confimi industria PIEMONTE

Confederazione dell'Industria Manifatturiera Italiana e dell'Impresa Privata

10 Giugno 2021

Risk & Insurance Management

Cyber Risk e Business Interruption

Relatore Dott. Franco Maiolo

Co relatore Dott. Domenico Aiello

In collaborazione con

MAG

I numeri del fenomeno Cyber in Italia

- **43 milioni:** numero di attacchi Cyber rilevati nel 2019
- **7 milioni:** costo medio annuo per violazioni della sicurezza informatica
- **62:** numero medio annuo di security breach per azienda
- **30 - 60:** Giorni necessari per risolvere le problematiche causate dai cyberattack

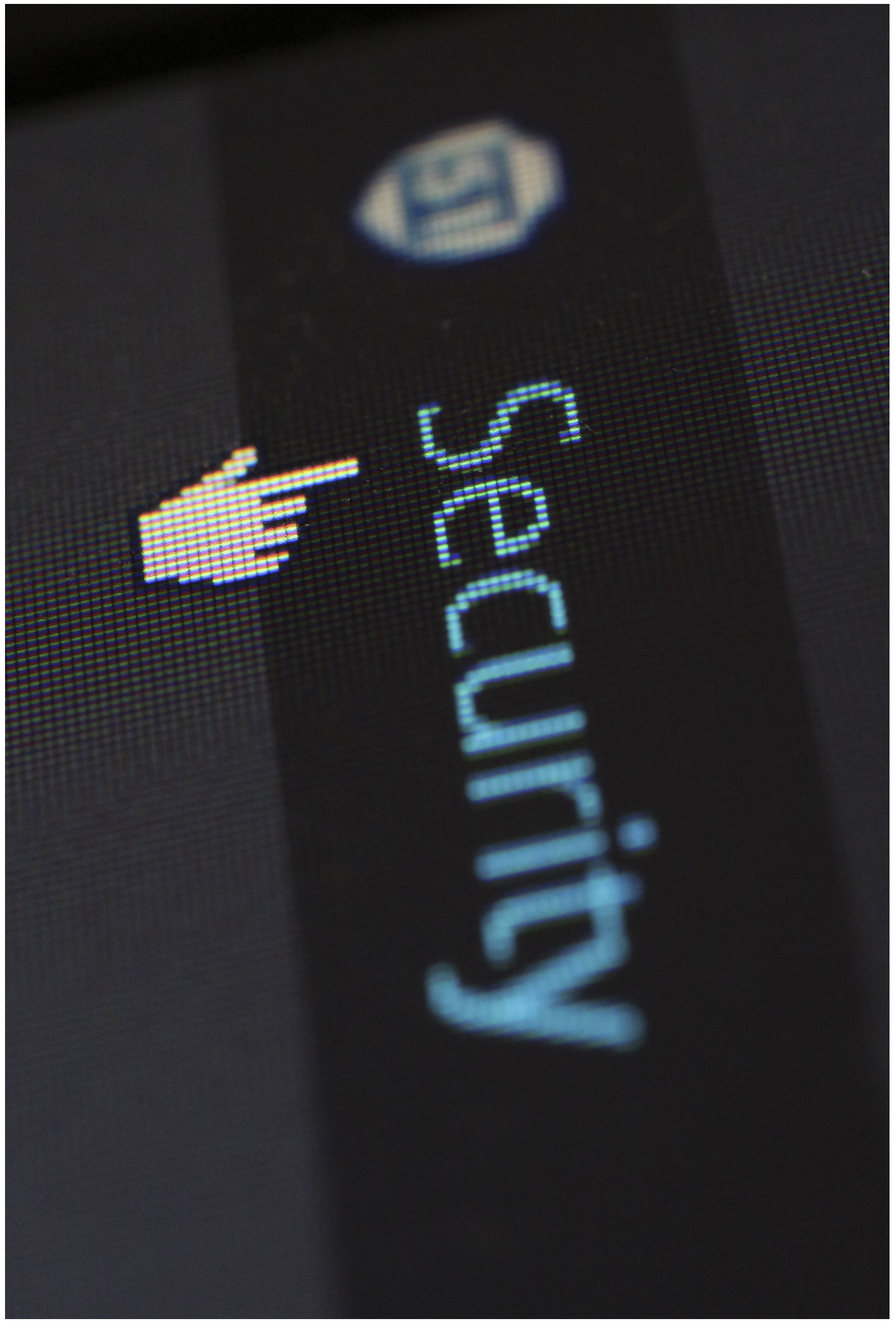
Gli hackers non sono più singoli che utilizzano il proprio PC per tentare attacchi sporadici: sono centinaia di gruppi criminali organizzati, multinazionali dotate di mezzi illimitati, stati nazionali con i relativi apparati militari e di intelligence, che operano su scala globale, 365 giorni all'anno.

