L’Incident Detection in una multinazionale

Panoramica dei principali problemi incontrati nell’organizzare la Sicurezza

Enrico Riccardi

Group CISO

Chiesi
People and ideas for innovation in healthcare

Chiesi nel mondo

Chiesi USA

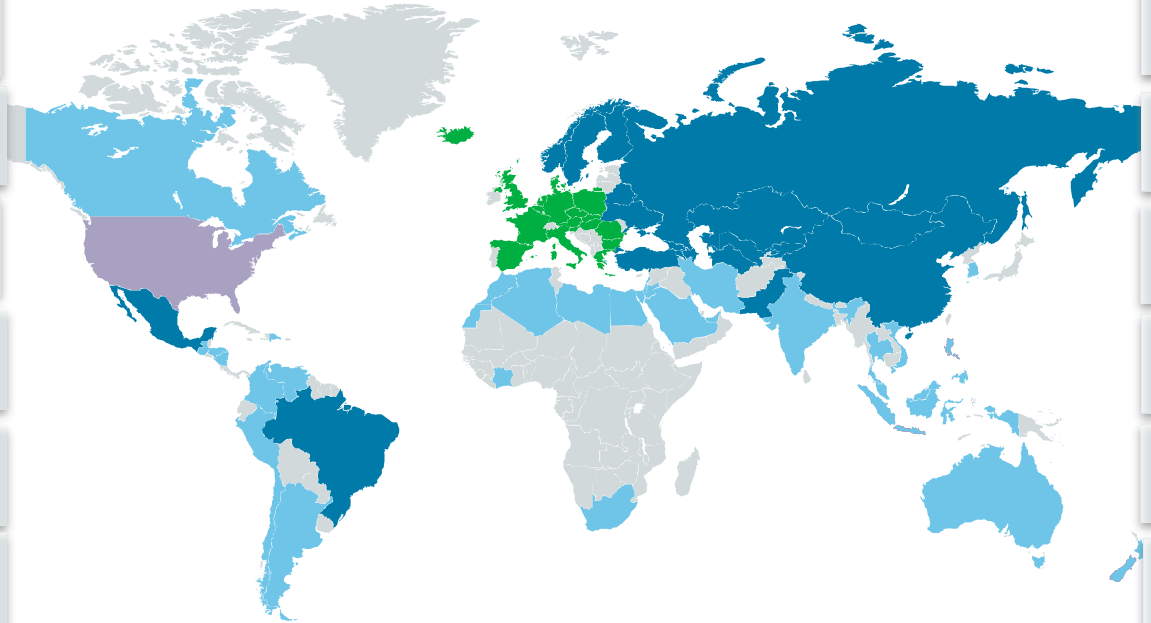
Chiesi Mexico

Chiesi Brasil

Chiesi Europa

Algeria

Tunisia



Chiesi Russia

Chiesi China

Chiesi Pakistan

Chiesi Turkey

Arabia Saudita

Iran

Local Companies | Chiesi USA | Chiesi Europa | Resto del mondo | Local Partners

Chiesi
People and ideas for innovation in healthcare

Le principali sfide

- Creare una cultura sull'Information Security
  - Sia all'interno dell'ICT che negli altri dipartimenti
- Aumentare il livello di sicurezza di ogni paese
  - Trovare soluzioni efficaci per gli ambiti scoperti
- Uniformare il livello di sicurezza tra i diversi paesi
  - Ogni filiale aveva i suoi propri punti deboli e di forza

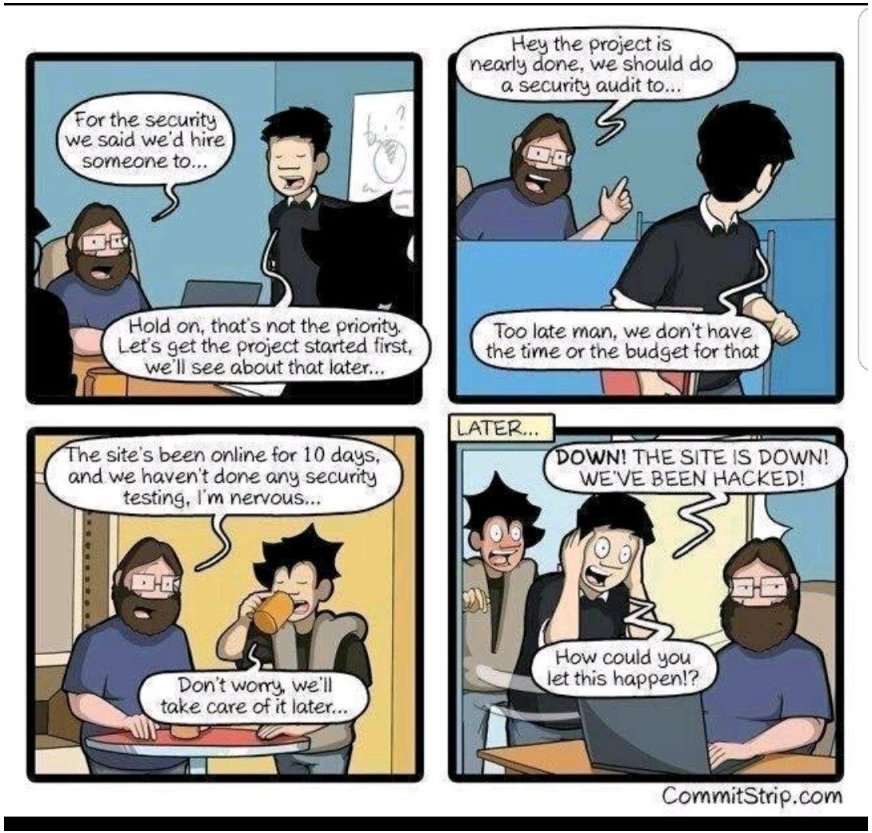
Perché la cultura è fondamentale?

