fowhe.com

# Le minacce informatiche alle PMI

Analisi ed esempi dei principali attacchi informatici alle piccole e medie imprese

*Settembre 2025*

# Sommario

## Phishing



- **Attacco:** email di phishing potenziate da AI per indurre bonifici fraudolenti, impersonando dirigenti o fornitori noti.
- **Conseguenze:** perdita economica immediata, interruzione dei processi aziendali, danno d'immagine e possibili responsabilità legali per la frode.
- **Azioni:** adottare filtri email avanzati, autenticazione a più fattori e verificare ogni richiesta sospetta tramite un secondo canale.

## Ransomware



- **Attacco:** accesso tramite falle di sicurezza, furto silenzioso di dati, crittografia dei file e minaccia di pubblicazione online.
- **Conseguenze:** blocco totale delle operazioni, costi di ripristino e riscatto elevati, sanzioni GDPR e grave danno reputazionale.
- **Azioni:** adottare filtri email avanzati, autenticazione a più fattori e verificare ogni richiesta sospetta tramite un secondo canale.

## Data Leak

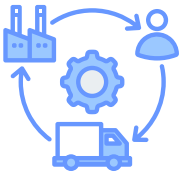


- **Attacco:** errore umano nella configurazione dei permessi di accesso a uno spazio cloud, rendendo i dati sensibili pubblicamente accessibili.
- **Conseguenze:** pesanti sanzioni GDPR, perdita di fatturato dovuta al calo di fiducia e grave danno all'immagine aziendale.
- **Azioni:** revisionare periodicamente i permessi, cifrare sempre i dati, monitorare le configurazioni con strumenti automatici e formare il personale.

# Sommario

## Supply Chain Attack

Pag. 13-14



- **Attacco:** compromissione di un fornitore IT per inserire codice malevolo in un aggiornamento software legittimo, infettando così i clienti.
- **Conseguenze:** perdita di controllo dell'infrastruttura, costi di bonifica molto elevati e crollo della fiducia nell'ecosistema dei fornitori.
- **Azioni:** valutare la sicurezza dei fornitori, segmentare la rete per isolare software di terze parti e monitorare il traffico.

## Insider Threat

Pag. 15-16

- **Attacco:** dipendente infedele che ruba dati di proposito o dipendente distratto che, per errore, causa una violazione.
- **Conseguenze:** perdita di vantaggio competitivo, costi di indagine, sanzioni per violazione dati e creazione di un clima sospetto.
- **Azioni:** applicare il principio del minimo privilegio, monitorare il comportamento degli utenti (UEBA) e usare strumenti di Data Loss Prevention.

## Vishing & Smishing

Pag. 17-18


- **Attacco:** truffe tramite SMS (Smishing) e telefonate (Vishing) per manipolare le vittime e farsi consegnare credenziali e codici.
- **Conseguenze:** furto di denaro, compromissione di account aziendali, forte impatto psicologico sulla vittima e danno alla cultura della sicurezza.
- **Azioni:** formare i dipendenti su attacchi multi-canale, adottare una policy di "fiducia zero" e usare MFA resistente al phishing.

# Sommario

## DDoS Attack

Pag. 19-20

- **Attacco:** una rete di computer infetti (botnet) sommerge un sito web di traffico inutile, rendendolo inaccessibile ai clienti reali.
- **Conseguenze:** perdita immediata e massiccia di vendite, costi di ripristino e grave danno d'immagine, specialmente durante eventi di punta.
- **Azioni:** utilizzare servizi professionali di mitigazione DDoS basati su cloud e implementare un Web Application Firewall (WAF).

## IoT device attacks

Pag. 21-22


- **Attacco:** sfruttamento di credenziali di default su dispositivi IoT (telecamere, router) per ottenere un punto d'ingresso nella rete aziendale.
- **Conseguenze:** uso del dispositivo come testa di ponte per attacchi più gravi, sanzioni GDPR e danno d'immagine per negligenza.
- **Azioni:** cambiare sempre le password di default, aggiornare il firmware e isolare i dispositivi IoT in una rete separata.

## Malvertising

Pag. 23-24

- **Attacco:** una pubblicità online malevola, anche su siti legittimi, installa silenziosamente un ransomware sfruttando vulnerabilità del browser.
- **Conseguenze:** blocco delle attività aziendali, costi di ripristino molto alti e rischio di furto dati con conseguenze legali (GDPR).
- **Azioni:** usare un Secure Web Gateway (SWG) per filtrare il traffico, aggiornare costantemente browser e plugin e installare ad-blocker.

# Sommario

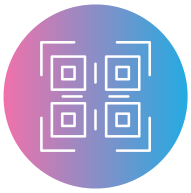
## Credential Stuffing

Pag. 25-26

- **Attacco:** bot automatici testano su larga scala milioni di credenziali rubate da altri siti, sfruttando il riutilizzo delle password.
- **Conseguenze:** furto di account su larga scala (ATO), frodi dirette ai danni degli utenti e grave perdita di fiducia nel servizio.
- **Azioni:** imporre l'autenticazione a più fattori (MFA), usare soluzioni anti-bot e formare gli utenti a usare password uniche.

## Quishing

Pag. 27-28



- **Attacco:** email contenente un codice QR che, scansionato con lo smartphone, porta a una pagina di phishing eludendo i filtri.
- **Conseguenze:** furto di credenziali aziendali, rischio di frodi (BEC), violazione del GDPR e danno all'immagine per la vulnerabilità dimostrata.
- **Azioni:** adottare sicurezza email con analisi delle immagini (OCR), formare i dipendenti a diffidare dei QR code e usare MFA.

## SQL Injection

Pag. 29-30


- **Attacco:** inserimento di codice malevolo in un campo di un sito web per manipolare il database e rubare dati.
- **Conseguenze:** furto di dati sensibili dei clienti, interruzione del servizio, pesanti sanzioni GDPR e perdita totale di fiducia.
- **Azioni:** scrivere codice sicuro (query parametrizzate), usare un Web Application Firewall (WAF) e limitare i permessi del database.

# Sommario

## Man-in-the-Middle



- **Attacco:** creazione di un hotspot Wi-Fi falso per intercettare tutto il traffico di un utente e rubare credenziali.
- **Conseguenze:** accesso non autorizzato alla rete aziendale, furto di dati critici, violazione del GDPR e danno reputazionale.
- **Azioni:** impostare come policy l'uso obbligatorio di una VPN su reti non fidate e formare i dipendenti sui rischi.

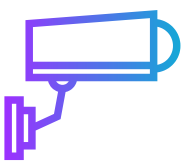
## Malware Mobile



- **Attacco:** una chiavetta USB infetta, lasciata deliberatamente in un luogo pubblico, viene raccolta e usata da un dipendente curioso.
- **Conseguenze:** infezione malware dell'intera rete, costi di bonifica molto elevati, interruzione operativa e rischio di sanzioni GDPR.
- **Azioni:** vietare l'uso di USB non autorizzate, disabilitare le porte sui computer e formare i dipendenti sui pericoli.

## IP Camera Attack





- **Attacco:** accesso a telecamere IP utilizzando password impostate di fabbrica per creare un punto d'ingresso nella rete aziendale.
- **Conseguenze:** grave violazione della privacy (GDPR), rischio di attacchi interni più gravi, compromissione della sicurezza fisica e danno reputazionale.
- **Azioni:** cambiare sempre le password di default, aggiornare il firmware e isolare le telecamere in una rete separata.

