- Le tecnologie abilitanti 4.0 -

Cybersecurity

A cura della Struttura
"Orientamento al lavoro e
digitalizzazione"

Camera di Commercio
Roma

Settembre 2022

Indice

1. Cosa si intende per *Cybersecurity*

2. Un po' di numeri:

- *l'ampliamento del mercato*

3. Gli attacchi informatici

4. Le misure di sicurezza:

- *Security Compliance & Policy*
- *Security Hardware & Software*

5. Il fattore umano

6. Strumenti gratuiti per le imprese

Cosa si intende per *Cybersecurity*?

«*La sicurezza informatica è l'insieme dei mezzi e delle tecnologie tesi alla protezione dei sistemi informatici in termini di disponibilità, confidenzialità e integrità dei beni o asset informatici*».

Appare piuttosto chiaro che la sicurezza informatica non viene assicurata da un apparato fisico, programma, persona o metodologia specifica ma dall'**insieme di questi fattori interdipendenti**.

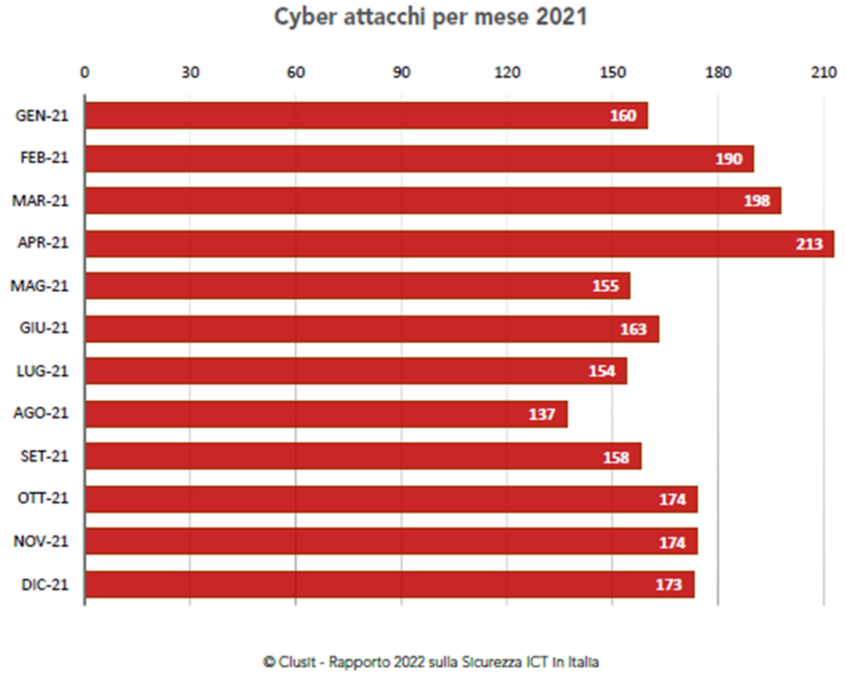
Un po' di numeri: il rapporto *Clusit 2022*

Perché investire sulla sicurezza informatica?

Le tendenze esposte nel rapporto **"Clusit 2022"** sulla sicurezza informatica in Italia indicano che, negli ultimi anni, c'è stata una crescita costante di **attacchi hacker**.

Il campione preso in esame comprende complessivamente **7.144 attacchi** classificati tra **gennaio 2018** e **dicembre 2021**, di cui **1.874 nel 2020** e **2.049 nel 2021**, con una **media complessiva di 171 attacchi gravi al mese** nel 2021.

Il picco massimo, come si evince dal grafico, **si è avuto ad aprile 2021 (213 attacchi).**



Un po' di numeri: l'ampliamento del mercato

Elaborazione di Unioncamere e InfoCamere sui dati del Registro delle Imprese delle Camere di Commercio, nel periodo tra **settembre 2021 e giugno 2022,** sull'ampliamento delle imprese del comparto della Cybersicurezza.

giugno 2022:
3.147 imprese (+ 5,4%)
(a settembre 2021 erano 2.985)

Crescita del comparto dopo il vero e proprio balzo fatto registrare nel biennio **2018-2020 (+32%).**

giugno 2022:
29.100 unità (+ 2,3%)
(a settembre 2021 erano 26.700)

La crescita include, oltre alla nascita di nuove imprese e alla riconversione di aziende preesistenti alle nuove attività, **l'aumento degli addetti di 29.100 unità, con una media di 9 addetti per azienda.**

Unioncamere, Economia & Imprese – il magazine delle Camere di Commercio N. 3 Luglio 2022, pag. 8

Un po' di numeri: l'ampliamento del mercato

La presenza più elevata di **imprese** è nel **Lazio**
dove, al 30 giugno 2022, avevano sede 708 imprese ,
pari al **22%** del totale.

