UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Security, Edge and Cloud Lab

Sensibilizzazione e formazione in ambito aziendale

Mirco Marchetti
Dipartimento di Ingegneria «Enzo Ferrari»
Università di Modena e Reggio Emilia

Mauro Andreolini
Dipartimento di Scienze Fisiche, Informatiche e Matematiche
Università di Modena e Reggio Emilia

Chi sono: Mirco Marchetti

- Professore Associato presso il Dipartimento di Ingegneria “Enzo Ferrari”
- Direttore del Centro di Ricerca Interdipartimentale sulla Sicurezza e la Prevenzione dei Rischi (CRIS), direttore della Unità Operativa “Sicurezza Informatica”
- Membro del laboratorio “Security, Edge and Cloud” (SECLoud https://secloud.ing.unimore.it/), leader delle attività cybersecurity e cybersecurity per sistemi cyber-fisici (ACES)
- Co-direttore dei corsi della Cyber Academy
- Titolare dei corsi “Sicurezza Informatica” e “Automotive Cyber Security”

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175
UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA
Security, Edge and Cloud Lab
CYBER ACADEMY
A.C.E.S
AUTOMOTIVE CYBER-PHYSICAL AND EMBEDDED SECURITY

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175
UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA
Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

Chi siamo: Mauro Andreolini

- Ricercatore presso il Dipartimento di Scienze Fisiche, Informatiche e Matematiche
- Membro del Centro di Ricerca Interdipartimentale sulla Sicurezza e la Prevenzione dei Rischi (CRIS), direttore della Unità Operativa “Sicurezza Informatica”
- Membro del laboratorio “Security, Edge and Cloud” (SECLoud https://secloud.ing.unimore.it/)
- Responsabile del nodo UniMoRe per la Cyber Challenge
- Co-direttore dei corsi della Cyber Academy
- Titolare dei corsi “Sviluppo Software Sicuro” e “Sistemi Operativi”

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Security, Edge and Cloud Lab

CYBER ACADEMY

A.C.E.S
AUTOMOTIVE CYBER-PHYSICAL AND EMBEDDED SECURITY

UNIVERSITAS STUDIORUM MUTINENSIS ET REGIENSIS 1175

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

Una PMI vista da un attaccante informatico

Sistemi obsoleti
(Rendono la violazione del sistema fattibile da attaccanti non esperti)

Osservazione:
- uso di sistemi operativi obsoleti in produzione (Windows XP, Windows Server 2003, Ubuntu 10.04).

Giustificazioni:
- ”il software di controllo dell’attuatore non funziona altrimenti.”

Rischio:
- violazione del sistema tramite programmi pubblicamente disponibili.

Assenza di asset management
(Semplifica la vita agli attaccanti)

Osservazione:
- i sistemi informatici non sono censiti;
- spesso esistono sistemi «dimenticati» e vulnerabili.

Giustificazioni:
- «quella macchina la uso ogni tanto per fare dei test».

Rischio:
- (ab)uso del sistema per raggiungere nuovi asset;
- (ab)uso del sistema per trafugare dati.

Assenza di isolamento
(Gli apparati sono raggiungibili tra loro, anche in reti diverse)

Osservazione:
- i sistemi informatici non sono opportunamente isolati (segmentazione delle reti)

Giustificazioni:
- «tanto il firewall impedisce gli ingressi nel sistema».

Rischio:
- una volta ottenuto accesso ad una macchina, l'attaccante ha spesso visione completa dell'infrastruttura informatica.
- → "Pivoting" nelle reti interne (amministrazione, produzione).

Software scritto in house
(Mai sottovalutare un amministratore improvvisatosi programmatore)

Osservazione:
- Il programmatore pensa solo alle funzionalità, pressato dalle scadenze

Giustificazioni:
- Pressing dei superiori, molteplici attività/mestieri in parallelo,

Rischio:
- Software privo di qualsivoglia controllo difensivo, zeppo di debolezze

(Mancata) Gestione delle password
(Free logins for everyone!)

Osservazione:

- Le password sono scritte in chiaro su carta (post-it, fogli, agende, …)
- Le password sono semplici (Password123! è un grande classico)
- Le stesse password sono riutilizzate per più servizi e identità
- L'autenticazione multifattore – questa sconosciuta

Giustificazioni:

- «così me la ricordo».

Rischio:

- Facile ottenere le password
- una volta ottenute le credenziali, l'attaccante accede a un portafoglio di sistemi

(Mancata) Gestione dei backup
(Il sogno di ogni ransomware)

Osservazione:

- Backup? Quali backup?
- Il sistema che ospita i backup è agganciato all'infrastruttura;
- Non è mai stato tentato un ripristino dei dati.

Giustificazioni:

- «Non ho tempo di guardarci, dobbiamo produrre e fatturare!»
- «Il software di backup è costosissimo e sicuramente funziona benissimo»

Rischio:

- In seguito ad un incidente informatico l'azienda rischia di perdere i propri dati (talvolta per sempre)

(Mancata) Cifratura dei dati in transito/a riposo
(Il sogno di ogni spia)

Osservazione:
- Dati (spesso sensibili) sono trasmessi e memorizzati in chiaro o «offuscati» in modo invertibile.

Giustificazioni:
- «Non ho tempo di guardarci, dobbiamo produrre e fatturare!»

Rischio:
- Un attaccante che ha accesso ai servizi è in grado di ottenere l'intera proprietà intellettuale e informazioni sensibili sui dipendenti (per poi spesso rivenderli al migliore offerente).

