UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA

CAMERA DI COMMERCIO MODENA

Clusit
Associazione Italiana per la Sicurezza Informatica

Attacchi informatici alle aziende modenesi

15:00 - Saluti istituzionali

Giuseppe Molinari – Presidente della Camera di Commercio di Modena
Luca Chiantore – Direttore Generale UniMoRe
Il ruolo della Camera di Commercio e di UniMoRe nella ricerca
Federica Venturelli – Assessora, Comune di Modena

La criminalità informatica oggi

Raffaele Grassi – Vice Capo della Polizia, Direttore Centrale della Polizia Criminale
Ivano Gabrielli – Direttore Nazionale della Polizia Postale e della Sicurezza Cibernetica
Luca Masini – Procuratore della Repubblica di Modena

Analisi della ricerca della Camera di Commercio e di UniMoRe in collaborazione con il Clusit

Mauro Cicognini – Comitato tecnico del Clusit: *Presentazione del rapporto Clusit*
Antonio Apruzzese – Dipartimento di Scienze Fisiche, Informatiche e Matematiche di UniMoRe: *Focus sul quadro emerso dalla ricerca*

Testimonianze aziendali

Paolo Boni – Amministratore Delegato INALCA S.p.A., Gruppo Cremonini
Andrea Ruscitti – Responsabile IT IRIS Ceramica Group
Difendersi e prevenire attacchi informatici

La cultura della sicurezza informatica

Mauro Andreolini – Dipartimento di Scienze Fisiche, Informatiche e di UniMoRe: *Una PMI vista da un attaccante informatico*
Mirco Marchetti – Dipartimento di Ingegneria "Enzo Ferrari" di UniMoRe: *Cenni di cybersecurity management per PMI. Riflessioni sulla ricerca svolta.*

19:00 - Conclusioni

A seguire aperitivo di networking

Modera Beppe Boni, editorialista e già Condirettore de *Il Resto del Carlino*

Sicurezza informatica in azienda: le tecnologie non bastano

Prof. Mirco Marchetti
Dipartimento di Ingegneria «Enzo Ferrari»
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

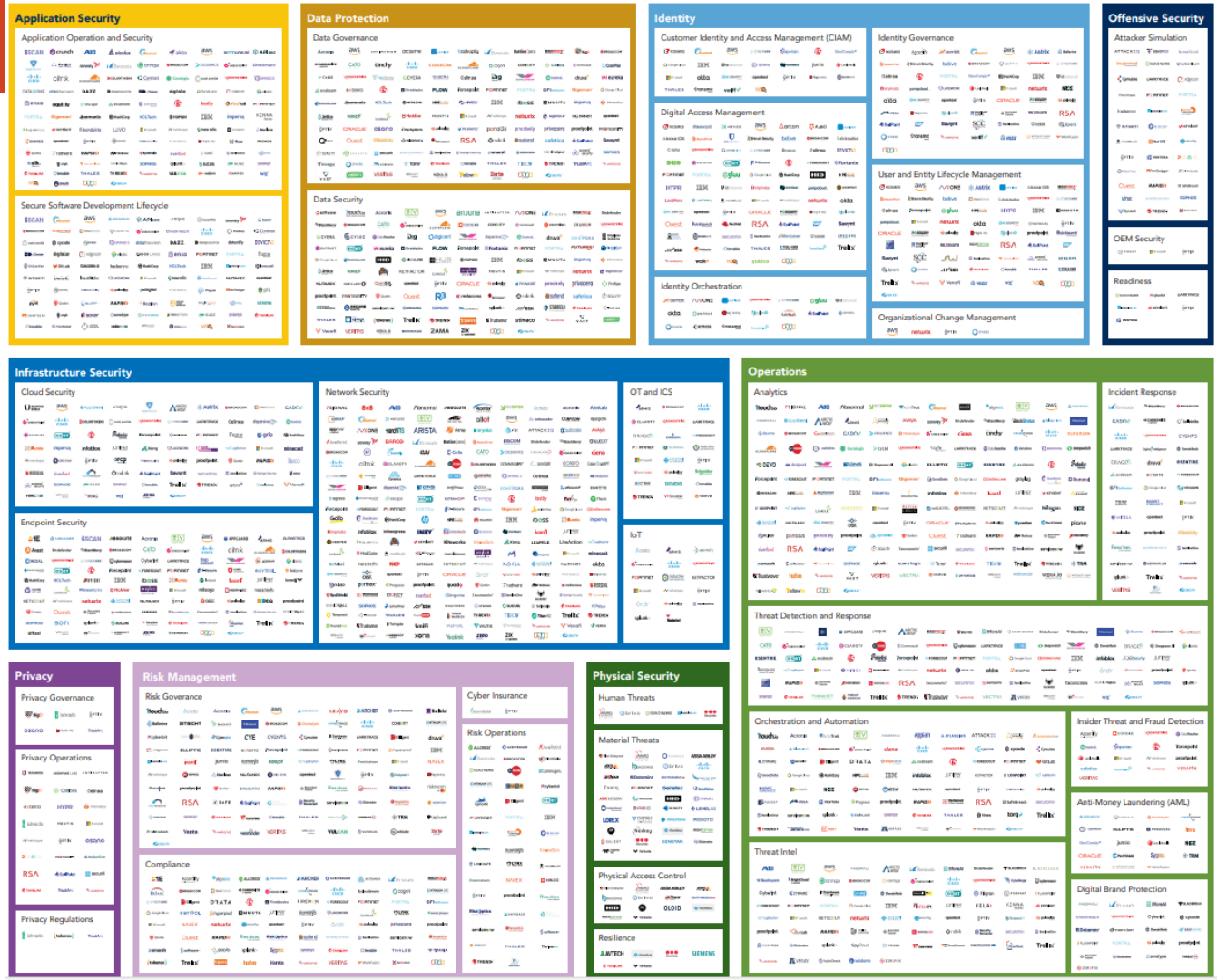
Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

