PMI E CYBER SECURITY READINESS

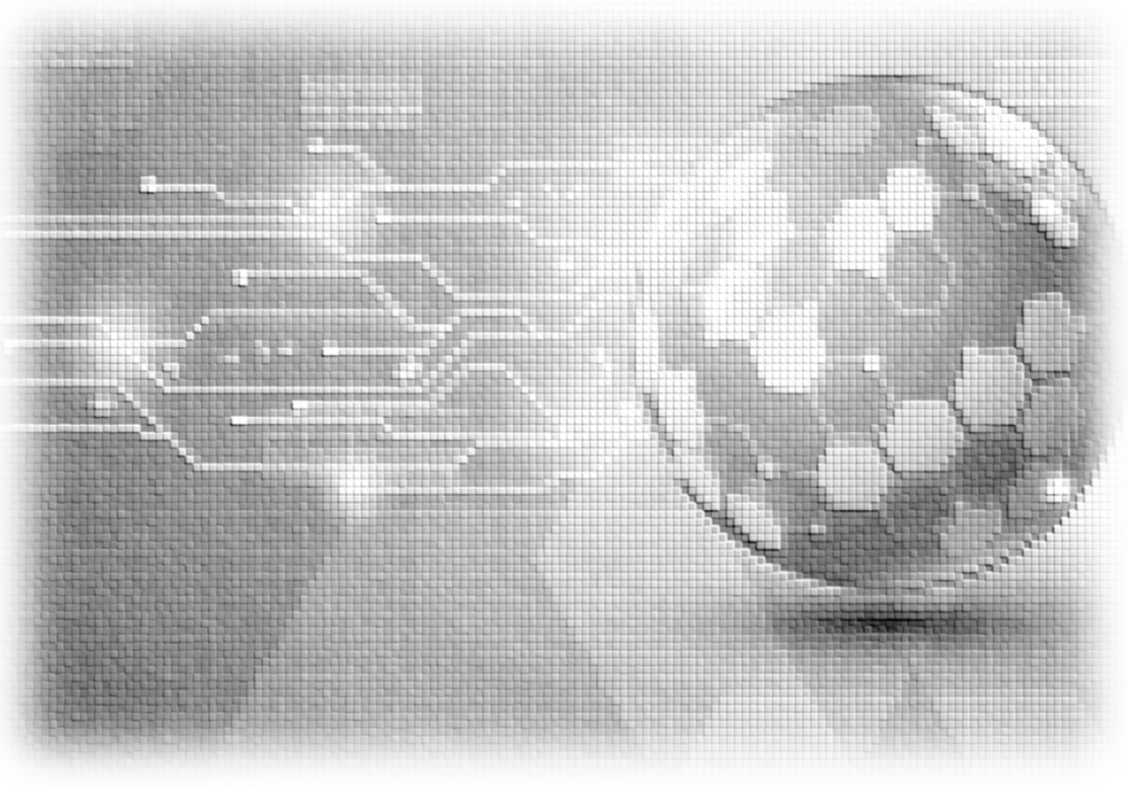
Cyber Risk Self Assessment

autovalutazione del livello di sicurezza informatica delle PMI

UNINDUSTRIA
UNIONE DEGLI INDUSTRIALI E DELLE IMPRESE
ROMA • FROSINONE • LATINA • RIETI • VITERBO

cini Cybersecurity National Lab

UNIVERSITÀ CAMPUS BIO-MEDICO DI ROMA



Responsabili del Progetto:

Rocco Mammoliti - *POSTE ITALIANE SPA, Sezione IT Unindustria, Cybersecurity*
Aniello Gentile - *ENEL SPA, Sezione IT Unindustria, Cybersecurity*

Progetto promosso da:

Vittoria Carli - *ISED SPA*, Presidente Sezione Information Technology Unindustria
in collaborazione con
Francesco d'Angelo - *TIM SPA*, Presidente Sezione Comunicazioni Unindustria

Elaborazioni a cura di:

Matteo Giacalone - *POSTE ITALIANE SPA*
Vincenzo Caserta - *CAPGEMINI ITALIA SPA*
Luigi Martino - *UNIVERSITA' DI FIRENZE, Laboratorio Nazionale di Cybersecurity*
Marco Angelini - *UNIVERSITA' LA SAPIENZA, CIS Sapienza, Laboratorio Nazionale di Cybersecurity*
Gabriele Oliva - UNIVERSITA' *CAMPUS BIO-MEDICO DI ROMA*
Roberto Setola - UNIVERSITA' *CAMPUS BIO-MEDICO DI ROMA*

Hanno collaborato nel Gruppo di lavoro:

Marco Massenzi - *TELECONSYS SPA*
Vincenzo Bianchini - *TECNOLOGIE E COMUNICAZIONI SRL*
Ascenzo Asseri - *TIM SPA*
Paolo Maria Innocenzi -*TIM SPA*
Antonio Amati - *ALMAVIVA SPA*
Marco Roberto Casini - *BT ITALIA SPA*
Marco Francola - *GFX SRL*
Michele Onorato - *WESTPOLE SPA*

PMI e Cyber Security

ESPOSIZIONE

L'Italia risulta essere uno dei Paesi più esposti, a livello internazionale, agli attacchi cyber per l'interesse verso il know-how delle PMI.

PERCEZIONE

Rischio sistemico dovuto alla percezione che la cyber security sia da intendere come una spesa invece che un investimento.

CONSAPEVOLEZZA

L'inadeguata cyber risks awareness implica la mancanza di attenzione verso il fattore umano che, nel contesto cyber, rappresenta la causa di più della metà degli incidenti informatici

Valutare il livello di sicurezza ed esposizione delle PMI ai rischi cyber, valutarne **i fabbisogni** in termini generali e, conseguentemente, **aumentarne consapevolezza e capacità di tutela del patrimonio aziendale**.

Il Progetto

1 . Definizione questionario

Selezione domande rilevanti ai fini della ricerca, suddivise tra domande di carattere generale e di carattere tecnico/organizzativo

2. Somministrazione Survey

Compilazione della checklist a cura della PMI, in **modalità anonima**

3. Clustering e stato della sicurezza

Categorizzazione in tre livelli di maturità e valutazione del livello di rischio della PMI tramite l'analisi dei risultati, con feedback immediato in modalità «risk radar»

4. Analisi ex-post dei dati

Analisi dei dati con il supporto di metodologie volte ad prioritizzare e correlare le informazioni raccolte

5. Controlli Essenziali di Cybersecurity

Mappatura della survey con i Controlli Essenziali al fine di focalizzare le **problematiche delle PMI**

La Survey

La Survey si compone di **32 domande** suddivise tra domande **di carattere generale** sull'organizzazione della società **e** domande **di carattere tecnico/organizzativo**.

Le domande di carattere tecnico/specifico si suddividono nelle seguenti macro categorie