Carenza di igiene informatica
(Personale non IT)

Osservazione:

- I dipendenti “non IT” non hanno una cultura di sicurezza e reagiscono infastiditi alle contromisure di prevenzione

Giustificazioni:

- «Devo lavorare, non ho tempo da perdere!»
- «toh, un allegato, fammi vedere che cosa contiene»
- «oddio, una denuncia, fammi vedere di cosa si tratta»

Rischio:

- Elevata efficacia degli attacchi di phishing
- → Furto di credenziali, (più raramente) esecuzione di codice

Carenza di igiene informatica
(Personale IT)

Osservazione:

- I dipendenti “IT” hanno una cultura di sicurezza di base e reagiscono infastiditi ai collaudi di sicurezza

Giustificazioni:

- «questo sistema è aggiornato, perché lo testi?»
- «hai testato questo sistema fuori orario, ti segnalo al GARR»
- «questo sistema è irraggiungibile, perché lo stati testando?»

Rischio:

- Elevata probabilità di introdurre configurazioni errate nell’infrastruttura aziendale

Carenza di igiene informatica
(Management aziendale)

Osservazione:

- i dirigenti aziendali vedono la sicurezza come un costo da sostenere e non come una opportunità di investimento.

Giustificazioni:

- «La sicurezza non fattura»

Rischio:

- la sicurezza fatturerà (in negativo, con cifre a sei zeri) in caso di incidente informatico grave

Una PMI vista da un difensore informatico

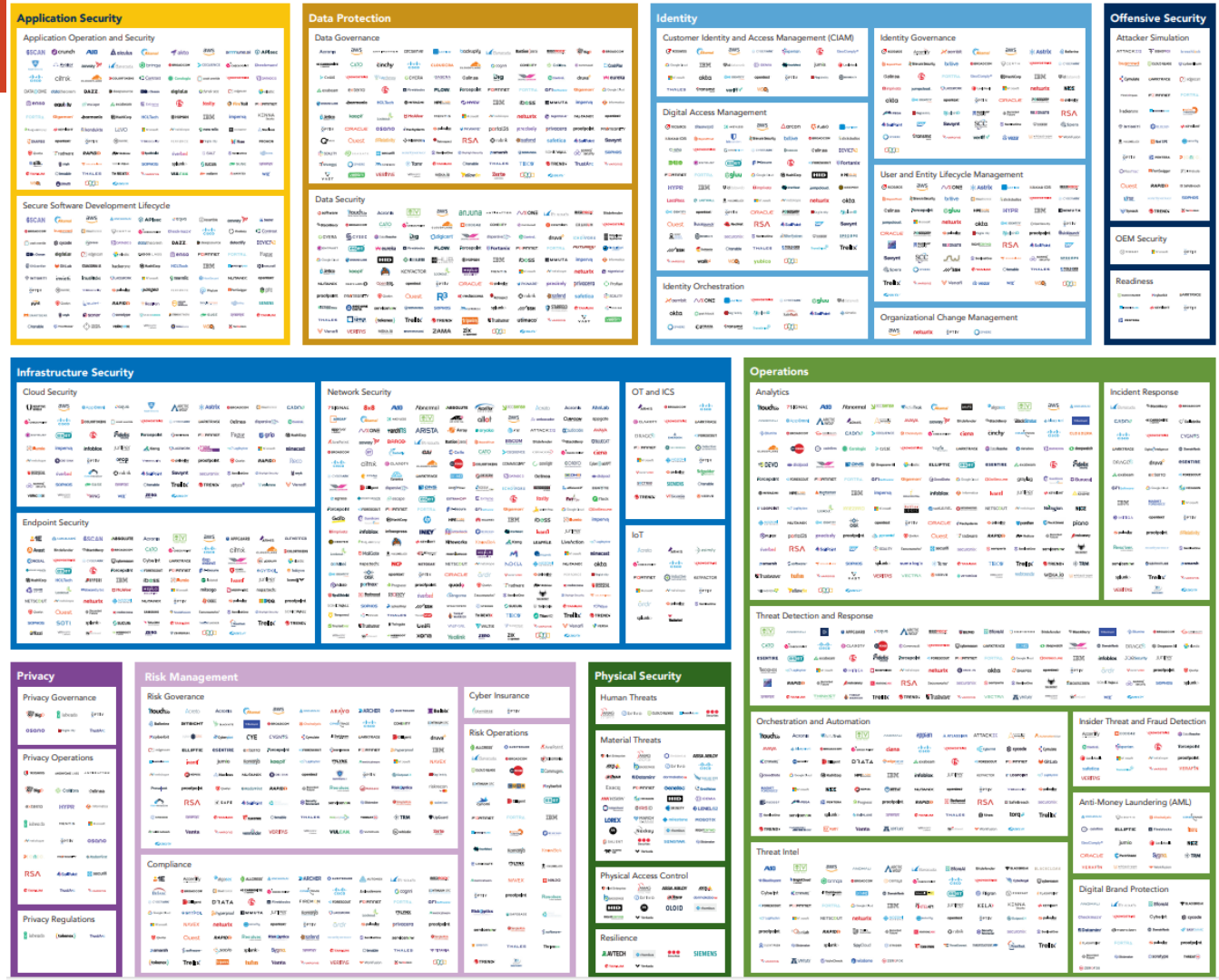
Sicurezza informatica: tecnologie

Mercato maturo, offerta enorme.

