ESERCIZIO 1 M5 D5

- **Phishing**: Gli attacchi di phishing coinvolgono l'invio di messaggi di posta elettronica o di testo fraudolenti che cercano di indurre le persone a rivelare informazioni sensibili, come password o dati finanziari. Questi attacchi mirano a rubare identità o ad accedere a informazioni riservate.
  - Il più grande attacco di phishing fu fatto verso Facebook e Google riuscendo a rubare oltre 100Milioni di Dollari

- **Malware**: Il malware è un software dannoso progettato per danneggiare, compromettere o ottenere accesso non autorizzato ai sistemi informatici. Può assumere varie forme, come virus, worm, trojan, ransomware e spyware. L'obiettivo principale del malware è compromettere l'integrità e la riservatezza dei dati. Spesso queste forme sono unite in un unico malware ad esempio:
  - il trojan/cryptoworm (ransomware) WannaCry che si diffondeva con le caratteristiche del work ma che una volta “arrivato” all’interno di una o più macchine eseguiva un encryptor che appunto criptava i dati della/e macchina/e stessa/e
  - Il Morris Worm, come si intende dal nome un worm autoreplicante che incautamente “scappò di mano” al suo autore (Morris) senza nessuna volta di nuocere.
  - Shady Rat, uno spyware che è riuscita a colpire più di 70 grandi organizzazioni
  - Virus Melissa, che infettava i file .doc e si autoinviava via mail ai primi 50 contatti di outlook
  - Stuxnet, virus che riuscì a fermare la produzione nucleare dell’Iran ma che poi si estese a macchia d’olio perdendone il controllo

- **Attacchi DDoS** (Distributed Denial of Service): Gli attacchi DDoS mirano a sovraccaricare un sistema o un servizio online inviando una grande quantità di traffico da più origini. L'obiettivo è rendere il servizio inaccessibile agli utenti legittimi, causando interruzioni operative e perdita di produttività.
  - Il più grande attacco DDoS è stato ricevuto da Google nel 2017 con una dimensione di 2,54 Tbps
  - GitHub con attacco da 1,3 Tbps

- **Furto di dati**: Questa minaccia implica l'accesso non autorizzato o il furto di dati sensibili o riservati di un'azienda. I criminali informatici possono sfruttare vulnerabilità nel sistema per ottenere informazioni come informazioni personali dei clienti, dati finanziari o proprietari, segreti commerciali o informazioni strategiche.

- **Attacchi di ingegneria sociale**: Questi attacchi coinvolgono la manipolazione psicologica delle persone per ottenere accesso non autorizzato ai sistemi o alle informazioni. Gli attaccanti possono cercare di convincere gli utenti a condividere password, fornire accesso a sistemi o rivelare informazioni riservate attraverso l'inganno e la manipolazione.
  - Ai danni di Ubiquity è stato messa in atto una frode da oltre 40MIlioni di dollari; gli attaccanti sono riusciti ad impersonare il CEO e l'avvocato dell'aziende riuscendo a far chiudere una trattativa "segreta" mai esistita realmente.

- **Vulnerabilità del software**: Le vulnerabilità del software rappresentano falle o debolezze nei programmi o nelle applicazioni utilizzate dall'azienda. Queste vulnerabilità possono essere sfruttate dagli attaccanti per ottenere accesso non autorizzato, eseguire codice malevolo o compromettere la sicurezza dei dati.

- **Attacchi di ransomware**: Il ransomware è un tipo di malware che blocca l'accesso a un sistema o a dati critici, richiedendo un pagamento (generalmente in criptovalute) per ripristinare l'accesso. Questi attacchi possono causare interruzioni significative delle operazioni aziendali e la perdita di dati se il pagamento non viene effettuato o se il ripristino dei dati non è possibile.
    - TeslaCrypt (Trojan-CryptoRansomware) prendeva di mira 185 file di gioco di 40 giochi popolari come la serie Call of Duty, World of Warcraft, Minecraft, World of Tanks, ecc. sul disco rigido del bersaglio. Le versioni successive di TeslaCrypt crittografavano anche file Word, PDF, JPEG e altri tipi di file. Ha spinto le vittime a pagare un riscatto di $ 500 per ottenere la chiave di decrittazione. Il ransomware TeslaCrypt è migliorato sempre di più e l'ultima versione riusciva a crittografare file di dimensioni fino a 4 GB. Gli autori del ransomware lo hanno chiuso a maggio 2016.
    - NotPetya (LockerRansomware) Petya era un virus ransomware emerso nel marzo 2016. Ha infettato il record di avvio principale dei computer Windows per prendere in ostaggio il sistema. NotPetya era una variante del Petya rilasciata nel giugno 2017. Differiva dal suo predecessore per due particolarità: -1 ha usato l'hack EternalBlue per infettare i sistemi 2- è stato modificato in modo che il suo effetto non potesse essere annullato. Si chiamava NotPetya e l'accusa era che questo attacco fosse politicamente motivato e mirato contro l'Ucraina dall'Agenzia militare russa. L'80% delle aziende interessate erano ucraine. È stato scoperto che una backdoor creata durante un aggiornamento della società ucraina ME Doc è stata utilizzata per diffondere questo malware. NotPetya è l'attacco ransomware più incisivo fino ad oggi, avendo causato perdite finanziarie per un valore di $ 10 miliardi.

- **Attacchi alle reti wireless**: Gli attaccanti possono cercare di sfruttare le debolezze nelle reti wireless per ottenere accesso non autorizzato alla rete aziendale o per intercettare il traffico dati sensibile. Questi attacchi possono compromettere la sicurezza delle comunicazioni e l'integrità dei dati trasmessi.

- **Attacchi alle applicazioni web**: Gli attaccanti possono mirare alle vulnerabilità presenti nelle applicazioni web per ottenere accesso non autorizzato o compromettere la sicurezza dei dati. Questi attacchi possono consentire agli aggressori di rubare informazioni, eseguire codice malevolo o manipolare i dati dell’azienda.

- **Violazioni della sicurezza fisica**: Anche se non si può parlare di cyber-attacchi, le minacce e possibili violazioni per la sicurezza personale non si limitano solo al mondo digitale. Le violazioni della sicurezza fisica includono l'accesso non autorizzato alle strutture aziendali, il furto di dispositivi o supporti di archiviazione fisici contenenti dati sensibili e altre attività che possono mettere a rischio la sicurezza delle informazioni.