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



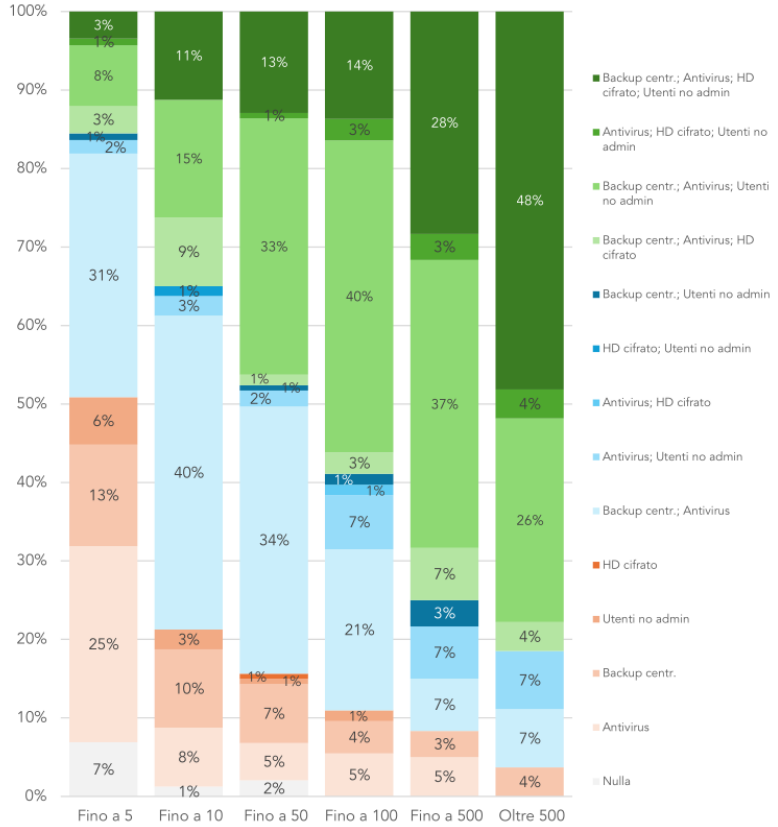
Tecnologie per la sicurezza: molto diffuse

Aziende prive di tecnologie specifiche

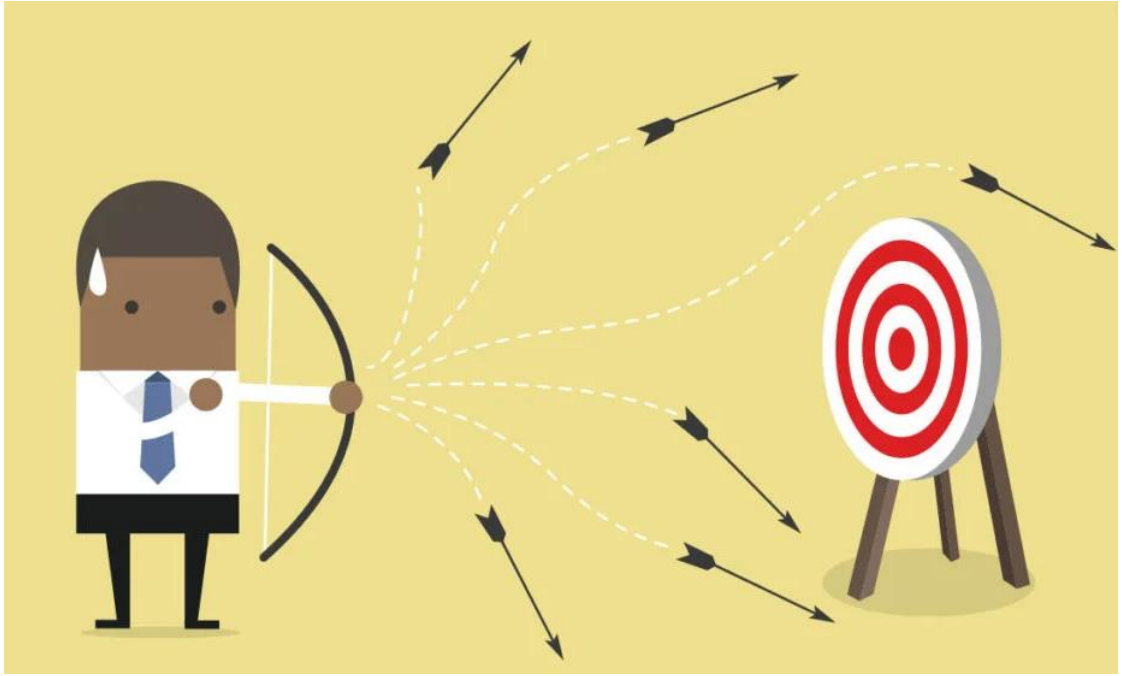
- 7% delle aziende con meno di 5 dipendenti
- 1% delle aziende tra 5 e 10 dipendenti
- 2% delle aziende tra 10 e 50 dipendenti

Tutte le altre hanno almeno qualche soluzione di base. Molte hanno soluzioni avanzate.