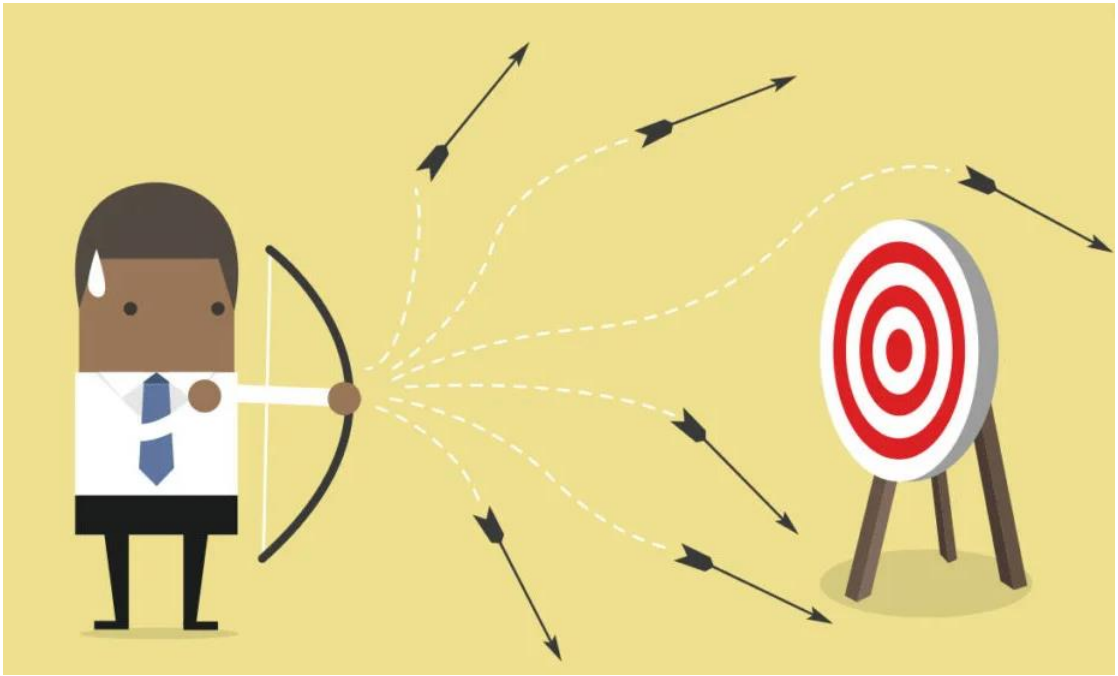
Problema risolto?

Fonte: Optive Cybersecurity Landscape Map

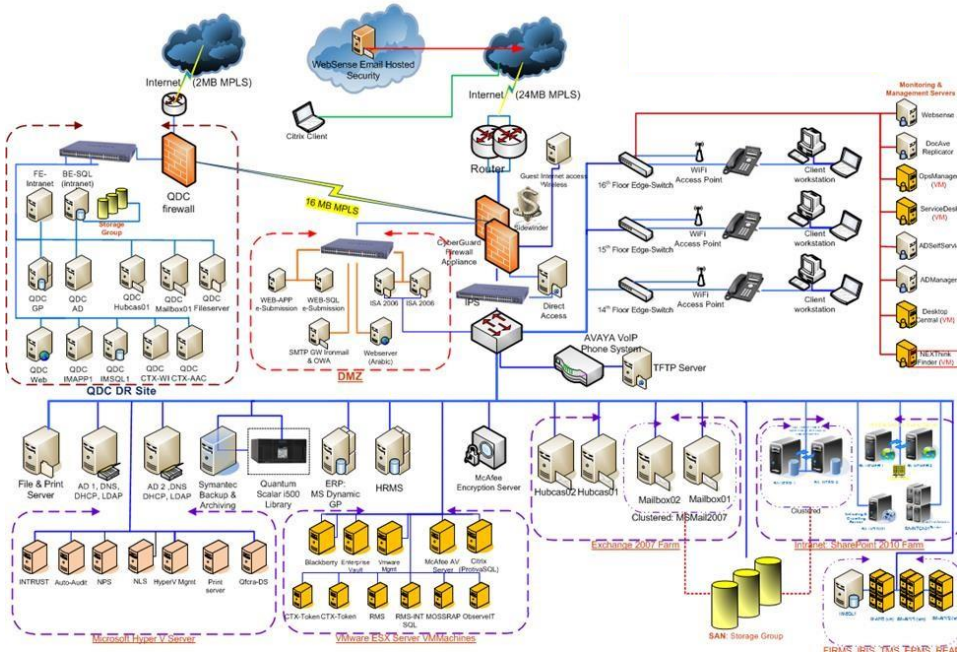
https://www.optiv.com/sites/default/files/2024-07/Cybersecurity-Landscape-Map-2024.pdf



