INDICE degli argomenti

Agli amici imprenditori,

artigiani e commercianti sparsi in tutta Italia,

piccoli e grandi eroi della quotidianità

Introduzione

Il tessuto imprenditoriale italiano

L'ITALIA è un paese fantastico. La nostra storia e la posizione geografica hanno modellato la nostra cultura rendendoci il popolo più creativo al mondo. Il senso del bello e l'inconfondibile stile italiano sono elementi unici rappresentati dal marchio MADE IN ITALY tanto ammirato (e spesso copiato) che è la sintesi di quella creatività e qualità, che da nord a sud è espressa dalle nostre imprese.

L'analisi del nostro mercato evidenzia che:
- Il 98% delle imprese italiane è al di sotto dei 20 dipendenti;
- Il 95% invece è al di sotto dei 10 dipendenti.

Ben lontani dai parametri di definizione delle mPMI a livello europeo[1], quello italiano è un tessuto imprenditoriale unico al

[1] Le piccole imprese, in ambito europeo, sono definite come quelle imprese con meno di 50 occupati e che realizzano un fatturato annuo oppure un totale di bilancio annuo non superiore a 10 milioni di euro, fonte: ec.europa.eu

mondo, che ci rende la 7ma potenza economica dopo USA, UK, Germania, Francia, Giappone e Canada.
Mettendo da parte la P.A., le mPMI italiane rappresentano quasi il 60% della forza lavoro del nostro paese.
È per questo motivo che abbiamo voluto realizzare una **guida per la sicurezza informatica dedicata alle mPMI italiane**.
Solitamente i temi della cybersecurity sono affrontati e approfonditi per realtà medio grandi e quando si cerca di rendere le contromosse applicabili anche alle imprese più piccole, ci si dimentica che la realtà italiana è molto particolare. Un tessuto fittissimo di microimprese tante volte con una gestione famigliare (altro enorme patrimonio nazionale), che operano nel mercato da più generazioni, segno di una forte tradizione, strettamente connessa al territorio, che allo stesso tempo è capace di rinnovarsi e competere a livello internazionale.

Un patrimonio da difendere

La nostra tradizione e le nostre imprese vanno salvaguardate e protette, rappresentano un patrimonio troppo prezioso, che ha bisogno di essere guidato nella competizione internazionale che vuole in tutti i modi indebolirlo. L'imprenditore sa che dovrà quotidianamente gestire innumerevoli **rischi**. Rischi di tipo economico-finanziario, rischi legati all'ambiente, alla sicurezza dei lavoratori, rischi di fornitura e non ultimi i rischi informatici.

L'ultimo rapporto per l'anno 2023 del **World Economic Forum** pone, la tecnologia in generale, come uno tra i più rilevanti rischi/opportunità per il mondo. In particolare:
"Il settore tecnologico sarà tra gli obiettivi centrali di politiche industriali più forti e di maggiore intervento statale. Spinti dagli aiuti di Stato e dalle spese militari, nonché dagli investimenti privati, la ricerca e lo sviluppo di tecnologie

emergenti continueranno a ritmo sostenuto nel prossimo decennio, producendo progressi nell'intelligenza artificiale, nell'informatica quantistica e nella biotecnologia, tra le altre tecnologie. Per i paesi che possono permetterselo, queste tecnologie forniranno soluzioni parziali a una serie di crisi emergenti, dall'affrontare nuove minacce per la salute e una crisi nella capacità sanitaria al ridimensionamento della sicurezza alimentare e alla mitigazione del clima. Per coloro che non possono, la disuguaglianza e la divergenza aumenteranno.
In tutte le economie, queste tecnologie comportano anche dei rischi, dall'ampliamento della disinformazione a un abbandono rapido e ingestibile sia nei lavori dei colletti blu che in quelli bianchi.
Tuttavia, il rapido sviluppo e l'implementazione di nuove tecnologie, che spesso sono accompagnate da protocolli limitati che ne disciplinano l'uso, comportano una serie di rischi. Il sempre crescente intreccio delle tecnologie con il funzionamento critico delle società sta esponendo le popolazioni a minacce interne dirette, comprese quelle che cercano di distruggere il funzionamento della società. Parallelamente all'aumento della criminalità informatica, i tentativi di interrompere le risorse e i servizi tecnologici critici diventeranno più comuni, con attacchi previsti contro ***l'agricoltura e l'acqua, i sistemi finanziari, la sicurezza pubblica, i trasporti, l'energia e le infrastrutture di comunicazione domestiche, spaziali e sottomarine****.*
I rischi tecnologici non sono limitati esclusivamente agli attori canaglia. Un'analisi sofisticata di set di dati più grandi consentirà l'uso improprio delle informazioni personali attraverso meccanismi legali legittimi, indebolendo la sovranità digitale individuale e il diritto alla privacy, anche in regimi democratici ben regolamentati."

