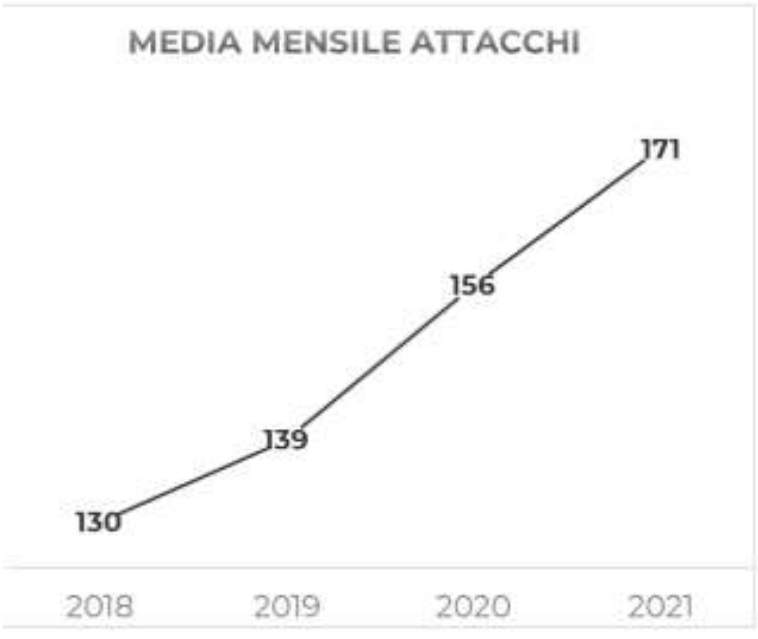
IN CRESCITA GLI ATTACCHI ALLA CIBERSICUREZZA

Nel mondo digitale connesso, i criminali informatici, utilizzano strumenti sempre più sofisticati per lanciare attacchi informatici contro le aziende e sono soprattutto le aziende sanitarie ad essere prese di mira. Stiamo imparando, poco a poco, a conoscere termini come *hacktivisti, terrorismo informatico, attacco digitale.*

Gli attacchi informatici si distinguono in livelli: *Basso, Medio, Alto, e Critico.*
Solo nel 2021 gli attacchi di livello Critico hanno rappresentato ben il 37% del totale mentre mentre, quelli di livello Alto, si sono verificati nella metà dei casi.
Ne deriva che quasi l'80% degli attacchi è Alto o Critico.
L'Italia risulta sopra la media mondiale per numero di attacchi critici e tra le tipologie di attacco quella *cybercrime* è la più frequente e fa registrare gli attacchi più elevati a partire dal 2011. Rimangono sostanzialmente stabili in termini percentuali le altre categorie come espionage/sabotage, Information malware e Hacktivism.

Dagli studi effettuati da alcune C*yber security company* nell'anno 2021 emerge che l'80% delle aziende sanitarie sono state a rischio hacker.



Negli ultimi 4 anni gli attacchi informatici hanno avuto un'ulteriore incremento e, come riportato dall'Associazione *Clusit* (Associazione Italiana per la sicurezza informatica – CEO gruppo digital360), sono stati in media al mese:
130 nel 2018, 139 nel 2019, 156 nel 2020 e 171 nel 2021.

Il rapporto *Clusit* ha anche evidenziato il record di incidenti informatici classificati come ***attacchi gravi.*** *Da 1.874 nel 2020 a 2.049 nel 2021.*
A livello mondiale si sono registrati 14.010 attacchi gravi nel periodo gennaio 2011-dicembre 2021 di cui oltre la metà, 7.144, sono avvenuti dal 2018 in poi.
Nel 2021 gli attacchi informatici verso l'Europa sono cresciuti dal 16% al 22% rispetto al 2020.
Se prendiamo come riferimento gli attacchi avvenuti dal 2018 al 2021 in Europa se ne registrano 900 e ben 185 di questi attacchi sono registrati in Italia.
Il nostro paese negli ultimi anni è diventato un bersaglio sempre più frequente.
Molti di questi attacchi avvengono con scopi estorsivi per i quali si richiede un riscatto.

E' interessante esaminare la distribuzione di questi attacchi e i loro bersagli.

I dati confermano che nel 2021 la categoria ***Gov*** (attacchi a siti governativi) sia stata al primo posto in

LOREDANA MASSERIA-|Responsabile social media

assoluto raggruppando il 15% del totale delle offensive su scale mondiale.
Se si focalizza l'attenzione sullo scenario degli attacchi in Italia, prendendo in esame il periodo tra gennaio 2018 e giugno 2021, con ben 143 attacchi, si comprende quanto la minaccia *cybercrime* sia reale e crescente anche nel nostro Paese.
Il 35% delle attività dei *cibercriminali* durante il periodo preso in esame ha colpito due comparti trainanti come la PA italiana e il settore della Sanità.