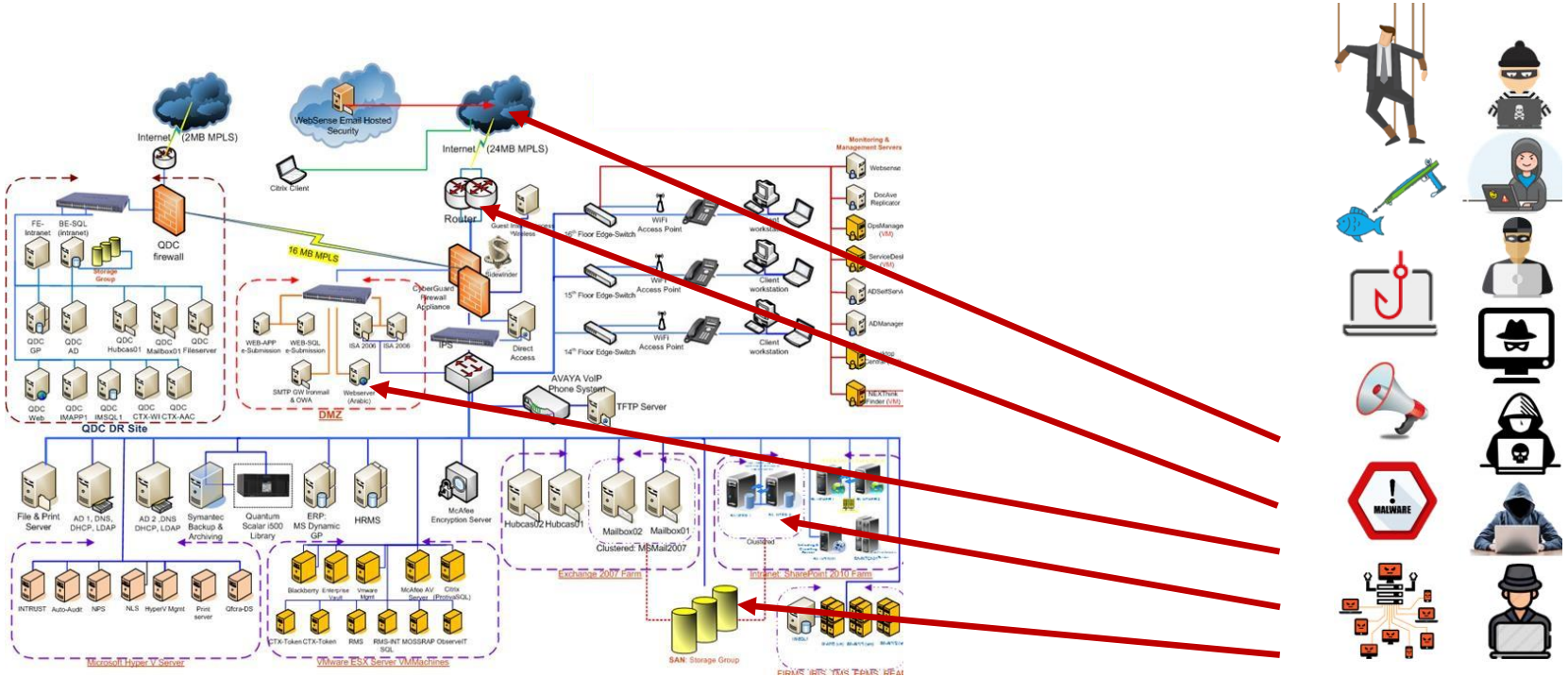
Cybersecurity:
non si tratta (solo) di tecnologie