Sul fronte degli **addetti,**
il Lazio si posiziona al secondo posto in
Italia, con **5.480 addetti.**

Gli attacchi informatici

Gli attacchi che possono subire le attività produttive si distinguono, in base alla finalità, in:

CYBER CRIME - (a scopo di lucro «diretto»)

HACKTIVISM - (per motivi di natura politica/sociale)

CYBER ESPIONAGE - (finalizzati al furto di informazioni)

Gli attacchi informatici

Le tipologie di attacchi informatici possono riassumersi in:

DDOS - Distributed denial of service - tentativo ostile di bloccare server, rete, servizi

RANSOMWARE - programma informatico dannoso (malevolo)

DATA BREACH - Violazione dei dati

Gli attacchi informatici

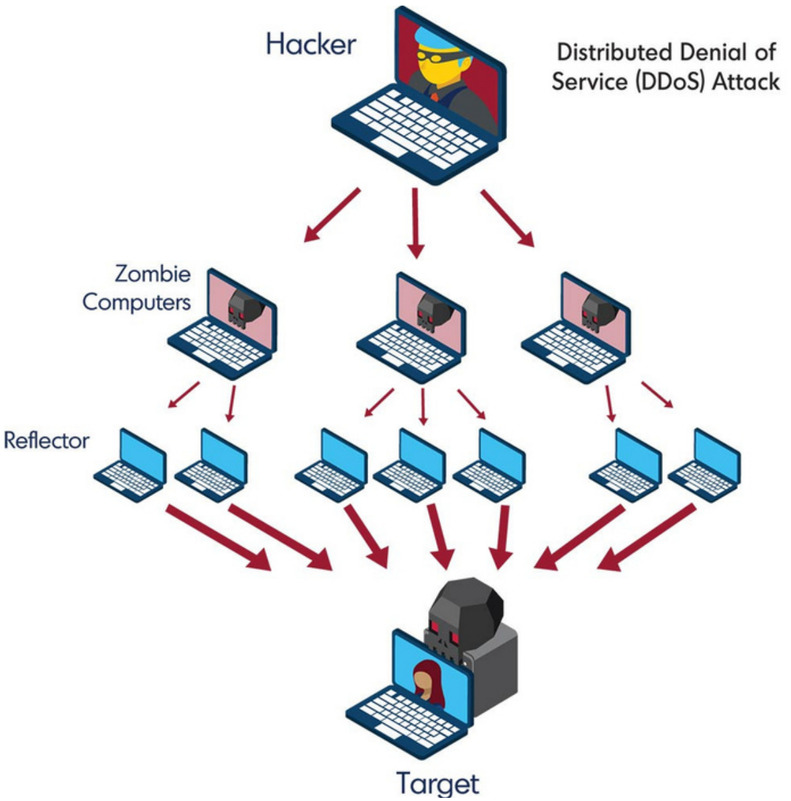
Ddos

Distributed denial of service

Attacchi mirati a causare un'interruzione dei servizi informatici o impedire l'uso di una risorsa di rete.

Metodo

Strumenti in grado di impegnare le risorse di rete oltre misura, impedendo o anche paralizzando l'attività (***ping flooding*** e ***stressors***).



Gli attacchi informatici

Ransomware

Attacchi mirati a crittare dati nella disponibilità dell'utente, sequestrandoli a scopo estorsivo fino al pagamento del «riscatto».

Metodo

Programmi malevoli (*malware*) in grado di infettare il sistema e occultarne i dati, salvo l'utilizzo di specifico codice noto solo agli hackers.

Gli attacchi informatici

Data Breach

(trad. violazione dei dati)

Attacchi tesi a carpire informazioni, dati rilevanti e *know-how*, quali atti di spionaggio vero e proprio.

Metodo

Programmi malevoli (malware), espedienti in grado di ingannare l'utente e indurlo a fornire le proprie credenziali di accesso (***phishing***).