# Phishing

## Phishing / Compromissione Email Aziendale (BEC) con uso di AI

**Target tipico/esempio: studio professionale o piccola e media impresa (PMI) che utilizza la posta elettronica per gestire fatture, pagamenti e comunicazioni importanti con clienti e fornitori. Il personale amministrativo e finanziario è il bersaglio più comune.**

### Come è avvenuto l'attacco

**Fase 1:** Raccolta di Informazioni. L'hacker studia l'azienda e i suoi dipendenti chiave usando informazioni pubbliche disponibili su piattaforme come LinkedIn o sul sito web aziendale. Questo gli permette di creare un profilo credibile per l'attacco.

**Fase 2**: Esecuzione dell'Attacco. Viene inviata un'email di phishing mirata e altamente personalizzata a un dipendente dell'ufficio contabilità. L'email è studiata per aggirare i filtri di sicurezza tradizionali, poiché non contiene virus o link palesemente sospetti. L'hacker utilizza tecniche come la falsificazione del dominio, creando un indirizzo email quasi identico a quello reale ma con una differenza minima che può sfuggire (es. nome.azienda.co invece di nome.azienda.com), oppure impersona un dirigente (Truffa del CEO) o un fornitore conosciuto (Frode della finta fattura). Grazie all'uso dell'Intelligenza Artificiale, il testo dell'email è impeccabile, privo di errori e usa un tono autorevole e urgente, chiedendo di effettuare un bonifico "urgente e riservato" per una finta acquisizione o di modificare le coordinate bancarie di un fornitore reale.

**Fase 3:** Esecuzione della Frode. Il dipendente, ingannato dall'apparente legittimità della richiesta e messo sotto pressione dall'urgenza, esegue il bonifico su un conto corrente controllato dall'hacker.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Perdita economica immediata. Per le PMI, i danni da false fatture si aggirano in media sugli 8.000 euro, mentre nei casi di compromissione dell'email aziendale (BEC) la perdita media può raggiungere i 46.000 euro per singolo incidente. A questi si aggiungono i costi per le indagini e le spese legali per tentare di recuperare i fondi.

**Operative:** Interruzione dei normali flussi di pagamento. Il personale e il management devono dedicare tempo prezioso alla gestione della crisi, causando un calo di produttività nel 53% delle aziende colpite. È inoltre necessario rivedere e rafforzare le procedure interne, causando ulteriori rallentamenti.

**Legali:** L'azienda potrebbe essere ritenuta legalmente responsabile se la frode coinvolge dati di terzi. È obbligatorio denunciare l'accaduto alle autorità competenti, come la Polizia Postale.

**Reputazionali:** Grave danno alla fiducia all'interno dell'azienda. Se la notizia diventa pubblica, si verifica una perdita di credibilità nei confronti di clienti, fornitori e banche.

# Phishing

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

### Prevenzione (Tecnologica e Processi e Persone)

*Filtri email avanzati:* Utilizzare software di sicurezza che non si limitano a controllare gli allegati, ma analizzano anche il contesto, il tono e le anomalie nelle comunicazioni, usando l'Intelligenza Artificiale per riconoscere i tentativi di truffa.

*Autenticazione delle email:* Implementare protocolli tecnici (DMARC, SPF, DKIM) che impediscono agli hacker di falsificare l'indirizzo email del mittente.

*Verifica su un secondo canale:* Stabilire come regola aziendale obbligatoria che ogni richiesta di modifica di IBAN o di bonifici urgenti/insoliti venga confermata tramite un canale diverso (ad esempio, una telefonata a un numero di telefono già noto e verificato).

*Formazione continua:* Organizzare regolarmente corsi di formazione e simulazioni di phishing per addestrare i dipendenti a riconoscere le tecniche di manipolazione psicologica. È un passo cruciale, considerando che il 58% dei dipendenti non sa riconoscere un'email di phishing.

### Mitigazione e Risposta:

*Autenticazione a Più Fattori (MFA):* Attivare questo sistema di sicurezza (che richiede un secondo codice oltre alla password) su tutti gli account di posta elettronica e finanziari. In questo modo, anche se un hacker ruba la password, non può accedere all'account.

*Piano di risposta agli incidenti:* Avere una procedura chiara da seguire in caso di attacco, che includa il contatto immediato con la propria banca per tentare di bloccare il bonifico e la denuncia alle autorità.

# Ransomware

## Ransomware con Doppia Estorsione (RaaS)

**Target tipico/esempio: piccola e media impresa o studio professionale con computer e server interni non sempre aggiornati e con copie di backup dei dati non adeguatamente isolate dalla rete principale.**

### Come è avvenuto l'attacco

**Fase 1:** *Accesso Iniziale.* L'attacco non inizia subito con il blocco dei file. Prima, gli hacker trovano un punto debole per entrare nella rete aziendale. Questo può avvenire sfruttando una falla di sicurezza in un software non aggiornato esposto su Internet (come una VPN o un accesso remoto) oppure tramite un'email di phishing con un allegato malevolo (ad esempio, un finto file Excel chiamato "Aggiornamento stipendi 2025.xlsx" che, una volta aperto, installa il malware).

**Fase 2**: *Movimento Silenzioso e Furto dei Dati.* Una volta dentro, l'hacker si muove silenziosamente all'interno della rete per settimane, senza farsi scoprire. In questa fase, identifica e copia i dati più importanti (database dei clienti, progetti, dati finanziari) su server esterni. Per non destare sospetti, utilizza strumenti informatici legittimi, una tecnica nota come "Living off the Land".

**Fase 3:** *Blocco dei File e Ricatto.* Solo dopo aver rubato i dati, l'hacker attiva il ransomware. Questo programma blocca (cripta) tutti i file sui computer e sui server, comprese le copie di backup collegate alla rete. A questo punto, lascia un messaggio di riscatto che non solo chiede un pagamento per sbloccare i file, ma minaccia anche di pubblicare i dati rubati su un sito del dark web. Questa tecnica è chiamata "doppia estorsione". Spesso, questi attacchi sono gestiti tramite un modello "criminale in abbonamento" chiamato Ransomware-as-a-Service (RaaS).

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:**
*Richiesta di Riscatto:* Il riscatto medio richiesto a una PMI si aggira intorno ai 32.000 euro, ma può essere molto più elevato.

*Costi di Ripristino:* Anche senza pagare il riscatto, i costi per recuperare i sistemi, pagare consulenti e implementare nuove misure di sicurezza possono superare i 500.000 euro. Il costo totale medio di un attacco ransomware per una PMI in Italia può arrivare a 700.000 euro.

*Perdita di Fatturato:* L'azienda è costretta a fermare completamente le attività per giorni o settimane. Per il 40% delle PMI colpite, il blocco operativo dura in media almeno otto ore.

**Operative:** Paralisi totale delle operazioni. È impossibile accedere ai dati dei clienti, agli ordini, alla produzione. Se anche i backup vengono bloccati, i dati possono essere persi per sempre.

**Legali:** Se vengono rubati dati personali di clienti o dipendenti, scattano gli obblighi del GDPR, il regolamento europeo sulla privacy. L'azienda deve notificare la violazione al Garante della Privacy entro 72 ore e comunicarla alle persone interessate. Il rischio è di subire sanzioni che possono arrivare fino a 20 milioni di euro o al 4% del fatturato globale.