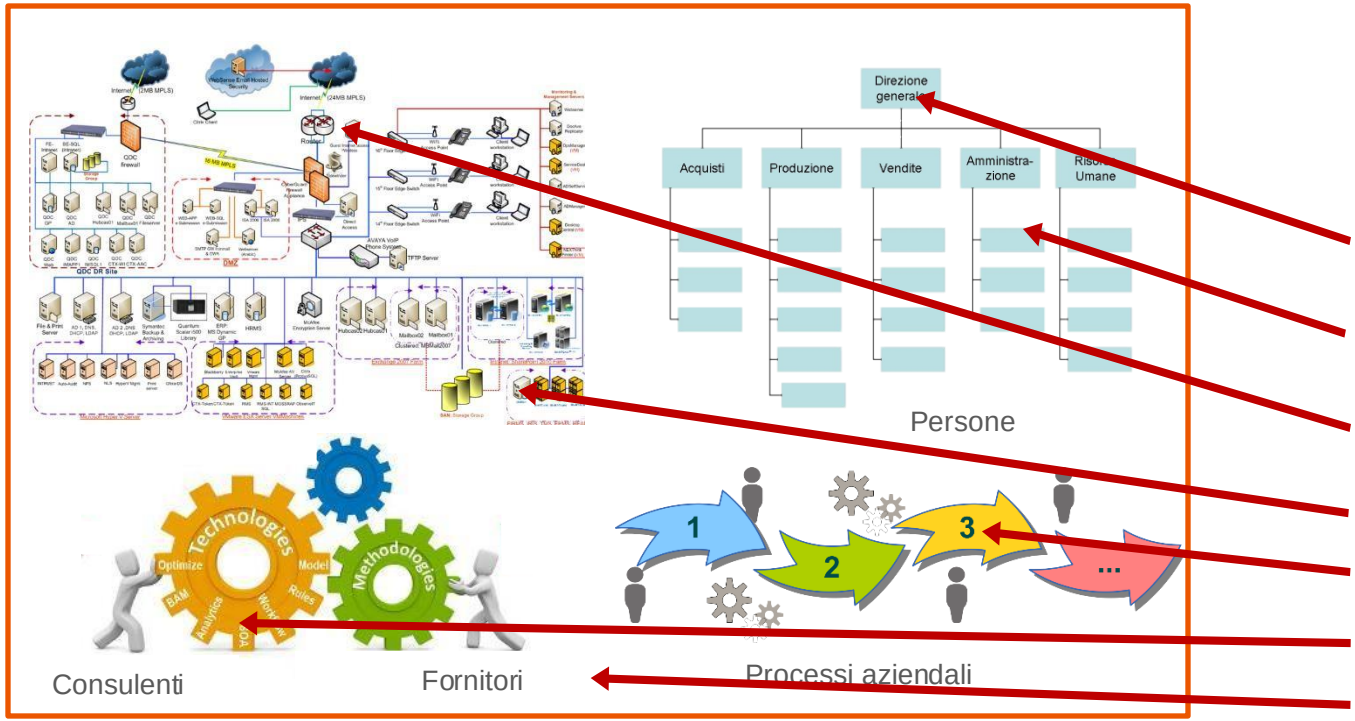
L'azienda vista da un tecnico

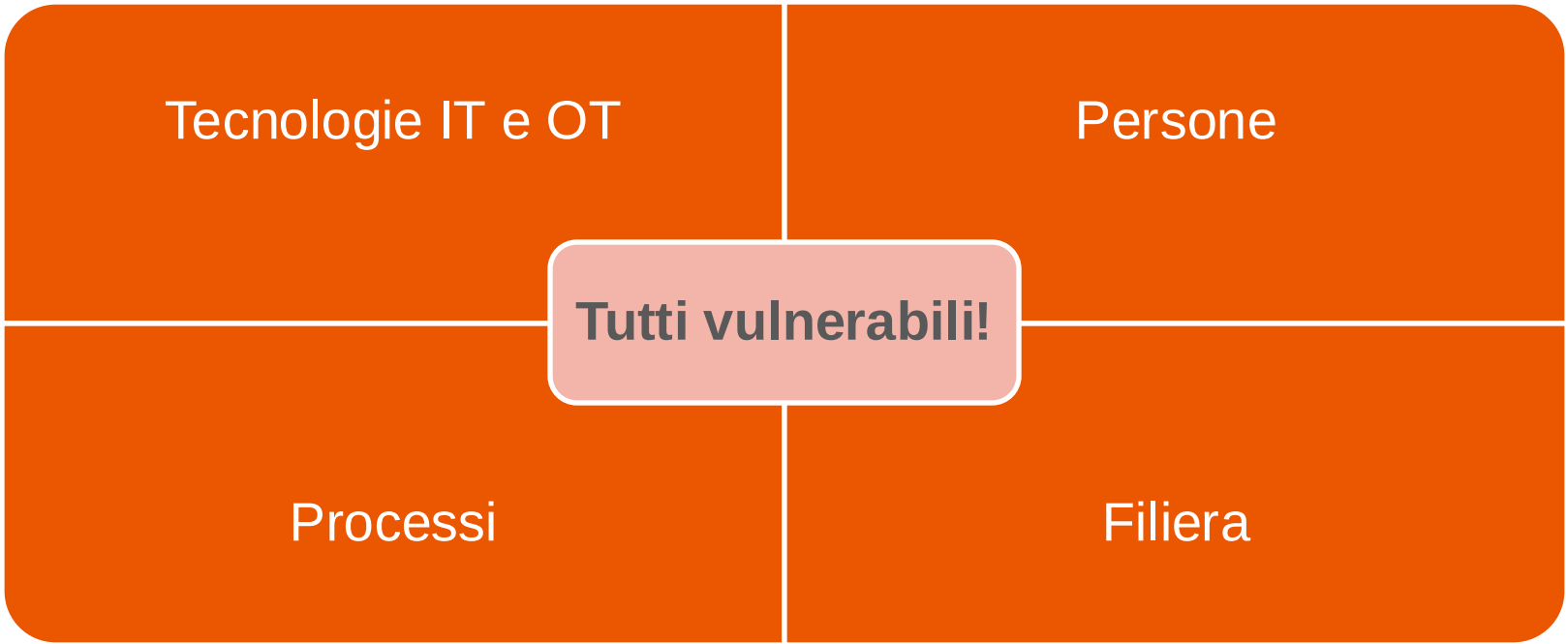


Gli attacchi informatici visti da un tecnico



Una visione più completa…




Tecnologie IT e OT
Persone
Tutti vulnerabili!
Processi
Filiera

Tecnologie a supporto

Le tecnologie sono utili per **applicare** politiche e procedure

- NON possono **sostituire** politiche e procedure
- Politiche e procedure non possono essere definite da tecnici

E quindi, chi le definisce? Il management aziendale!

- … aiutato da fornitori e consulenti …
- … in conformità con vincoli legali, regolamentari e standard …
- … entro limiti di budget …

Princìpi di cybersecurity management

Si parte dall'analisi dei rischi

- Alcuni sono comuni
- Altri sono specifici

Per identificare i rischi specifici occorre

- Sapere quali sono gli asset aziendali
- Conoscerne le vulnerabilità
- Conoscere le minacce

