CONTROLLARE I DISPOSITIVI AZIENDALI PER PREVENIRE I CRIMINI INFORMATICI

Relatore: Francesco Cossettini

17 Ottobre 2017 – 18:00

FP1640985001
#Sharing3FVG

Webinar realizzato da IALFVG e parte degli 80 di #Sharing3FVG, progetto cofinanziato dal Fondo Sociale Europeo nell'ambito del Programma Operativo Regionale 2014/2020

Presentazione

Darnet

Keep IT safe and simple

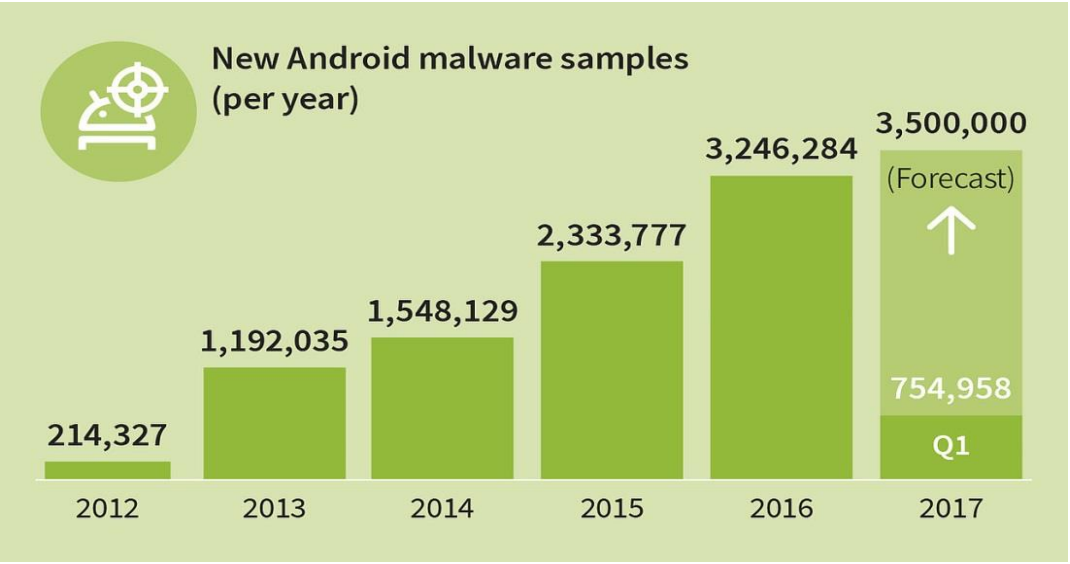
Consulenza
Risk Assessment
Security Assessment
Monitoraggio di sistemi
Supporto sistemistico
Incident response
Perizie forensi
Formazione

Di cosa parliamo oggi

- 56% of corporate data is accessible on PCs and mobile.