Viviamo una **società iperconnessa** dal punto di vista tecnologico e anche il servizio apparentemente lontano dalle problematiche digitali può essere fortemente influenzato da un attacco informatico. Noi stessi, persone fisiche che utilizziamo a casa o talvolta in azienda i nostri dispositivi (smartphone, tablet o portatili personali), siamo un obiettivo per chi intende operare un attacco, e allo stesso tempo una minaccia (in quanto vettori inconsapevoli) per l'attività e la continuità aziendale nostra e dei soggetti collegati all'impresa (come, ad esempio, clienti e fornitori).

La **sicurezza informatica**, dunque, è un requisito fondamentale che deve essere presente e controllata lungo l'intera catena di approvvigionamento (supply chain), per garantire una continuità operativa per il nostro business e la sicurezza personale e dei nostri famigliari.

Tuttavia, l'adozione dell'ICT e ancora di più della sicurezza delle informazioni è scarsa. Nel 2019 Eurostat ha stimato che solo il 33% delle imprese dell'UE dispongono di documenti relativi a misure, pratiche o procedure sulla sicurezza ICT, mentre il 24% ha definito o riesaminato i documenti di sicurezza negli ultimi 12 mesi[2].

È necessario, dunque, dotarsi di una strategia chiara, con obiettivi adeguati per un'efficiente implementazione dei controlli di sicurezza, sia per proteggere le proprie informazioni che per provare a crescere e resistere in un mercato sempre più aggressivo e competitivo.

[2] SME Guide Information Security Controls (European DIGITAL SME Alliance)

Capitolo 1 - Perché deve interessarmi

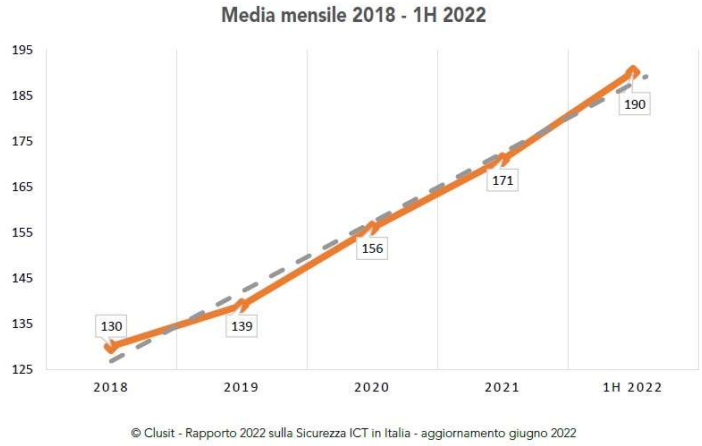
Quello della **sicurezza delle informazioni** e della **protezione dei dati personali** è senza dubbio un problema globale. Nel 2020 il costo totale per la protezione dei dati e le conseguenze da cyber attacchi è stato di oltre 1.000 mld di dollari, mentre il mercato dei prodotti e servizi per la sicurezza informatica è stato di circa 180 mld.
Spesso nelle indagini a livello mondiale, l'Italia è risultata all'apice di tali attacchi. Infatti, pur non essendo tra le nazioni più appetibili, il numero di attacchi informatici verso entità italiane è stato tra i più alti in assoluto. Il fatto che solo da ottobre 2020 in Italia si sia iniziato a parlare di "perimetro di sicurezza nazionale cybernetica" la dice lunga sulla criticità che possono avere questi attacchi sulle infrastrutture di servizi a livello nazionale.

Alcuni dati dal rapporto CLUSIT 2022

Il **Clusit** è l'Associazione Italiana per la Sicurezza Informatica, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed

autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 600 organizzazioni, appartenenti a tutti i settori del Sistema-Paese. Dal 2011 pubblica il rapporto annuale sulla sicurezza ICT in Italia.

Nell'ultimo rapporto, aggiornato ad ottobre 2022[3], i dati e i grafici mostrano in modo efficace quanto il sistema Italia sia sottoposto ad attacchi informatici con un trend di crescita preoccupante.



Per tipologia di attacchi si evidenzia come ci sia stato un grande aumento con finalità **spionaggio/sabotaggio** a causa del conflitto in Europa. Sebbene il principale rimanga sempre il cybercrime, la crescita di tutti gli altri con l'aggiunta di nuovi non lascia sperare bene per il futuro.

