Mercoledì 12 Luglio 2023

J.M. Consulting S.r.l.

WEBINAR

“PER UNA CORRETTA DIGITAL TRANSFORMATION CI VUOLE UN’INFRASTRUTTURA SISTEMISTICA SICURA”

VULNERABILITY ASSESSMENT & PENETRATION TEST

J.M. Consulting S.r.l.

Relatore

GIOVANNI BERTONI

SALES MANAGER
IT SERVICE
di J.M. Consulting S.r.l.

INFORMAZIONI SUL WEBINAR:

Durante il webinar:

Sarà possibile fare domande nell'apposita sezione della piattaforma a cui risponderemo via mail.

Dopo il webinar:

Riceverete una mail per accedere al materiale:

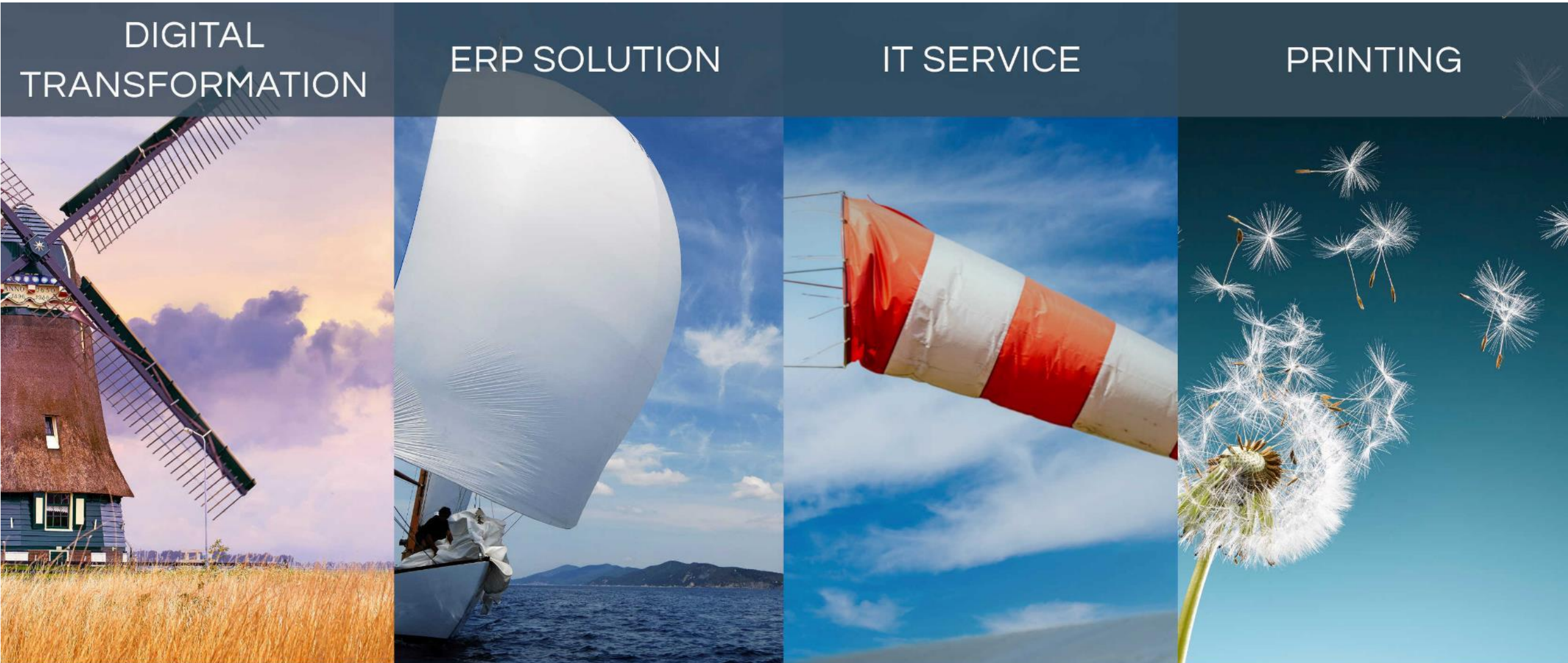
- ✓ PRESENTAZIONE
- ✓ VIDEO

J.M. Consulting S.r.l.

