CYBER | FPI FONDAZIONE PIEMONTE INNOVA

fondirigenti

CYBERSECURITY: A CHE PUNTO SIAMO?

Risultati dell'indagine sulla consapevolezza delle imprese in tema di sicurezza informatica

GLOBAL OVERVIEW: cyber attacchi noti a livello globale 2018 - 2021

Fonte: Clusit - Rapporto 2022 sulla Sicurezza ICT in Italia

Il commento di Stefano Gorla

Indagine condotta su oltre **100 imprese** da Fondazione Piemonte Innova nell'ambito del #progettoCYBER di Fondirigenti, in collaborazione con Unione Industriali Torino e Federmanager Torino.

- **69%** proviene dal Piemonte
- **40%** attiva nei diversi comparti del settore industria
- **41%** di piccola dimensione

Percezione e consapevolezza

44% delle imprese valuta il **grado** di sicurezza aziendale di **medio livello**

66% delle imprese guarda con attenzione al tema della **cybersecurity**

Le imprese investono in cybersecurity per motivi di natura esterna:

- rispetto delle normative **46%**
- eventi avversi **42%**
- evidenza di attacchi **32%**

Le azioni che possono contribuire a proteggere i sistemi sono:

- controllo e verifica periodica dei sistemi **61%**
- aggiornamento tecnologico **58%**
- cultura aziendale orientata alla sicurezza **57%**

Da qui, la necessità di una formazione a tutti i livelli aziendali, top management compreso.

Quali sono i primi passi delle imprese per aumentare le proprie difese?

- **promuovere un approccio multidisciplinare alla cybersecurity**
- **coinvolgere funzioni organizzative**
- **sviluppare una cultura aziendale orientata alla sicurezza**

A seguire:

- definire il **perimetro aziendale da difendere**
- affidarsi a **partner tecnologici qualificati**
- dotarsi di **Chief Information Security Officer – CISO**, una figura competente in tema di sicurezza dedicata alla gestione della cybersecurity (oggi solo il 10% delle imprese intervistate ne ha uno).

#progettoCYBER

I 5 attacchi cyber più comuni

Cyber ha definito, attraverso il coinvolgimento diretto delle imprese, un **modello per supportare le aziende**, in particolare le PMI, nell'individuare e implementare strategie **per prevenire e sostenere la capacità di risposta e di resilienza ad attacchi cyber**.

METODI, STRUMENTI E PERSONE

La cybersecurity non è (solo) una questione di tecnologie.

METODI

È fondamentale strutturare processi per:

Organizzare tavoli stabili multifunzione

tra livelli aziendali diversi e funzioni aziendali differenti

Simulare attacchi informatici

per gestire gli eventi avversi, comprendere chi e quando coinvolgere, rispettare le normative vigenti ecc.

STRUMENTI

TECNOLOGICI → **IT**

Autenticazione multi fattore, anti-malware, aggiornamento automatico sistemi, monitoraggio continuo, data protection e gestione accessi

ORGANIZZATIVI → **HR, LEGAL E COMUNICAZIONE**

Tavoli stabili multifunzione, governance, budget dedicato, controlli organizzativi, figure aziendali preposte (CISO)

NORMATIVI → **LEGAL**

Informazioni su enti esistenti, figure aziendali preposte (DPO), valutazione applicazione norme ISO, in particolare la ISO/IEC 27001

CYBER READINESS LEVEL → **TOP MANAGEMENT**

PERSONE

1

EDUCAZIONE DI BASE

È necessario creare una conoscenza di base sui rischi informatici tramite un percorso di alfabetizzazione alla sicurezza informatica

2

FORMAZIONE

A tappeto, nessuno escluso, per rispondere a esigenze e obiettivi specifici: top management, personale e tecnici

3

AGGIORNAMENTO

La formazione va mantenuta e aggiornata in modo continuativo

LA PAROLA AGLI ESPERTI

Gli impatti e i costi di una scarsa consapevolezza sul tema della cybersecurity
STEFANO GORLA