Princìpi di cybersecurity management

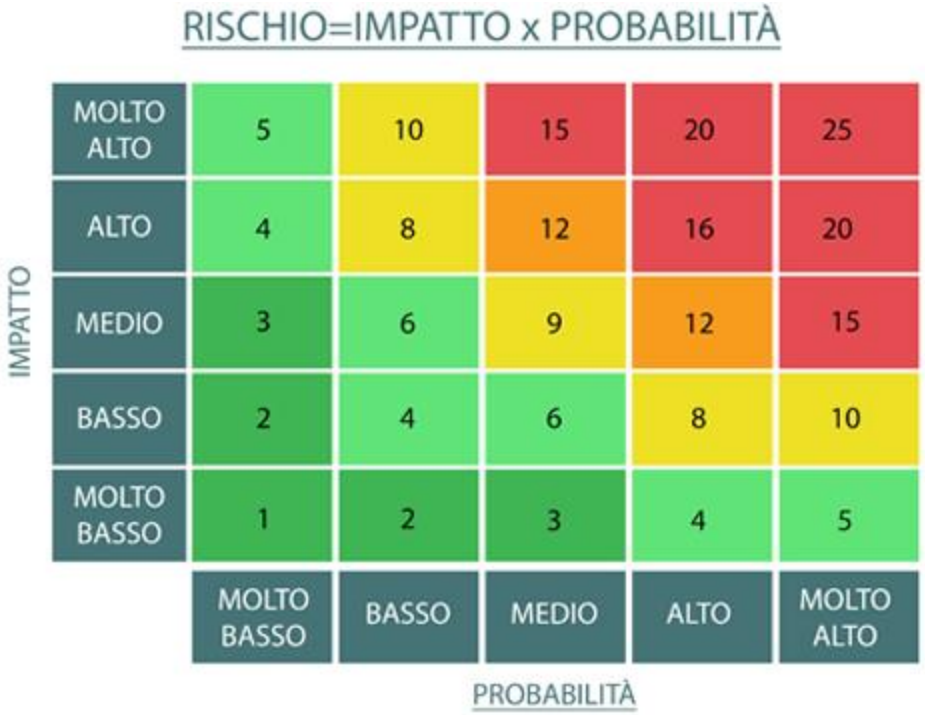
Non tutti i rischi sono uguali

- Cambia l'impatto
- Cambia la probabilità di accadimento

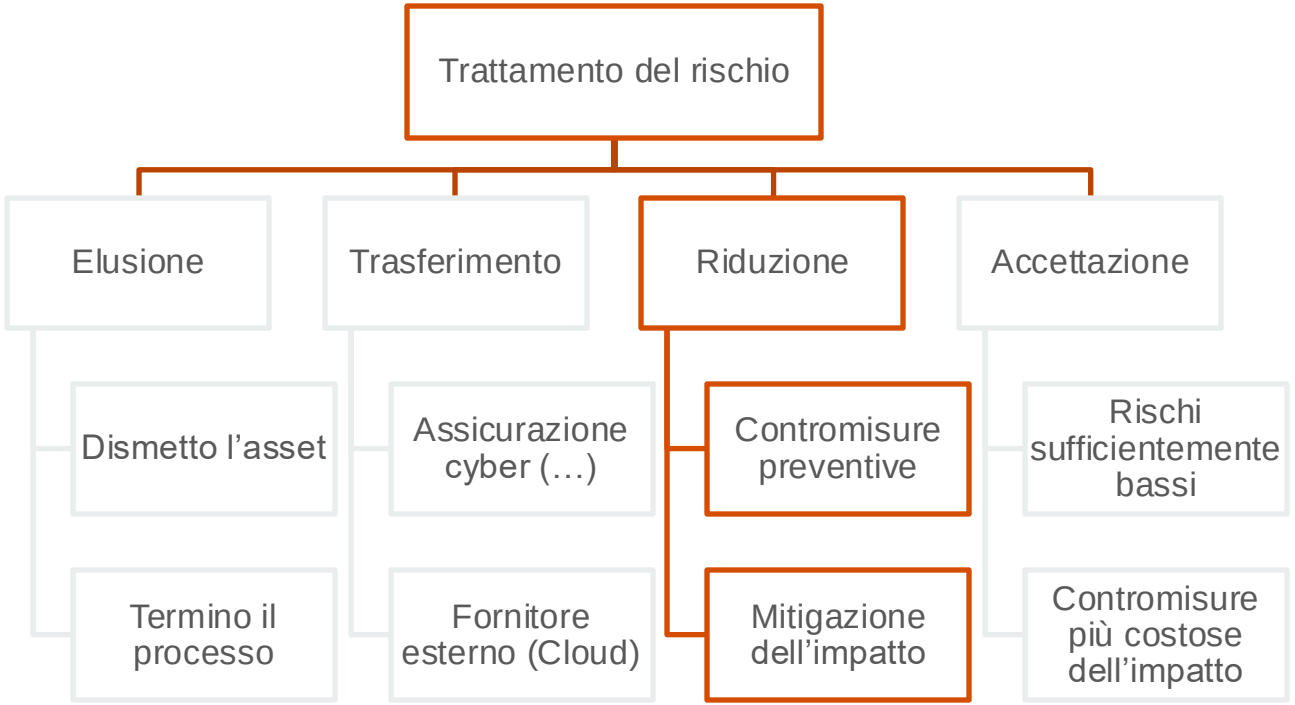
Come misuro l'impatto?

- Sarebbe bello poterlo misurare in €
- … ci accontentiamo di una analisi qualitativa

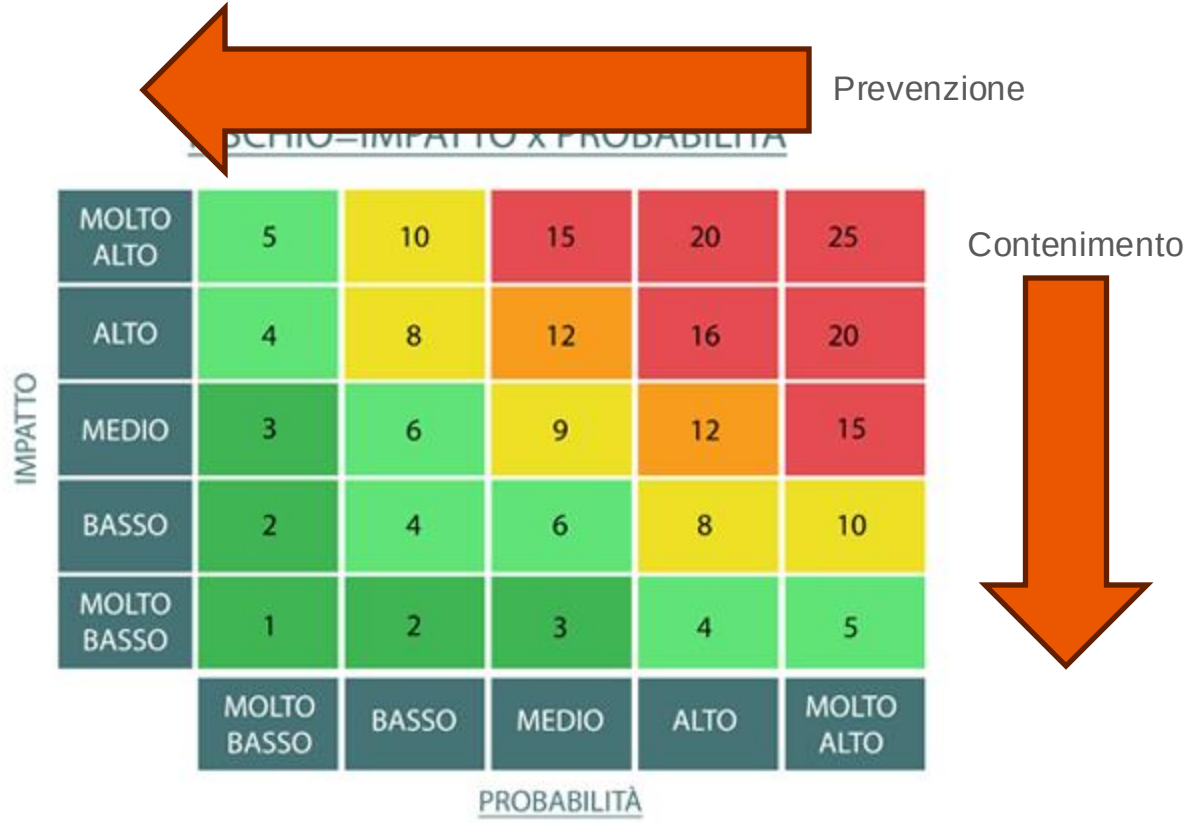
E poi?