Cod.	Domanda
A1.1	Organizzazione dell'azienda - Tipologia di azienda
A1.2	Organizzazione dell'azienda - Anni di attività dell'azienda
A1.3	Organizzazione dell'azienda - N° sedi dell'azienda
A1.4	Organizzazione dell'azienda - Provincia della sede operativa principale
A2.1	Dimensione dell'azienda - Numero di dipendenti dell'azienda
A2.2	Dimensione dell'azienda - Fatturato medio annuo nell'ultimo triennio
A3	Selezionare la sezione di appartenenza a UNINDUSTRIA / attività prevalente
A4	La tua azienda ha un reparto interno che cura gli aspetti di Cyber Security?
A5	Nella tua azienda vengono censiti i sistemi e gli apparati fisici in uso (dispositivi mobili, computer, server, etc)?
A6	I server della tua azienda dove sono collocati?
A7	Le applicazioni della tua azienda (acquistate e/o sviluppate internamente) sono utilizzate da:
A8	Per la sicurezza delle applicazioni della tua azienda vengono acquistati prodotti/servizi?
A9	Nella tua azienda è previsto l'accesso alle applicazioni aziendali da parte di personale in mobilità (tramite App su smartphone/tablet)? Se sì, sono previste azioni finalizzate a prevenire possibili rischi?
A10	Nella tua azienda il personale accede a sistemi esterni (di clienti per manutenzione, di committenti per condivisione dati, etc.)? Se sì, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
A11	Puoi indicarci il principale strumento di approvvigionamento di servizi/prodotti di sicurezza della tua azienda?
A12	Ritieni che nella tua azienda ci sia una adeguata consapevolezza rispetto agli impatti connessi alle problematiche legate ai rischi di sicurezza informatica?
A13	Quale ritieni sia per la tua azienda il budget annuo adeguato da destinare alla protezione contro le minacce informatiche?
A14	Sei interessato ad approfondire il tema della sicurezza informatica?
B1	L'azienda è inserita in una filiera "sensibile" per le minacce cyber (energia, sanità, finance, etc)?
B2	I processi aziendali necessitano di accesso a Internet per poter funzionare? Se sì, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B3	I prodotti dell'azienda possono essere (o saranno) connessi a Internet? Se sì, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B4	I servizi dell'azienda richiedono connessione a Internet? Se sì, l'azienda ha posto in essere delle azioni finalizzate a prevenire possibili rischi?
B5	È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda?
B6	È prevista una politica di aggiornamento del software/firmware dei dispositivi utilizzati nell'azienda da remoto ?
B7	I prodotti dell'azienda possono essere impiegati in sistemi/applicazioni critiche (sistemi che in caso di malfunzionamento possono provocare morte o gravi rischi alla persone, perdita o grave danneggiamento di mezzi e materiali, gravi danni ambientali, danno economico)?
B8	È previsto un controllo di qualità certificato ed una fase di collaudo per tutti i prodotti/servizi dell'azienda?
B9	L'azienda utilizza software di protezione (antivirus, antimalware, ecc) regolarmente aggiornato su tutti i dispositivi?
B10	Nell'ultimo biennio è stato effettuato un corso di formazione sulla cyber security al personale non tecnico? (es riconoscere allegati e-mail malgrè, utilizzare solo software autorizzato, ecc)?
B11	Escludendo software antivirus ed eventuale formazione del personale, l'azienda ha investito parte del budget dello scorso anno in attività relative alla sicurezza informatica?
B12	Utilizzate soluzioni di backup delle informazioni mantenuti fisicamente separati e periodicamente testati?
B13	L'azienda ha subito nel corso dell'ultimo biennio attacchi informatici?
B14	Il controllo di qualità considera anche la sicurezza informatica?

COMMITMENT AZIENDALE

misurare l'attenzione del management in termini di risorse, budget e awareness sulle tematiche di cyber security.

LIVELLO DI ESPOSIZIONE

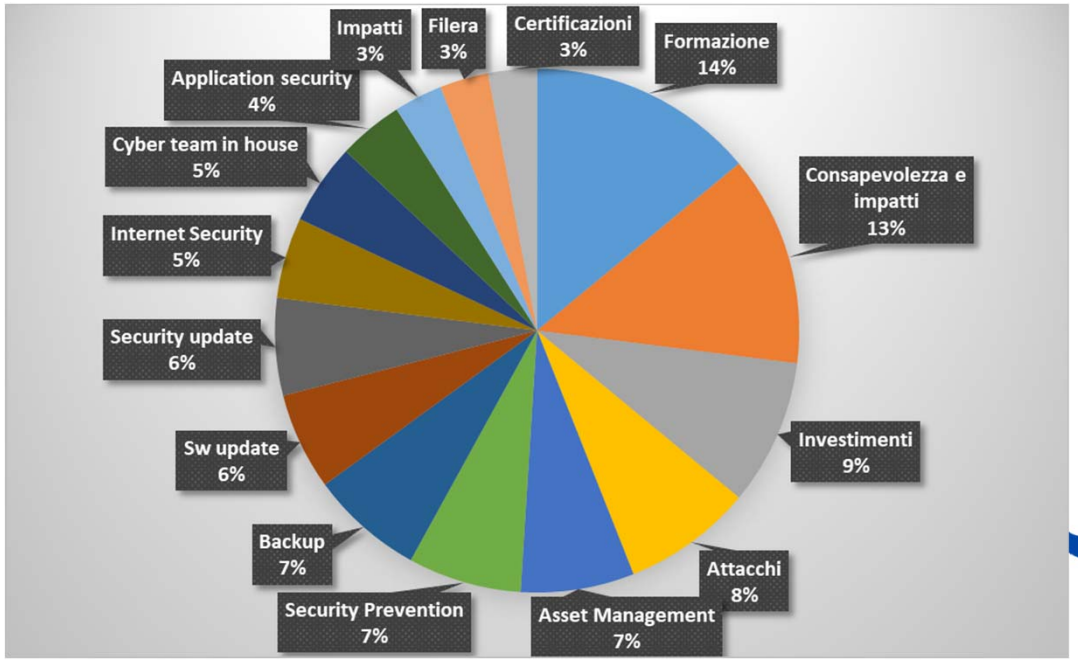
misurare l'esposizione dell'azienda a minacce/attacchi cyber in funzione della rilevanza servizi/prodotti erogati dall'Azienda