- La sicurezza è sempre il problema di qualcun altro
  - Dal Business: spesso viene vista solo come una questione tecnica
  - Dall'ICT: spesso viene vista solo come una questione per esperti

- Parole chiave per aprire il dialogo:
  - Fornitori, partner, consulenti, SaaS, …

- La sicurezza non può esistere separata dai sistemi e dai processi

La sicurezza va considerata dall'inizio, non dopo



Chiesi

Come aumentare e uniformare la sicurezza?

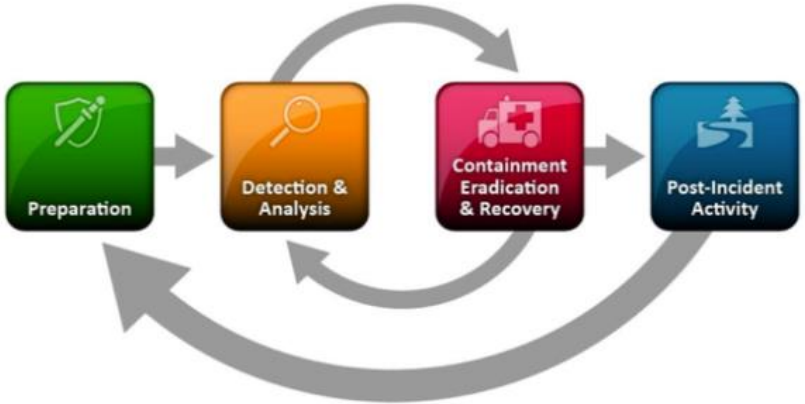
- Linee guida
- Strumenti e servizi standard
  - \+ Efficienza nel processo di acquisto
  - \+ Risparmio sui costi, specialmente per le filiali
  - \+ Possibile condivisione di competenze
  - \+ Visione centralizzata
  - \- Flessibilità
  - \- Tempi per una nuova iniziativa

Un progetto: la gestione degli incidenti

- Assessment su tutte le filiali per valutare:
  - Prevenzione
  - Individuazione
  - Risposta
  - Chiusura

Area storicamente più forte

Area critica, da migliorare subito



Chiesi

Individuazione vs prevenzione

- Non è un’alternativa, occorre lavorare su entrambi i fronti

- Non si può prevenire al 100%
  - Nuove vulnerabilità e nuovi tipi di attacco
  - Perimetro indefinito (dispositivi mobili, lavoro da casa e da remoto)

- Maggiore è il tempo di rilevamento dell’attacco, maggiore è il danno subito

Le possibili soluzioni

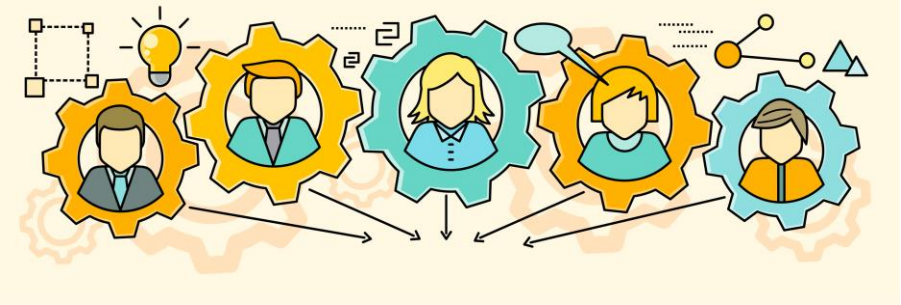
- Interna: aumentando le competenze in ambito
  - In parte va fatto comunque, sia per la parte di prevenzione, sia perché un minimo di competenza interna è indispensabile

- Esterna: acquisizione di servizi da parte di un Security Operation Center
  - Punto critico: processo di gestione delle segnalazioni

Chiesi

Gli aspetti da non dimenticare

- Comunicazione
  - Verso il management
  - Verso i colleghi ICT



- Gestione progetto (sia assessment che rollout)
  - Budget
  - Hardware (spedizione vs acquisto locale)
  - Configurazione e supporto

Grazie per l’attenzione!

Chiesi