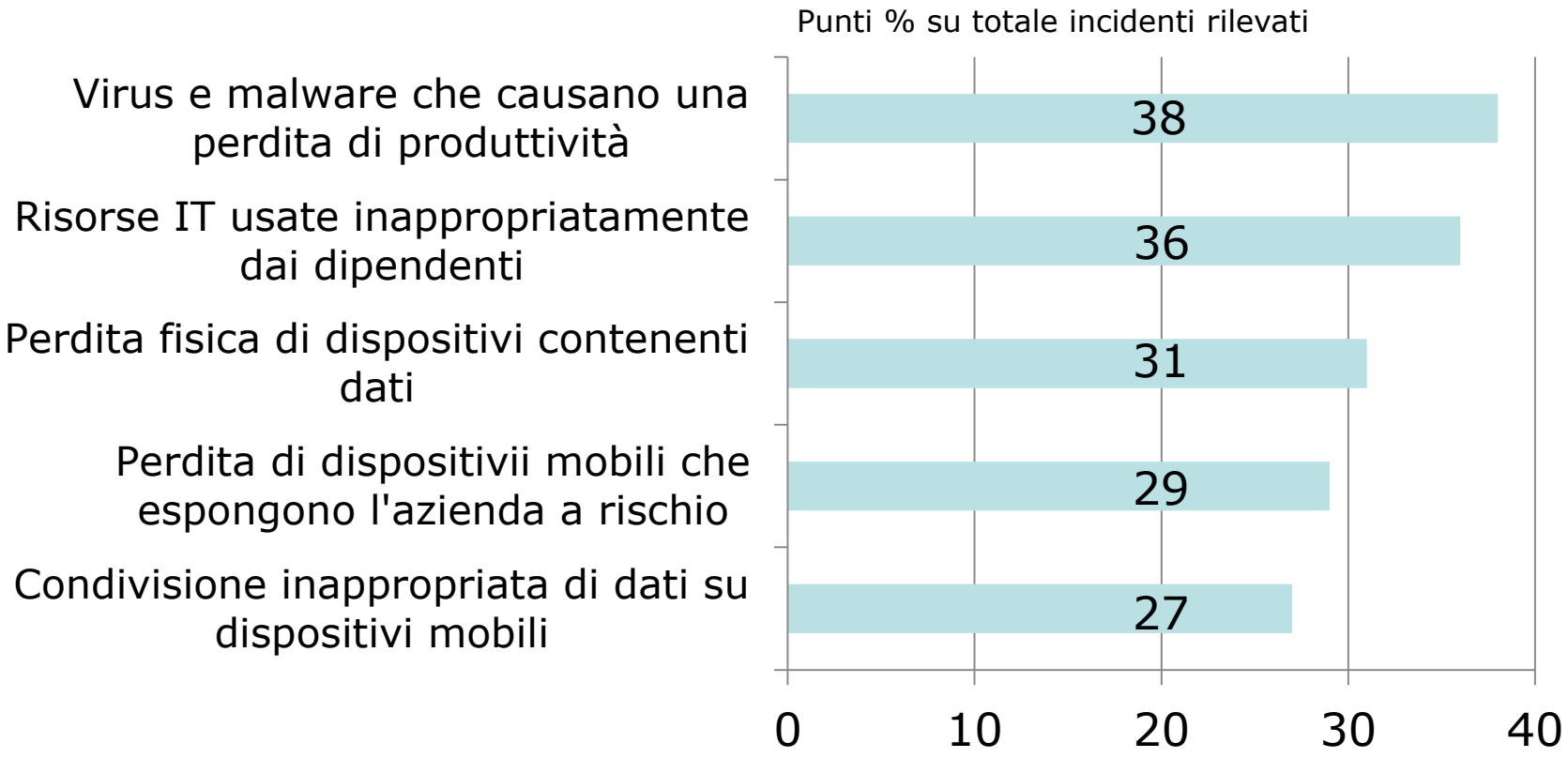
Perché ne parliamo?

- Dove stanno i miei dati?
- E il concetto di «Perimetro Aziendale»?
  In azienda ho firewall, antivirus, monitoraggio…
- Come sono protetti miei dati sul mobile?



Perché ne parliamo?

Incident Experience



Come sono gestiti questi dispositivi?

- Dispositivi Aziendali
  - Corporate Owned, Businnes Only (COBO)
  - Corporate Owned, Personally Enabled (COPE)

- Dispositivi Personali
  - Bring Your Own Device (BYOD)

- Alternative?
  - Choose Your Own Device (CYOD)

BYOD: cosa comporta? Vantaggi

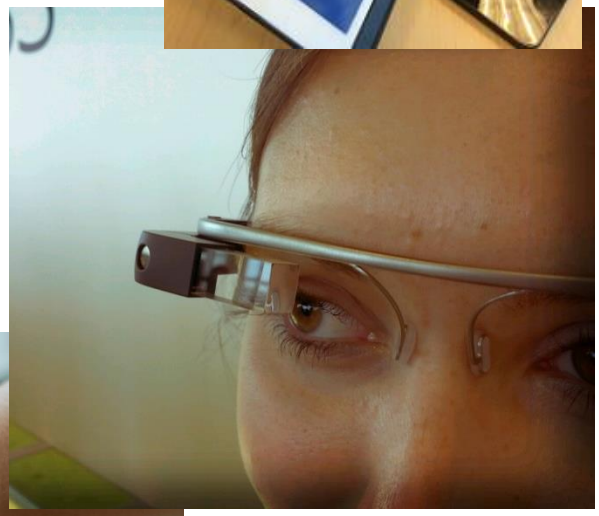
- Per il dipendente
  - Tecnologia preferita
  - Proprie App
- Per l'azienda
  - Minori costi (?)
  - Innovazione tecnologica

BYOD: ma anche..