Lo sviluppo delle tecnologie comporta, di pari passo, la creazione di nuove metodologie di attacco sempre più «raffinate» e di impatto potenzialmente letale per un'Azienda.

Si prevede che la frequenza e l'impatto degli attacchi cyber in termini di costi (di risarcimento, recupero dati, pagamento riscatti, etc..) e danni di immagine siano destinati ad aumentare in maniera rilevante nei prossimi mesi.

In questo contesto, inoltre, la formazione informatica rivolta ai propri dipendenti è solitamente trascurata.

Oltre il 70% dei sinistri (noti e denunciati) è causato da errori / negligenze del personale.



Impatto del virus COVID sui rischi Cyber

La pandemia COVID-19 ha determinato un grande e inaspettato cambiamento nella vita sociale (isolamento domiciliare), in quella lavorativa (smart-working) e nelle modalità di vendita di beni (e-commerce).

Non solo la vita privata, ma anche, e soprattutto, la vita lavorativa, sono ora fortemente caratterizzate dalla dipendenza dai canali virtuali ed elettronici.

Così facendo la pandemia ha aumentato il rischio di subire attacchi cyber (cyber attacks), favoriti in particolare da alcuni fattori quali:

- Difficoltà per le aziende a controllare l'utilizzo dei devices da parte dei dipendenti durante lo smart-working (connessioni su siti non sicuri, utilizzo delle mail personali, etc..)
- Utilizzo, in alcuni casi, anche di devices personali da parte dei dipendenti, che sono potenzialmente meno sicuri di quelli aziendali (assenza o non aggiornamento dei firewall, assenza di blocchi a navigare in siti non sicuri, assenza di blocchi in caso di download di programmi non sicuri)
- Utilizzo di reti private dotate di sistemi di sicurezza inadeguati

Impatto del virus COVID sui rischi Cyber

I criminali informatici cercheranno, nel breve e nel lungo periodo, ogni modo per sfruttare tali nuove vulnerabilità, ricorrendo anche a metodi già collaudati quali e-mail di phishing, per introdurre malware nei sistemi o ingannare gli utenti nel divulgare informazioni sensibili aziendali.

- **68%**: dipendenti che utilizzano device personali per proseguire l'attività lavorativa
- **50%**: aziende che adottano tecnologie di connessione (VPN)
- **+1000%**: tentativi di phishing dall'inizio del lockdown

