

CPS – Cyber Physical Security



L'evoluzione della sicurezza fisica

Pietro Blengino, Group Security

UniCredit SpA – Public

Milano, 29 novembre 2016



Il nuovo mondo é già arrivato...

La sicurezza fisica come l'abbiamo conosciuta non esiste più

Se alcuni mesi fa citavamo V. Hugo "*Niente è più irresistibile di un'idea il cui tempo sia giunto*" oggi sappiamo che in quel "tempo" siamo ormai completamente immersi



2010: game changer



L'elemento di continuità importante è la necessità di un accesso fisico

Wired.it article: **Bancomat e cybercriminali, 150 milioni di danni in 6 mesi**. In forte crescita gli assalti digitali agli Atm, complici software sempre più specifici, malware e sistemi operativi non aggiornati.

Infosec Institute article: **Hacking ATMs: The New Wave of Malware**. POSTED IN GENERAL SECURITY ON OCTOBER 21, 2014.

TechEconomy article: **ATM MALWARE**. Tyupkin è questo il nome di uno dei più famosi malware in circolazione che prende di mira gli ATM. Tyupkin è in grado di prendere il totale controllo del bancomat e creare una backdoor accessibile direttamente dal pinpad per permettere ai criminali di fare il incassar contanti ogni volta che vuole.

