cyber.3techgroup.it

CYBER SECURITY.

La **difesa** prima dell'*attacco*.

3tech

Vittime
2020.

Attacco Ransomware all'azienda Geox, giugno 2020
ENEL: 7 giugno e 19 ottobre 2020
Enac, l'Ente Nazionale per l'Aviazione Civile, il 10 luglio del 2020.
Attacco alle Amministrazioni: i casi Tor Vergata e Spallanzani
Malware a Luxottica: settembre 2020
Campari: richiesta di riscatto record
Il gruppo Carraro: cassa integrazione per i dipendenti
Comune di Rieti: chiesto un riscatto da 500mila euro
Irpinia ambiente

Vittime
2021.

21 febbraio - Ospedali Francesi
14 marzo - Microsoft Exchange Server
10 aprile - Scuola Italiana - Boggi Milano
12 aprile - Atc Torino
14 aprile - Comune di Brescia, FBI
22 aprile - Zambon 11 maggio - Colonial pipeline
Phishing - Pec Italia
15 maggio - Servizio sanitario irlandese
25 maggio - Bose Sony LittleBigPlanet
3 giugno - Jbs fornitore mondiale carne
8 giugno - New York Times, Financial Times, Guardian, Spectator, El Mundo, Verge, Le Monde, Corriere della Sera, Gazzetta dello sport, Amazon, Reddit, Twich, GitHub.

14 giugno - Luxottica
2 luglio - Kaseya e la rete di 200 aziende utilizzatrici Usa
6 luglio - Miroglio di Alba
17 luglio - EA Electronic Arts
1 agosto - Regione Lazio 12 agosto - Accenture
20 ottobre - Siae
26 ottobre - San Carlo Italia - distributori di benzina Iran - Javascript
10 novembre - MediaMarket Media World, Gruppo Argos, Robinhood (trading online)
15 novembre - FBI, Comune di Torino
19 novembre - ALIBABA, GODADDY
28 novembre - Windows
15 dicembre - ISTAT

Vittime di cosa?

Il concetto di Risk Management è entrato in azienda, specie nella piccola e media, grazie essenzialmente al D.l. 81/08 sulla salute dei luoghi di lavoro e solo dopo una pressione a livello legislativo e mediatico mai visto nella storia dell'industria italiana, ma non è entrato nel DNA dell'imprenditore che è orientato al risultato e alle performance e troppo spesso non considera rischi diversi da quelli commerciali, amministrativi, finanziari o al limite reputazionali.

Si parla di attacchi e di hacker ma in maniera troppo generica e superficiale.

I professionisti, le società pubbliche e private, gli enti no profit e tutte le categorie commerciali in generale sono vittime della propria leggerezza e della scarsissima attenzione al problema.

Risk management, cybersecurity e budget.

«Risk management» significa letteralmente «gestione del rischio», cioè valutare il grado di rischio di un evento e prevenirne gli effetti prima che questo si verifichi.

Se c'è una cosa OGGI che possa fermare in pochi istanti l'operato di anni di impegno, fatica, sforzo, rischio, passione, lavoro, dedizione, controllo, affidamento, delega, fiducia... è un VIRUS INFORMATICO.

Allora la Cybersecurity DEVE essere uno degli asset aziendali e deve avere una propria voce di spesa dedicata nel budget.

3tech

cyber.3techgroup.it

Lo strumento informatico in azienda oggi è:

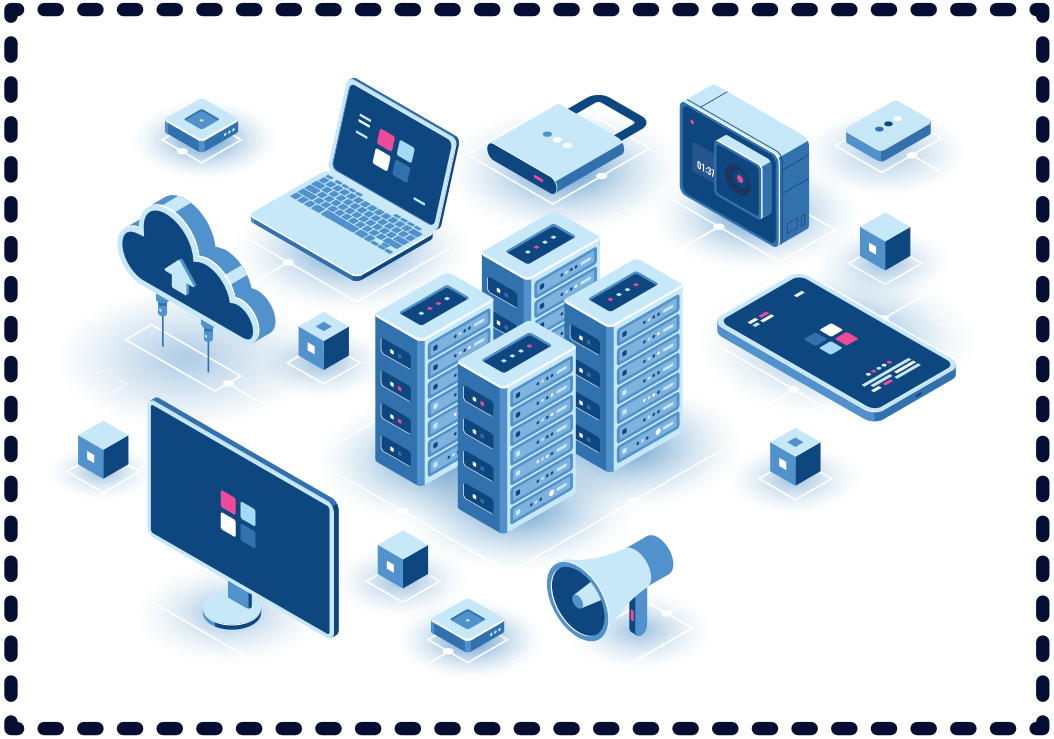
- Ricerca della massima efficienza del sistema azienda, sia in presenza che in telelavoro.
- Gestione ottimale dei workflow per risparmiare tempo e denaro.
- Massima velocità di esecuzione delle statistiche.

3tech

cyber.3techgroup.it

Il nuovo paradigma Cyber Security Perimeter (CSP):

Va considerato però che solo il 30% delle vulnerabilità è dovuto a gap tecnologico, mentre il restante è nelle mani delle persone che lavorano dentro, fuori e per l'azienda.



Perimetro di Sicurezza (CSP)

3tech

cyber.3techgroup.it

Da cosa ci difendiamo?

Il peggiore nemico dell'azienda allo stato attuale della conoscenza è il **CRYPTOLOCKER** o **RANSOMWARE.**

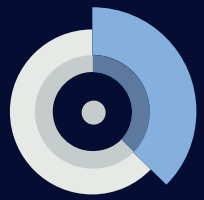
Che cosa fa?

Crittografa e rende illeggibili i dati contenuti nei server e nei pc e pretende un riscatto per de-crittografarli e tornare alla normalità

Come fare per evitarlo?

Prima di tutto bisogna capire da dove viene e come viene inoculato nel sistema....

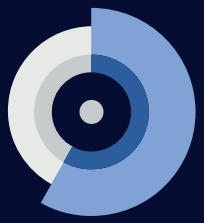
Come si infetta un sistema informatico?



Vulnerabilità tecnica
Ipotesi molto probabile

30% dei casi

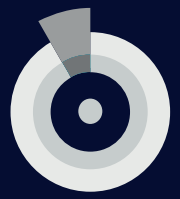
Updating SO
Updating policies...



Vulnerabilità uomo
Ipotesi estremamente probabile

70% dei casi

Man in the middle
Phishing
Usb Key...



Attacco diretto
Ipotesi remota

Riservata ad aziende «visibili»

3tech

cyber.3techgroup.it

E quindi come ci difendiamo?

Vulnerabilità tecnica

Audit + Vulnerability assessment continuo + remediation plan continuo + **Verifica CDA**

Vulnerabilità uomo

Formazione costante, continua, specializzata in casi reali – essenziale la **verifica** del grado di conoscenza

Telelavoro su dispositivi non adeguati

Blocco USB e dispositivi esterni

Attacco diretto

Quanto già detto + **penetration test**

3tech

cyber.3techgroup.it

Ma che costi dobbiamo sostenere?

Ci sono voci di spesa **vitali**:

- Backup reale con accurati test di ripristino
- Sistemi firewall aggiornati e presidiati sia come policy che come updating di software e firmware
- Sistemi antivirus di ultima generazione con RDR su TUTTI i dispositivi connessi, fissi, mobili, macchine utensili, rulliere, cartesiani....
- Formazione del personale con test di avvenuto trasferimento di consapevolezza e competenze

Altre voci non meno importanti, ma da affrontare quando le prime sono completamente implementate e gestite:

- Vulnerability assessment network & WEB
- Consulenza continua da parte di un Security Officer con comprovata esperienza
- Penetration Test

Quanto ci costerebbe un attacco informatico?