Il ruolo delle tecnologie cyber



Princìpi di cybersecurity management



E non tutte le contromisure sono tecnologiche!

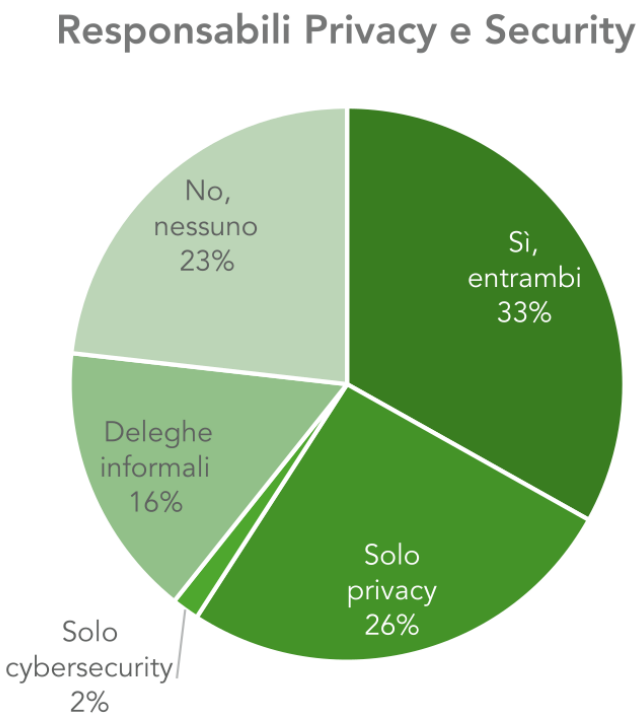
Non esistono contromisure puramente tecnologiche, esistono contromisure non tecnologiche!

- Riduzione dell'impatto del phishing → formazione!
- Riduzione dell'impatto dei «CEO Scam» → formazione + procedure!
- Riduzione dell'impatto di un malware? → formazione + minimizzazione dei privilegi!

Anche le contromisure prevalentemente tecnologiche sono dei **progetti** non dei prodotti. Devono essere gestiti, manutenuti, verificati periodicamente. Devono avere un budget e un responsabile.

- Backup → definizione di RPO e RTO, prove periodiche di ripristino, …
- Next Generation FireWall → definizione delle politiche di filtro, delle eccezioni, delle regole di accesso in VPN, …
- Identity Access Management → definizione dei ruoli, delle regole di autorizzazione, delle regole di autenticazione, dei requisiti di accounting, …

Alcuni problemi…

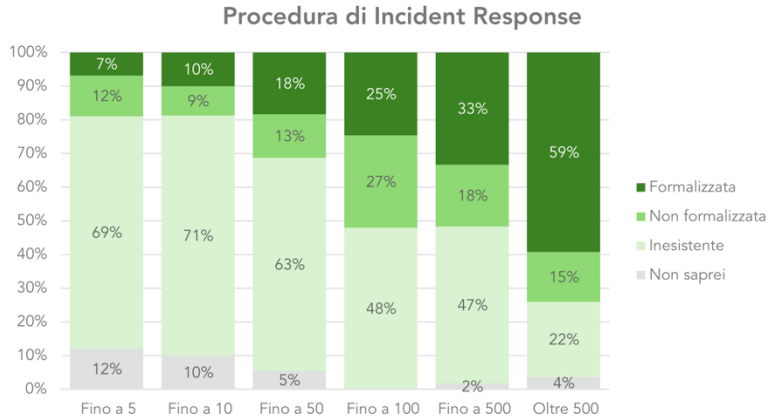


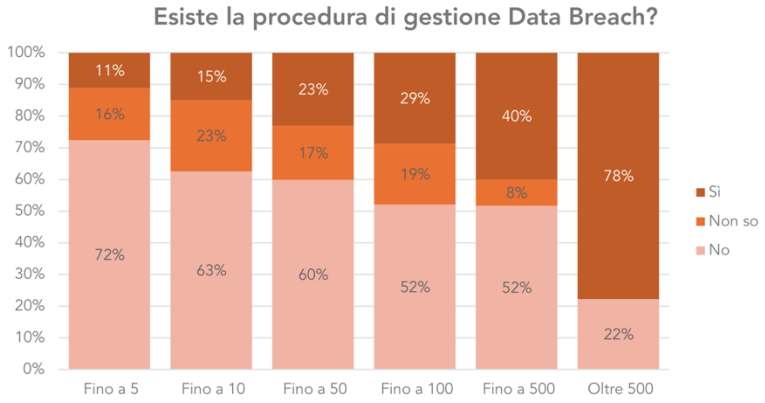
Nelle microimprese, nel 72% dei casi non c'è alcuna persona dedicata alla cybersecurity