Regole e processi per una corretta gestione della cybersecurity
CESARE GALLOTTI

La mia rete è pronta contro attacchi cyber?
NICOLA NAPOLI

CONTROLLI BASE CYBERSECURITY

Misure: organizzative | tecnologiche | normative

POLITICHE

- Valutazione del rischio e piano di trattamento del rischio
- Politiche e regole al personale

RESPONSABILITÀ

- Identificazione di un responsabile per la sicurezza (CISO) e di un responsabile GDPR (DPO)
- Censimento degli amministratori di sistema
- Monitoraggio delle fonti di informazione in merito alla sicurezza

PERSONALE

- Formazione al personale anche con corsi online
- Formazione ai dirigenti
- Prevedere formazione tecnica ai tecnici sugli strumenti usati
- Partecipazione ad associazioni che si occupano di sicurezza

INVENTARIO

- Inventario dei server e delle applicazioni
- Inventario dei dispositivi assegnati agli utenti

CONTROLLO ACCESSI

- Limitazione degli accessi
- Segregazione dei dati
- Modalità di archiviazione dei dati
- Processo di gestione delle credenziali con canali di comunicazione ben definiti
- Processo di gestione delle autorizzazioni, con canali di comunicazione ben definiti
- Riesame periodico delle autorizzazioni assegnate
- Controllo degli accessi degli amministratori di sistema

SICUREZZA FISICA

- Manutenzione degli impianti, inclusi quelli collegati all'informatica

GESTIONE DEI SISTEMI IT E DEI DISPOSITIVI

- Processo di gestione dei cambiamenti dei sistemi informatici
- Processo di ritiro dei dispositivi e cancellazione delle memorie
- Cifratura dei dispositivi
- Anti-malware
- Backup
- Logging con raccolta su sistema dedicato
- Aggiornamento automatico o semi-automatico di dispositivi e server

SICUREZZA DI RETE

- Firewall
- Canali di trasmissione cifrati

SICUREZZA APPLICATIVA

- Regole per lo sviluppo delle applicazioni

GESTIONE DEI FORNITORI

- Contratti con i fornitori con clausole di sicurezza e privacy

GESTIONE DEGLI INCIDENTI

- Procedura di gestione degli incidenti relativi alla sicurezza delle informazioni e alla privacy
- Piano di comunicazione ai clienti in caso di incidenti con impatto sui loro dati

CONTINUITÀ OPERATIVA

- Piano e sito di Disaster Recovery (DR)
- Fare test del DR

CONFORMITÀ

- Audit interni periodici
- Verifica dell'operato degli amministratori di sistema

CYBER READINESS LEVEL

Strumento in grado di raccogliere e misurare lo stato di consapevolezza generale in merito alla sicurezza dei dati e dei processi, individuando **possibili aree di miglioramento e crescita di competenze manageriali e tecnologiche** sulle quali investire per una migliore gestione della sicurezza.

Il CRL è strutturato su 5 dimensioni, ognuna articolata in **5 criteri**; per ogni criterio sono poi descritti **5 differenti scenari**.

Dimensioni

- **Protezione**
- **Compliance e normative**
- **Gestione e tecnologie**
- **Fattore umano**
- **Organizzazione e processi**

Valore target del campione di imprese

Impresa A

Overall score impresa A

Criteri

- Aggiornamento software
- Policy di sicurezza
- Crittografia
- Backup
- Sicurezza della rete

- Strumenti cloud
- Vulnerability Assessment e Penetration Test
- Inventario
- Gestione applicativi
- Amministratori di sistema

- Manutenzione IT
- Piano di rientro
- Autenticazione
- Segregazione della rete
- Acquisizione strumenti di sicurezza

- Adeguamento privacy (GDPR)
- Monitoraggio normativa
- Conformità ISO/IEC 27001
- Valutazione del rischio
- Esecuzione audit interni/esterni

- Formazione e sensibilizzazione
- Ruoli e responsabilità
- Gestione regole
- Partecipazione ad associazioni
- Gestione autorizzazioni

#progettoCYBER

In collaborazione con:

UNIONE INDUSTRIALI Torino | FEDERMANAGER Torino e Valle d'Aosta

Scopri quanto è cyber-ready la tua azienda