In uno scenario in cui il patrimonio informativo aziendale acquisisce un valore sempre più elevato e il perimetro di sicurezza delle organizzazioni, anche per via di nuove tecnologie come 5G e cloud, diventa sempre più vasto, si assiste contestualmente a una continua evoluzione delle tecniche di attacco e delle metodologie utilizzate dai criminal hacker, il cui scopo non è più soltanto quello di danneggiare i sistemi e le infrastrutture critiche dei loro target, ma soprattutto impossessarsi di dati e informazioni riservate.

Parlando di costi di un attacco informatico, quindi, non ci si può più limitare a quelli relativi al ripristino del corretto funzionamento di un sistema: qualunque violazione al perimetro di sicurezza delle aziende può causare notevoli danni non solo materiali, ma anche e soprattutto a operation, vendite e reputazione online e nei confronti dei clienti.

Non a caso, l'*Allianz Risk Barometer 2020*, il più importante sondaggio sui rischi a livello mondiale, riconosce le interruzioni del business causate da violazioni di sicurezza IT come il rischio più grave per qualsiasi organizzazione.

Per rispondere correttamente e reagire velocemente a minacce e attacchi sempre più evoluti, mantenendo comunque l'attività aziendale, è opportuno pianificare un piano di difesa e resilienza che consenta di strutturarsi al meglio per rispondere a qualunque tipologia di minaccia e ridurre la superficie di attacco.

Non è semplice valutare quanto costa, alle aziende, un attacco informatico: nonostante i beni aziendali siano sempre più digitali e il perimetro di sicurezza sempre più "liquido" ed esteso per via della diffusione di nuove tecnologie disruptive come il 5G e il cloud, tutte le organizzazioni e in particolar modo le PMI rischiano di essere messe in ginocchio da attacchi informatici sempre più mirati e sofisticati. Infatti, oltre ai costi diretti dovuti al fermo produttivo e alla conseguente riattivazione dei servizi, l'impatto di un attacco cyber sulle aziende si misura anche in termini di mancate opportunità di investimenti e di immagine dell'azienda stessa.

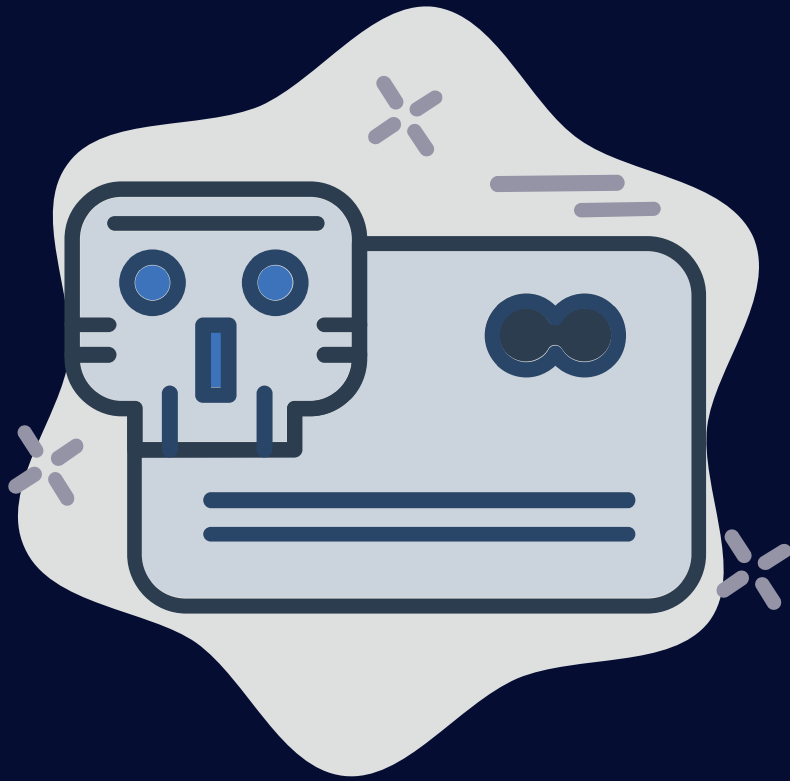
Sempre più spesso, infatti, il danno maggiore causato da un attacco informatico è quello reputazionale, connesso molte volte all'interruzione o comunque al malfunzionamento dei servizi offerti dall'azienda, e che rischia di incidere anche pesantemente sulle vendite, sui rapporti con i clienti e sul rapporto con investitori e finanziatori.