**Reputazionali:** Danno gravissimo alla fiducia di clienti e partner, soprattutto se i loro dati vengono resi pubblici. Se vengono rubati progetti o segreti industriali, l'azienda perde un importante vantaggio competitivo.

# Ransomware

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

### Prevenzione (Tecnologica e Processi e Persone)

*Aggiornamenti Costanti:* Implementare un processo rigoroso per installare tempestivamente tutti gli aggiornamenti di sicurezza (patch) su sistemi operativi e software, dando priorità alle vulnerabilità più critiche.

*Strategia di Backup 3-2-1:* Seguire la regola del 3-2-1: mantenere almeno 3 copie dei dati, su 2 supporti diversi, con 1 copia conservata offline (scollegata dalla rete) o su un servizio cloud "immutabile", per renderla inaccessibile al ransomware. È fondamentale testare regolarmente il ripristino dei backup per assicurarsi che funzionino.

*Riduzione della Superficie d'Attacco:* Disabilitare porte e servizi di rete non necessari, in particolare gli accessi remoti (come RDP) se non sono protetti da VPN e Autenticazione a Più Fattori.

*Sicurezza dei Computer (EDR/XDR):* Utilizzare soluzioni di sicurezza avanzate (Endpoint Detection and Response) che non si basano solo su virus noti, ma monitorano i comportamenti anomali, come un processo che tenta di bloccare migliaia di file contemporaneamente.

### Mitigazione e Risposta:

*Segmentazione della Rete:* Isolare i sistemi più importanti in segmenti di rete separati. In questo modo, se un computer viene infettato, il ransomware non può diffondersi facilmente al resto dell'azienda.

*Principio del Minimo Privilegio:* Assicurarsi che ogni dipendente e ogni account di servizio abbia accesso solo alle risorse strettamente necessarie per svolgere il proprio lavoro.

*Piano di Risposta agli Incidenti:* Avere un piano d'azione chiaro e testato da seguire in caso di attacco: isolare i sistemi infetti, attivare il team di emergenza, valutare il danno, comunicare con le autorità (come previsto dal GDPR) e avviare il ripristino dai backup sicuri.

*Protezione Anti-Ransomware Specifica:* Installare soluzioni software progettate appositamente per rilevare e bloccare i processi di crittografia non autorizzati, in grado di ripristinare automaticamente i file modificati.

# Data Leak

## Fuga di Dati da un Servizio Cloud Configurato Male (Data Leak)

**Target tipico/esempio: studio di consulenza o azienda che utilizza servizi cloud (come Amazon S3, Google Drive, Microsoft Azure) per archiviare documenti dei clienti, dati anagrafici e altri file importanti, ma non dispone di un team specializzato in sicurezza cloud.**

### Come è avvenuto l'attacco

**Causa Principale:** Errore Umano e Mancanza di Controlli. Durante la configurazione di uno spazio di archiviazione online (ad esempio, una cartella su Google Drive o un "bucket" su Amazon S3), un dipendente o un consulente esterno imposta per errore i permessi di accesso su "pubblico" anziché "privato". Questo può accadere per semplificare una condivisione temporanea di file o per semplice inesperienza.

**Mancanza di Monitoraggio:** L'azienda non utilizza strumenti automatici (noti come CSPM) per controllare costantemente le configurazioni dei servizi cloud e segnalare questi errori. Non c'è un monitoraggio attivo su chi accede ai dati, quindi nessuno si accorge che informazioni sensibili sono liberamente accessibili da chiunque su Internet.

**Scoperta da parte dell'Hacker:** I criminali informatici usano programmi automatici che scandagliano continuamente Internet alla ricerca di questi archivi cloud aperti. Una volta trovato un archivio non protetto, possono visualizzare e scaricare tutto il suo contenuto senza bisogno di forzare alcun sistema o rubare password. Il furto dei dati avviene in modo silenzioso e senza lasciare tracce evidenti.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:**
*Sanzioni GDPR:* La perdita di dati personali dovuta a misure di sicurezza inadeguate è una violazione diretta del regolamento europeo GDPR. Le sanzioni possono essere molto pesanti, arrivando fino a 20 milioni di euro.

*Costi di Notifica e Supporto:* L'azienda deve sostenere i costi per informare i clienti della violazione, creare un call center di supporto e, in alcuni casi, offrire servizi di monitoraggio del credito per proteggerli da future frodi.

*Perdita di Fatturato:* Il 75% dei costi legati a una violazione di dati deriva dalla perdita di fatturato, causata dal calo di fiducia dei clienti e dalla difficoltà ad acquisirne di nuovi. In Italia, il costo medio totale di una violazione di dati per un'azienda è di circa 4,37 milioni di euro.

**Operative:** Enorme dispendio di tempo e risorse per identificare quali dati sono stati esposti, correggere le configurazioni, revocare gli accessi e condurre un'indagine di sicurezza completa.

**Legali:** Obbligo di notificare la violazione al Garante della Privacy e ai clienti interessati. Rischio di subire cause legali da parte dei clienti i cui dati sono stati resi pubblici.

**Reputazionali:** Danno gravissimo all'immagine aziendale. L'impresa viene percepita come negligente e inaffidabile nella gestione dei dati, un danno da cui è molto difficile riprendersi.

# Data Leak

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

### Prevenzione (Tecnologica e Processi e Persone)

*Revisione Periodica dei Permessi:* Eseguire controlli regolari su tutte le configurazioni dei servizi cloud per garantire che sia applicato il principio del minimo privilegio (dare accesso solo a chi ne ha strettamente bisogno). Utilizzare strumenti automatici (CSPM) per un monitoraggio continuo.

*Cifratura dei Dati:* Cifrare sempre i dati sensibili, sia quando sono archiviati (at-rest) sia durante il trasferimento (in-transit). In questo modo, anche se i dati venissero rubati, sarebbero illeggibili senza la chiave di decifrazione.

*Politica di "Negazione di Default":* Adottare una politica in cui tutti gli accessi sono negati per impostazione predefinita. I permessi devono essere concessi solo in modo esplicito e solo quando necessario.

*Formazione Specifica sul Cloud:* Formare il personale tecnico sulle corrette pratiche di sicurezza per le piattaforme cloud utilizzate.

### Mitigazione e Risposta:

*Gestione degli Accessi (IAM):* Implementare politiche rigorose per la gestione delle identità e degli accessi, utilizzando ruoli con permessi specifici invece di accessi generici. Richiedere sempre l'Autenticazione a Più Fattori (MFA) per tutti gli accessi amministrativi al cloud.

*Prevenzione della Perdita di Dati (DLP) per il Cloud:* Utilizzare soluzioni software che monitorano e bloccano i tentativi di trasferire dati sensibili al di fuori degli ambienti cloud autorizzati.

*Registrazione e Monitoraggio (Logging):* Abilitare e conservare i registri di accesso a tutti i servizi cloud. Utilizzare strumenti di analisi per rilevare attività anomale, come download di enormi quantità di dati da indirizzi IP sospetti.

# Supply Chain Attack

## Attacco alla Catena di Fornitura del Software (Supply Chain)

**Target tipico/esempio: PMI che si affida a fornitore di servizi esterno (Managed Service Provider - MSP) per la gestione della sua infrastruttura informatica, o che utilizza un software specifico per il proprio settore (ad esempio, un gestionale o un software di contabilità) fornito da un'altra azienda.**

### Come è avvenuto l'attacco

**Fase 1:** *Compromissione del Fornitore.* L'hacker non attacca direttamente la PMI, ma individua un suo fornitore di software o servizi IT come anello debole della catena. Il fornitore viene compromesso con varie tecniche, come il phishing o lo sfruttamento di una vulnerabilità.