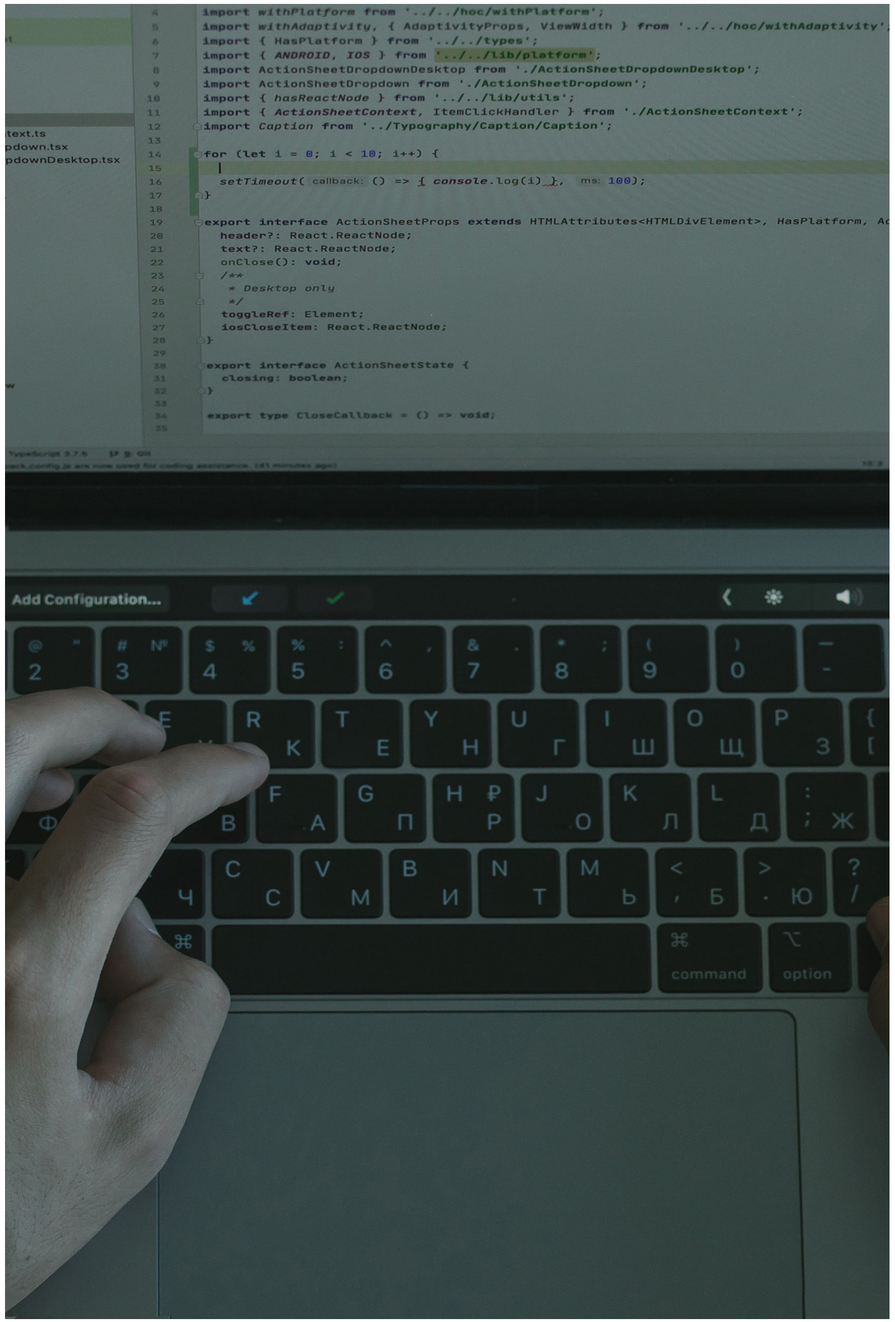
Nessuna realtà è immune da attacchi cyber

- Un gruppo di hacker ucraini e russi dal 2005 al 2012 rubò oltre 160 milioni di informazioni bancarie, successivamente messe all'asta sul web.
  Danno provocato: oltre 300 milioni di dollari.

- Un ragazzino di appena 15 anni, riuscì a insinuarsi nei sistemi della NASA e del Dipartimento di Stato Americano spiando migliaia di e-mail, contenenti molti documenti riservati, tra cui anche password di dispositivi militari, ed impossessandosi di un pezzo di codice di un programma della NASA.