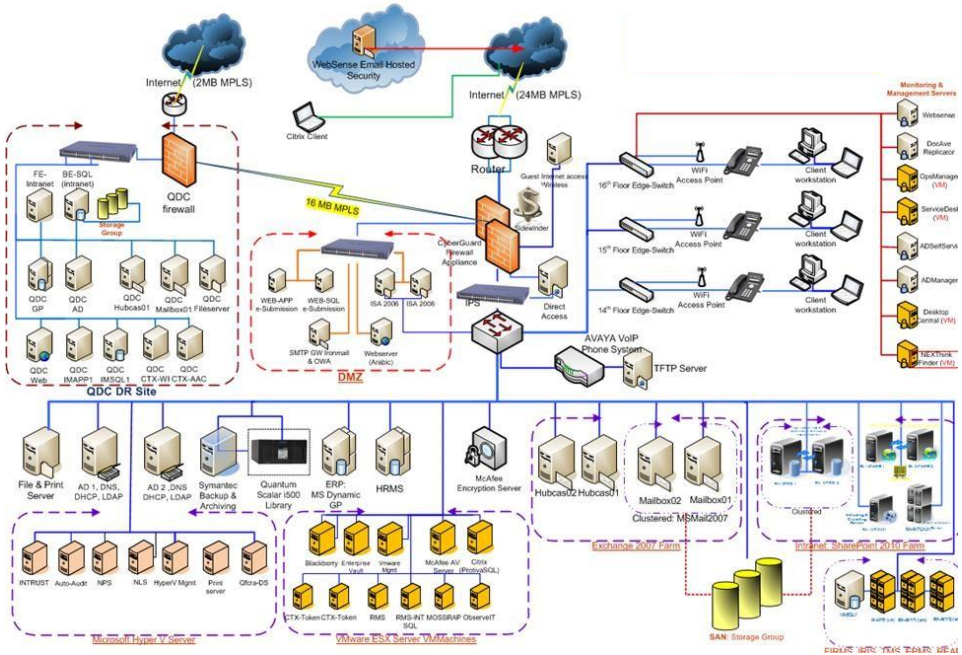
Problema risolto?



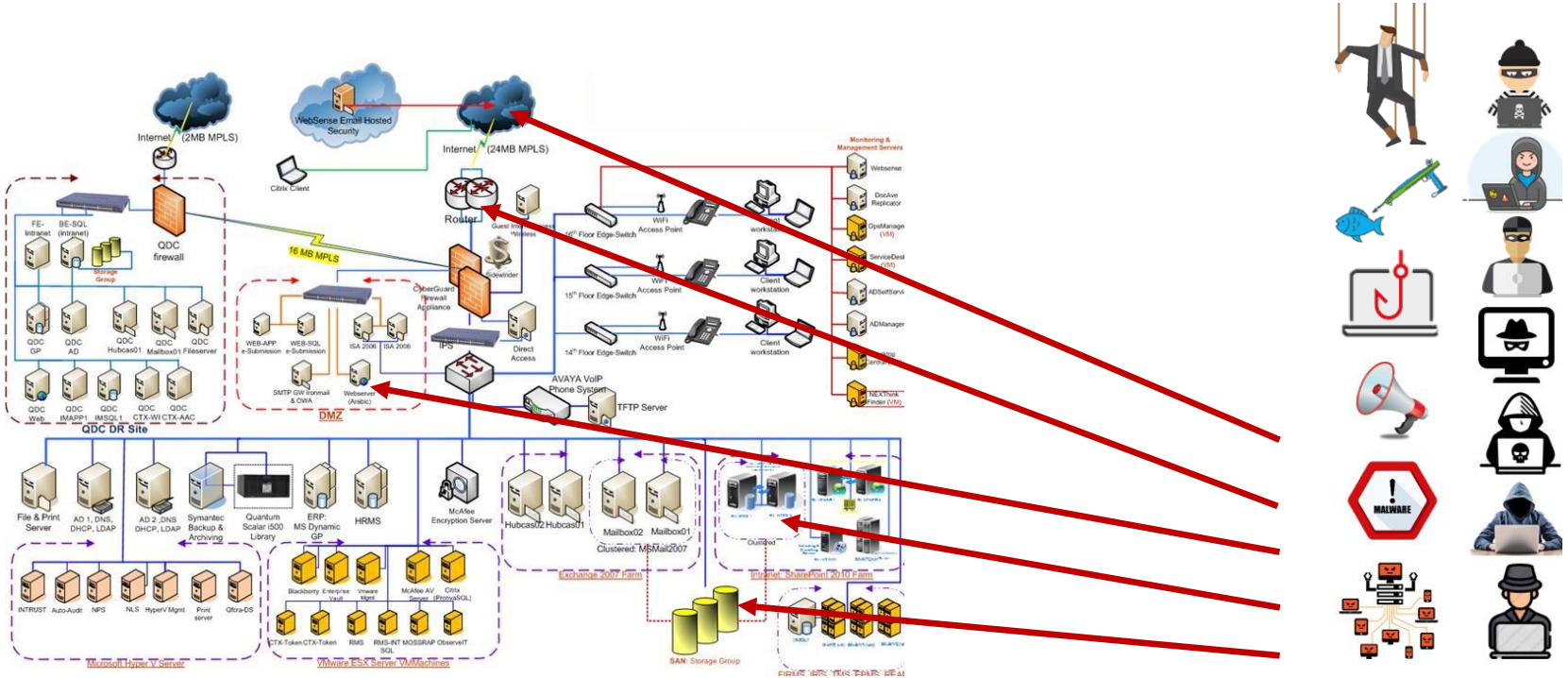
Cybersecurity:
non si tratta (solo) di tecnologie