**Fase 2:** *Iniezione di Codice Malevolo.* L'hacker ottiene l'accesso all'ambiente di sviluppo del fornitore e inserisce una "backdoor" (una porta di servizio nascosta) o un virus all'interno del codice del software legittimo. Questo codice dannoso viene poi "firmato" digitalmente con i certificati ufficiali del fornitore, facendolo apparire autentico e sicuro (un esempio famoso a livello internazionale è stato l'attacco a SolarWinds).

**Fase 3:** *Distribuzione su Larga Scala.* Il fornitore, ignaro della compromissione, distribuisce un aggiornamento del software ai suoi clienti, inclusa la PMI. La PMI installa l'aggiornamento, fidandosi della sua provenienza, ma in realtà sta installando la backdoor sulla propria rete. Questo permette all'hacker di avere un accesso nascosto e persistente a centinaia o migliaia di aziende contemporaneamente.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi molto elevati per eliminare la minaccia, un'operazione che richiede competenze tecniche specialistiche. Costi legati all'interruzione del servizio causata dal software compromesso. Rischio di subire ulteriori attacchi (come ransomware o furto di dati) attraverso la backdoor installata

**Operative:** L'azienda perde il controllo della propria infrastruttura informatica. L'hacker può spiare le attività, rubare dati o lanciare altri attacchi a suo piacimento. È necessario disconnettere i sistemi infetti, attendere una versione sicura del software dal fornitore e, in molti casi, reinstallare e ripulire l'intera infrastruttura.

**Legali:** Situazione complessa nel definire le responsabilità legali tra la PMI e il fornitore compromesso. Se i dati dei clienti vengono rubati a causa della backdoor, scattano gli obblighi previsti dal GDPR.

**Reputazionali:** Crollo della fiducia nell'intero ecosistema di fornitori digitali. Il danno d'immagine colpisce sia il fornitore compromesso sia la PMI, nel caso in cui i dati dei suoi clienti vengano violati.

# Supply Chain Attack

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

### Prevenzione (Tecnologica e Processi e Persone)

*Gestione del Rischio dei Fornitori:* Prima di firmare un contratto, è fondamentale implementare un processo per valutare la sicurezza dei fornitori critici. È importante richiedere informazioni sulle loro pratiche di sviluppo sicuro, eventuali certificazioni (come la ISO 27001) e i loro piani di risposta agli incidenti.

*Clausole Contrattuali:* Includere nei contratti con i fornitori clausole specifiche sulla sicurezza, che li obblighino a notificare tempestivamente eventuali incidenti e che definiscano chiaramente le responsabilità.

### Mitigazione e Risposta:

*Principio del Minimo Privilegio:* Anche un software proveniente da un fornitore fidato deve funzionare con i minimi privilegi necessari. È fondamentale limitare l'accesso del software a dati e aree della rete che non sono essenziali per il suo funzionamento.

*Segmentazione della Rete:* Isolare i sistemi su cui gira il software di terze parti in un segmento di rete dedicato, con regole di firewall restrittive che limitino la comunicazione con il resto della rete aziendale.

*Monitoraggio del Traffico di Rete: Monitorare il traffico in uscita dalla rete per individuare comunicazioni anomale verso server sconosciuti, che potrebbero essere il segnale dell'attività di una backdoor.*

*Endpoint Detection and Response (EDR):* Le soluzioni EDR possono rilevare comportamenti anomali generati dal software compromesso, anche se il file di installazione è firmato digitalmente e sembra legittimo.

# Insider Threat

## Minaccia Interna (Insider Threat) – Intenzionale e Accidentale

**Target tipico/esempio: azienda i cui i dipendenti hanno accesso a dati sensibili, come progetti, liste clienti o informazioni finanziarie. Lo scenario si applica sia a un dipendente scontento che agisce con dolo (intenzionale), sia a un dipendente distratto o non adeguatamente formato (accidentale).**

### Come è avvenuto l'attacco

**Scenario A:** *Dipendente Infedele (Intenzionale).* Un dipendente che sta per licenziarsi per passare a un'azienda concorrente, o che è insoddisfatto per una mancata promozione, decide di rubare dati aziendali. Nei mesi precedenti, inizia ad accedere lentamente a file e cartelle che non sono strettamente legati alle sue mansioni. Sfruttando il suo accesso legittimo, copia grandi quantità di dati (come progetti o database clienti) su una chiavetta USB personale o li invia al suo indirizzo email privato. Queste azioni possono passare inosservate se l'azienda non monitora attivamente il comportamento degli utenti.

**Scenario B:** *Dipendente Distratto (Accidentale).* Un dipendente, lavorando da casa, riceve un'email di phishing che lo invita a scaricare un "nuovo software per la collaborazione". Clicca sul link e inserisce le sue credenziali aziendali su una pagina web falsa, compromettendo così il suo account. Oppure, per comodità, salva file di lavoro su un servizio cloud personale non approvato dall'azienda e configurato male, esponendo i dati a rischi. L'intento non è malevolo, ma il risultato è comunque una violazione della sicurezza.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:**
*Perdita di Vantaggio Competitivo:* Il furto di proprietà intellettuale o di strategie commerciali può causare un danno economico incalcolabile e a lungo termine.

*Costi di Indagine:* Costi elevati per condurre indagini interne e forensi per determinare l'entità del furto o della perdita di dati.

*Sanzioni GDPR:* La perdita di dati personali dovuta a negligenza o a controlli interni inadeguati è sanzionabile secondo il regolamento europeo.

**Operative:** Necessità di revocare immediatamente gli accessi, recuperare i dispositivi aziendali e, in alcuni casi, avviare azioni legali contro l'ex dipendente. Nel caso accidentale, è necessario bonificare i sistemi compromessi e recuperare i dati esposti.

**Legali:** Possibili azioni legali per violazione del segreto industriale (nel caso intenzionale) e obblighi di notifica previsti dal GDPR (in entrambi i casi).

**Reputazionali:** Grave danno al morale e alla cultura aziendale, con la creazione di un clima di sospetto. La fiducia dei clienti viene minata se i loro dati sono coinvolti nell'incidente.

# Insider Threat

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

### Prevenzione (Tecnologica e Processi e Persone)

*Politiche Chiare:* Stabilire e comunicare a tutti i dipendenti regole chiare sull'uso corretto dei dati e dei sistemi aziendali, e sulle conseguenze in caso di violazione.

*Procedure di Uscita (Offboarding):* Avere una procedura rigorosa per la cessazione di un rapporto di lavoro, che includa la revoca immediata di tutti gli accessi (sia fisici che digitali) e il recupero di tutti i dispositivi aziendali.

*Formazione sulla Sicurezza:* Organizzare corsi di formazione continui non solo sul phishing, ma anche sull'importanza della gestione sicura dei dati e sui rischi legati alle minacce interne.

### Mitigazione e Risposta:

*Principio del Minimo Privilegio (PoLP):* Questa è la contromisura più efficace. I dipendenti devono avere accesso solo ed esclusivamente ai dati e ai sistemi necessari per svolgere il loro lavoro. È fondamentale revisionare i permessi regolarmente.