- Morris Worm sviluppò un codice per misurare la vastità del cyber spazio. Quando fu immesso in rete, però, si trasformò in un malware capace di infettare più di 6.000 computer e provocare dei danni vicini ai 100 milioni di dollari.

https://cybermap.kaspersky.com/it
https://www.enforcementtracker.com/



Nessuna realtà è immune da attacchi cyber

Prima di implementare un'adeguata strategia di trasferimento del rischio al mercato assicurativo, è fondamentale supportare i propri Clienti nell'identificazione e nell'analisi delle principali aree critiche interessate dal rischio Cyber.

Abbiamo implementato, in collaborazione con alcuni consulenti informatici specializzati, un efficace sistema di Cyber Risk Assessment al fine di prevenire e mitigare le principali fonti di rischio che potrebbero dare origine ad un sinistro:

- Valutazione della resilienza

- Controllo e implementazione di adeguate strategie di «incident response», «business continuity» e «disaster recovery»

- Analisi dei controlli di sicurezza IT fondamentali e delle buone pratiche da seguire per minacce specifiche come il ransomware e la compromissione della posta elettronica aziendale

Nessuna realtà è immune da attacchi cyber

- Formazione dei dipendenti

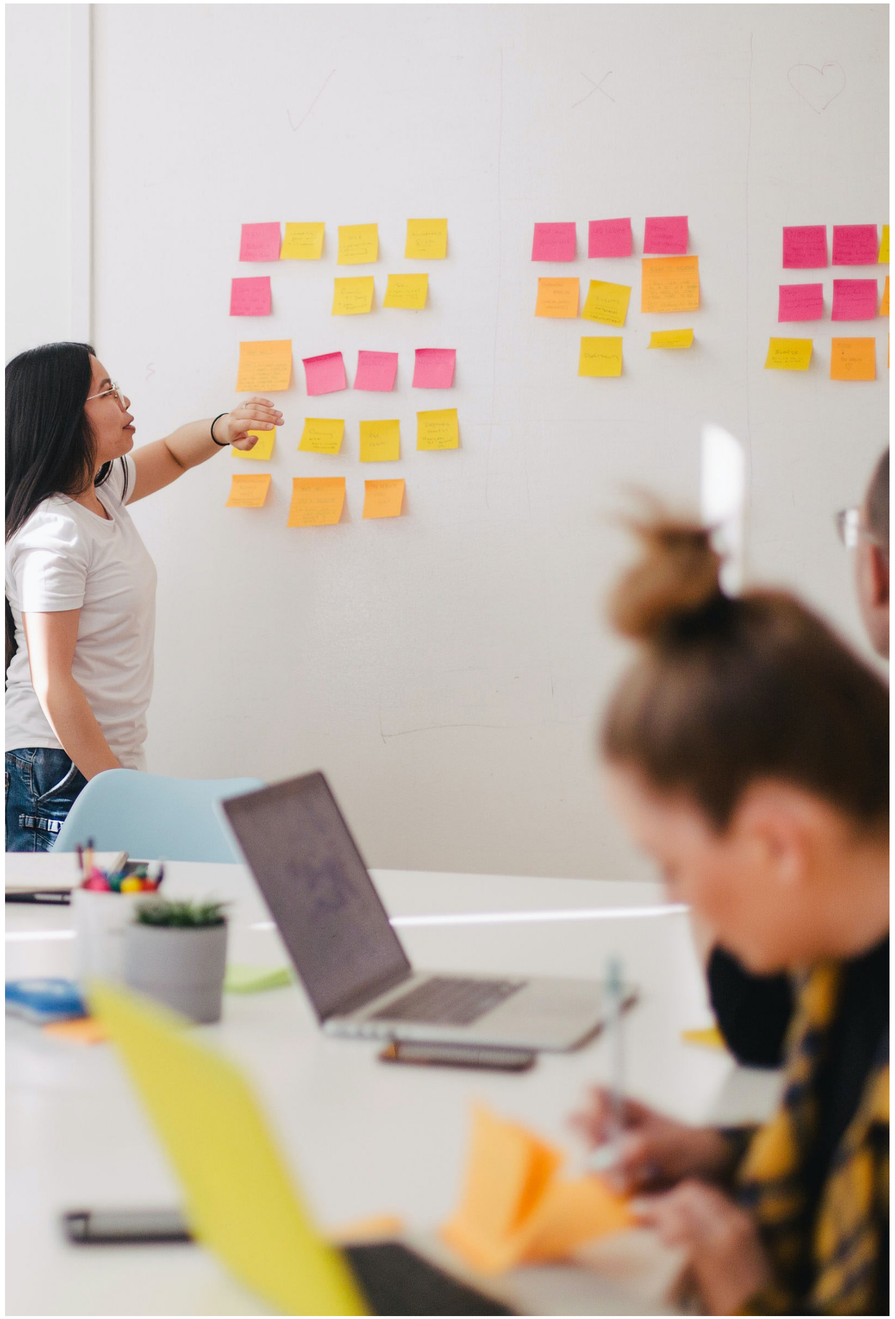
– Il comportamento dei dipendenti è ancora uno dei rischi maggiori garantiamo l'accesso a materiale formativo che tratta argomenti quali phishing e malware, sicurezza mobile e Wi-Fi, furto d'identità e sicurezza delle password