Uno scenario, come conferma il *Rapporto Clusit 2020*, in cui il più delle volte gli attacchi informatici, sempre più sofisticati e mirati, non sono più condotti da semplici "artigiani" del cyber crimine, ma da veri e propri *threat actors* organizzati e dotati di mezzi tecnici ed economici illimitati, il cui obiettivo è quello di colpire le infrastrutture, le reti, i device mobili e gli oggetti IoT che ormai sono sempre più diffusi anche in ambito produttivo (soprattutto in situazioni critiche come quella attuale dovuta all'emergenza sanitaria per la pandemia di coronavirus). Una situazione aggravata, tra l'altro, dal fatto che il tessuto industriale italiano è costituito principalmente da piccole e medie imprese che, a differenza di organizzazioni Enterprise in grado di strutturarsi al proprio interno per stare al passo con le esigenze di cyber security, non sono capaci di affrontare in autonomia le minacce informatiche, anche perché il budget a disposizione

è notevolmente diverso.

Diventa, dunque, di fondamentale importanza comprendere che, per rispondere correttamente e reagire velocemente a minacce e attacchi sempre più evoluti, mantenendo comunque l'attività aziendale, è opportuno pianificare un piano di difesa e resilienza che consenta di strutturarsi al meglio per rispondere a qualunque tipologia di minaccia e ridurre la superficie di attacco.

In parole povere, le aziende devono organizzarsi in maniera tale da poter sopportare il contraccolpo di un attacco informatico e garantire la disponibilità dei servizi erogati grazie alla capacità di anticipare, resistere, superare e adattarsi alle condizioni avverse successive alla compromissione
delle risorse informatiche.



I costi di un attacco informatico.

Calcolare i costi di un attacco informatico non è ovviamente un'operazione semplice: sono tanti, infatti, i fattori che entrano in gioco e che bisogna valutare con attenzione. In linea di massima, comunque, è possibile misurare l'impatto di un cyber attacco sulle aziende in questo modo:

• **Costi diretti:** come il nome stesso lascia intuire, sono tutti i costi dovuti, innanzitutto, al fermo produttivo. È importante effettuare una stima di quanto costi "restare fermi" a causa dell'attacco informatico e per quanti giorni. All'interno dei costi diretti rientrano, poi quelli sostenuti per effettuare le necessarie investigazioni alla ricerca del punto debole o della falla nei sistemi informatici sfruttata dai criminal hacker per portare a termine l'attacco, i costi sostenuti per la notifica di un eventuale data breach, nonché quelli sostenuti per eventuali spese legali. Infine, bisogna considerare tutti i costi correlati al ripristino dei servizi e della normale operatività aziendale.

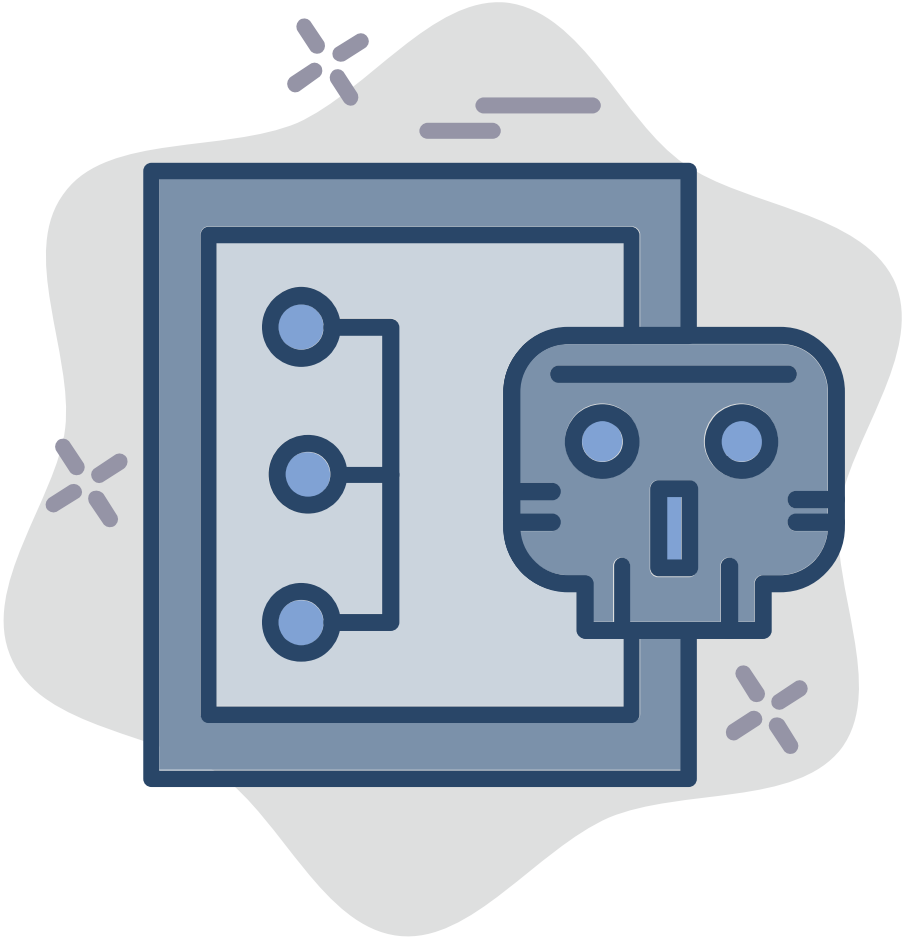
• **Costi di opportunità:** includono opportunità di affari persi o minore produttività, perdita del vantaggio competitivo, perdita di redditività o persino perdita di intere linee di business a vantaggio dei concorrenti. Nel 2016, il 23% delle organizzazioni ha subito una perdita di opportunità a causa di intrusioni e tra queste il 42% ha registrato una perdita di opportunità che rappresenta oltre il 20% del valore della società stessa.