*Analisi del Comportamento degli Utenti (UEBA):* Implementare soluzioni software che creano un profilo del comportamento "normale" di ogni utente e segnalano automaticamente le deviazioni significative (ad esempio, accesso a file insoliti, download di grandi quantità di dati, attività fuori dall'orario di lavoro).

*Prevenzione della Perdita di Dati (DLP):* Utilizzare strumenti DLP per monitorare, segnalare e bloccare i tentativi di trasferire dati sensibili al di fuori del perimetro aziendale (tramite email, USB, caricamento su servizi cloud, ecc.).

*Monitoraggio dei Dispositivi:* Controllare le attività sui dispositivi aziendali, inclusa la connessione di dispositivi di archiviazione esterni come le chiavette USB.

# Vishing & Smishing

## Attacco di Social Engineering Avanzato (Vishing & Smishing)

**Target tipico/esempio: PMI i cui dipendenti utilizzano i propri smartphone personali anche per lavoro (BYOD - Bring Your Own Device) e le comunicazioni avvengono su più canali: email, telefono, SMS e app di messaggistica come WhatsApp.**

### Come è avvenuto l'attacco

**Fase 1:** *Smishing (Phishing via SMS).* Un dipendente riceve un SMS sul proprio smartphone che sembra provenire da una fonte attendibile, come un corriere (es. "Il tuo pacco è in giacenza. Clicca qui per sbloccarlo") o la propria banca (es. "Accesso anomalo rilevato. Verifica il tuo account qui"). Il messaggio crea un forte senso di urgenza. Cliccando sul link, l'utente viene indirizzato a un sito web falso, identico a quello reale, che gli chiede di inserire le sue credenziali personali o aziendali.

**Fase 2:** *Vishing (Phishing Vocale).* Per rendere l'attacco ancora più credibile, segue una telefonata. L'hacker, utilizzando una tecnica che falsifica il numero di telefono del chiamante per far apparire quello della banca o dell'azienda, contatta il dipendente. Si presenta come un operatore del supporto tecnico o della sicurezza e, facendo riferimento all'SMS appena inviato, guida la vittima a "risolvere il problema". In questo modo, la convince a comunicare codici di sicurezza (MFA), password o persino a installare un software di accesso remoto sul proprio dispositivo, che darà all'hacker il pieno controllo.

**Evoluzione con AI:** Gli hacker possono utilizzare l'Intelligenza Artificiale per creare "deepfake audio", ovvero per imitare perfettamente la voce di un dirigente in una telefonata, rendendo l'inganno quasi impossibile da scoprire.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Furto diretto di denaro da conti bancari personali o aziendali. Costi legati alla compromissione degli account aziendali e al conseguente furto di dati. Se viene installato un software di accesso remoto, l'hacker può entrare nella rete aziendale e causare danni ancora maggiori, come un attacco ransomware.

**Operative:** Blocco degli account compromessi e necessità di bonificare i dispositivi infetti. Perdita di produttività a causa del tempo dedicato alla gestione dell'incidente.

**Legali:** Se l'account aziendale compromesso viene utilizzato per accedere a dati personali, si applicano le normative del GDPR, con obblighi di notifica e possibili sanzioni.

**Reputazionali:** Forte impatto psicologico sulla vittima, che si sente violata e ingannata. Questo tipo di attacco danneggia la cultura della sicurezza aziendale, perché dimostra che anche i dipendenti più attenti possono essere ingannati da attacchi sofisticati e multi-canale.

# Vishing & Smishing

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Formazione Multi-Canale:* La formazione sulla sicurezza non deve limitarsi alle email. Deve includere esempi concreti e realistici di Smishing e Vishing, insegnando ai dipendenti a riconoscere i segnali di allarme: senso di urgenza, richieste insolite di dati sensibili, offerte troppo belle per essere vere.

*Politica di "Fiducia Zero" per le Richieste:* Insegnare ai dipendenti a non fidarsi mai di richieste non sollecitate di informazioni personali o finanziarie, indipendentemente dal canale. La regola d'oro deve essere: riagganciare e richiamare l'ente (banca, fornitore, ecc.) utilizzando un numero di telefono ufficiale preso dal loro sito web, mai quello fornito nel messaggio o dalla chiamata.

**Mitigazione e Risposta:**

*Gestione dei Dispositivi Mobili (MDM):* Per le aziende che consentono l'uso di dispositivi personali, è fondamentale utilizzare soluzioni MDM per separare i dati aziendali da quelli personali e per applicare policy di sicurezza sui dispositivi (ad esempio, installando un software anti-malware).

*Autenticazione a Più Fattori (MFA) Resistente al Phishing:* Utilizzare metodi di autenticazione moderni (come lo standard FIDO2, che usa chiavette di sicurezza fisiche) che legano crittograficamente l'autenticazione al sito legittimo. Questo rende inefficace il furto di codici temporanei, poiché non possono essere utilizzati su un sito falso.

*Filtri SMS:* Alcune soluzioni di sicurezza per smartphone possono filtrare e bloccare automaticamente gli SMS di phishing noti.

*Limitare l'Esposizione dei Numeri di Telefono:* Incoraggiare i dipendenti a non pubblicare i propri numeri di telefono aziendali su profili social o altri siti pubblici.

# DDoS Attack

## Attacco DDoS Volumetrico contro Infrastrutture Critiche

**Target tipico/esempio: piattaforma di e-commerce in occasione di eventi di vendita importanti, come Black Friday o periodo natalizio. In questi momenti, il traffico di clienti legittimi è al suo apice e qualsiasi interruzione del servizio ha un impatto economico e di immagine devastante. Gli hacker scelgono deliberatamente questi periodi per massimizzare il danno.**

### Come è avvenuto l'attacco

**Fase 1:** *Invio di Richieste Falsificate.* L'hacker utilizza una rete di computer infetti (una botnet) per inviare migliaia di piccole richieste a server di terze parti legittimi ma mal configurati (ad esempio, server DNS o NTP). L'indirizzo IP del mittente di queste richieste viene falsificato, inserendo al suo posto quello del sito e-commerce da colpire.

**Fase 2:** *Sfruttamento del Protocollo.* Le richieste sono formulate in modo da generare una risposta molto più grande della richiesta stessa (ecco perché si parla di "amplificazione").

**Fase 3:** *Riflessione.* I server di terze parti, rispondendo, inviano queste risposte enormi non all'hacker, ma all'indirizzo falsificato, cioè al sito e-commerce ("riflessione").

**Fase 4:** *Saturazione.* Il sito della vittima viene sommerso da questo diluvio di traffico indesiderato, la sua connessione a Internet si satura e diventa inaccessibile per i clienti reali.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** La perdita di vendite è immediata e massiccia. Si stima che il blocco di un sito durante i periodi di punta possa costare fino a 275.000 euro all'ora. Per le PMI, il costo medio per ripristinare il servizio dopo un attacco si aggira intorno ai 110.000 euro.

**Operative:** Interruzione completa del servizio e paralisi delle vendite online. I team tecnici sono costretti a una corsa contro il tempo per mitigare l'attacco, trascurando altre attività importanti. A volte, l'attacco DDoS viene usato come diversivo per distrarre i team di sicurezza mentre, di nascosto, viene perpetrato un attacco più grave, come il furto di dati.