[3] L'ultimo rapporto Clusit è scaricabile dal sito: https://clusit.it/rapporto-clusit/

ATTACCANTI PER TIPOLOGIA	2018	2019	2020	2021	1H 21	1H 22	1H 2021 su 1H 2022	Trend 2022
Cybercrime	1.229	1.381	1.518	1.763	925	894	-3.4%	
Espionage-Sabotage	203	203	264	217	95	154	62.1%	
Information Warfare	58	35	44	49	26	57	119.2%	
Hacktivism	64	48	48	20	7	36	414.3%	
Espionage-Sabotage + Inf. Warfare	261	238	308	266	121	211	74,4%	
Totale	1.554	1.667	1.874	2.049	1.053	1.141	+8,4%	

Il **Malware** si riconferma la prima tecnica di attacco, seguono le **tecniche sconosciute**, **Phishing / Social Engineering** e lo sfruttamento delle **Vulnerabilità**.

Tecniche di attacco	2018	2019	2020	2021	1H 21	1H 22	2021 su 2020	TREND
Malware	601	737	775	850	454	433	-4.6%	
Unknown	429	309	372	433	230	253	10.0%	
Vulnerabilities	143	158	200	320	164	120	-26.8%	
Phishing / Social Engineering	170	291	299	203	94	154	63.8%	
Multiple Techniques	64	57	86	103	48	93	93.8%	
Identity Theft / Account Cracking	67	71	90	76	31	35	12.9%	
Web Attack	43	21	18	33	20	4	-80.0%	
DDoS	37	23	34	31	12	49	308.3%	
TOTAL	1.554	1.667	1.874	2.049	1.053	1.141		

Come mostra la tabella gli obiettivi sono tutti i settori della vita del paese, dove le mPMI sono comunque inserite come attori trasversali, essendo talvolta clienti/utenti e altre volte fornitori.

VITTIME PER CATEGORIA	2018	2019	2020	2021	1H 21	1H 22	1H 2021 su 2022	TREND 2022
Gov. / Mil. / LE	220	233	225	307	167	135	-19.2%	↘
ICT	191	233	269	278	113	126	11.5%	↗
Multiple Targets	326	406	401	274	121	252	108.3%	↑
Healthcare	161	186	210	262	139	142	2.2%	↗
Education	106	140	174	174	100	54	-46.0%	↓
Financial / Insurance	162	107	122	137	60	106	76.7%	↑
Prof. / Scientific / Technical	18	19	65	82	50	32	-36.0%	↓
Wholesale / Retail	33	45	54	82	50	26	-48.0%	↓
Transportation / Storage	33	16	39	75	48	25	-47.9%	↓
Manufacturing	34	36	65	72	47	63	34.0%	↑
News / Multimedia	70	69	43	69	38	57	50.0%	↑
Organizations	40	35	46	52	30	28	-6.7%	↘
Energy / Utilities	24	25	39	43	19	20	5.3%	↗
Arts / Entertainment	68	55	40	42	26	18	-30.8%	↓
Telco	13	19	32	36	9	16	77.8%	↑
Hospitability	44	27	22	30	17	14	-17.6%	↘
Other Services	9	14	15	25	13	17	30.8%	↑
Agriculture / Forestry / Fishing	0	0	5	6	3	2	-33.3%	↓
Construction	1	2	7	3	3	6	100.0%	↑
Mining / Quarrying	1	0	1	0	0	2	-	-
TOTALE	1.554	1.667	1.874	2.049	1.053	1.141		

Le **tecniche multiple**, così come gli attacchi multipli, lasciano pensare a delle tecniche sempre più complesse e pericolose, probabilmente non completamente rese efficaci, ma tenute dormienti in attesa di un momento più performante per lo scopo criminale.

Un problema che riguarda tutti

Lo dicevamo in apertura, nessuno è al sicuro. Quello della sicurezza informatica, infatti, non è più solo un problema delle grandi aziende. I criminali informatici (non chiamiamoli più hacker) hanno trovato un nuovo bersaglio: le micro e le piccole e medie imprese (mPMI), che spesso non hanno la concentrazione, le competenze interne o le risorse per stare al passo con le crescenti minacce alla sicurezza.
Allo stesso tempo però le mPMI sono costrette ad utilizzare le tecnologie innovative per rimanere al passo con un mercato sempre più competitivo e clienti sempre più esigenti. Manca però la consapevolezza dei pericoli che queste comportano. Sapere a cosa prestare attenzione e come difendersi dalle minacce dovrebbe essere ormai tra le priorità di qualsiasi impresa.

