

Attacchi comuni per aziende:

1 | phishing mail e pubblicità ingannevole, secondo il sito della polizza postale il phishing E' una particolare tipologia di truffa realizzata sulla rete Internet attraverso l'inganno degli utenti. Si concretizza principalmente attraverso messaggi di posta elettronica ingannevoli.

2 | malware sono virus prendiamo un virus "ransomware" secondo il sito malwarebytes Il ransomware, è un tipo di malware che blocca l'accesso ai sistemi o ai file personali degli utenti e chiede il pagamento di un riscatto per renderli nuovamente accessibili.

3 | DDOS, L'acronimo sta per Distributed Denial of Service, traducibile in italiano come Interruzione distribuita del servizio, e consiste nel tempestare di richieste un sito, fino a metterlo ko e renderlo irraggiungibile.

4 | furto di dati è vago perché molti virus possono rubare qualcosa mail etc.

Utilizzo:

phishing per rubare dati a qualche dipendente informazioni personali così da causare un danno anche a livello monetario all'utente dell'azienda o dell'azienda stessa.

i ransomware servono a rubare dati cifrarli e sbloccarli solo sotto pagamento e possono essere un danno grave per i dati nei server e per i soldi dell'azienda o per altro.

il ddos potrebbe essere usato per bloccare un'azienda e non svolgendo il lavoro a pieno carico si perdono soldi

il furto di dati può avvenire in tanti modi ad esempio attraverso keylogger per rubare dati utenti ma ce ne sono molti di virus simili

Info attacchi comuni:

Malware, phishing, ddos, mitm (tramite ausilio di vittima si ottengono info reti etc.), oday (vulnerabilità su software) e alcune volte comprendono sql injection