**Legali:** Se l'interruzione del servizio causa la violazione di accordi contrattuali (Service Level Agreement - SLA) con partner o clienti, l'azienda potrebbe essere soggetta a penali.

**Reputazionali:** Un sito inaccessibile durante un evento atteso come il Black Friday genera enorme frustrazione nei clienti, che si rivolgono alla concorrenza. Questo erode la fiducia nel marchio e danneggia le vendite future.

# DDoS Attack

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Servizi di Mitigazione DDoS basati su Cloud:* Affidarsi a servizi specializzati che filtrano il traffico malevolo prima che raggiunga il sito. Questi servizi dispongono di una capacità di rete enorme, in grado di assorbire anche gli attacchi più potenti.

*Web Application Firewall (WAF):* Utilizzare un WAF per proteggere da attacchi più sofisticati che mirano non solo a saturare la banda, ma anche a colpire le vulnerabilità delle applicazioni web.

**Mitigazione e Risposta:**

*Piano di Risposta agli Incidenti:* Avere un piano d'azione predefinito per gestire un attacco DDoS è fondamentale per ridurre i tempi di reazione e minimizzare i danni. Il piano deve includere procedure di comunicazione chiare e i contatti di emergenza del fornitore di servizi di mitigazione.

# IoT device attacks

## Compromissione di Reti Aziendali tramite Dispositivi IoT Insicuri

**Target tipico/esempio: una rete aziendale o un ufficio, dove sono presenti numerosi dispositivi IoT (Internet of Things): telecamere di sicurezza, router, stampanti di rete, sistemi di archiviazione (NAS) e altri sensori connessi a Internet. Questi dispositivi vengono spesso installati e poi dimenticati, senza che vengano applicate le normali pratiche di sicurezza.**

### Come è avvenuto l'attacco

**Fase 1:** *Scansione e Scoperta.* I dispositivi già infetti da malware come Mirai scandagliano continuamente Internet alla ricerca di altri dispositivi IoT.

**Fase 2:** *Sfruttamento delle Credenziali di Default.* Una volta trovato un dispositivo, il malware tenta di accedervi usando una lista di password predefinite, quelle impostate in fabbrica dai produttori (es. "admin/admin", "user/user"). Milioni di dispositivi non vengono mai riconfigurati, lasciando questa porta spalancata.

**Fase 3:** *Infezione e Arruolamento.* Se una delle password funziona, il malware viene installato sul dispositivo, che viene trasformato in uno "zombie" e si unisce a una vasta rete di bot (una botnet), controllata dall'hacker.

**Fase 4:** *Persistenza.* Il dispositivo infetto continua a funzionare normalmente, rendendo l'infezione difficile da notare. Se il dispositivo viene riavviato, la sua vulnerabilità di base (la password di default) rimane, e verrà quindi re-infettato nel giro di pochi minuti.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi per l'indagine, la bonifica dei dispositivi e il rafforzamento della rete. Aumento dei costi della bolletta internet a causa del traffico generato dalla botnet. Potenziali sanzioni se il dispositivo viene usato come punto di partenza per un furto di dati.

**Operative:** Un dispositivo IoT infetto può essere usato come "testa di ponte" per attaccare altri sistemi critici all'interno della rete aziendale (PC, server), portando a interruzioni operative ben più gravi.

**Legali:** Se il dispositivo compromesso viene utilizzato per accedere e rubare dati personali, si applicano gli obblighi del GDPR. Inoltre, l'azienda potrebbe essere ritenuta corresponsabile per gli attacchi DDoS lanciati dalla sua rete.

**Reputazionali:** Danno d'immagine per l'azienda, che dimostra di non avere il controllo della propria infrastruttura. Se vengono rubati dati di clienti o partner, la perdita di fiducia è inevitabile.

# IoT device attacks

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Gestione delle Credenziali e degli Aggiornamenti:* La prima e più critica azione è cambiare immediatamente tutte le password di default con password complesse e uniche per ogni dispositivo. È altrettanto importante aggiornare regolarmente il firmware di tutti i dispositivi IoT per correggere le vulnerabilità note.

*Disabilitazione di Servizi Inutili:* Servizi non sicuri e spesso non necessari, come Telnet e UPnP (Universal Plug and Play), dovrebbero essere disabilitati.

*Segmentazione della Rete:* La strategia di difesa più efficace è isolare i dispositivi IoT dal resto della rete aziendale, ad esempio creando una rete Wi-Fi "ospiti" dedicata o una VLAN (Virtual LAN).

.

**Mitigazione e Risposta:**

*Monitoraggio del Traffico:* Controllare costantemente il traffico di rete per individuare attività anomale provenienti dai dispositivi IoT.

*Isolamento e Bonifica:* In caso di infezione, il primo passo è isolare immediatamente il dispositivo dalla rete per impedirgli di comunicare con l'hacker e di infettare altri sistemi. Successivamente, si procede con la bonifica (spesso un reset di fabbrica) e la riconfigurazione sicura.

# Malvertising

## Infezione da Ransomware via Malvertising

**Target tipico/esempio: dipendente che utilizza il proprio computer aziendale per navigare su un sito web legittimo e considerato affidabile, come un portale di notizie, un blog di settore o un noto sito di e-commerce. La minaccia non si trova nel sito stesso, ma all'interno di una pubblicità online apparentemente innocua.**

### Come è avvenuto l'attacco

**Fase 1:** *Iniezione dell'Annuncio Malevolo.* I criminali informatici acquistano spazi pubblicitari su reti legittime e inseriscono un annuncio (un banner, un pop-up) che contiene codice dannoso.

**Fase 2:** *Reindirizzamento Silente ("Drive-by Download").* Spesso non è necessario che l'utente clicchi sull'annuncio. Il semplice caricamento della pagina web che ospita l'annuncio malevolo può innescare un reindirizzamento automatico e invisibile verso una pagina web controllata dall'hacker.

**Fase 3:** *L'Exploit Kit (EK).* La pagina di destinazione ospita un Exploit Kit, un software criminale che scansiona il computer della vittima alla ricerca di vulnerabilità note e non corrette nel browser o nei suoi componenti aggiuntivi (plugin).

**Fase 4:** *Sfruttamento e Infezione.* Se l'Exploit Kit trova una vulnerabilità, la sfrutta per installare il payload finale, ovvero il vero e proprio virus. In questo caso, il payload è un ransomware, che inizia a criptare i file. L'intera operazione avviene in pochi secondi e in modo completamente silente.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi diretti legati alla richiesta di riscatto e costi indiretti, ancora più alti, per il ripristino dei sistemi, il fermo della produzione e la consulenza specializzata. Il costo totale di un attacco ransomware per una PMI può facilmente superare i 700.000 euro.

**Operative:** Blocco totale o parziale delle attività a causa della cifratura dei file. Perdita di produttività e, nei casi peggiori, perdita permanente di dati se i backup non sono efficaci.

**Legali:** Se l'attacco include anche il furto di dati (doppia estorsione), scattano gli obblighi di notifica previsti dal GDPR, con il rischio di pesanti sanzioni.

**Reputazionali:** Danno all'immagine aziendale, che appare vulnerabile a minacce diffuse. La fiducia di clienti e partner viene compromessa, specialmente se i loro dati sono coinvolti.

# Malvertising

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Secure Web Gateway (SWG):* Questa è la difesa più efficace. Un SWG è una soluzione di sicurezza che si interpone tra gli utenti e Internet, filtrando il traffico web. Può bloccare i reindirizzamenti verso le pagine degli Exploit Kit e impedire il download del virus prima che raggiunga il computer dell'utente.