SEDE:
Via Donatori Sangue 3,
29020 Gossolengo (PC)

Di cosa ci occupiamo?

4 BUSINESS UNIT:



SCENARIO

LA DIGITAL TRASFORMATION:

- opportunità di crescita
- efficienza dei processi aziendali

Ma anche...

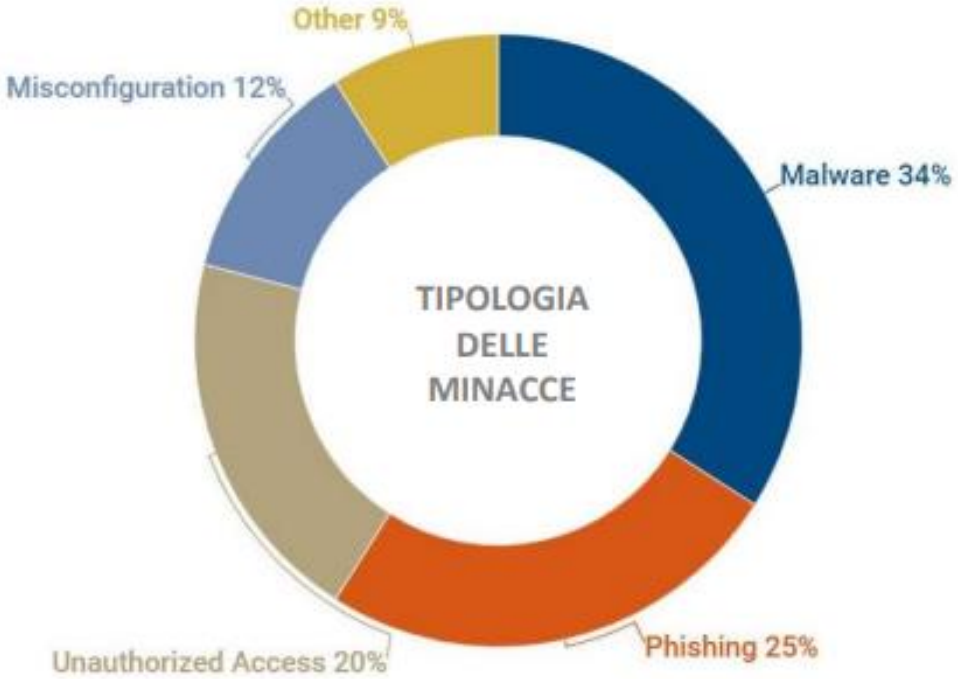
- maggiori rischi
- impatti in caso di danno informatico

MA QUALI SONO I RISCHI INFORMATICI?

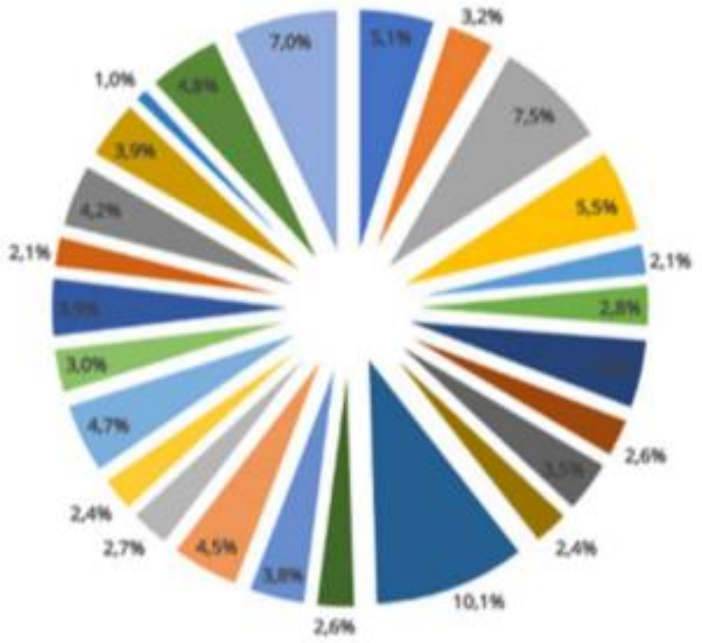
PERCHÈ DOBBIAMO AUMENTARE LA NOSTRA SICUREZZA?