- Per il dipendente
  - Privacy dati personali
  - Geolocalizzazione
  - Traffico
  - Responsabilità sui dati
- Per l'azienda
  - Esposizione di dati
  - Policy di sicurezza
  - Eterogeneità e quantità di dispositivi
  - Gestione incident

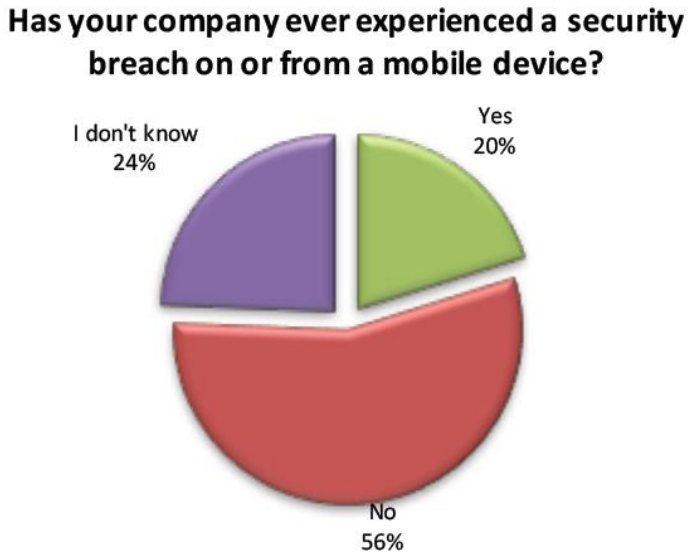
Non fermiamoci qui… il futuro?

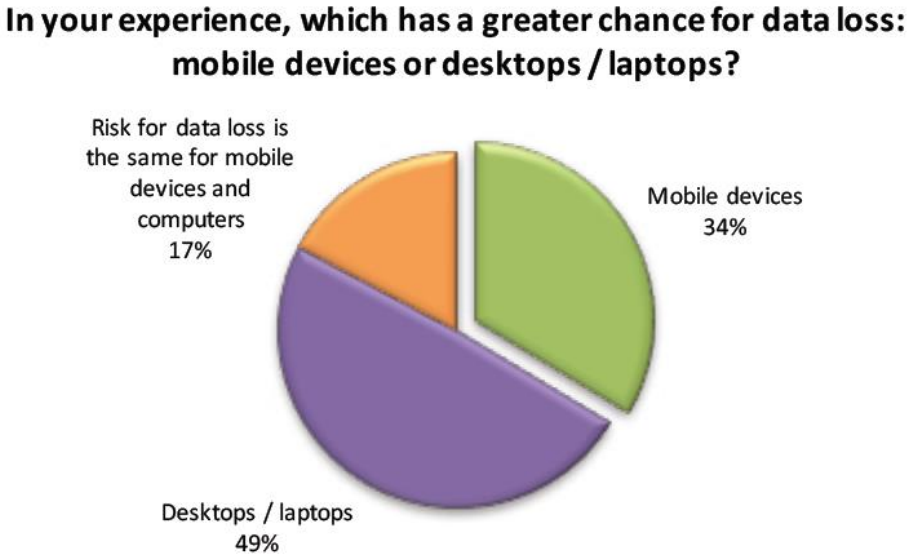
- BYO(x)
  - Device
  - Identity
  - Encryption
  - Tecnology
  - . .
- WYOD?
  Wear Your Own Device!



Quali sono le difficoltà?

- Fino a qualche hanno fa:
  - Costi
  - Gestione
- Ora? Security!





Fonte: Dimensional Research – Checkpoint – Aprile 2017

Quali sono le minacce?