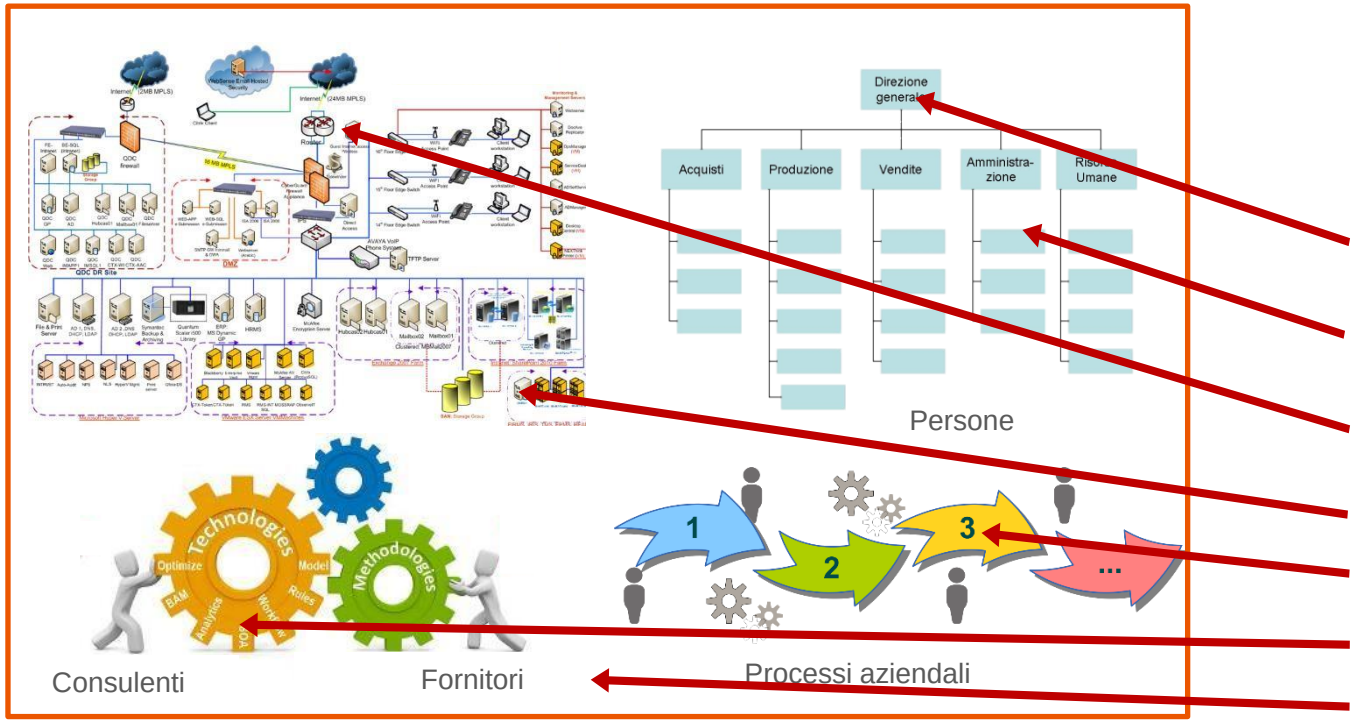
L'azienda vista da un tecnico

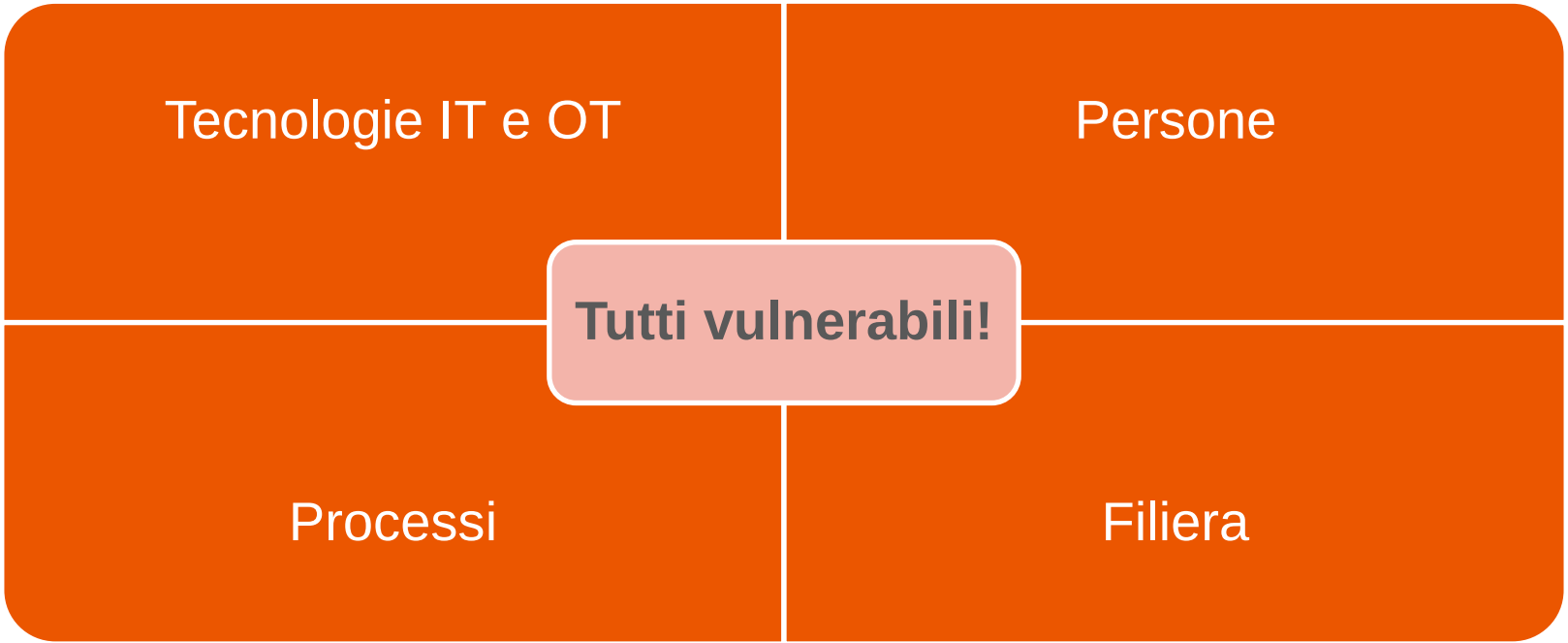


Gli attacchi informatici visti da un tecnico



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

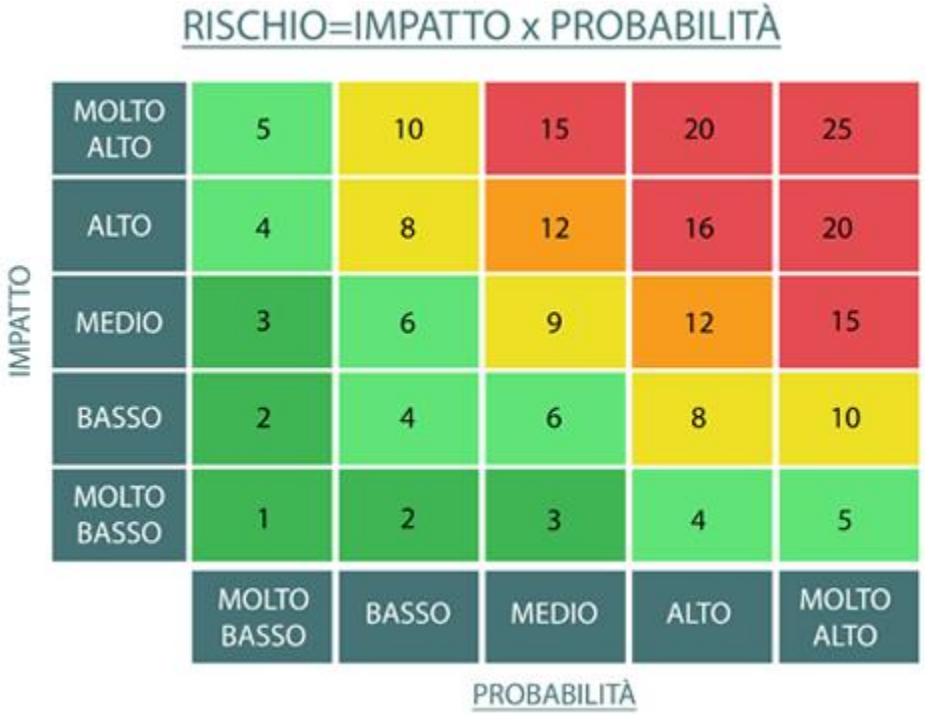