- Conformità alle leggi e ai regolamenti

– Comprensione della normativa di riferimento

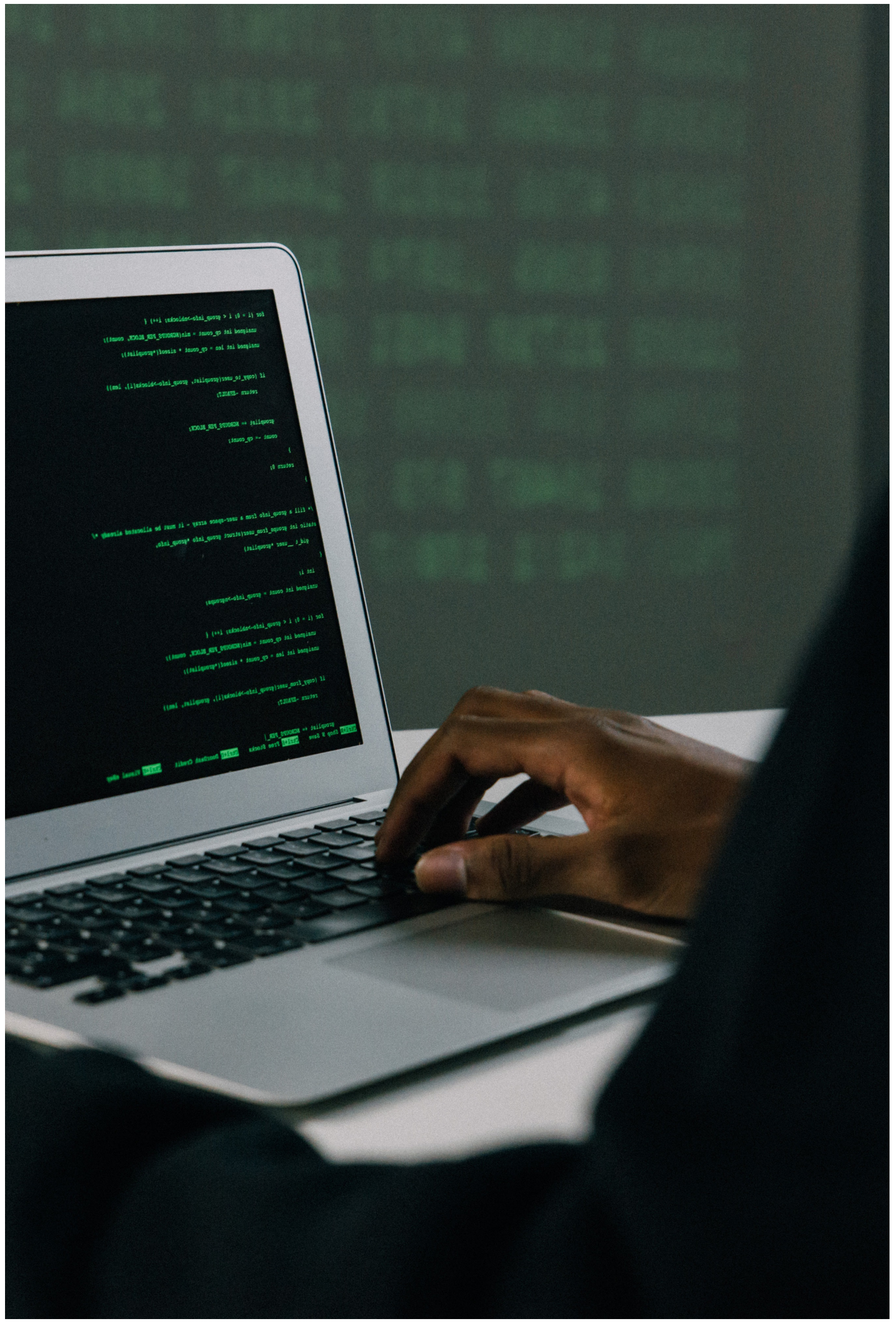
– Esempi di policies interne e procedure per il rispetto del GDPR