- Furto o Smarrimento
- Perdita di dati
  - Malware
  - Reti insicure
- Phishing
- Spyware
- Bugs (App o OS)

Statistiche

- Oltre metà dei dispositivi Mobile non è aggiornata
- Negli ultimi 36 mesi attacchi su Mobile in crescita del 100% (Gartner – luglio 2017)

Altre attenzioni da porre

Regolamenti

- Geo-localizzazione
- Gestione Incident
- Chiaro limite tra azienda e privato

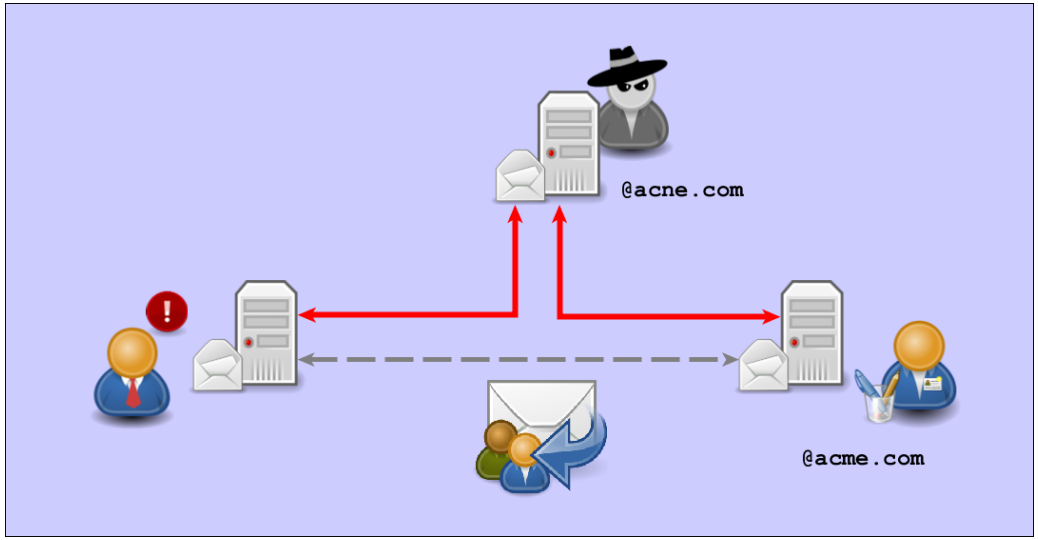
Horror Stories

> Da una «App» a padroni della rete aziendale

- Social Engineering
- App Malevola
- Accesso alla rete
- Accesso a server
- Accesso ai dati!

Horror Stories

- Man-in-the-Mail



- CEO Frauds

Suggerimenti

Come tenere a bada dispositivi ed utenti?

- Inventario
- Cifratura
- Obbligo di PIN/Password

Suggerimenti

- Controllo delle Applicazioni
- Evitare Jailbreak / Root
- Patch management
- Configurazione
  - Backup
  - Connettività (WiFi – VPN)
  - Dispositivi rimovibili

Suggerimenti

- Preparare la vostra rete aziendale
  - Sovradimensionare
  - Segmentare
  - Controllo del traffico
  - Logging accessi + Report
  - WiFi sicuro

Suggerimenti

- Regolamentazione!
  - Geolocalizzazione
  - Procedure di Incident Response
- Comunicazione, Formazione e Informazione!
- **Non è un problema solo IT!**

Mobile Device Management

- Soluzioni Cloud/On Premise
- Dashboard + Repor
- Configurazione rapida (QR Code/email)
- Controllo tipo «Desktop Remoto»
- Wipe/Lock Remoto
- Localizzazione
- Gestione connettività
- Telecom Expense Management

Mobile App Management (MAM)