MATURITA' TECNOLOGICA/ORGANIZZATIVA

misurare il grado di maturità tecnologica/organizzativa dell'azienda nel prevenire, contrastare, mitigare le minacce del cyber spazio.

Metodologia di assegnazione dei pesi alle domande

Alle domande è stato attribuito un peso applicando la metodologia **Sparse Analytic Hierarchy Process (SAHP),** che ha richiesto l'intervista a esperti nazionali della Cyber Security appartenenti sia al mondo aziendale che a quello accademico.



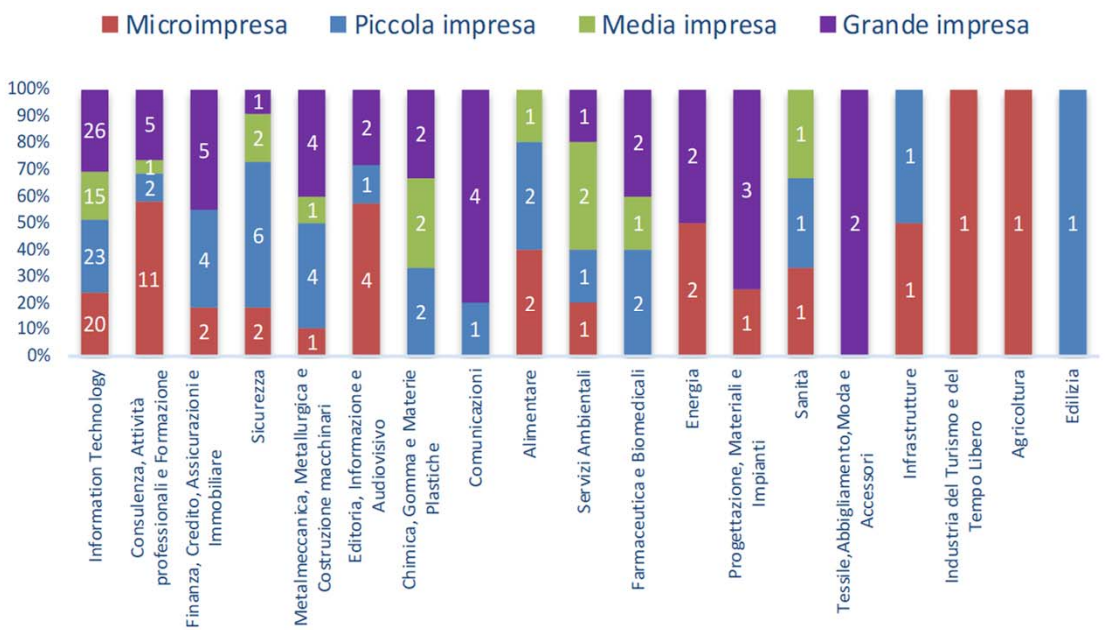
Formazione: *"Non aver svolto corsi di formazione in cyber security per personale non tecnico nell'ultimo biennio"*