Gentile cliente,
ti informiamo che il dominio scadrà il giorno: **xx/xx/xxxx**

La registrazione del nome a dominio te ne assicura l'esclusività ed evita che altri possano acquistarlo.
Proteggi la tua attività, il tuo lavoro o la tua immagine, rinnovalo subito!

RINNOVA ORA CON UN CLICK

Per visualizzare il riepilogo dell'ordine e l'importo da pagare, puoi procedere al rinnovo da questa pagina inserendo la tua login e la relativa password.

Cordiali saluti

Customer Care.

Le misure di sicurezza

L'ecosistema della sicurezza informatica racchiude **diversi elementi interconnessi**; nessuno di essi è in grado, da solo, di arginare il problema.

La soluzione non può essere rinunciare alla digitalizzazione, in quanto la transizione verso le tecnologie 4.0 è ormai un passaggio obbligato per molti business.

Non si tratta di digitalizzarsi o meno, ma di farlo bene e in sicurezza.

Misure di carattere organizzativo e dispositivo

1° macro categoria: ***Security compliance e policy***

2° macro categoria: ***Security Hardware & Software***

3° macro categoria: **il fattore umano**

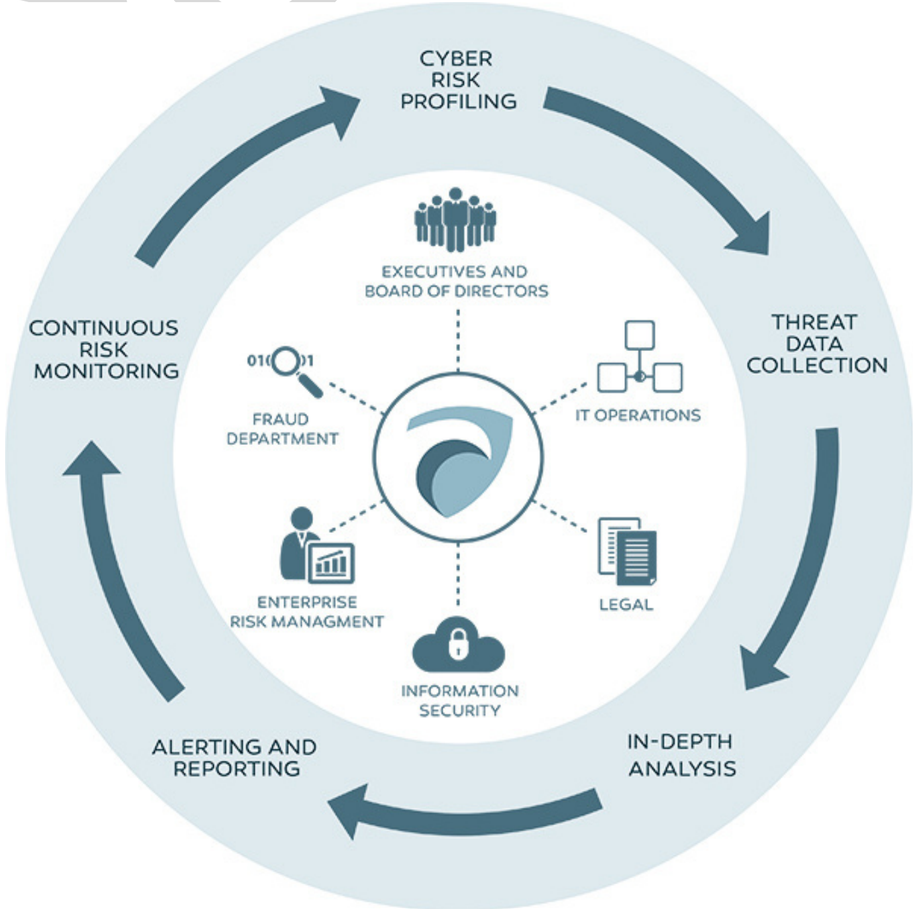
1° - Security Compliance & Policy

- L'adozione di modelli ***Security Governance*** adeguati che valorizzino figure professionali specializzate, come **il Direttore della Sicurezza Informatica** o ***CISO*** (*Chief Information Security Officer*);
- L' approccio alla **gestione del rischio in maniera concreta**, tramite valutazioni che tengano conto sia della tecnologia sia delle informazioni sia dei soggetti chiamati a maneggiarle.

