Mobile Protection 2.0

Smart working, mobilità e Industry 4.0, la nuova frontiera lavorativa. Facciamolo in sicurezza!!!"

Autore Luca Bechelli, Michele Onorato, Riccardo Canetta

SECURITY SUMMIT

TECHNOLOGIES

MANAGEMENT

COMPLIANCE

Clusit

Clusit Education

Minacce

THREAT	DEFINITION	EXAMPLES
Denial of Service	Deny or degrade service to users	Jamming of wireless communications, overloading networks with bogus traffic, ransomware, theft of mobile device or mobile services
Geolocation	Physical tracking of user	Passively or actively obtaining accurate three-dimensional coordinates of target, possibly including speed and direction
Information Disclosure	Unauthorized access to information or services	Interception of data in transit, leakage or exfiltration of user, app, or enterprise data, tracking of user location, eavesdropping on voice or data communications, surreptitiously activating the phone's microphone or camera to spy the user
Spoofing	Impersonating something or someone	Email or SMS message pretenging to be from boss or colleague (social engineering); fraudulent Wi-Fi access point or cellular base station mimicking a legitimate one
Tampering	Modifying data, software, firmware, or hardware without authorization	Modifying data in transit, inserting tampered hardware or software into supply chain, repackaging legitimate app with malware, modigyinf network or device configuration (e.g., jailbreaking or rooting a phone)

Minacce

MOBILE DEVICE TECHNOLOGY STACK

- Delays in Security Updates
- Exploitation of OS or Baseband Vulnerabilities
- Deliberate Bootloader Exploitation
- Jailbreak/Rooting
- Supply Chain Compromise
- TEE/Secure Enclave Exploitation
- Compromised Cloud System Credentials

MOBILE NETWORKS

- Data/Voice Eavesdropping
- Data/Voice Manipulation
- Device and Identity Tracking
- Denial of Service/Jamming
- Rogue Base Stations & Wi-Fi Access Points
- Interference with 911 Calls

DEVICE PHYSICAL SYSTEMS

- Device Loss or Theft
- Physical Tampering
- Malicious Charging Station
- Attacks on Enterprise PCs

MOBILE APPLICATIONS

- Malicious and/or Privacy-Invasive Practices
- Vulnerable Third-Party Libraries
- Exploitation of Vulnerable App
- Insecure App Development Practices
- Exploit Public Mobile App Store
- Malware, Ransomware

MOBILE ENTERPRISE

- Compromised EMM/MDM System or Admin Credentials
- Man-in-the-Middle Attacks on Devices
- EMM/MDM system impersonation
- Compromised Enterprise Mobile App Store or Developer Credentials
- Bypass App Vetting

Ciclo di vita per una soluzione di sicurezza dei dispositivi mobili aziendali

Iniziale

1

Utilizzo dei dispotivi:

Per quali obiettivi di business

Rischi

Definizione di una politica e di procedure di riferimento

Conformità alle politiche di sicurezza e alle normative

Sensibilità dei dati trattati

Costi

Luoghi di lavoro

Requisiti utenti addizionali

Sviluppo

2

Caratteristiche Tecniche:

Dispositivi mobili da utilizzare (sistemi operativi)

Metodi di autenticazione

Crittografia per protezione comunicazione e dati

Altri aspetti in base alla policy (limitazione operatività)

Integrazione con altri sistemi

Applicazioni

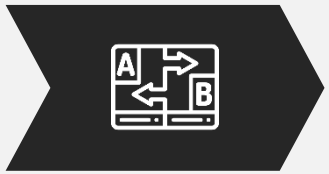
Logging

Awareness

Implementazione

3

Delivery



Testing

Esercizio

Mantenimento

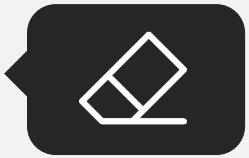
4

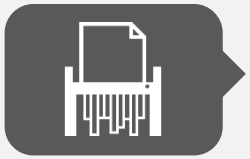
Ritiro

5

Requisiti normativi

Sanificazione degli apparati





Smaltimento

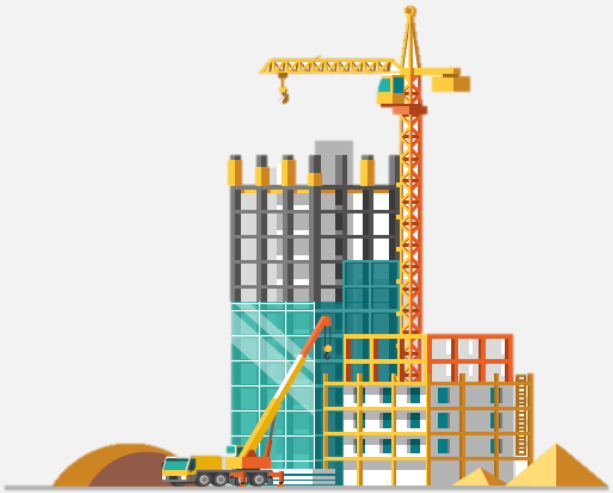
Field Work Support Service

Field Work Support Service

Sistema IoT implementato con l'obiettivo di rendere più efficiente l'operatività e le attività di manutenzione

Il Field Work Support mira alla riduzione degli oneri e al miglioramento della qualità del lavoro degli operatori di manutenzione e intervento, applicabile ai diversi settori industriali

FSS: il target



Campi di applicazione

Servizio di manutenzione e ispezione di impianti / attrezzature ecc.

Le sfide del cliente

- Riduzione del carico di lavoro sul luogo di lavoro e miglioramento della qualità del lavoro
- Trasferimento delle conoscenze e competenze da un esperto

FSS: la soluzione

La soluzione

- Attraverso l’utilizzo di un tablet, il carico di lavoro è ridotto alla stampa del documento, alla cattura di foto per eventuali prove e verifiche, e alla creazione di un report
- La comunicazione e la risoluzione dei problemi sono semplificate grazie alla condivisione di immagini e video con l'amministratore di controllo
- E’ possibile accrescere il proprio know-how direttamente sul luogo di lavoro con video e materiali di formazione