REPORT ATTACCHI E VITTIME

Attacchi Cyber 2021 / Q1- 2022



TIPOLOGIA DELLE VITTIME (Italia)



- Agricoltura / Pesca
- Ind. Elettronica/Elettrotecnica
- Fabbricazione Mobili
- Utilities
- Costruzioni
- Commercio / produzione automotive
- Commercio all'ingrosso
- Commercio al dettaglio
- Logistica e trasporti
- Alloggio e ristorazione
- Information Technology / Telecom.
- Industria
- Servizi finanziari
- Attività immobiliari
- Servizi di consulenza
- Servizi Governativi
- Servizi Pubblica utilità (Sanità / PA)

Possiamo sentirci immuni
da un attacco?

CERTAMENTE

....perchè
siamo
piccoli?

....perchè
non c'è nulla
da rubare?

...perchè
siamo
un'impresa
semplice

Possiamo sentirci immuni da un attacco?

CERTAMENTE

SBAGLIATO

SBAGLIATO

....perchè siamo piccoli?

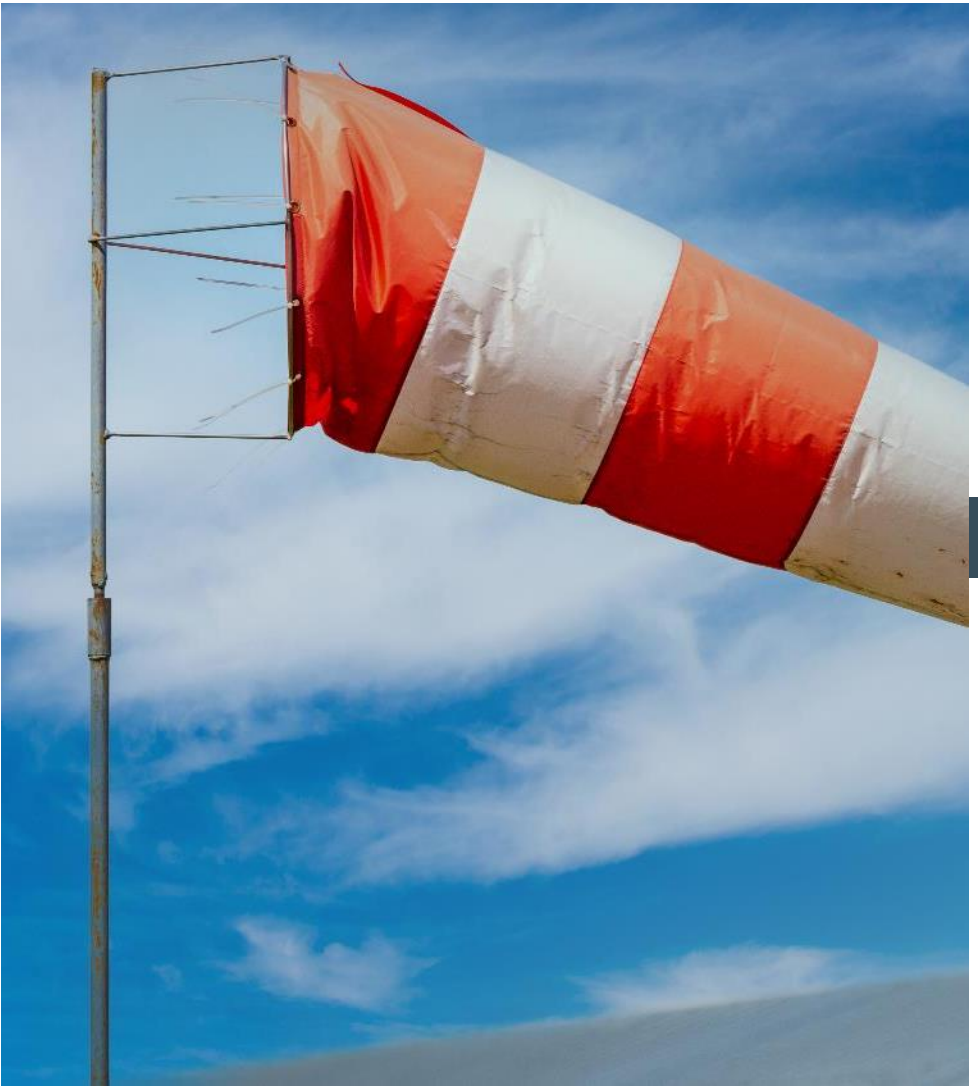
....perchè non c'è nulla da rubare?