- Sapere quali sono gli asset aziendali
- Conoscerne le vulnerabilità
- Conoscere le minacce

Princìpi di cybersecurity management

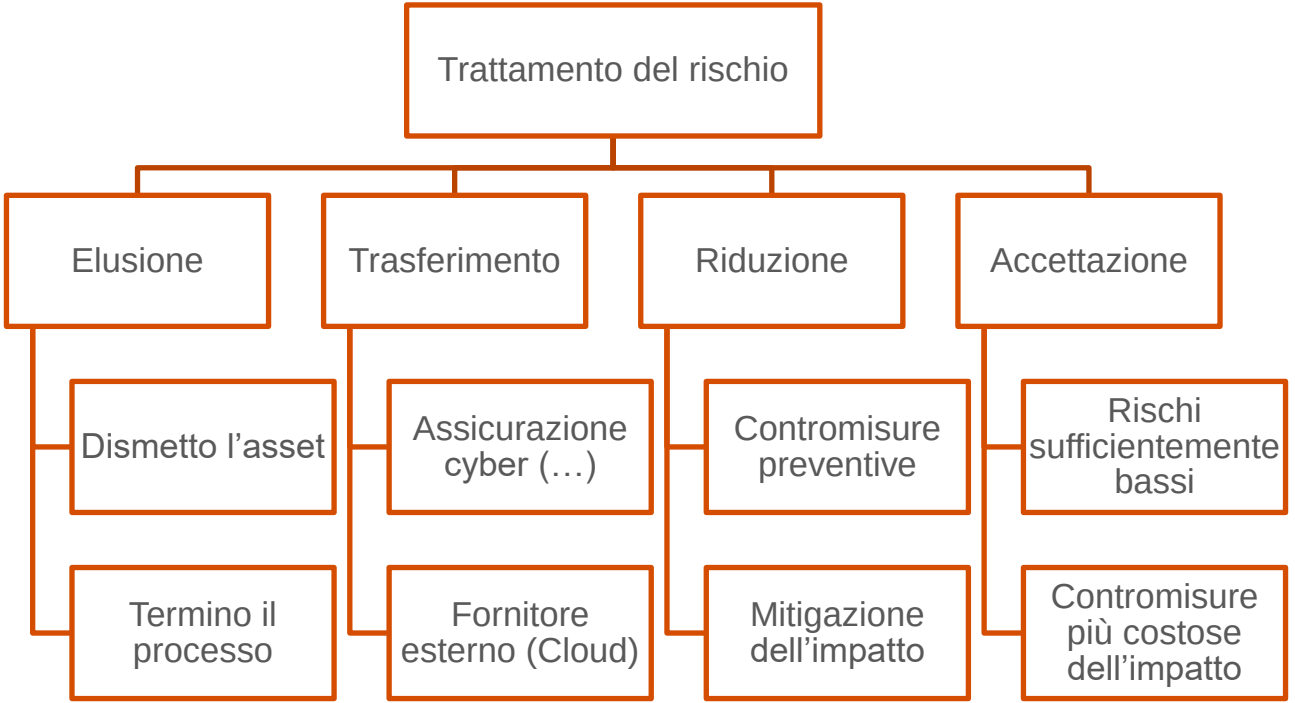
Non tutti i rischi sono uguali
- Cambia l'impatto
- Cambia la probabilità di accadimento