*Aggiornamenti Tempestivi:* Mantenere i browser e tutti i relativi plugin costantemente aggiornati è una misura fondamentale, poiché gli Exploit Kit funzionano cercando vulnerabilità note.

*Ad-Blockers:* L'utilizzo di software per il blocco della pubblicità può impedire il caricamento degli annunci malevoli, interrompendo la catena di attacco all'origine.

*Formazione degli Utenti:* Sebbene la difesa principale sia tecnologica, la formazione può aiutare gli utenti a riconoscere i segnali di un comportamento anomalo del browser.

**Mitigazione e Risposta:**

*Isolamento e Risposta:* In caso di infezione, la prima azione è isolare immediatamente il computer infetto dalla rete per evitare la propagazione del ransomware.

*Piano di Risposta agli Incidenti:* Attivare il piano di emergenza aziendale, che deve includere le procedure per il ripristino dei dati dai backup sicuri e la comunicazione con le autorità competenti.

.

# Credential Stuffing

## Furto di Account di Massa tramite Credential Stuffing

**Target tipico/esempio: qualsiasi servizio online con un'ampia base di utenti: una piattaforma di social media, un sito di e-commerce, un servizio di streaming o una piattaforma software aziendale. La vulnerabilità non risiede in un difetto del servizio, ma in un comportamento umano molto diffuso: il riutilizzo delle password. Si stima che fino all'85% degli utenti utilizzi le stesse credenziali per più servizi online.**

### Come è avvenuto l'attacco

**Fase 1:** *Raccolta delle Credenziali.* Gli hacker acquisiscono enormi elenchi di credenziali (coppie email/password) trapelate da precedenti violazioni di dati di altri siti web. Queste liste sono facilmente reperibili sul dark web.

**Fase 2:** *Attacco Automatizzato con Bot.* Utilizzando software specializzati, gli hacker lanciano un attacco su larga scala contro il servizio target. I bot "imbottiscono" ("stuff") sistematicamente i campi di login con milioni di credenziali rubate.

**Fase 3:** *Elusione delle Difese.* I bot moderni sono progettati per aggirare le misure di sicurezza tradizionali. Invece di lanciare migliaia di tentativi da un singolo indirizzo IP (che verrebbe bloccato), distribuiscono l'attacco su una vasta rete di IP diversi, facendo sembrare ogni tentativo di login come proveniente da un utente legittimo diverso.

**Fase 4:** *Sfruttamento dei Successi (Account Takeover).* Sebbene il tasso di successo di un singolo tentativo sia molto basso (circa lo 0,1%), l'enorme volume dell'attacco garantisce un numero significativo di accessi riusciti, portando al furto e al controllo dell'account (Account Takeover - ATO).

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Frodi dirette se l'account compromesso contiene informazioni di pagamento. Costi per rimborsare i clienti truffati, per il supporto clienti e per implementare nuove misure di sicurezza.

**Operative:** Enorme dispendio di tempo per i team di sicurezza e supporto, che devono gestire gli account compromessi, assistere gli utenti e investigare l'attacco.

**Legali:** L'accesso non autorizzato a dati personali costituisce una violazione del GDPR, con conseguenti obblighi di notifica e rischio di sanzioni.

**Reputazionali:** Grave danno all'immagine del servizio. Gli utenti lo percepiranno come insicuro, portando a una perdita di fiducia e all'abbandono della piattaforma.

# Credential Stuffing

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Autenticazione a Più Fattori (MFA):* Questa è la contromisura più efficace. L'MFA richiede un secondo fattore di verifica oltre alla password (un codice ricevuto via SMS, un'app di autenticazione, un'impronta digitale). Anche se un hacker possiede la password corretta, non può superare questo secondo step.

*Formazione degli Utenti:* È fondamentale educare costantemente gli utenti sull'importanza di utilizzare password uniche e complesse per ogni servizio e incoraggiare l'uso di gestori di password (password manager).

**Mitigazione e Risposta:**

*Soluzioni di Gestione dei Bot:* Esistono piattaforme di sicurezza avanzate che utilizzano l'analisi comportamentale e l'intelligenza artificiale per distinguere il traffico umano legittimo da quello automatizzato dei bot, bloccandoli in tempo reale.

*Monitoraggio dei Login Anomali:* Monitorare i registri di autenticazione per rilevare pattern sospetti, come un alto numero di tentativi di login falliti da una vasta gamma di IP, può aiutare a identificare un attacco in corso.

*Risposta all'Incidente:* In caso di account compromesso, la procedura prevede di bloccare l'account, notificare immediatamente l'utente e guidarlo nel processo di recupero sicuro.

.

# Quishing

## Furto di Credenziali tramite Quishing (Phishing con QR Code)

**Target tipico/esempio: dipendente che riceve un'email sul proprio account aziendale. L'email è costruita per impersonare un servizio ampiamente utilizzato e considerato affidabile come ad esempio Microsoft 365, un servizio di firma digitale o persino un reparto interno come le Risorse Umane. Il messaggio crea un senso di urgenza, ad esempio notificando la presenza di un messaggio vocale da ascoltare o la necessità di verificare le proprie credenziali di sicurezza.**

### Come è avvenuto l'attacco

**Fase 1:** *Bypass delle Difese Email.* Il corpo dell'email non contiene un link testuale, che verrebbe facilmente analizzato e bloccato dai filtri di sicurezza. L'hacker inserisce invece un'immagine: un codice QR. Molti sistemi di sicurezza tradizionali non sono in grado di analizzare il contenuto delle immagini per estrarre e verificare l'URL nascosto nel QR code. L'email viene quindi classificata come sicura e consegnata.

**Fase 2:** *Il "Salto di Dispositivo".* Questa è la componente tattica cruciale. L'email viene letta sul computer aziendale, ma le istruzioni richiedono di scansionare il QR code con la fotocamera di un altro dispositivo: lo smartphone personale. Questo "salto" sposta l'azione dal perimetro di sicurezza aziendale (il PC, protetto da software di sicurezza) a un ambiente esterno e non gestito (il telefono personale).

**Fase 3:** *Raccolta delle Credenziali.* Una volta scansionato il QR code, il browser dello smartphone viene reindirizzato a una pagina di phishing, una replica perfetta della pagina di login legittima (es. quella di Microsoft). L'utente, ingannato, inserisce le proprie credenziali aziendali, che vengono immediatamente rubate dall'hacker.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Rischio di perdite economiche dirette se l'account compromesso viene utilizzato per autorizzare bonifici fraudolenti (BEC). Costi per l'indagine, la bonifica dei sistemi e il rafforzamento delle difese.

**Operative:** L'account compromesso diventa un punto di partenza per lanciare altri attacchi all'interno dell'azienda. I team di sicurezza devono dedicare tempo per investigare la violazione, revocare gli accessi e mettere in sicurezza l'account.

**Legali:** L'accesso non autorizzato a un account email contenente dati personali è una violazione del GDPR, che comporta obblighi di notifica e il rischio di sanzioni.

**Reputazionali:** Danno all'immagine aziendale, che dimostra di essere vulnerabile a tecniche di phishing moderne. Se l'account viene usato per attaccare clienti o partner, la perdita di fiducia può essere irreparabile.