...perchè siamo un'impresa semplice

Possiamo sentirci immuni
da un attacco?

**TUTTI POSSIAMO ESSERE
VITTIMA DI UN ATTACCO
INFORMATICO**

COSA POSSO FARE?



LA DIGITAL TRASFORMATION NECESSITA DI UN PROCESSO DI MIGLIORAMENTO DELLA SICUREZZA INFORMATICA

Prevenzione dei rischi informatici

Gestione del problema nel caso si verifichi

OBIETTIVO DEL PROCESSO

Rendere maggiormente sicura e affidabile l'infrastruttura

Abbattere la probabilità di eventi malevoli e il loro impatto

PREVENZIONE: COS'E'?

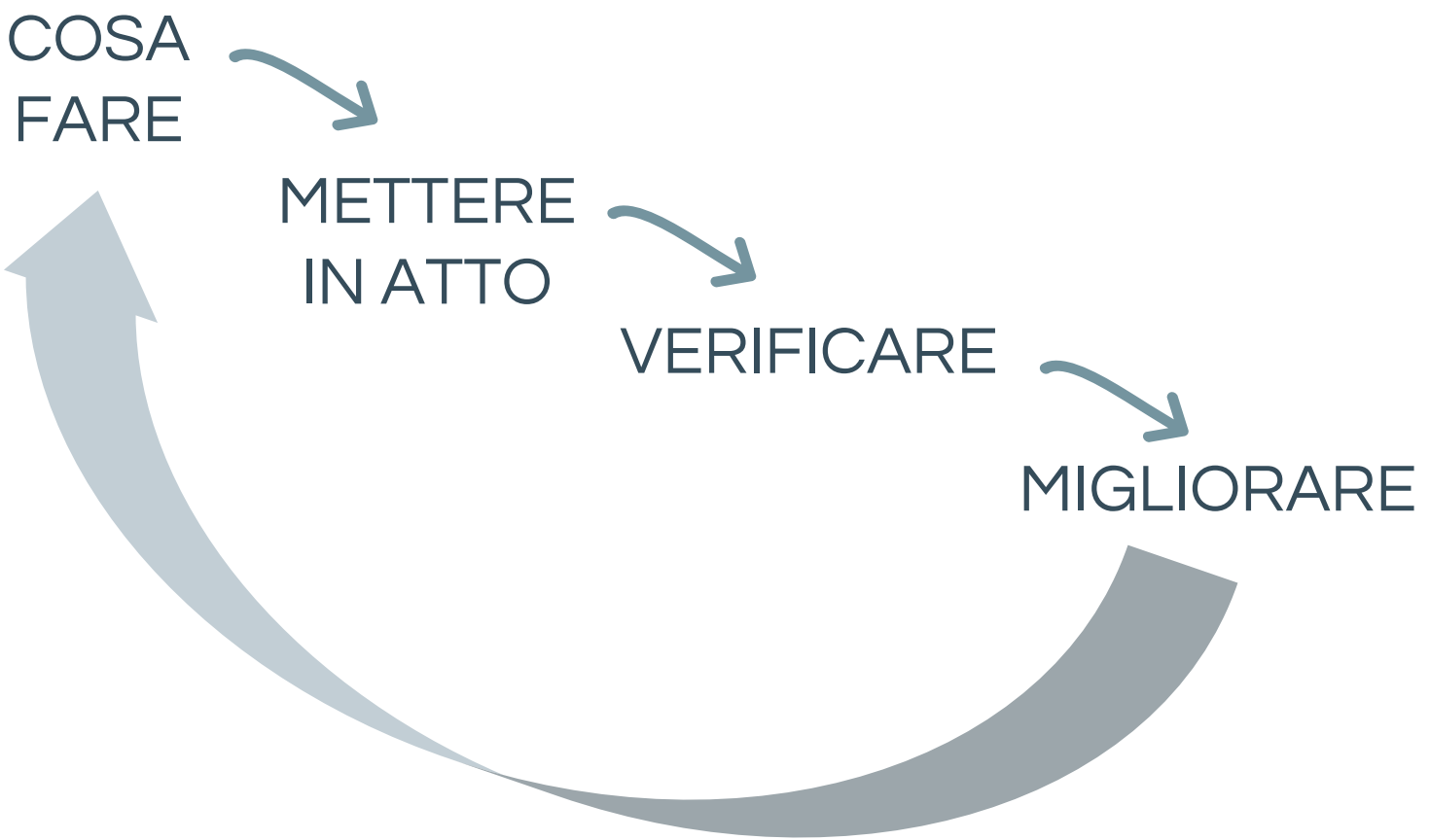
ART. 2 D.LGS 81/08

«Prevenzione»:

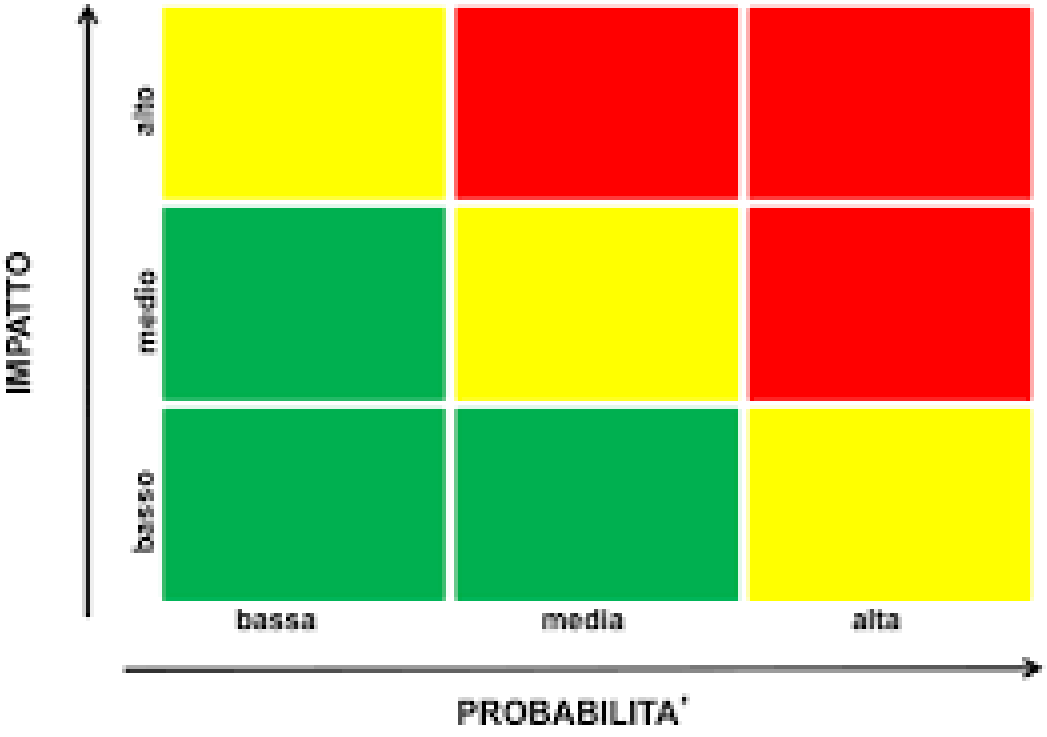
il complesso delle disposizioni o misure necessarie anche secondo la particolarità del lavoro, l'esperienza e la tecnica, per evitare o diminuire i rischi.

GESTIONE DELL'EVENTO: COS'E'?

L'insieme di procedure e azioni necessarie per "rimediare" all'evento in modo da ridurre il più possibile il suo impatto sull'azienda

