TERZO INTERVENTO · VOCE DELLE IMPRESE

PMI e Cybersicurezza:
paure, errori e problemi che devono essere superati

Essere PMI oggi

La difficoltà di sopravvivere in un mondo difficile

Le preoccupazioni degli imprenditori

L’arrivo della NIS2 nelle PMI

Black hacking, Phishing, Ransomware, Identità digitale, etc…
Come esperto in digitale, non posso che apprezzare quanto fatto dalla NIS2 come spinta al miglioramento della sicurezza.

Ma cosa succede quando queste parole arrivano in una PMI italiana ?

La prima domanda dell'imprenditore

«Quanto mi costa?»

Non è cinismo.
Non è ignoranza.
È la voce di chi ha già troppo da tenere in piedi.

La sicurezza informatica è come le cinture di sicurezza: non ti rendi conto della loro importanza finché non ne hai bisogno.

Anonimo

---

*È ancora vista, **da troppi**, come una tassa travestita da obbligo normativo.*

Le paure delle PMI

L’incertezza del mondo moderno paralizza le aziende

Tre paure che bloccano le PMI

01

L'incomprensibilità

NIS2, DORA, ISO 27001, GDPR — ogni normativa è percepita come un sistema chiuso, scritto da esperti per esperti.

02

L'asimmetria

Le grandi imprese hanno CISO interni. Le PMI hanno, nel migliore dei casi, un responsabile IT che fa anche altro.

03

La sicurezza percepita

«Perché dovrebbero attaccare me? Sono piccolo.»
«Ho comprato l'antivirus»
Convinzioni sbagliate, pericolose e larghissimamente diffuse.

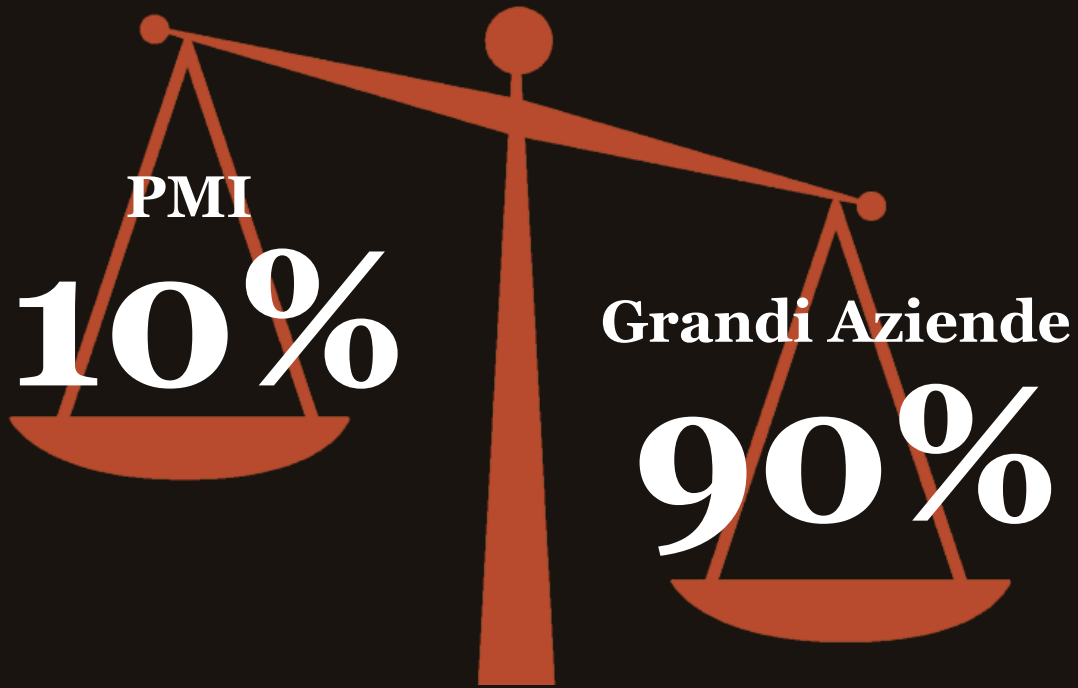
«…Qualora sia necessario sensibilizzare il pubblico per evitare un incidente significativo o affrontare un incidente significativo in corso, o qualora la divulgazione dell'incidente significativo sia altrimenti nell'interesse pubblico, dopo aver consultato il soggetto interessato il CSIRT di uno Stato membro o, se del caso, la sua autorità competente e, se opportuno, i CSIRT o le autorità competenti degli altri Stati membri interessati, possono informare il pubblico riguardo all'incidente significativo o imporre al soggetto di farlo…»

DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

L'imprenditore è frastornato da mille normative complesse, disgiunte che cambiano frequentemente e scritte in una lingua non loro.

Anche quando chiedono aiuto ai consulenti, trovano «esperti» ma non «sistemisti» che possano dare un quadro complessivo e strutturato del problema.

Quante Aziende hanno un CISO (Chief Information Security Officer) ?



60%

degli attacchi informatici colpisce organizzazioni con meno di 250 dipendenti

Non perché siano bersagli appetibili in sé, ma perché sono il punto di accesso più debole verso la supply chain di qualcuno che lo è.

"La cyber sicurezza è come la serratura della casa o dell'auto: non ferma i cattivi ma, se abbastanza buona, li fa andare su obiettivi più facili"

Paul Herbka
Information Systems Security Association

La percezione del valore

Quanto la cybersicurezza e la NIS2 sono valutate dagli imprenditori ?

Ma superate queste paure rimane sempre la domanda:

«Quanto mi costa?»

Quanto vale un'adeguamento a NIS2

Nuovo server
12.500 €

Nuovo Firewall
3.500 €

Adeguamento sistemi backup
2.500 €

Consulenza NIS2
18.500 €

Formazione
3.400 €

Tante voci, spesso non comprensibili dall'imprenditore…che, sfinito, chiede:

ma in totale?

Parliamo di costi... ma quali ?

Costo adeguamento NIS2

25.000 - 70.000 €

Investimento pianificabile, deducibile, spalmabile nel tempo. Con benefici in termini di filiera e competitività.

Costo medio di un data breach

120.000 €+

Fermo operativo, recupero dati, comunicazioni obbligatorie, sanzioni, clienti persi. Nella versione non catastrofica.

Il confronto tra i due costi è semplice e porta facilmente a capire che investire in cyber sicurezza è la decisione giusta.

Allora partiamo…

Ma come ?

Errori da evitare prima di partire

01 Il prodotto

«La sicurezza non è un prodotto.»

02 Il progetto «una tantum»

La cybersicurezza non è un cantiere che si apre e si chiude. È un processo continuo, non un'installazione.

03 Il costo «ridotto»

«Non possiamo tagliare qualcosa ?». I costi sono collegati i rischi che possono essere accettati dall’Azienda.

04 L'isolamento normativo

Trattare NIS2 come adempimento separato da GDPR, ISO 9001 e filiera significa sprecare risorse e perdere sinergie.

Non stiamo parlando di comprare un sistema di sicurezza.

Firewall, antivirus, SIEM sono componenti ma non sono un sistema di sicurezza.
Si deve capire che si tratta di mettere insieme diversi componenti informatici con politiche, procedure e approccio culturale.
Dobbiamo mettere in piedi un processo

NIS2 prevede che la cybersicurezza sia presidiata costantemente

Le PMI dovrebbero avere un CISO che è un componente fondamentale per controllare lo stato del rischio, proporre miglioramenti e adeguare la sicurezza alle esigenze aziendali in modo continuo e perpetuo.

NIS2 chiede di valutare le minacce e poi di decidere il «cosa fare»

Il buon consulente NIS2 non propone pacchetti preconfezionati, ma aiuta l'Azienda ad avere una corretta visione di se stessa e dei propri problemi.
Quindi propone soluzioni, anche scaglionate nel tempo, per percorrere un percorso virtuoso.

