NIST SP800-124r2:

Guidelines for Securing Mobile Devices in the Enterprise

The National Institute of Standards and Technology (NIST) released Special Publication 800-124- Revision 2 (NIST SP800-124r2), **"Guidelines for Managing the Security of Mobile Devices in the Enterprise,"** providing readers with comprehensive guidelines and recommendations for managing the security of mobile devices.

01 EXPLOITATION OF UNDERLYING VULNERABILITIES IN DEVICES

- Security-focused device selection
- OS and application isolation
- Rapid adoption of software updates
- Application vetting
- Mobile threat defense

02 DEVICE LOSS AND THEFT

- EMM technologies
- Mobile device security policies
- Remote/secure wipe
- Notification/revocation of enterprise access for policy violations
- Strong authentication

03 CREDENTIAL THEFT VIA PHISHING

- User education
- Mobile threat defense
- Mobile device security policies
- Strong authentication (e.g., MFA)
- Remote/secure wipe

04 INSTALLATION OF MALICIOUS DEVELOPER AND EMM PROFILES

- User Education
- Application vetting
- Mobile threat defense

05 EXPLOITATION OF SUPPLY CHAIN VULNERABILITIES

- User education
- Security-focused device selection

06 ACCESSING ENTERPRISE RESOURCES VIA A MISCONFIGURED DEVICE

- EMM technologies
- Mobile device security policies
- Notification/revocation of enterprise access for policy violations

07 INSTALLATION OF UNAUTHORIZED CERTIFICATES

- Mobile Threat Defense

08 USE OF UNTRUSTED MOBILE DEVICES

- Security-focused device selection
- EMM technologies
- Mobile device security policies
- Notification/revocation of enterprise access for policy violations

09 WIRELESS EAVESDROPPING

- Use of secure connection to resources (e.g., VPN)
- Mobile Threat Defense

10 MOBILE MALWARE

- User education
- Security-focused device selection
- Rapid adoption of software updates
- Application vetting
- OS and application isolation
- Mobile threat defense

11 INFORMATION LOSS DUE TO INSECURE LOCK SCREEN

- EMM technologies
- Mobile device security policies
- User education

12 USER PRIVACY VIOLATIONS

- User education
- EMM technologies
- Application vetting

13 DATA LOSS VIA SYNCHRONIZATION

- EMM technologies
- Mobile device security policies
- User education

14 SHADOW IT USAGE

- Mobile Device security policies
- User education

15 EXPLOITATION OF VULNERABILITIES WITHIN THE UNDERLYING EMM PLATFORM

- Cybersecurity recommended practices
- User education

16 EMM ADMINISTRATOR CREDENTIAL THEFT

- Additional authentication for system administrators

17 INSIDER THREAT

- EMM technologies
- Mobile device security policies
- User education

Zimperium MTD, z3A, and zScan capabilities provide coverage for multiple mitigations and countermeasure recommended by NIST. Zimperium aims to help organizations enhance the security of mobile devices to protect sensitive data, mitigate security risks, and ensure the integrity, confidentiality, and availability of information in the context of a mobile-centric world.

NIST

Contact us for more information on how Zimperium can help you meet NIST SP800-124r2 standards.

www.zimperium.com

ZIMPERIUM®