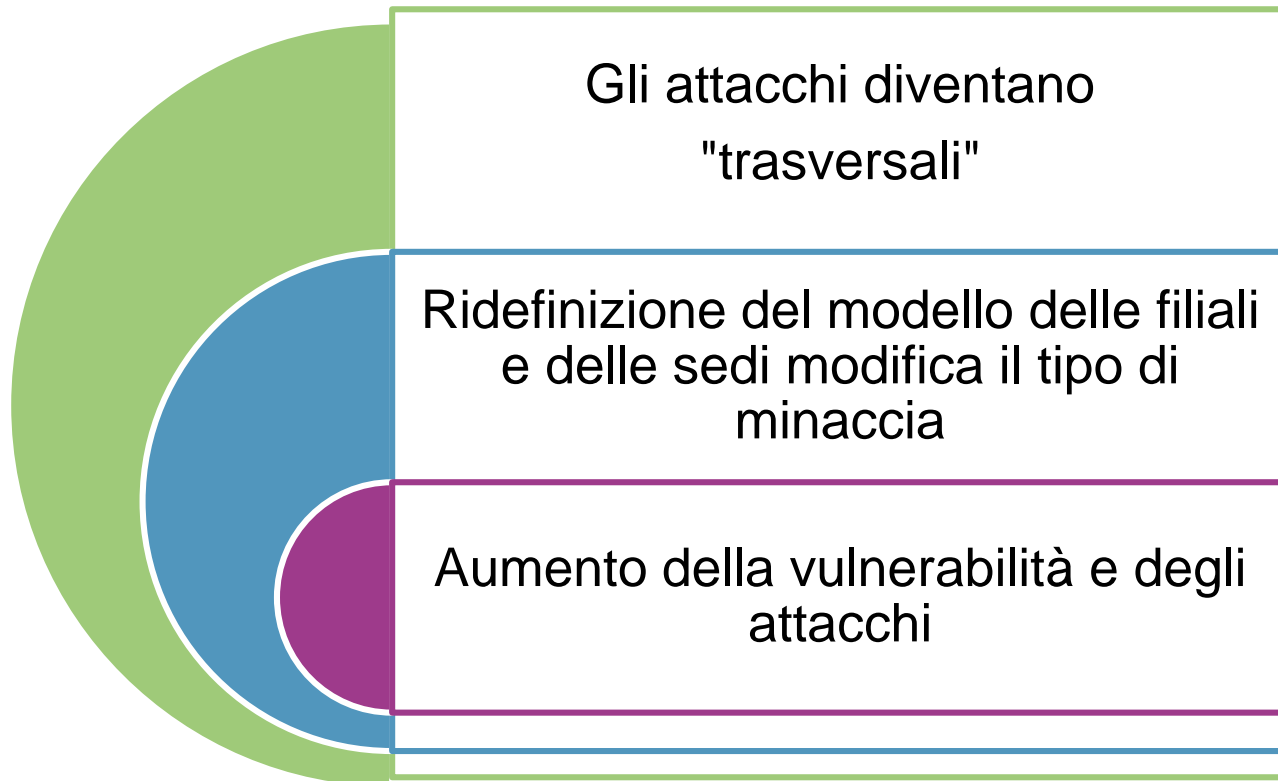
TYUPKIN
PADPIN
PLOUTUS



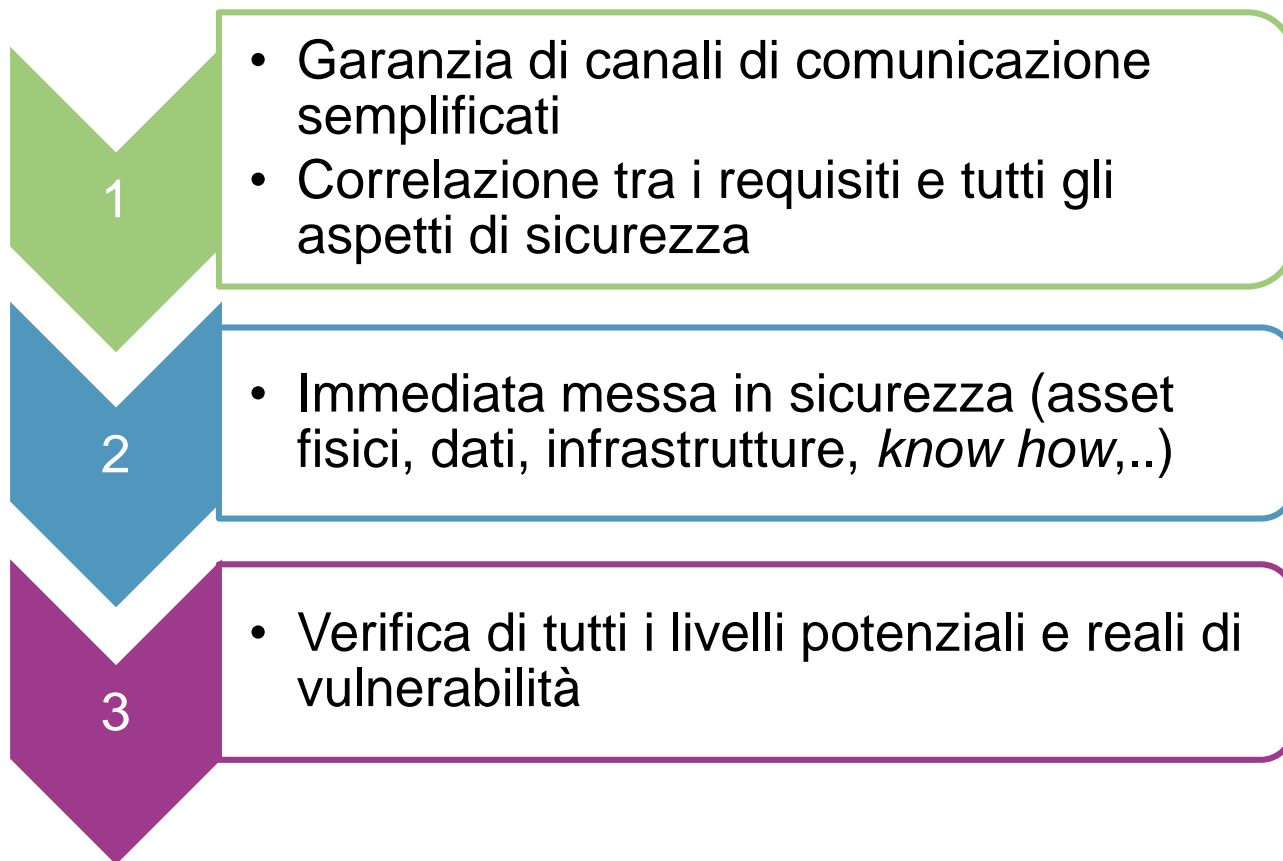
Siamo di fronte a nuovi scenari di rischio