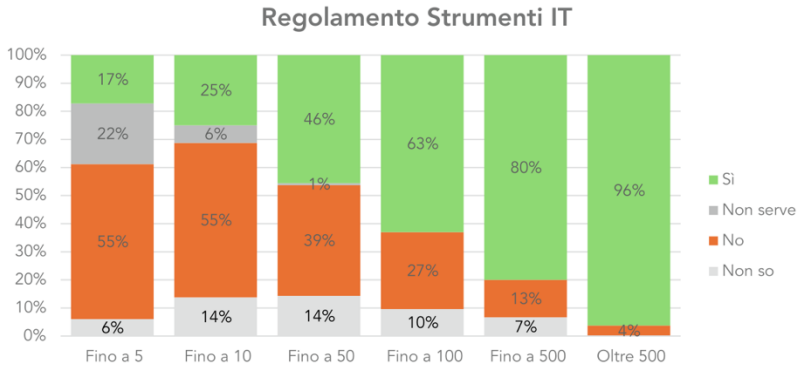
Nelle realtà più grandi in circa 1/3 dei casi non c'è alcuna delega formale (e in 1/4 dei casi la delega è solo per la privacy);

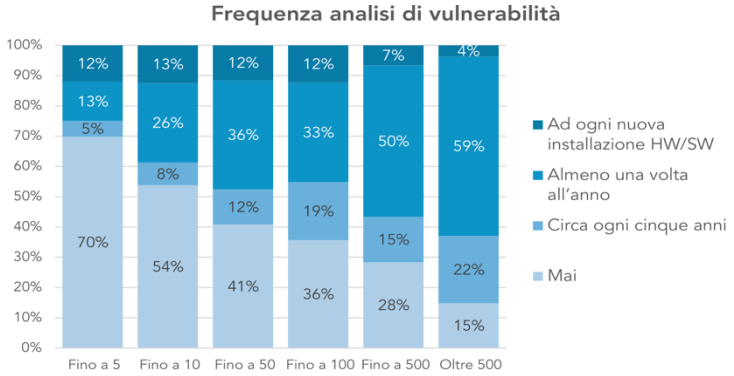
Solo nel 17% dei casi queste persone hanno ricevuto una formazione certificata sui temi di cui sono incaricate di occuparsi.

Alcuni problemi…









Nuove iniziative di formazione

Corso di perfezionamento Penetration Tester
Corso base

Data inizio:	primavera 2026
Durata:	40 ore
Erogazione:	online
Programma:	Ciclo di vita di una attività di VAPT (contratto, attività operative, report). Svolgimento di una attività realistica di VAPT su un laboratorio di 20 macchine (GNU/Linux, Windows, BSD UNIX).
Valutazione:	Produzione di un report di attività.
Prerequisiti:	Diploma di scuola secondaria superiore.

Corso di perfezionamento Penetration Tester
Corso avanzato

Data inizio:	autunno 2025
Durata:	40 ore
Erogazione:	online
Programma:	Svolgimento di una attività realistica di VAPT su un laboratorio di 30 macchine (GNU/Linux, Windows, BSD UNIX). Focus: enumerazione Active Directory, Evasione difese, persistenza.
Valutazione:	Produzione di un report di attività.
Prerequisiti:	Esperienza pregressa in cyber security.

Rischi cyber e come difendersi: migliorare la sicurezza delle imprese

Corso in presenza (Modena), quattro tematiche principali - lezioni in quattro fine settimana tra settembre e novembre 2025

L’importanza delle persone per la cybersecurity	La gestione della cybersecurity in azienda
Le tecnologie per la cybersecurity	Gestire la compliance in azienda: rischi e opportunità

Rischi cyber e come difendersi: migliorare la sicurezza delle imprese

Corso in presenza (Modena), quattro tematiche principali - lezioni in quattro fine settimana tra settembre e novembre 2025

L'importanza delle persone per la cybersecurity

- Comportamenti a rischio del personale aziendale
- Le attività dei social engineer
- Testimonianze di aziende che hanno subito attacchi mediante ingegneria sociale
- Progetto e valutazione di campagne di formazione

Le tecnologie per la cybersecurity

Rischi cyber e come difendersi: migliorare la sicurezza delle imprese

Corso in presenza (Modena), quattro tematiche principali - lezioni in quattro fine settimana tra settembre e novembre 2025

Concetti fondamentali di cybersecurity management e business continuity

Testimonianze di CISO provenienti da aziende

Esercizio guidato di cybersecurity management

La gestione della cybersecurity in azienda

Gestire la compliance in azienda: rischi e opportunità

Rischi cyber e come difendersi: migliorare la sicurezza delle imprese

Corso in presenza (Modena), quattro tematiche principali - lezioni in quattro fine settimana tra settembre e novembre 2025

L'importanza delle persone per la cybersecurity

Le tecnologie per la cybersecurity

Analisi delle principali soluzioni tecnologiche: cosa possono e **non** possono fare

Focus su backup e security monitoring

Rischi cyber e come difendersi: migliorare la sicurezza delle imprese

Corso in presenza (Modena), quattro tematiche principali - lezioni in quattro fine settimana tra settembre e novembre 2025

Responsabilità in capo al personale aziendale

NIS2

GDPR

Gestione della catena di fornitura

La gestione della cybersecurity in azienda

Gestire la compliance in azienda: rischi e opportunità

Contatti e ulteriori informazioni

mirco.marchetti@unimore.it
mauro.andreolini@unimore.it

Le iniziative di formazione saranno presto pubblicate su **cyber.unimore.it**