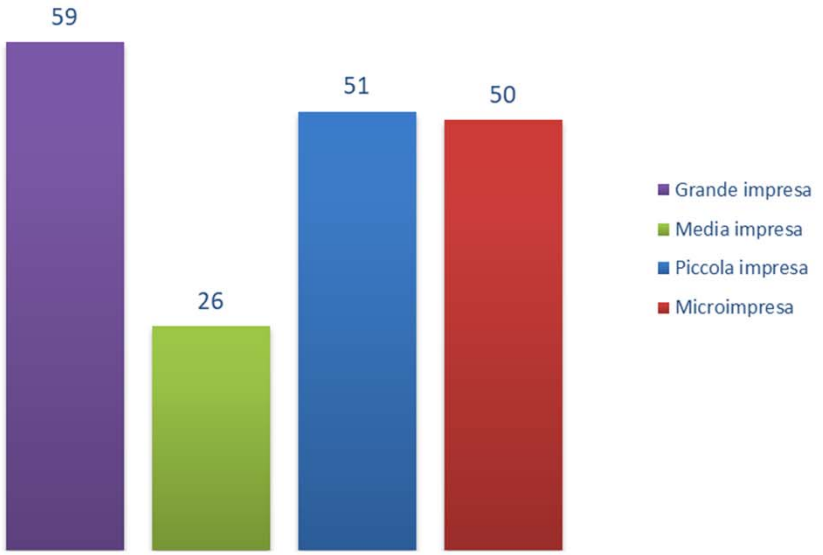
Consapevolezza e impatti: *"Non diffondere la consapevolezza in azienda degli impatti legati ai rischi di sicurezza informatica"*

Investimenti: *"Non aver investito in Sicurezza Informatica, escludendo antivirus e formazione del personale, nell'ultimo biennio"*

Statistiche

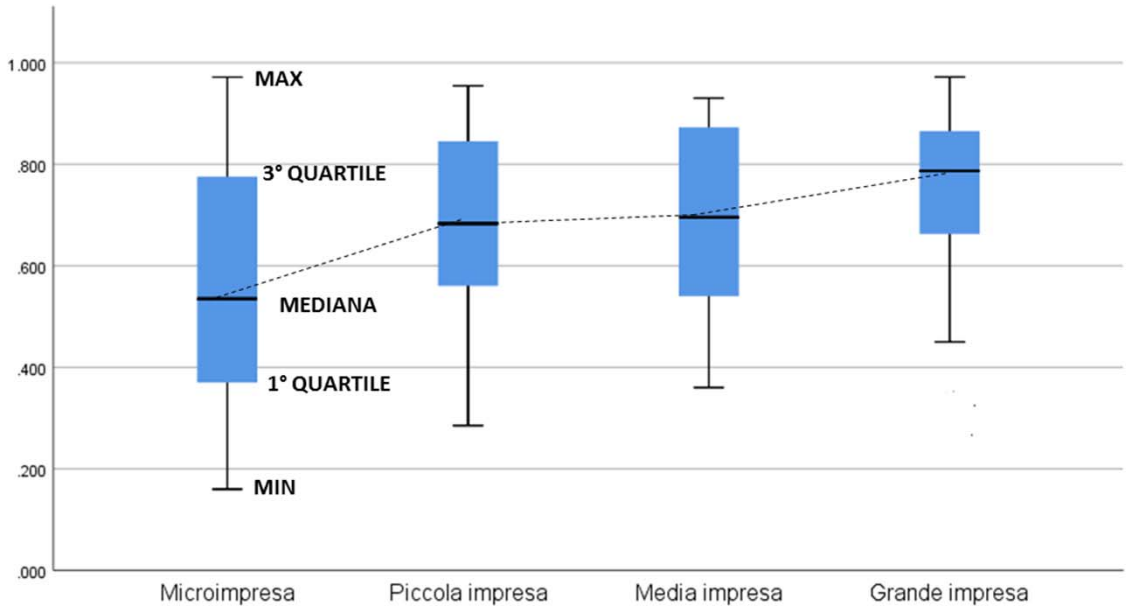
186 questionari da aziende appartenenti a diversi settori merceologici e diversificate tra Micro, Piccola, Media e Grande Impresa





Cyber Security Score (CSS) e Dimensione Societaria

Il grafico a Boxplot indica la distribuzione del CSS nelle quattro tipologie di dimensioni aziendali.