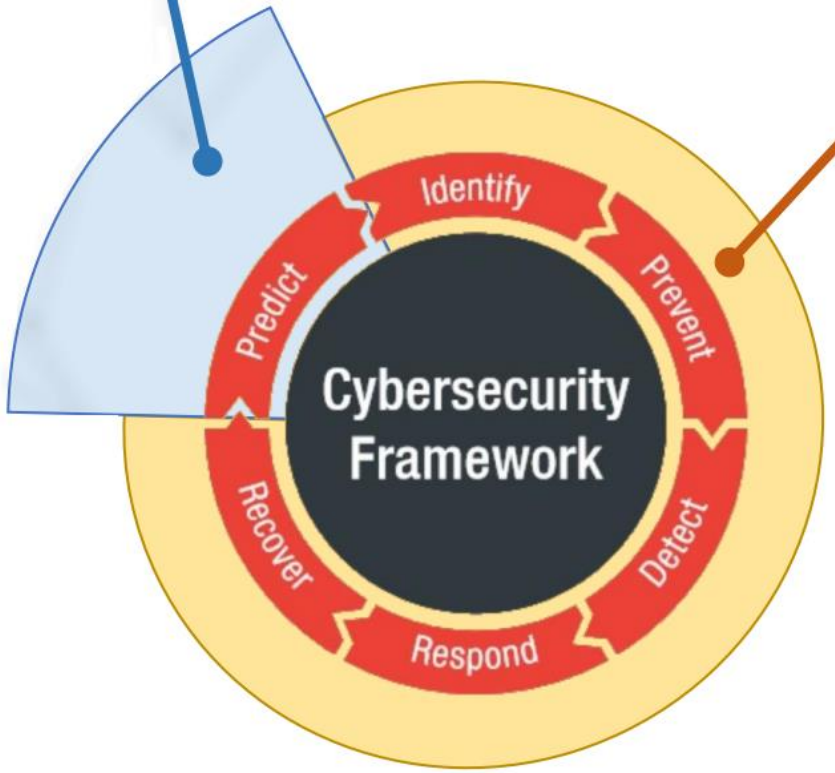


LA VALUTAZIONE DELLA PROBABILITÀ E DELL'IMPATTO

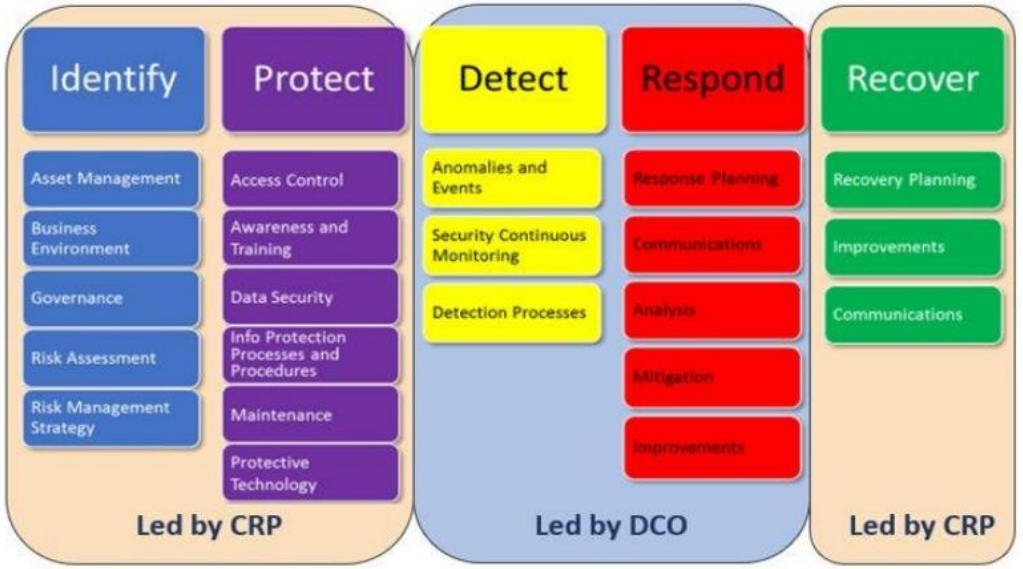


La PROBABILITA'
indica la frequenza di
accadimento degli specifici rischi,
mentre l'IMPATTO
indica il danno che, il verificarsi
dell'evento rischioso,
può causare al sistema.

AGGIUNGIAMO UN TASSELLO AL NOSTRO CICLO VIRTUOSO



PREVENZIONE E CONTRASTO



COS'È UN VULNERABILITY ASSESSMENT

E' il pilastro di qualsiasi strategia di sicurezza informatica.

Permette di individuare e classificare le vulnerabilità dell'infrastruttura aziendale e, di conseguenza, mettere in atto un piano di remediation periodico.

Si tratta di attività e di analisi, per lo più automatizzate, che controllano lo stato dell'infrastruttura.