1° - Security Compliance & Policy

- **Documentare la propria *policy* e i protocolli di sicurezza**, stabilendo degli standard che si collocano nella realtà contingente e non come mero adempimento amministrativo;
- **Includere tutta la «superficie intelligente»**, pianificando e regolando l'utilizzo degli strumenti *smart*, anche mobili o indossabili, fino a quelli nella disponibilità del personale (***BYOD***).

1° - Security Compliance & Policy



- L'integrazione della ***Cyber Threat Intelligence*** come processo aziendale cardine, cioè lo studio, analisi ed elaborazione strategico-tattico-operativa per la prevenzione e reazione alle minacce;
- Aggiornamento continuo e costante condivisione delle informazioni con **una rete collaborativa** di soggetti, sia pubblici sia privati, in grado fornire un quadro il più completo e attuale possibile.

2°: *Security Hardware & Software*

Software **Anti-Virus** e **Anti-Malware**
(sempre aggiornati)

Vpn e dispositivi avanzati di tipo
Firewall

Data Loss Protections - DLP
(soluzioni avanzate di monitoraggio
e protezione dei dati)

Honeypots
(vulnerabilità fittizie per distrarre gli
hackers)

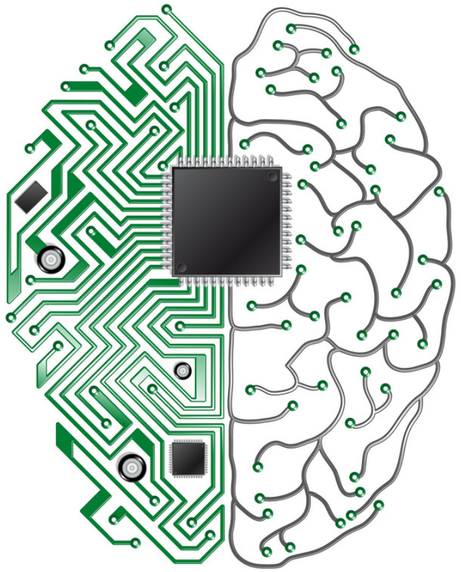
URL Filters e Content Filters
(che inibiscono siti o contenuti «rischiosi»)

Anti-Bot Protections
(che limitano l'attività di bots malevoli)

Sandboxes
(«posti sicuri» dove disinnescare
le minacce)

Sistemi autenticazione avanzata
(a due fattori, con token, biometrici etc)

3° - Il fattore umano



Puntare sulla tecnologia senza **prima investire nella formazione, sensibilizzazione e reclutamento** di personale in grado di adoperarla adeguatamente rischia di essere un'arma a doppio taglio.

Non solo l'investimento tecnologico non darà i frutti sperati ma aumenterà esponenzialmente la **superficie di vulnerabilità informatica** dell'impresa e la «fragilità» del proprio business.

Allo stesso modo, se **manca la consapevolezza** delle finalità dei protocolli di sicurezza, anche se ben progettati, gli utenti ottempereranno solo sul piano formale.

Urge quindi una sicurezza reale e concreta.

3° - Il fattore umano

Dall'analisi dei dati globali più aggiornati, la stragrande maggioranza delle vulnerabilità informatiche delle imprese dipende da un **errore umano**.

Il **personale impreparato** è facile preda di attacchi informatici, anche banali ma che possono infliggere ingentissimi danni all'impresa.

In tutti i campi della sicurezza, il fattore umano può essere l'anello debole oppure la **componente che fa la differenza.**

3° - Il fattore umano

La *condicio sine qua non* per l'ecosistema della *cyber security* è la ***Security Staff Awareness*** *e cioè* la **conoscenza e consapevolezza delle implicazioni e significati della propria attività nell'ottica della sicurezza informatica.**

La *Security Staff Awareness* coinvolge molti aspetti:

3° - Il fattore umano

Il personale, a tutti i livelli, deve essere posto in condizione di

- **Conformarsi** alle normative e agli standard vigenti in materia di sicurezza informatica e protezione dei dati;
- **Conoscere**, comprendere e applicare a pieno i protocolli e procedure interne;
- **Interiorizzare** la *ratio* delle disposizioni e misure previste.

3° - Il fattore umano

Ogni utente deve avere contezza di:

- **Rischi** concreti connessi alla specifica attività che si è chiamati a compiere in base alla tipologia dei dati trattati, criticità delle operazioni e dei possibili danni conseguenti;
- **Minacce** ed espedienti tipicamente adoperati dagli hackers, in modo da scongiurare gli attacchi o **reagire** in maniera tempestiva e adeguata (obbligo di segnalazione interna).