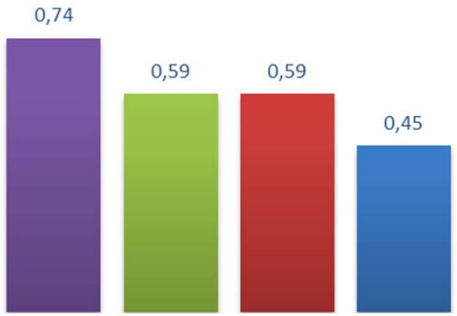
- il «CSS» cresce sensibilmente al crescere della dimensione societaria.
- All'aumentare della dimensione dell'azienda diminuisce la variabilità ovvero diminuisce la distanza tra i valori massimo e minimo

il «CSS» non è solo maggiore nelle imprese più strutturate, ma anche soggetto a minori variazioni.

Risultati e macro categorie domande

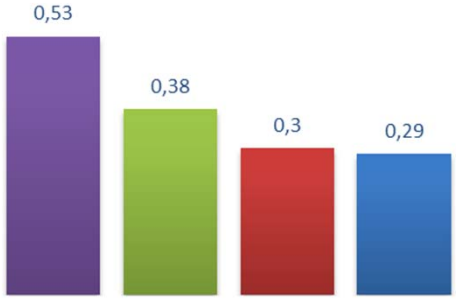
Si riportano di seguito i risultati relativi alle tre macro categorie di carattere tecnologico/organizzativo

COMMITMENT AZIENDALE



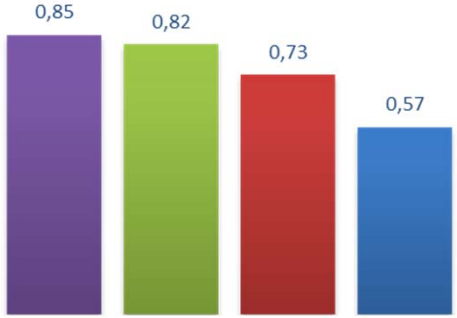
Il CSS relativo al commitment aziendale sulle tematiche di cyber security in termini di risorse, budget e awareness decresce con il diminuire della dimensione societaria.

LIVELLO DI ESPOSIZIONE



Il CSS associato alle domande relative al livello di esposizione è maggiore per le grandi aziende rispetto alle micro e PMI.

MATURITA' TECNOLOGICA/ORGANIZZATIVA



Il CSS relativo alla maturità tecnologica delle aziende è maggiore per le grandi imprese e cresca all'aumentare della dimensione societaria.