– Notizie e aggiornamenti sulle modifiche legislative e normative e sulle ultime tendenze in materia di applicazione da parte delle autorità di regolamentazione



Danni causati da Attacchi Cyber alle Imprese

- Business Interruption
  - Perdita di profitto
  - Spese extra per mitigare un mancato guadagno (consulenti, straordinari dipendenti,...)
- Ripristino dei dati
  - Sostituzione, ripristino o costi di correzione
  - Costi per determinare se tali dati e programmi possano essere rimpiazzati
- Trasferimento di fondi
  - Sottrazione di denaro, moneta virtuale o altro bene equivalente
- Cyber extortion
  - Danni da estorsione
  - Costi di consulenza sostenute da un esperto IT



Responsabilità verso Terzi

Le imprese, anche alla luce del nuovo regolamento europeo 2016/679 sulla protezione dei dati, risultano esposte a potenziali ingenti richieste di risarcimento da parti di terzi / autorità regolamentari e relative spese di difesa.

- Privacy
  - Difesa contro azioni regolamentari
  - Divulgazione non autorizzata di informazioni di società di terze
  - Divulgazione non autorizzata di informazioni strettamente personali
- Sicurezza della rete
  - Distruzione di dati elettronici di terzi
  - Trasmissione virus a computer o sistemi di terzo
  - Coinvolgimento inconsapevole del proprio network in attacchi DoS
- Multimedia
  - Diffamazione
  - Invasione della privacy
  - Violazione Proprietà Intellettuale
  - Pubblicazione negligente o rappresentazione ingannevole

Le risposte del mercato assicurativo

Collaborazione con i principali Assicuratori, nazionali ed internazionali, operanti nel ramo Cyber garantendo ai propri Clienti prodotti assicurativi:

- Economicamente convenienti
- Aderenti ai migliori standard qualitativi offerti
- Taylor - made in base alle specifiche esigenze di copertura
- Operanti anche per le spese legali ed i costi di consulenza sostenuti

Al fine di ottenere una prima indicazione di quotazione sono sufficienti:

- 3-5 giorni per la compilazione del questionario
- 5-10 giorni per l'analisi dei dati da parte degli Assicuratori

webinar

confimi industria PIEMONTE

Confederazione dell'Industria Manifatturiera Italiana e dell'Impresa Privata

C.so Vittorio Emanuele II, 107 - 10128 Torino
011 191.16.682 - info@confimiindustriapiemonte.it