• **Impatto negativo** sull'innovazione: se i risultati della R&S sono mal riposti e utilizzati liberamente da tutti, compresi i concorrenti, la R&S non offre sostanziali vantaggi competitivi. Inoltre, finché la minaccia del cyber-furto continua a crescere, le aziende potrebbero diventare meno desiderose di investire nell'innovazione, a causa del rischio di appropriazione indebita della loro R&S. In particolar modo ad essere impreparate sono tutte quelle PMI che, a causa di uno scarso budget dedicato alla

sicurezza e alla poca consapevolezza, considerano questa spesa solo un costo e non un investimento.

- **Investimento:** questi costi includono la spesa annuale globale per i software di cybersecurity, delle risorse e dell'assicurazione relativa alla sicurezza informatica. A tale riguardo, SSP Blue prevede che le aziende di tutto il mondo spenderanno circa 170 miliardi di dollari per la sicurezza informatica entro il 2020 (con un tasso in crescita di quasi il 10% dal 2015).

- **Reputazione:** le aziende possono subire un deprezzamento sostanziale se la notizia della violazione viene resa pubblica; a questo si aggiunge il valore perso delle relazioni con i clienti, la perdita di contratti e la svalutazione del nome commerciale.
600 aziende di medie dimensioni in sei paesi europei hanno segnalato il verificarsi di danni alla reputazione nel 48% degli incidenti e perdite finanziarie nel 33% dei casi.



Dopo un attacco, in quanto tempo torniamo alla normale operatività?

Nel **caso migliore** in cui l'azienda abbia backup consolidati e affidabili e la capacità di ripristinarli, bisogna affrontare i seguenti step:

- Bonifica di tutti i sistemi
- Ripristino
- Test
- Ritorno alla normalità:
  - **Per una PMI con 15 postazioni di lavoro?** Almeno 10 giorni di fermo totale, ma bisogna essere davvero preparati, perché potrebbero diventare almeno il doppio
  - **Per una Grande azienda?** Non è quantificabile.

Nel **caso peggiore** in cui i backup sono corrotti dall'attacco o non sono usufruibili:

- Resta il pagamento del riscatto (anche se si tratta di reato di favoreggiamento secondo l'art.379 c.p) e la speranza.
- Diversamente? Si ricomincia da capo.

3tech

cyber.3techgroup.it

Come agisce 3tech?

La **mission** di 3tech è salvaguardare le aziende.
Come?

Primo Audit
Remediation Plan
Gestito
Attuato

Vulnerability assessment continuo
Network
WEB

Presentazione dei risultati al CDA / Imprenditore

Reiterazione del processo

Call to action:

- Effettuare quanto prima un audit specifico sul proprio livello di vulnerabilità
- Scegliere un partner altamente specializzato e *super partes*
- Mettere a calendario secondo una cadenza almeno semestrale la formazione specifica per gli utenti
- Deliberare un budget che preveda un *vulnerability assessment* continuativo
- Inserire l'area "cybersecurity" all'ordine del giorno del CDA
- Utilizzare un sistema di newsletter interno per tenere i dipendenti e i collaboratori sempre aggiornati
- Indire un sistema di alerting da parte degli utenti

CYBER SECURITY.

La **difesa** prima dell'*attacco*.

3tech srl
Via A. Grandi 3

info@3techgroup.it

071 22191

cyber.3techgroup.it