OBBIETTIVI

Generare consapevolezza
sui problemi della propria infrastruttura.

che permetta all'azienda di programmare
azioni atte a mitigare i rischi e le conseguenze.

= RIDURRE GLI EVENTI MALEVOLI
ED EVENTUALI DANNI

...ecco allora l'importanza di un vulnerability assessment

Analisi approfondita della rete per individuare OGNI apparato collegato

Verifiche sistemi operativi e AGGIORNAMENTI

Verifiche APPLICAZIONI E SW

Compromissione pwd nel DARKWEB

Uso di pwd semplici o di DEFAULT

Verifica sicurezza apparati secondari

Risultato di un monitoraggio di vulnerabilità

Generazione di una reportistica, obbiettiva, dove vengono messi in luce i punti deboli dell'infrastruttura e a loro assegnato un indice di gravità

Permettere di generare un piano di miglioramento

Controllare periodicamente l'infrastruttura, le vulnerabilità non solo statiche

COS'È
UN PENETRATION TEST

Una serie di attività e processi, per lo più manuali, che simulano un vero attacco informatico per individuare eventuali falle e misurare l'impatto che ne deriva.

E' un processo particolarmente complesso e invasivo svolto, se necessario, da ethical hacker che partono dalla raccolta di informazioni interne ed esterne all'azienda per poter mettere sotto stress i sistemi di sicurezza e valutare la loro reazione.

PENETRATION TEST: COME?

TEST ESTERNO

Svolto dall'esterno cercando di penetrare nei sistemi informatici. Di solito si parte dalla ricerca di informazioni dell'azienda, sul web e sul dark web, che permettano di individuare punti deboli.

TEST INTERNO

Svolto da qualcuno all'interno dell'azienda con l'intento di mettere a prova i sistemi in caso di perdita o divulgazione di password degli utenti.

TARGET TEST

Attività focalizzate su determinati elementi dell'infrastruttura per metterne alla prova la loro sicurezza.

BLIND TEST

Test più affascinante e dispendioso in quanto è "alla cieca“: si parte solo dal nome dell'azienda e da qui si cerca di entrare nei sistemi.

PENETRATION TEST: RISULTATO

EVIDENZIARE VULNERABILITÀ PIÙ O MENO NASCOSTE, SPESSO DOVUTE A SISTEMI SECONDARI DELL'AZIENDA O ALL'ATTIVITÀ QUOTIDIANA DEI COLLABORATORI, CHE POSSONO ESSERE USATE PER AGGIRARE I SISTEMI DI SICUREZZA E DI CONTROLLO MESSI IN ATTO.

ABBIAMO FINITO?

Abbiamo parlato
di prevenzione
e di attività dei
collaboratori.

I COLLABORATORI
POSSONO ESSERE
UNA VULNERABILITÀ?

IL VERO ANELLO DEBOLE

A prescindere dalla complessità e evoluzione dei servizi di sicurezza, il vero punto debole rimane sempre l'UTENTE

Regolamentare
l'uso degli strumenti
informatici

COSA
POSSO
FARE ?

Mettere
alla prova/testare
l'attenzione

Formare
le persone

Benefici di una VA e PT

Aiutare il reparto IT aziendale a ridurre le possibilità che un attacco informatico vada a buon fine.

L'infrastruttura, più sicura e protetta, garantisce all'organizzazione continuità lavorativa e protezione del knowhow.

La protezione delle informazioni genera valore aziendale.

Migliora la propria reputazione aziendale.

"L'ARTE DELLA GUERRA"

CITAZIONE:

“Se conosci il nemico e te stesso,
la tua vittoria è sicura.