Come misuro l'impatto?
- Sarebbe bello poterlo misurare in €
- … ci accontentiamo di una analisi qualitativa

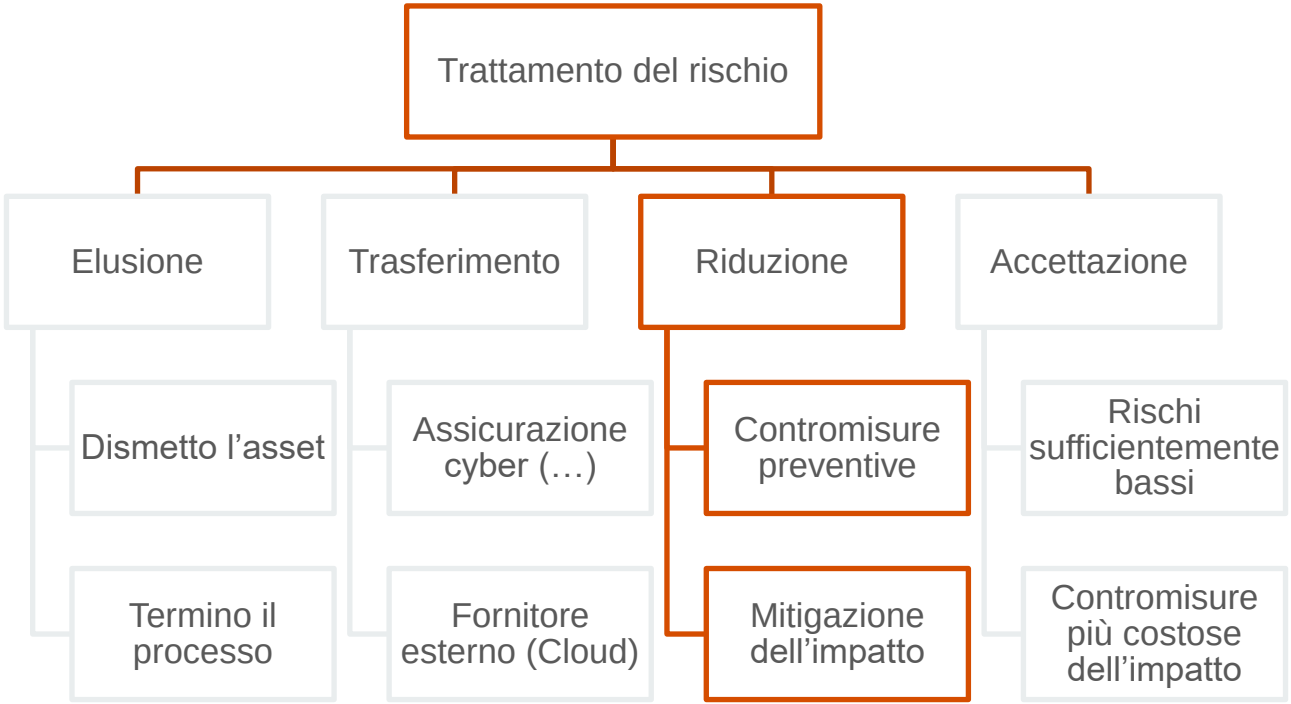
E poi?