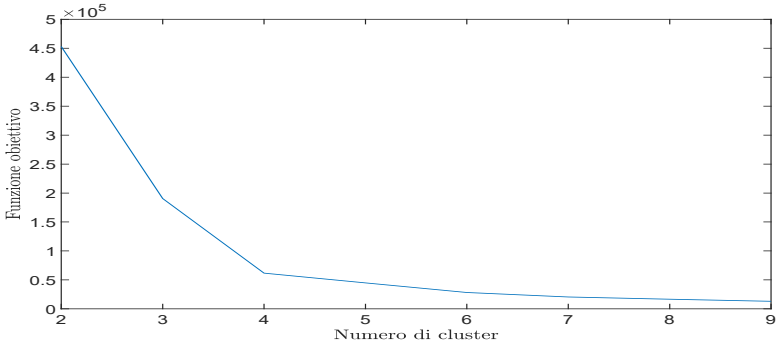
Clustering Analysis

C-MEANS

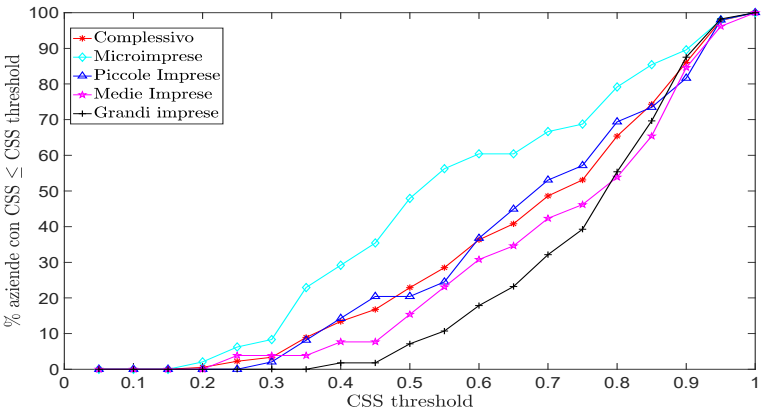
Anni	Dipendenti	Fatturato	Reparto Cyber	Budget sicurezza	CSS	Numerosità
11.03	25.08	4.03M€	0.02	14.35k€	0.49	28.03%
5.82	29.77	4.10M€	0.95	22.25k€	0.73	22.21%
22.81	107.85	20.96M€	0.94	52.76k€	0.76	23.37%
23.84	297.34	141.93M€	0.99	138.67k€	0.78	26.39%

La tecnica di clustering ha prodotto gruppi caratterizzati da dimensioni societarie e di «CSS» crescenti, contribuendo a validare la connessione tra CSS e dimensione societaria.

K-MEANS E PCA



Confermata la relazione tra dimensione societaria e gruppi, in quanto ogni gruppo risulta caratterizzato da intervalli di valori di CSS quasi del tutto privi di sovrapposizione.

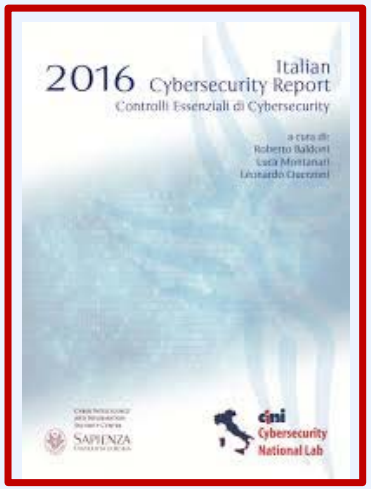


Survey e Controlli Essenziali

In considerazione del target comune a cui mirano il Cyber Risk Self Assessment e i ***15*** *Controlli Essenziali di Cybersecurity*, si è scelto di identificarne innanzitutto il legame e conseguentemente individuare i principali punti di debolezza delle PMI, in relazione alle «*tematiche di sicurezza*» di appartenenza dei Controlli.

CYBER RISK SELF ASSESSMENT

CONTROLLI ESSENZIALI CYBER SECURITY



- 15 Controlli Essenziali di Cybersecurity
- 8 Tematiche di sicurezza

L'aumento del rischio implica che l'operatività, la riservatezza dei dati dell'organizzazione e la loro integrità potrebbero essere lese da attaccanti con una probabilità troppo alta per essere considerata accettabile.

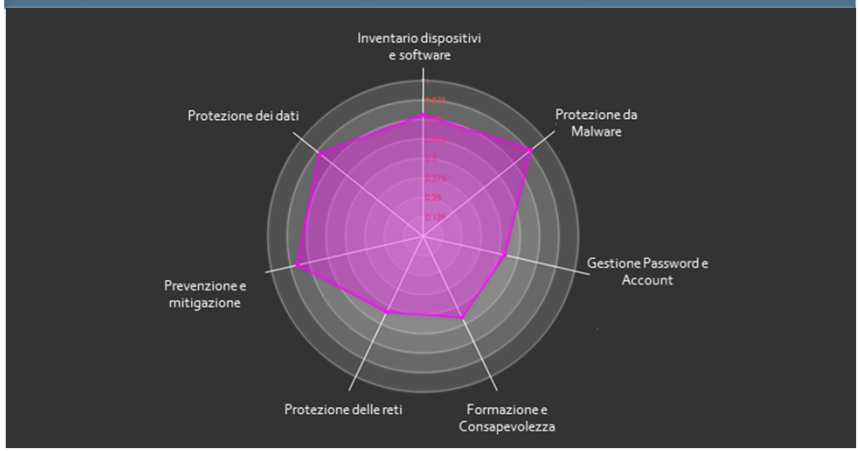
Tematiche di Sicurezza e risultati

Il legame tra Cyber Risk Self Assessment e Controlli Essenziali di Cybersecurity è stato riscontrato in **7 tematiche di sicurezza**