- Gestione applicazione (black/whitelist)
  + Enterprise App Store

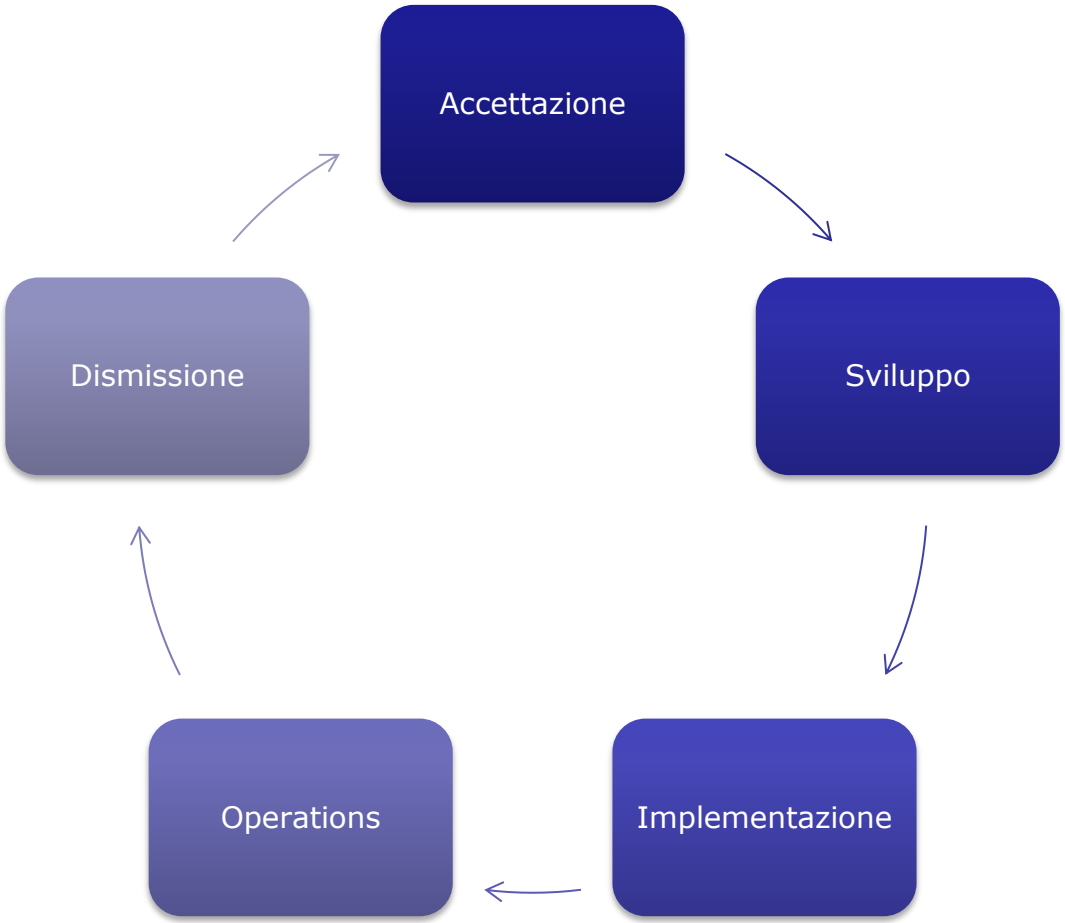
Mobile Device Management e BYOD?

→ Container!

- Dati aziendali in area isolata e cifrata
- Inibito «copia-incolla»
- VPN-per App
- Wipe dei soli dati aziendali
- Sharing documentale

Linee Guida - Pianificazione

> Mobile Device Solution Life Cycle



Mobile Device Management Life Cycle

Accettazione

- HR, Ufficio Legale, CISO/CIO, Direzione
- Quali sono i bisogni?

- Livelli di accesso? → Policy!
  - COBO: accesso documentale
  - BYOD + Device Management: risorse limitate
  - BYOD: solo webmail
  - Informazioni sensibili: nessun accesso mobile

35% of corporate not have a formal security policy for corporate data available to mobile devices (Ponemon Institute, 2016)

Mobile Device Management Life Cycle

Sviluppo

- Architettura / Autenticazione / Crittografia
- Requisiti di configurazione
- Fornitura
- Esame applicazioni e certificazione

Implementazione

- Connessione / Protezione
- Gestione
- Report e Performance

Mobile Device Management Life Cycle

Operations and Maintenance

- Upgrade / Patch
- Verifica modifiche Policy
- Inventario
- Formazione
- Revoca accessi / revisione App

Dismissione

- Wipe completo

GRAZIE PER L'ATTENZIONE!

Domande?

cossettini@darnet.it

DARNET
IT security consulting