Anche *Trend Micro* (Multinazionale americano-giapponese di software per la sicurezza informatica) nella presentazione del report annuale ha rilevato che l'Italia è il quarto paese al mondo e il primo in Europa più colpito dai malware.
A questo si aggiunge il fatto che mancano circa 1000 esperti di *cyber security*.

Ma quali sono gli attacchi informatici più eclatanti e curiosi della storia cibernetica?

Ad esempio, durante la guerra fredda tra URSS e Stati Uniti, le operazioni di spionaggio informatico erano fondamentali per le due nazioni. Rimase famoso nel 1982 un fatto emblematico che vide i tecnici del CIA riuscire ad introdursi all'interno del sistema di gestione delle pompe del gas che aveva il compito di controllare il funzionamento di un impianto situato in Siberia. Gli hacker statunitensi mandarono in tilt il protocollo di sicurezza del sito, causando l'aumento incontrollato della pressione interna del gasdotto e l'esplosione di quest'ultimo. Ciò dimostrò che la guerra cibernetica può sostituire le bombe.

Nel 2012 le due multinazionali del settore bancario Visa e Mastercard sono state oggetto Black Hacking, il quale ha comportato il furto dei dati di oltre 10 milioni di carte di credito. Tra le due, Mastercard è stata particolarmente bersagliata in quanto nel 2005 è stata compromessa nei suoi meccanismi di difesa cibernetica.

Da ricordare anche WannaCry, un particolare Trojan diffuso nel maggio del 2017 che nel giro di un paio di settimane ha sfruttato un punto vulnerabile di Windows arrivando ad infettare centinaia di migliaia di computer in almeno 150 paesi del mondo riuscendo a criptare i dati trovati all'interno.

Parlando del mondo sanitario, ospedali, centri medici, laboratori analisi, ecc. come già detto, sono sempre di più nel mirino degli attacchi hacker.
Possiamo ricordare l'attacco Hacker del maggio 2022 ai sistemi gestionali informatici dell'ASST Fatebenefratelli Sacco di Milano (azienda che comprende che comprende 4 ospedali e 33 sedi sanitarie e sociosanitarie territoriali) che ha messo fuori uso i portali di ogni struttura gestita dall'azienda costringendo il personale sanitario a ripiegare su procedure cartacee. La regione Lombardia ha confermato l'attacco nonostante l'accrescimento delle misure di sicurezza che aveva posto in essere negli ultimi anni.

LOREDANA MASSERIA- | Responsabile social media

Nell'ottobre 2021 l'attacco informatico al Data Center dell'Unione Terre di Pianura – Bologna – ha bloccato i servizi in sei comuni per un totale di 70 mila residenti.

Nella Regione Lazio ricordiamo tutti l'attacco degli hacker dello scorso anno che ha interessato la rete informatica della Regione Lazio mandando in tilt i servizi privati e le aziende tra cui il sistema informatico sanitario e quello dedicato alla vaccinazione contro il covid-19 e il rilascio del Green Pass. I danni ai sistemi comportarono un mese di interruzione dei servizi, dal sistema sanitario online per i cittadini ai registri dei dati delle farmacie e perfino settori come quello urbanistico.

Nello stesso anno anche nella regione Toscana sono andati distrutti molti dati epidemiologici. Un attacco Hacker ai server dell'Agenzia Regionale della Sanità della Toscana ha causato la distruzione di numerosi dati epidemiologico-statistici.

L'elenco è davvero lungo:
- Comune di Palermo: giugno 2022 - l'attacco informatico ha colpito i sistemi informatici all'interno della rete su cui è ospitato il sito istituzionale, la gestione della centrale operativa della polizia municipale e il sistema di gestione della video sorveglianza.
- NeL maggio 2022 l'attacco hacker alla ASP di Messina da un gang ransomware Lokbit ha causato 27 mila dati sanitari finiti in rete.
- Ferrovie Calabria – sempre 2022, il sistema Treniitalia per il blocco della vendita dei biglietti a causa di un attacco hacker.
- marzo 2022 attacco all'ARPAM (Agenzia regionale per protezione ambientale delle Marche) Regione Marche- nel mese di marzo un attacco ransomware subito con tentata estorsione e successiva diffusione in rete dei dati rubati dagli hacker.
E l'elenco potrebbe continuare.

La situazione è davvero grave tanto da parlare di guerra ibrida. La preoccupazione dell'Europa, dopo lo scoppio della guerra in Ucraina è cresciuta in quanto sono cresciuti gli attacchi ai sistemi informatici dei governi. La guerra cibernetica tra Russia ed Europa oggi si svolge anche on line. Recentemente la Russia ha subito gli attacchi di Anonymous che ha colpito banche e ministeri russi mandando in crisi stazioni televisive e siti di propaganda.
Occorre che tutti i cittadini e in particolare gli operatori delle strutture sanitarie, divenute ormai obiettivi sensibili, imparino ad essere più prudenti anche nella gestione della propria casella di posta elettronica. Spesso basta aprire inavvertitamente una e-mail che sembra innocente per innescare la diffusione del virus.

di Loredana Masseria