

CYBERSECURITY

(ottobre 2021)

Nel 2020 l'incremento degli attacchi cyber a livello globale è stato pari al 29% rispetto alla media degli attacchi per anno del triennio precedente.

Nel 2020 gli attacchi cyber sono stati messi a segno prevalentemente utilizzando Malware (42%), tra i quali spiccano i cosiddetti Ransomware, una tipologia di malware che limita l'accesso ai dati contenuti sul dispositivo infettato, richiedendo un riscatto, utilizzati in quasi un terzo degli attacchi.

Sono alcuni dei dati contenuti nel Rapporto Clusit 2021. Secondo i dati di Check Point, una tra le principali aziende di sicurezza informatica, in media, ogni 10 secondi un'azienda nel mondo è vittima di un attacco ransomware.

Tornando ai dati del rapporto Clusit, a fronte di 945 miliardi di dollari di danni generati dal solo cybercrime nel 2020 (erano 600 miliardi nel 2018), nello stesso anno la spesa globale in ICT security è stata di 145 miliardi di dollari (di cui 1,5 miliardi in Italia), ovvero per ogni dollaro investito in sicurezza dai difensori gli attaccanti hanno causato (considerando solo gli attacchi realizzati con finalità cybercriminali) 7 dollari di perdite.

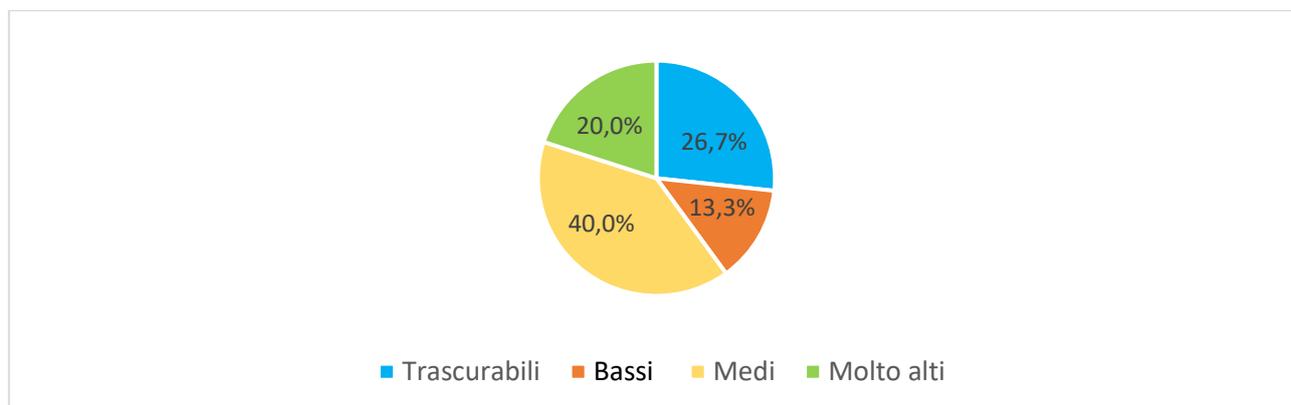
La maggior consapevolezza dei rischi legati agli attacchi informatici in periodo di pandemia ha spinto le aziende ad innalzare i propri livelli di protezione dotandosi di strumenti tecnologici, come ad esempio firewall o VPN per garantire la continuità operativa. Tali strumenti da un lato hanno consentito ai dipendenti l'accesso da remoto alle reti virtuali aziendali, dall'altro ad avere una maggiore protezione perimetrale e una conseguente riduzione della superficie di attacco.

Questa novità, sicuramente positiva, ha spinto i criminali informatici a spostare la loro attenzione verso un punto più debole della catena ovvero verso il pc del dipendente. Si è infatti notata una crescita del numero di attacchi indirizzati ai pc personali che sono raddoppiati rispetto allo stesso periodo del 2019. Questo fenomeno è spiegabile

considerando che, durante il periodo di emergenza, molte aziende non sono riuscite a dotare i propri dipendenti di laptop aziendali, con conseguente utilizzo di dispositivi personali, solitamente maggiormente vulnerabili a malware e attacchi di phishing.

Secondo un sondaggio riguardante le imprese italiane contenuto nel rapporto Clusit, il 23,8% delle aziende del campione riporta di aver subito attacchi informatici nel corso dello scorso anno. I danni subiti sono stati valutati trascurabili per il 26,7% dei soggetti coinvolti, bassi per il 13,3%, di media entità per il 40%, e molto alti per il 20%. La tipologia di danni subiti risulta essere per il 37,5% riconducibile ad una perdita di dati, per il 25% di natura economica, per il 16,7% ad un danno di immagine, il 16,6% di tipo fisico/infrastrutturale e di tempo. Mentre il 4,2% non ha rilevato alcun danno a seguito dell'attacco ricevuto. Si evince dal sondaggio, infine, che le aziende, a seguito della pandemia, stiano cambiando la loro percezione sul livello di consapevolezza della sicurezza informatica.

Attacchi Cybercrime nel corso del 2020 in Italia Come valuta i danni subiti l'azienda



Elaborazione Ufficio Studi Confindustria Udine su dati dell'Osservatorio sulla CyberSecurity di Exprivia – Rapporto Clusit 2021

La rivoluzione tecnologica e la conseguente elaborazione di modelli di business fondati sull'utilizzo dei sistemi informatici costituiscono un fenomeno innegabile ed in continua accelerazione. Considerati i rischi e le conseguenze degli attacchi informatici e l'estensione capillare di tale tecnologia in tutti i settori produttivi è dunque essenziale che le imprese, nello svolgere l'analisi dei rischi legati all'attività e al modello di business, tengano in adeguata considerazione il rischio informatico ed investano budget adeguati per ridurre al minimo le esternalità negative associate a tale fattore di pericolo.

Info: Gianluca Pistrin – studi@confindustria.ud.it