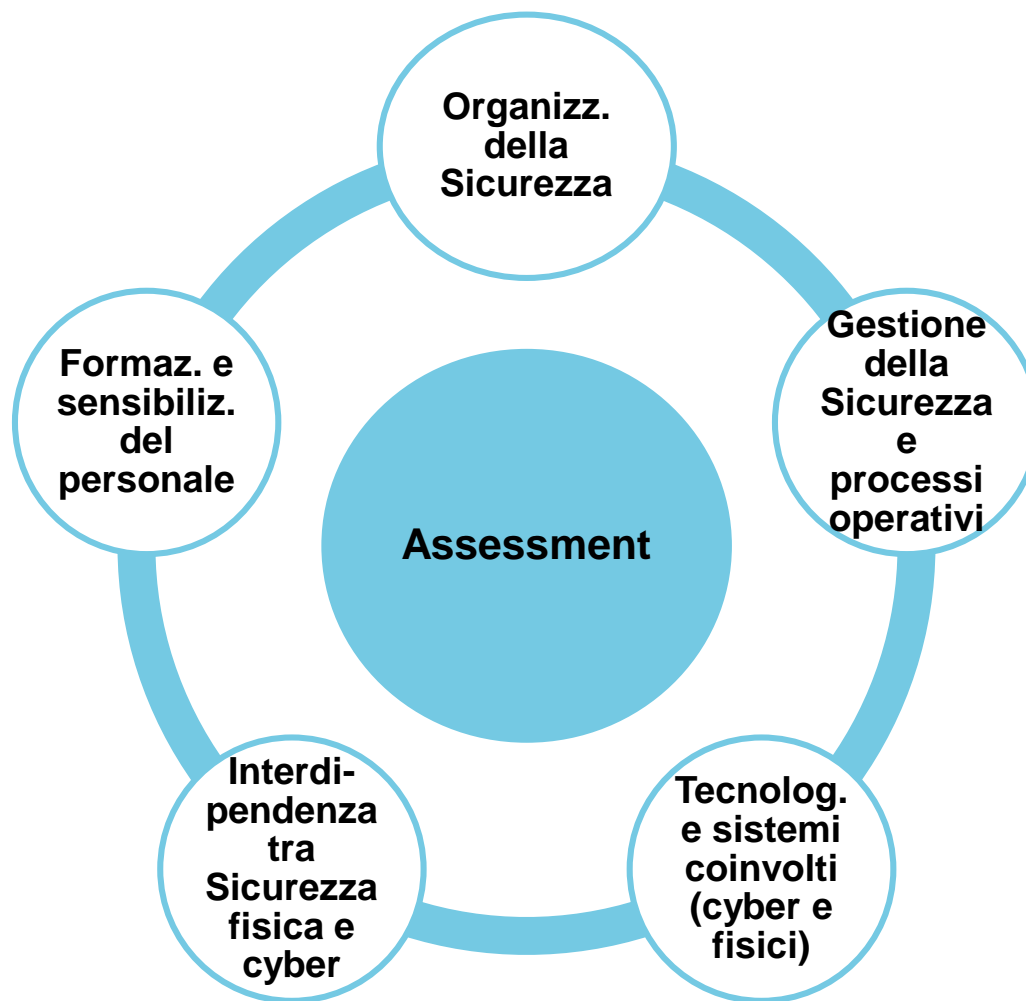
I nuovi strumenti tecnologici così come la nuova organizzazione del lavoro e il nuovo modello di servizio aumentano fortemente i rischi...



..da fronteggiare con nuove metodologie di intelligence e strumenti innovativi di mitigazione