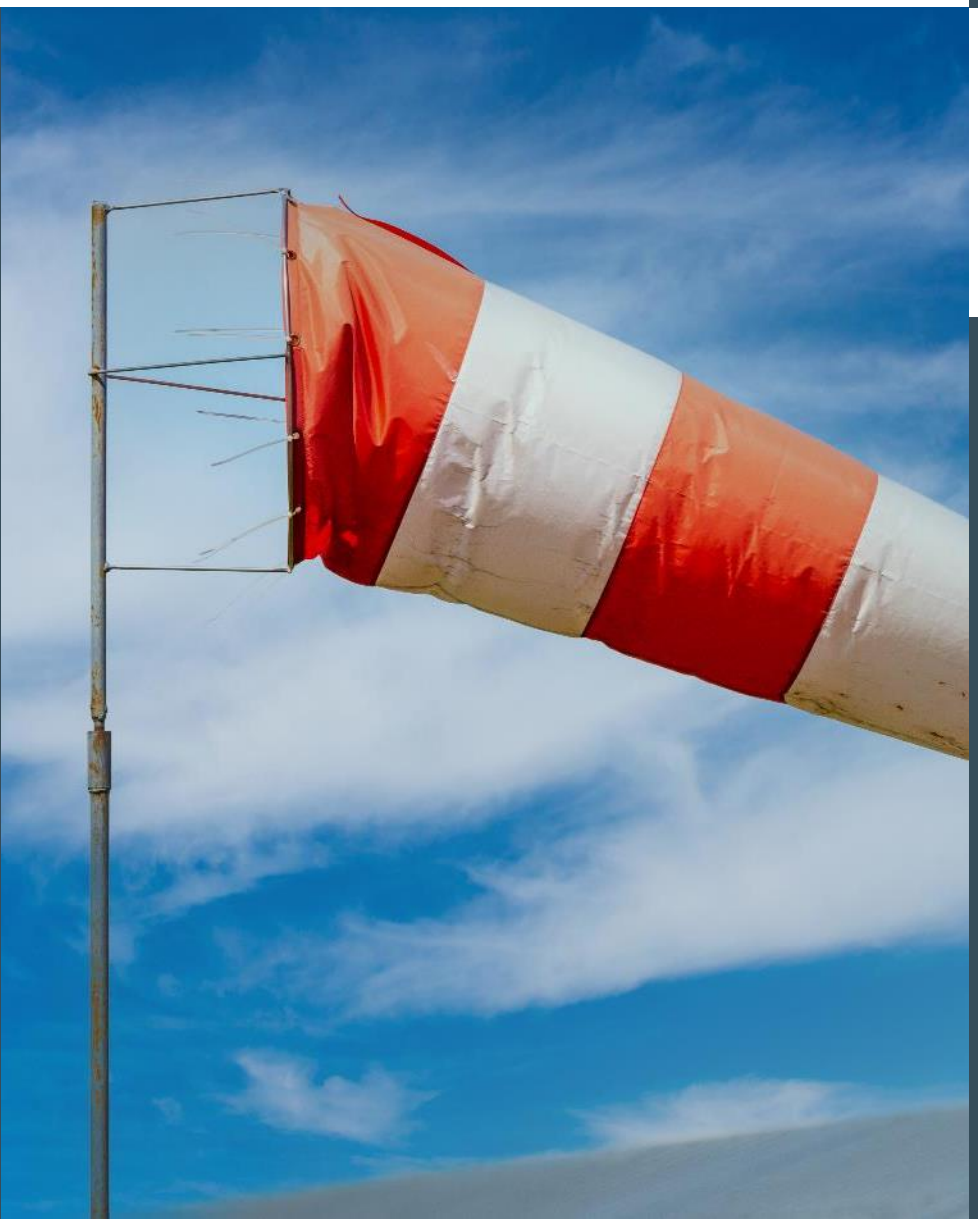
Se conosci te stesso ma non il
nemico, le tue probabilità di vincere
e perdere sono uguali.

Se non conosci il nemico e nemmeno
te stesso, soccomberai in ogni
battaglia.”

SUN TZU

CONOSCERE IL NEMICO NON È SEMPLICE, MA COMINCIAMO ALMENO AD AVERE CONOSCENZA DI NOI

CONCLUSIONE



FARE UNA SCELTA CONSAPEVOLE DELLE SOLUZIONI DI SICUREZZA AZIENDALE

Ognuno ha il diritto di fare le proprie scelte di sicurezza

IL NOSTRO DOVERE È QUELLO DI PERMETTERVI DI FARLE CON **CONSAPEVOLEZZA**

PER LE DOMANDE:

SCRIVETECI IN CHAT

PER INFORMAZIONI COMMERCIALI:

commerciale@jmconsulting.it


J.M. Consulting S.r.l.
GRAZIE PER L'ATTENZIONE

www.jmconsulting.it