au/previous-webinars/smart-phone-security

Governance

What can be done to manage the risk?

- Policies, procedures and standards
- Mobile device management solutions
  - Deploy profiles, configurations and applications over-the-air to devices
  - Implement application white-listing
  - Detect jailbroken devices and trigger precautionary actions
- Patching

Conclusions

Can smart phones be deployed and managed securely?

- Mobile devices can be integrated securely by:
  - Updating policies, procedures and standards
  - Enforcing fundamental network security principles
  - Considering mobile device management solutions
  - Providing user education and training

Thank You

Your time and attendance is greatly appreciated!

Kaan Kivilcim
Security Consultant
Sense of Security
kaank@senseofsecurity.com.au
+61 2 9290 4444

Recognised as Australia's fastest growing information security and risk management consulting firm through the Deloitte Technology Fast 50 & BRW Fast 100 programs

T: 1300 922 923
T: +61 (0) 2 9290 4444
F: +61 (0) 2 9290 4455
info@senseofsecurity.com.au
www.senseofsecurity.com.au