Si rende necessario un assessment mirato su alcuni aspetti cruciali



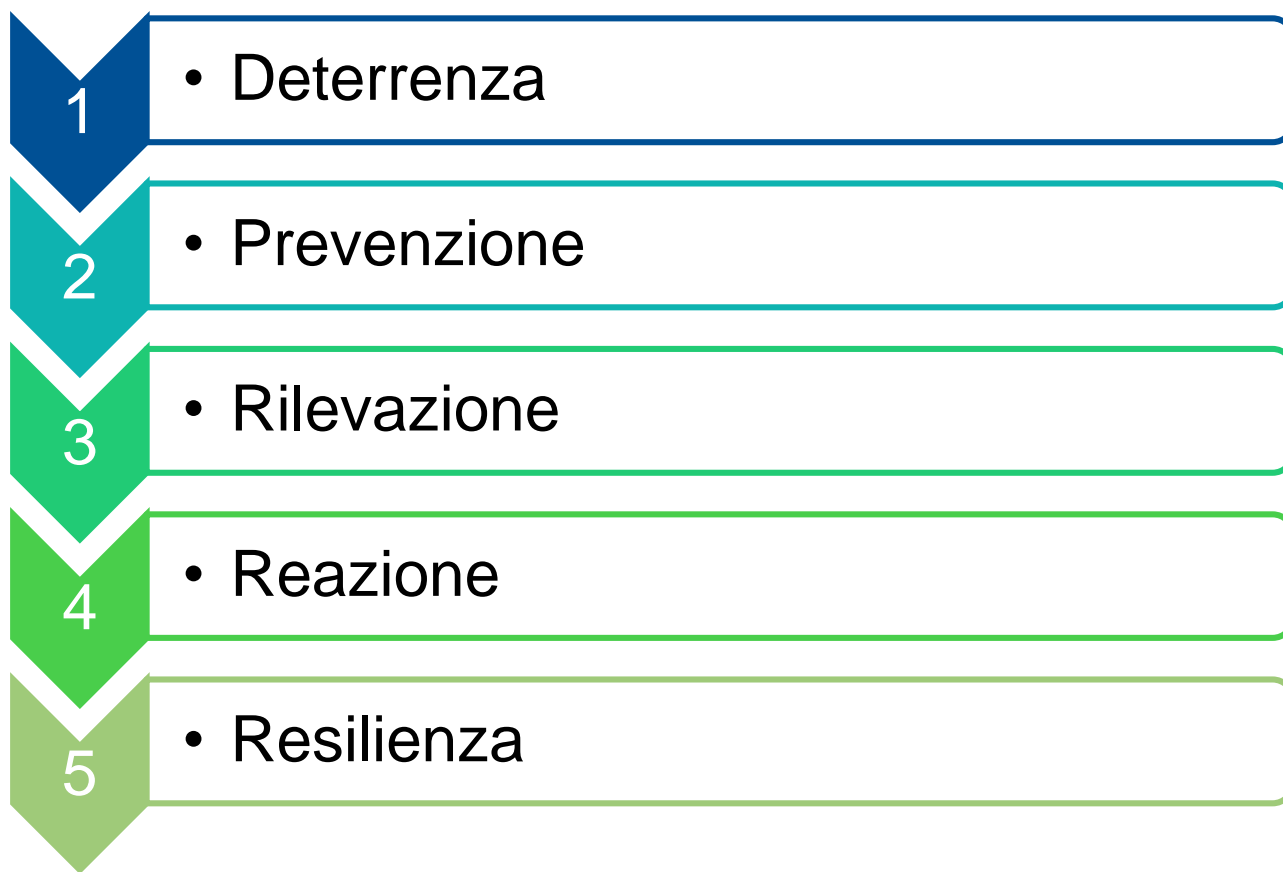
Tenendo conto delle peculiarità dei sistemi CPS

Sistemi CPS hanno specifiche vulnerabilità

- Attenzione all'aggiornamento del software
- Sviluppo di tecniche di rilevazione e identificazione mirate
- Forte numero di sistemi legacy
- Necessità di profonda comprensione degli attacchi, delle proprietà e delle conseguenze