3° - Il fattore umano

La dirigenza e le figure chiave nella struttura dell'impresa devono:

- Essere sempre al corrente di ogni dettaglio relativo agli accessi al proprio sistema, potendo individuare **chi ha effettuato l'accesso, quando, a cosa e da dove**;
- **Conoscere il fabbisogno di accesso** e distribuirlo solo a coloro che ne hanno necessità **(principio del *need-to-access*);**
- Prestare particolare attenzione all'accesso da «**terze parti**».

3° - Il fattore umano

Nell'approcciarsi alle nuove tecnologie:

- Ogni utente deve essere ben conscio della natura degli **strumenti «intelligenti» e come vengono utilizzati** anche nella propria attività: uno *smart phone* e uno *smart watch* non sono più soltanto un telefono e un orologio ma porte aperte sul mondo;
- La scelta dei dispositivi deve essere guidata dalla ricerca della **sicurezza quale requisito imprescindibile**, investendo nell'analisi e progettazione dell'attività.

3° - Il fattore umano

Tutti gli utenti devono essere educati sui principi base della gestione delle credenziali d'accesso, come:

- **Modificare la password** d'accesso predefinita al primo accesso;
- **Personalizzare le proprie credenziali** per renderle più difficili da «bucare»;
- **Non utilizzare la medesima password** per l'accesso a diversi sistemi o piattaforme;
- **Conservare le credenziali** in maniera sicura e non comunicarla mai a nessuno.

Cybersecurity: alcuni servizi gratuiti di *assessment* della Camera di Commercio di Roma e del PID nazionale

CHECKUP
Sicurezza IT

PID
Cyber
Check

servizio consultabile sulla pagina
della Camera di Commercio di Roma all'indirizzo:
https://www.rm.camcom.it/pagina3801_cybersecurity.html

Qual è il livello
di sicurezza informatica
della tua impresa?

Scoprilo con
Minerva

servizio consultabile sulla pagina
della Camera di Commercio di Roma all'indirizzo:
https://www.rm.camcom.it/pagina3764_cultura-digitale-per-limpresa.html

Il servizio *PID Cyber Check*

La rete dei PID delle Camere di Commercio ha predisposto un **servizio specifico e gratuito di assessment** in grado di dare un'autovalutazione del livello di rischio di un attacco informatico al quale l'impresa può essere esposta.

"PID *Cyber Check*":

- non fornisce indicazioni sui presidi da mettere in atto per proteggere l'impresa da attacchi *cyber*, ma permette di **focalizzare gli eventuali rischi a cui si può andare in contro;**
- restituisce una stima del danno economico derivante dai possibili attacchi attraverso un ***report* personalizzato** elaborato sulla base delle risposte fornite al test.

CHECKUP Sicurezza IT PID Cyber Check

Il servizio "Minerva"

Minerva è un progetto ideato nel 2021 dalla **Camera di Commercio di Roma** per la diffusione della cultura digitale in tema di ***Cybersecurity***, una delle tecnologie abilitanti del Piano Nazionale Industria 4.0. Si tratta di uno strumento sviluppato su due livelli:

- la realizzazione di un elenco di **"buoni consigli"** sulle accortezze da seguire durante le attività di connessione.
- un breve questionario specifico, che avrà valore di ***self-assessment***, rivolto alle imprese e alle organizzazioni che vogliono conoscere il loro grado di consapevolezza sul tema della sicurezza informatica.

Sentieri digitali per le PMI

Guide e manuali:
- Competenze digitali di base
- Internet e dati
- Pensiero computazionale

La bussola digitale:
- il *web*
- il *marketing online*
- i *social network*

Minerva:
Self-assessment sulla *Cybersecurity*

Le professioni del futuro:
- l'*innovation manager*
- il *data scientist*

Cultura digitale per l'impresa

Le tecnologie abilitanti:
- Realtà aumentata
- Intelligenza artificiale

***Suite* orientamento formazione lavoro**

Camera di Commercio di Roma
Struttura "Orientamento al lavoro e digitalizzazione"

Via de' Burrò 147
www.rm.camcom.it
orientamentoedigitalizzazione@rm.camcom.it