# Fare Sicurezza e non essere APM

Salvatore Todaro
Università di Messina

WORKSHOP GARR 2021

NET MAKERS

# Chi Sono

- Una persona che vede il mondo da più punti di vista
- Svolgo con passione il lavoro che desideravo fare da giovane studente di informatica
- Vedo e faccio attività che la maggior parte dei tecnici informatici ignora
- Si dice che io sia paranoide e rompiscatole

# Non sono APM GARR

- Non configuro router/switch/ap
- Non so cosa sia una fibra
- Non configuro DNS, DHCP, TFTP etc
- Vedo ogni giorno alert di sicurezza e data breach
- Analizzo anomalie e fonti OSINT
- Con un cappello bianco cerco e segnalo vulnerabilità nell’ecosistema UniME proponendo soluzioni

# Sicurezza (Non solo Network Security)

- Non solo Network / DDOS / Open Relay
- Non solo applicazioni vulnerabili e applicazione di patch
- APM ”Mero spalatore di bit”
  (cit. Melchiorre Monaca Ex APM UniME ora UniRC)
- Fare sicurezza non è (solo) un firewall e un antivirus

NON esiste più il perimetro e la “Fiducia”

# Sicurezza (Non solo Network Security)

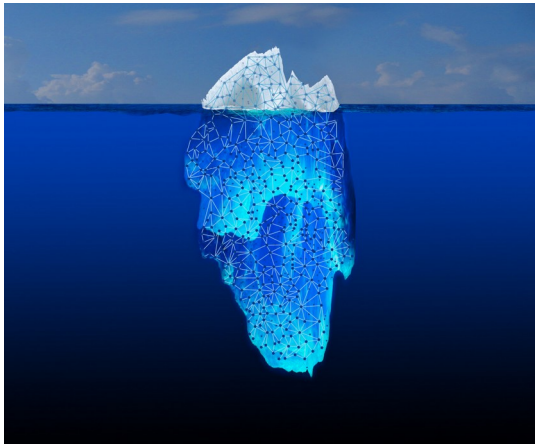
- Alert di sicurezza inviati ad un indirizzo diverso da apm AT unime.it (2016)
- Canale di supporto sicurezza agli utenti (2016)
- Unità Operativa Sicurezza Informatica (2020)

# Alcune Attività Recenti

- Consulenza Security nuove applicazioni:
  - Analisi Vulnerabilità
  - Analisi Architettura
  - Proposte e soluzioni tecniche per incrementare la sicurezza totale
- Esporre (con parole semplici) i rischi

# Comunicazione Efficace

- Verso gli utenti
- Verso i tecnici
- Verso chi prende decisioni



Linguaggi, priorità e punti di vista diversi

# Sicurezza

Priorità diverse:

- Per l’APM è far funzionare la rete
- Per Cybersec è dare servizi in sicurezza

Ago della bilancia RTD (supportato da ICT)

che accetta i rischi residui

# Sicurezza

E’ una cultura ed un lavoro multidisciplinare e trasversale:

- Network
- Applicazioni
- Education
- Comunicazione
- Legale
- Etc ...

# Sicurezza

Il Cloud/Outsourcing non azzerano i rischi:

- Li diversificano
- Li potrebbero amplificare
- Aumentano il rischio supply chain

# Un Referente Security e poi ... ?

Rischio di essere “atolli” in mezzo all’oceano

Necessità di:

- Una rete “Operativa” di rapporti e collaborazioni
- Professionalità e Competenza
- Formazione Continua

# Bisogni Operativi

- Sto notando una attività o comportamento anomalo, da distorto penso possa trattarsi di un attacco, con chi mi confronto in maniera riservata?
- Non posso sempre attaccare i miei servizi, li vedo in maniera distorta, mi servirebbero amici “fidati” e “riservati” con cui condividere la “cortesia” …
- Dove trovo PERSONE che hanno i miei stessi problemi (Ente) e certamente sono “bravi” e “fidati”?

# Gli enti della community GARR

- Minacce analoghe
- Organizzazioni ed esigenze analoghe
- Strumenti più o meno omogenei (convenzioni e accordi consip/CRUI)
- Soluzioni analoghe? → verifichiamole insieme (dividendoci il lavoro)

# IDEM GARR – Il Modello Collaborativo

- Membri del CTS IDEM → Ore Allocabili e Dedicate
- Gruppi di Lavoro → Approfondimenti e Risultati
- Condivisione della conoscenza → Aumento di competenze
- Condivisione degli scenari → Proattività
- Figure dedicate:
  Referente Tecnico e Referente Organizzativo

# GARRLab – Il Modello Sperimentale


- Ambiente per sperimentare nuove soluzioni
- HackLab “istituzionalizzato”
- Condivisione
- Soluzioni “Portabili”, facilmente replicabili
- Evitare, se possibile, (Vendor | Platform) lock-in

# Proposte – Fare Community

- Creazione di un gruppo di lavoro permanente
- Scambio Informazioni
- Creazione/Utilizzo strumenti condivisi

# Ringraziamenti

Grazie alla Governance di UniME

Grazie a Giuseppe Mannino (RTD UniME)

Grazie a Fabrizio La Rosa (Responsabile U.Org ICT)

Grazie a GARR per l’invito e le competenze messe a disposizione

Grazie a tutta la community per le preziose informazioni e competenze condivise

# Domande

salvatore.todaro@unime.it
Unità Operativa “Sicurezza Informatica”
Centro Informatico Ateneo Messina (CIAM)
Università degli Studi di Messina