E' necessaria l'elaborazione di una strategia che individua le contromisure

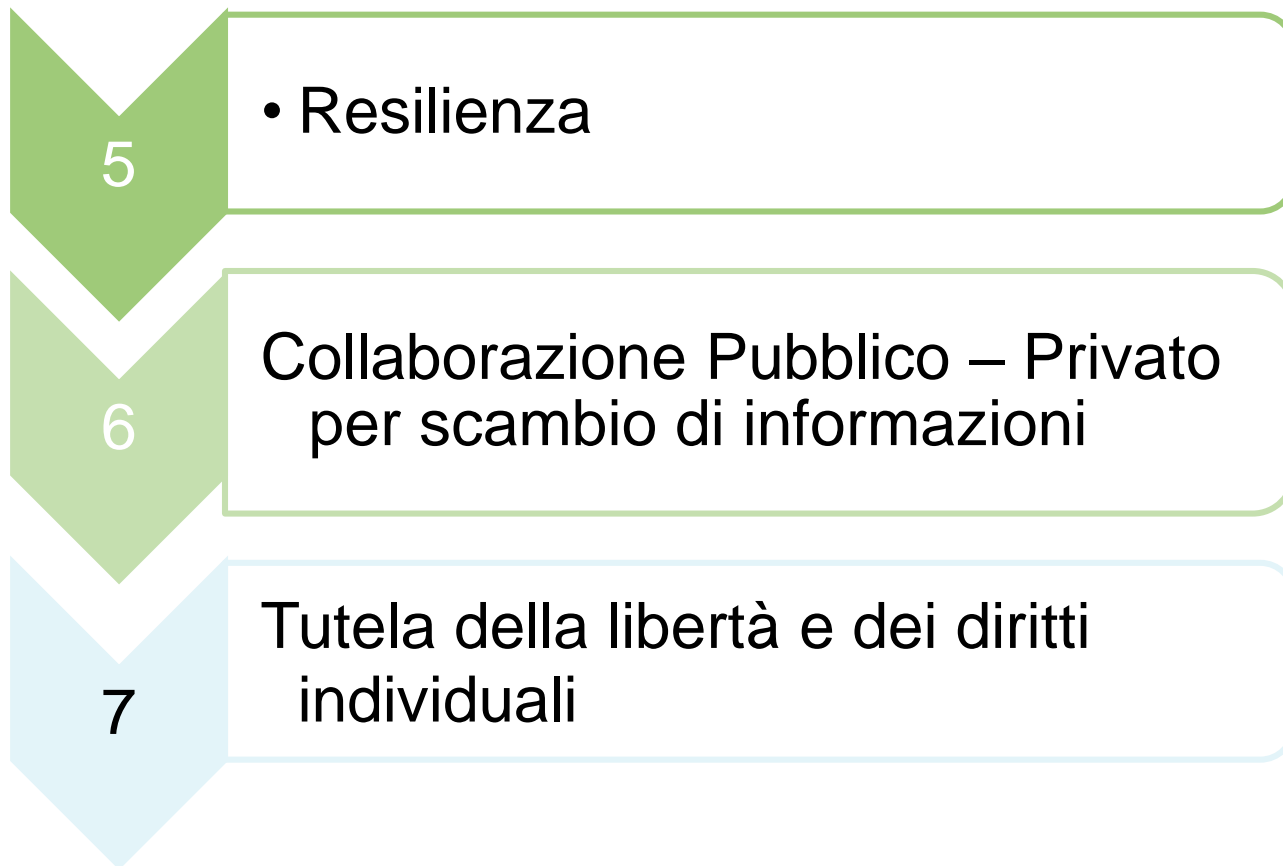


Un punto di vista diverso anche sulle norme

- ~~Direttiva Europea su Cybersecurity~~
- Decreto del Presidente del Consiglio dei Ministri 24 gennaio 2013
- Decreto Ministero dell'Interno 9 gennaio 2008
- Art. 615 ter c.p. accesso abusivo a sistema informatico e 640 ter c.p. frode informatica
- Circolari Banca d'Italia n. 263 del 27 dicembre 2006 "Nuove disposizioni di vigilanza prudenziale per le banche" e n. 285 del 17 dicembre 2013 "Disposizioni di vigilanza per le banche"
- Sentenza Corte Cassazione 29/4/2015



Dalla nuova normativa emergono dei valori chiave che riprendono i concetti della strategia e li ampliano



La nostra analisi che si basa su un approccio globale ci porta a individuare chiaramente quali sono i target da proteggere



Il leitmotiv è la convergenza delle soluzioni



Emerge il concetto chiave di "interoperabilità"

Fondamentale diventa la capacità di una tecnologia o di un sistema di interagire e funzionare con soluzioni o sistemi complessi, esistenti o ancora in divenire, senza alcuna restrizione



Grazie per l'attenzione
pietro.blengino@unicredit.eu

Cyber Physical Security – L'evoluzione della sicurezza fisica