NIS2 non è un manuale da mettere su uno scaffale

NIS2 condivide parte di definizioni, di politiche e di procedure con altre normative già presenti in azienda.
Quindi lo sviluppo deve essere condiviso e organico.

Costruire su ciò che già esiste

1

Analisi dei rischi e dei gap

Capire cosa c'è già, cosa manca, quali sono le priorità cosa può essere riutilizzato di quanto esistente.

2

Progettazione integrata

NIS2 come livello aggiuntivo ed integrativo, non come sistema separato.
Sinergie con GDPR e ISO.

3

Approccio di filiera

E’ necessario che tutta la filiera sia integrata e che le relazioni con le altre aziende considerino i requisiti NIS2.

Politiche e procedure.

Evitare la mimicry normativa.

Purtroppo è una tendenza che si è evidenziata sin dalle certificazioni ISO 9001: fare il minimo per non avere problemi con il controllo, senza cambiare la sostanza.

Ma questo approccio espone a rischi invariati con la sola apparenza di conformità e sicurezza.

Cosa manca per finire

Imprenditore, manager e consulenti hanno fatto il loro lavoro.
Abbiamo tutto?

Il fattore umano è il principale anello debole nella cyber sicurezza

Oltre il 90% degli incidenti causati da errori involontari, phishing o comportamenti imprudenti di chi usa gli strumenti.

Step 1: formazione

20 anni fa non c'erano gli smartphone.

20 anni fa non c'erano i social.

In 20 anni abbiamo fatto un salto tecnologico paragonabile al passaggio dal cavallo alle vetture elettriche (che ha richiesto oltre 150 anni) ma senza una adeguata formazione.

Una formazione su informatica e cyber sicurezza è fondamentale.

Step 2: Dal «devi farlo» al «conviene farlo»

Narrativa attuale

"Devi farlo perché te lo impone la normativa"

Genera resistenza e approccio minimalista.

Narrativa efficace

"Conviene farlo: protegge l'azienda, Il tuo posto e quello dei colleghi"

Crea valore, genera responsabilità.

Vantaggio competitivo

La strategia di una azienda deve essere lungimirante in particolare nei momenti di crisi di settore

PARTE V · COMPETITIVITÀ DI FILIERA

La cybersicurezza diventerà un requisito di accesso

Molte grandi imprese si stanno adeguando alla NIS2 e dal 2027 andranno a richiedere ai propri fornitori — spesso PMI — prove documentate di adeguamento alla NIS2.

Chi arriva preparato

vince appalti e contratti di fornitura con vecchi e nuovi clienti

Chi arriva impreparato

Rischia di non poter essere considerato per nuovi contratti e vedrà chiuse le porte di nuovi clienti

Quattro richieste concrete dalle imprese

Abbiamo visto i problemi e le difficolta delle PMI.
Ma cosa serve loro per aiutarli nel processo di miglioramento della cyber sicurezza ? Queste le loro richieste.

Cosa chiedono le PMI ?

01 Semplificazione dell'accesso agli strumenti

Voucher, crediti d'imposta, fondi europei esistono ma sono dispersi. Serve uno sportello unico, una mappa chiara.

02 Approccio integrato

I consulenti dovrebbero lavorare in Team per rendere più agevole il percorso alle Aziende e ai dipendenti.

03 Pacchetti scalabili

La soglia di ingresso a livello di hardware/software/servizi è ancora troppo costosa per le piccole imprese.

04 Un approccio di filiera responsabilizzante

Chi impone requisiti di sicurezza ai fornitori deve avere un ruolo attivo nell'accompagnarli.

Oggi la cybersicurezza non è il problema delle PMI italiane.

La cyber sicurezza sarà la condizione necessaria affinché le PMI italiane restino protagoniste in Europa e nel mondo.