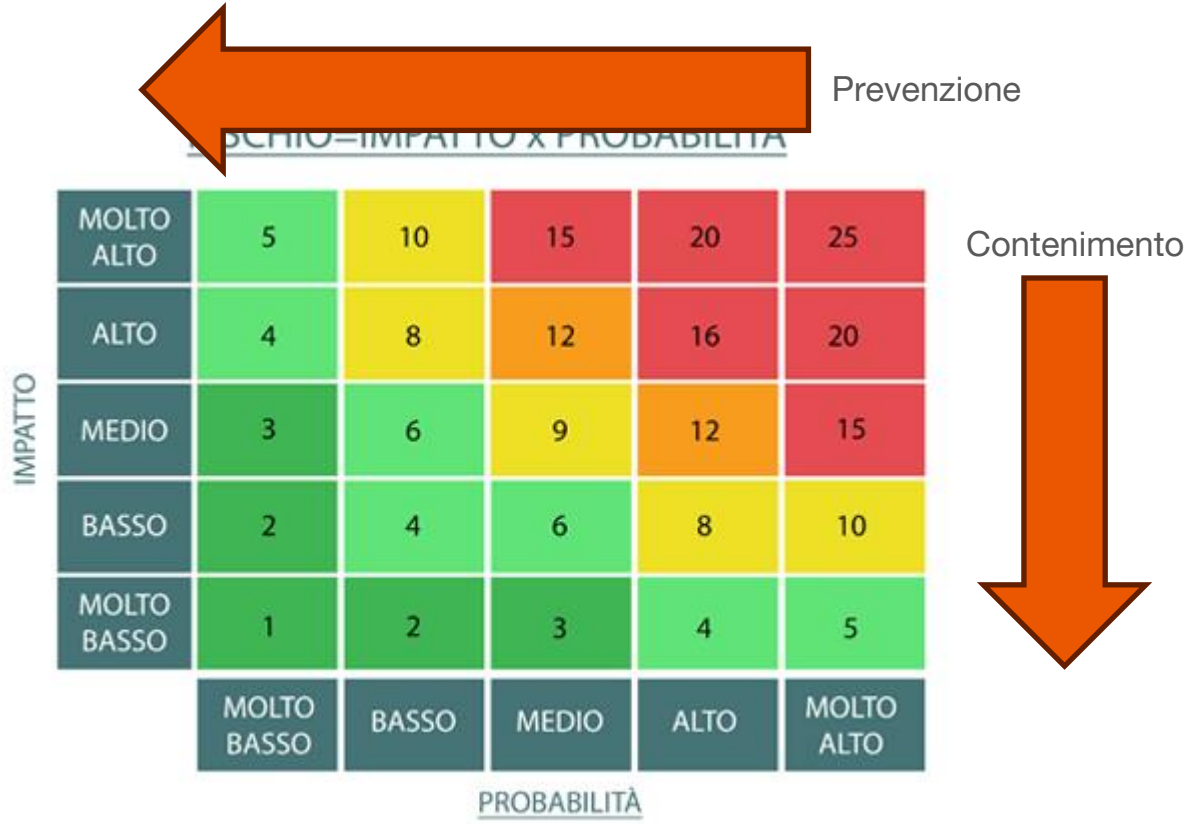
Princìpi di cybersecurity management



Il ruolo delle tecnologie cyber



Princìpi di cybersecurity management



E non tutte le contromisure sono tecnologiche!

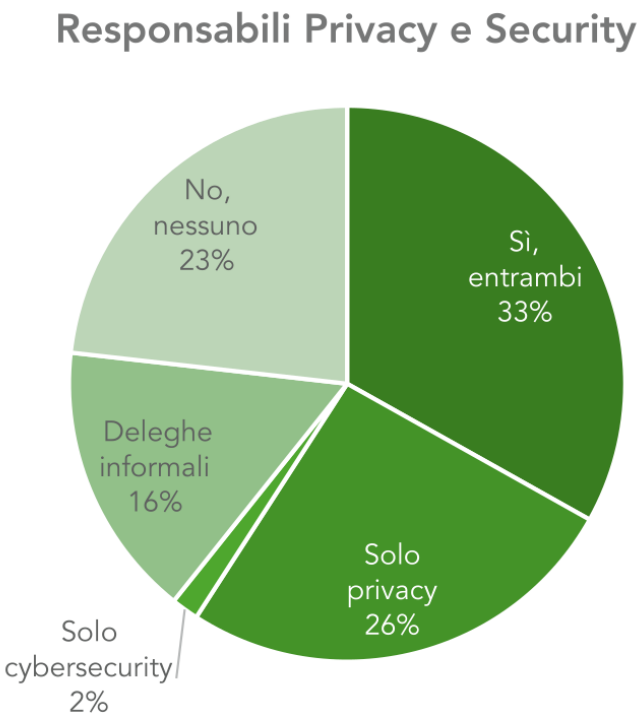
Non esistono contromisure puramente tecnologiche, esistono contromisure non tecnologiche!

- 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.

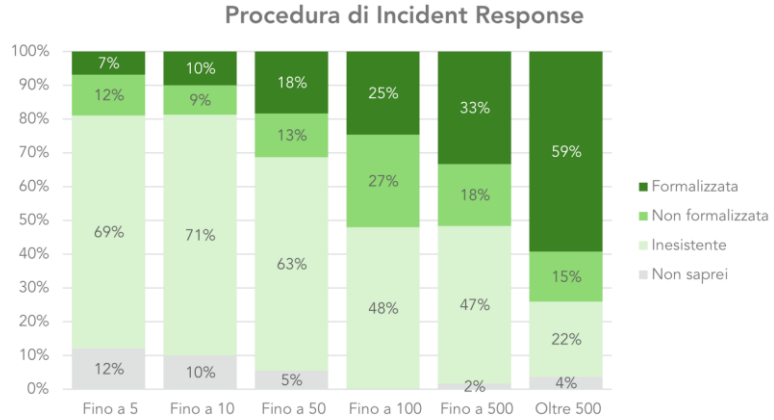
- Backup → definizione di RPO e RTO, prove periodiche di ripristino, …
- Next Generation FireWall → definizione delle politiche di filtro, delle eccezioni, delle regole di accesso in VPN, …
- Identity Access Management → definizione dei ruoli, delle regole di autorizzazione, delle regole di autenticazione,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