Il **Regolamento Europeo per la Protezione dei Dati**, noto come **GDPR**, mal digerito dalle piccole imprese, ha però avuto il grande merito di sollevare l'attenzione sul tema della **sicurezza dei dati personali** e in generale delle informazioni.
Oggi, infatti, subire una violazione di dati personali, siano essi riferiti a dipendenti, clienti o fornitori, può avere conseguenze alquanto spiacevoli per qualsiasi titolare d'impresa. Dalle sanzioni pecuniarie alla possibilità di essere soggetto a verifiche e controlli da parte dei corpi ispettivi della Guardia di Finanza, gli effetti e lo stress a cui l'intera azienda può essere soggetto vanno di gran lunga oltre il costo generato dal beneficio che invece si può avere dal tenere sotto controllo dati e informazioni della nostra organizzazione. Non solo in termini di "conformità" rispetto ad una normativa, ma anche e soprattutto in termini di efficienza che è possibile migliorare a vantaggio dell'intero processo produttivo. Senza contare la serenità di aver fatto le cose bene e non temere nessun tipo di sanzione, a vantaggio,

anche questo della propria concentrazione sulle cose che contano e dunque della nostra produttività.

La storia di Gianni

"Gianni è il responsabile finanziario di una grossa azienda. L'azienda ha un suo sistema di gestione per la sicurezza delle informazioni e Gianni segue metodicamente le policy aziendali e non si permetterebbe mai di usare il proprio account ufficiale per siti non pertinenti o poco sicuri, nemmeno per accedere al forum di finanzaemercati.com tanto è scrupoloso.
Però Gianni ha una vita privata e quando non è spinto dalle policy aziendali, decide di usare la password luca2019 (nome del figlio e anno di nascita) per iscriversi al sito della sua passione personale (ballidigruppo.it).
Il sito si rivela con una pessima sicurezza e viene facilmente "bucato" dai criminali informatici che, subito dopo, pubblicano le credenziali degli utenti sui canali telegram specializzati e sul darkweb.
Succede dunque che uno di questi criminali decide di tentare il colpo e fa un po' di indagini sui vari utenti trovati. Scopre che Gianni è presente sui maggiori social e nei gruppi di ballo vengono condivise anche parecchie foto, taggati amici e parenti. Tra i commenti pubblici ci sono anche complimenti e amichevoli battute dei suoi colleghi. Da qui (questo si chiama ***Social Engineering****), il criminale deduce che Gianni è un personaggio di un certo rango all'interno dell'azienda e, indagando ancora più a fondo, riesce a trovare la sua casella di posta aziendale. Ma niente da fare: le attenzioni usate dal nostro soggetto nella gestione del suo account aziendale non consentono all'attaccante di accedere alla mailbox.*
Allora l'attaccante decide di provare gli altri account social che nel frattempo è riuscito a trovare, profilando Gianni in una maniera degna dei servizi segreti. Caso vuole che abbia utilizzato la password luca2019 per un altro account personale.

Questo ha permesso al criminale di ottenere parecchi dati speciali su passioni e attività di Gianni, oltre a numerosi numeri di telefono.
A questo punto il nostro attaccante ha forgiato una campagna mirata (includendo anche attacchi di tipo ***SMS spoofing****) per far sì che il suo ufficio emettesse un bonifico di 50 mila euro ad una fantomatica ditta filippina. La truffa ha dato i suoi frutti."*

Una delle tecniche potenzialmente utilizzate dal criminale, è ad esempio **MITM - Man in The Middle** o più probabilmente **Man in The Mail**.

Il caso è inventato e il Gianni della storia può essere uno qualsiasi dei casi reali di Treviso (25 mila euro da un giroconto mai arrivato da Intesa Sanpaolo filiale di Treviso alla BCC di Casale sul Sile), Levico Terme (600 mila euro finiti sul conto di una società fantasma di Bologna e da lì hanno iniziato un lungo viaggio), Torino etc…
Gianni può essere il tuo funzionario di banca di riferimento, la tua segretaria con accesso ai conti aziendali, il tuo fornitore, tuo figlio.
Ognuno di noi rischia di essere il prossimo Gianni. Tutti abbiamo un cellulare, una casella di posta elettronica personale, dei contatti, un conto bancario personale o aziendale e tanti *hobbies*.

Come è emerso dall'ultimo rapporto CLUSIT, negli anni cambiano le tecniche e le tipologie di attacco. In cima alla lista però ritroviamo sempre le stesse, anche se con forme diverse:

- Phishing
- Social Engineering

I soggetti colpiti negli ultimi mesi sono la P.A. (ad es. Comuni e Ministero dell'Istruzione), l'INPS (con l'invio anche di pec agli utenti) e gli Istituti finanziari che chiaramente vengono colpiti per il tramite dei correntisti.

- Malware per il furto di credenziali;
- Ransomware con richiesta di riscatto per "liberare" i dati aziendali;
- Attacco MITM per bonifici a destinatari "diversi';
- Truffa del CEO;
- EMOTET per rubare conversazioni, credenziali banche e ransomware.

Sono solo alcuni esempi di attacchi perpetrati quotidianamente dai criminali informatici.

E se la minaccia è **interna all'azienda**? Ne parliamo più avanti.