TEMATICHE DI SICUREZZA

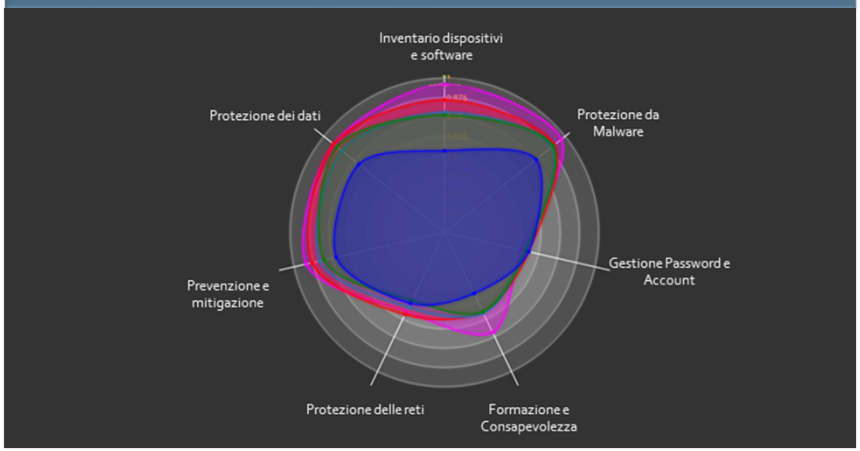
- INVENTARIO DISPOSITIVI E SOFTWARE
- PROTEZIONE DA MALWARE
- GESTIONE PASSWORD E ACCOUNT
- FORMAZIONE E CONSAPEVOLEZZA
- PROTEZIONE DEI DATI
- PREVENZIONE E MITIGAZIONE
- PROTEZIONE DELLE RETI

RISULTATO COMPLESSIVO



Media

RISULTATO PER DIMENSIONE AZIENDALE



Grande impresa | Media impresa | Piccola impresa | Microimpresa

Principali criticità

La corretta implementazione di tutti i controlli di cybersecurity ritenuti essenziali ha, come immediata conseguenza, una riduzione importante, ma non totale, del rischio. Di contro, queste pratiche qualora ignorate, oppure implementate in modo non appropriato, causano un aumento considerevole del rischio

Aree tematiche di sicurezza che hanno riscontrato un livello di maturità critico

FORMAZIONE E CONSAPEVOLEZZA

Il fattore umano continua a costituire il punto debole della sicurezza.
È necessario sensibilizzare e rendere consapevoli dei rischi tutti gli operatori che possono accedere a dati o ad altre risorse attraverso l'uso dei vari dispositivi.

Raccomandazioni

1) **Adeguata formazione dei dipendenti relativa alla cybersecurity e aggiornamento periodico**
2) **La formazione progettata in base a ruoli e competenze pregresse del personale.**

GESTIONE PASSWORD E ACCOUNT

I meccanismi di autenticazione tramite nome utente e password sono fondamentali nella protezione delle identità digitali e dei dispositivi a cui questi accedono. Una corretta gestione delle password è quindi indispensabile per garantire la sicurezza dei sistemi aziendali e delle informazioni che questi contengono

Raccomandazioni

1) **Corretta definizione delle password**
2) **Corretta educazione degli utenti nell'uso delle password.**

PROTEZIONE DELLE RETI

Al fine di impedire l'accesso indiscriminato di persone non autorizzate ai sistemi aziendali attraverso internet è necessario che le reti siano adeguatamente protette attraverso strumenti che permettano il controllo di quanto accade all'interno delle reti stesse.

Raccomandazioni

1) **Firewall**
2) **Intrusion Detection/Prevention System**
3) **Mail/Web Filter**

FINE