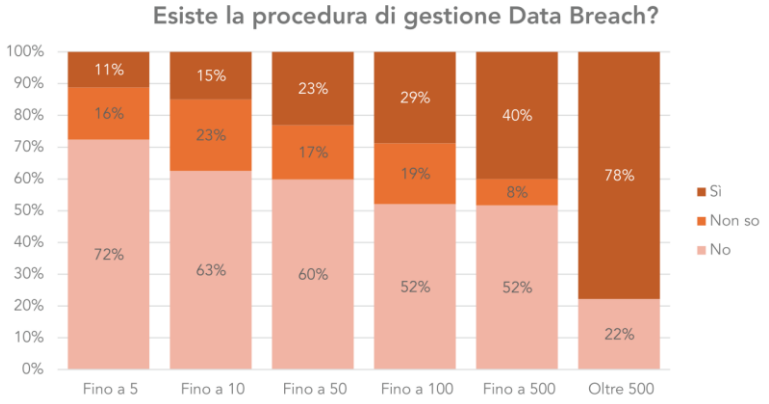
Alcuni problemi…

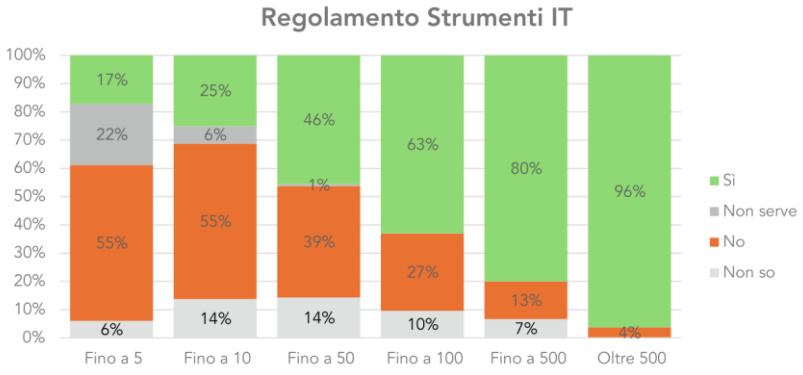


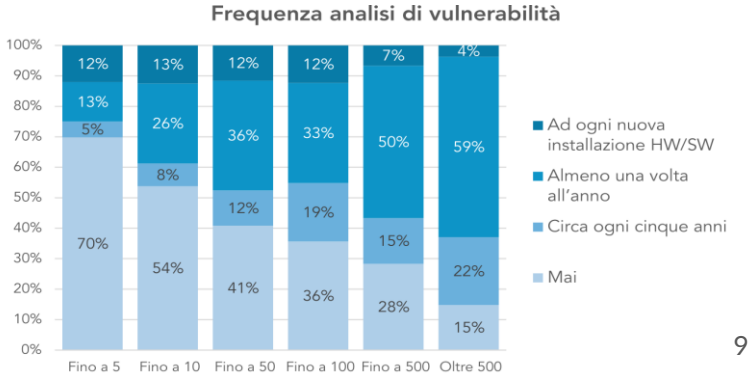
Nelle microimprese, infatti, nel 72% dei casi non c'è alcuna persona dedicata alla cybersecurity; ma anche nelle realtà più grandi in circa 1/3 dei casi non c'è alcuna delega formale (e in 1/4 dei casi la delega è solo per la privacy); e solo in circa il 17% dei casi queste persone hanno ricevuto una formazione certificata sui temi di cui sono incaricate di occuparsi.

Alcuni problemi…









Tre messaggi

Non possiamo «fare tutto noi», ma non possiamo delegare tutto ai tecnici!

Non ci si salva da soli… Per contrastare un ecosistema criminale serve un ecosistema sano: aziende, istituzioni, esperti, **fiducia**

Non ci si salva da soli… Supply chain, norme, regolamenti

Cybersecurity for Smart Industry (C4SI)

UNIMORE
UNIVERSITÀ DEGLI STUDI DI MODENA E REGGIO EMILIA
Centro di Ricerca Interdipartimentale sulla Sicurezza e Prevenzione dei Rischi - CRIS

ALMA MATER STUDIORUM
UNIVERSITÀ DI BOLOGNA
CENTRO INTERDIPARTIMENTALE DI RICERCA INDUSTRIALE ICT

Università degli Studi di Ferrara
IN4 innovazione ingegneria integrazione industria

crit
SCOUTING YOUR NEXT TECHNOLOGY

SACMI

IMA SPA

VEM sistemi

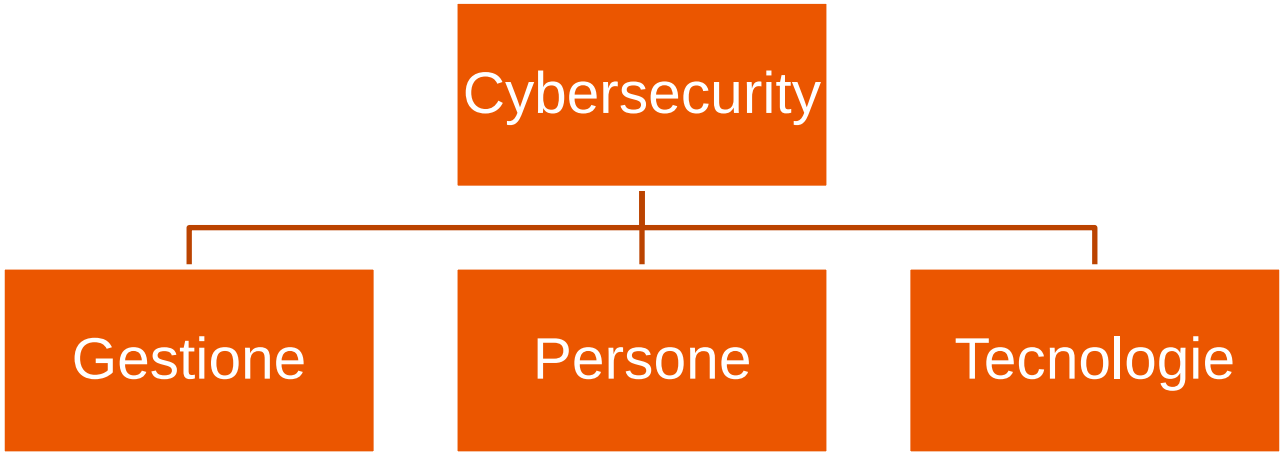
COESIONE ITALIA 21-27
EMILIA-ROMAGNA

Cofinanziato dall'Unione europea

Regione Emilia-Romagna

Formazione continua

Tre minicorsi (venerdì pomeriggio/sabato) progettati per le PMI del nostro territorio in collaborazione con esperti aziendali, erogati nell'arco del 2025.



Per informazioni e aggiornamenti: http://cyber.unimore.it e mirco.marchetti@unimore.it