# Quishing

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Tecnologia Avanzata di Sicurezza Email:* Le soluzioni di sicurezza email di nuova generazione devono impiegare tecnologie basate su Intelligenza Artificiale che integrino l'analisi delle immagini e il Riconoscimento Ottico dei Caratteri (OCR) per identificare i QR code, estrarre l'URL di destinazione e analizzarlo prima che l'email raggiunga l'utente.

*Formazione Specifica e Simulazioni (Il Firewall Umano):* La formazione sulla sicurezza deve essere costantemente aggiornata per includere le nuove tattiche come il quishing. I dipendenti devono essere addestrati a trattare qualsiasi QR code ricevuto via email con estremo scetticismo e a seguire una regola semplice: non scansionare mai QR code provenienti da fonti non verificate o inaspettate. L'uso di simulazioni di quishing è uno strumento di formazione estremamente efficace.

**Mitigazione e Risposta:**

*Autenticazione a Più Fattori (MFA) come Rete di Sicurezza:* Ancora una volta, l'MFA si rivela essere l'ultima e più critica linea di difesa. Anche se un dipendente cade nella trappola e le sue credenziali vengono rubate, l'hacker non sarà in grado di accedere all'account senza il secondo fattore di autenticazione.

*Piano di Risposta agli Incidenti:* Se un account viene compromesso, è fondamentale attivare il piano di emergenza: isolare l'account, investigare l'entità della violazione, forzare il reset della password e comunicare l'incidente secondo le procedure interne e legali.

.

# SQL Injection

## Attacco alle Applicazioni Web tramite SQL Injection

**Target tipico/esempio: PMI con sito di e-commerce o portale clienti che si basa su un database per funzionare (ad esempio, per gestire prodotti, utenti e ordini).**

### Come è avvenuto l'attacco

**Fase 1:** *Scansione e Individuazione della Vulnerabilità.* L'hacker utilizza strumenti automatici per scandagliare il sito web alla ricerca di punti deboli, in particolare nei moduli di inserimento dati come campi di login, barre di ricerca o form di contatto.

**Fase 2:** *Iniezione di Codice SQL.* Una volta trovato un campo vulnerabile, l'hacker inserisce stringhe di codice SQL malevolo al posto dei dati normali (es. un nome utente). Se l'applicazione web non è programmata per filtrare e validare correttamente questi input, esegue il codice dell'hacker direttamente sul database.

**Fase 3:** *Estrazione dei Dati.* Eseguendo comandi specifici, l'hacker può leggere, modificare o cancellare i dati nel database. Può estrarre informazioni sensibili come anagrafiche dei clienti, cronologia degli ordini, credenziali di accesso e, nei casi peggiori, dettagli delle carte di credito.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi significativi per il ripristino del sito e del database. Perdite economiche dirette se i dati delle carte di credito vengono rubati e utilizzati per transazioni fraudolente. Pesanti sanzioni previste dal GDPR per la violazione dei dati personali.

**Operative:** Interruzione del servizio e-commerce o del portale clienti, con conseguente blocco delle vendite e delle operazioni. È necessario mettere offline il sito per condurre indagini e bonificare il sistema, attivando procedure di emergenza per il ripristino dei dati.

**Legali:** Violazione diretta del GDPR a causa del furto di dati personali dei clienti. Scatta l'obbligo di notificare l'incidente al Garante della Privacy e a tutti gli utenti interessati. Rischio di azioni legali da parte dei clienti danneggiati.

**Reputazionali:** Perdita totale della fiducia da parte dei clienti, che non si sentiranno più sicuri a effettuare acquisti o a inserire i propri dati sul sito. Il danno d'immagine può essere grave e molto difficile da recuperare.

# SQL Injection

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Sviluppo di Codice Sicuro:* È la misura più importante. Gli sviluppatori devono utilizzare query parametrizzate (o "prepared statements"), che separano nettamente i comandi SQL dai dati inseriti dagli utenti, rendendo impossibile l'iniezione di codice. È inoltre fondamentale validare e "sanificare" tutti gli input degli utenti.

*Web Application Firewall (WAF):* Implementare un WAF, ovvero un firewall specifico per le applicazioni web, che è in grado di filtrare il traffico e bloccare le richieste che contengono tentativi di SQL injection noti.

*Scansioni di Vulnerabilità:* Eseguire regolarmente scansioni di sicurezza e test di penetrazione (penetration test) per identificare e correggere le vulnerabilità prima che vengano sfruttate dagli hacker.

**Mitigazione e Risposta:**

*Principio del Minimo Privilegio:* Configurare l'account del database utilizzato dal sito web con i minimi permessi strettamente necessari. In questo modo, anche se un hacker riesce a sfruttare una vulnerabilità, i danni che può fare sono limitati.

*Monitoraggio e Logging:* Monitorare costantemente i log del database e del server web per individuare attività sospette o query anomale.

*Piano di Risposta agli Incidenti:* Avere un piano d'azione chiaro per isolare il sistema, analizzare la violazione, notificare le autorità e i clienti, e ripristinare i dati da backup sicuri.

.

# Man-in-the-Middle

## Attacco Man-in-the-Middle (MitM) su Wi-Fi Pubblico

**Target tipico/esempio: dipendente o consulente di una PMI che, lavorando in mobilità (ad esempio in un aeroporto, in un hotel o in un bar), si connette a una rete Wi-Fi pubblica non sicura per accedere a risorse aziendali.**

### Come è avvenuto l'attacco

**Fase 1:** *Creazione di un Hotspot Malevolo.* L'hacker crea un punto di accesso Wi-Fi falso con un nome credibile e allettante (es. "Aeroporto_WiFi_Gratis"). Questa tecnica è nota come "Rogue Access Point".

**Fase 2:** *Connessione della Vittima.* Il dipendente, alla ricerca di una connessione gratuita, si collega all'hotspot controllato dall'hacker.

**Fase 3:** *Intercettazione del Traffico.* Tutto il traffico internet del dipendente (email, navigazione web, accesso a file) passa ora attraverso il computer dell'hacker. Utilizzando software di "sniffing", l'hacker può catturare e analizzare tutti i dati trasmessi. Se le connessioni non sono criptate (HTTP invece di HTTPS), l'hacker può leggere in chiaro password, email e altre informazioni sensibili.

**Fase 4:** *Furto di Credenziali.* L'hacker può anche utilizzare tecniche più avanzate, come lo "stripping SSL" per forzare il browser a usare connessioni non sicure, o il "DNS spoofing" per reindirizzare la vittima a siti di phishing identici a quelli reali (ad esempio, una finta pagina di login della webmail aziendale o di Microsoft 365) e rubare le sue credenziali.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Perdite economiche dirette se vengono rubate credenziali bancarie o se l'accesso alla rete aziendale viene usato per compiere frodi. Costi elevati per la bonifica dei sistemi e la gestione dell'incidente.i.

**Operative:** Con le credenziali rubate, l'hacker può ottenere un accesso non autorizzato alla rete aziendale, interrompere le operazioni, rubare dati critici (progetti, dati clienti) o lanciare attacchi più gravi come il ransomware.

**Legali:** Se l'accesso alla rete aziendale porta a una violazione di dati personali di clienti o altri dipendenti, scattano gli obblighi previsti dal GDPR, inclusa la notifica al Garante e agli interessati.

**Reputazionali:** Grave danno alla reputazione dell'azienda se l'incidente diventa pubblico, dimostrando una scarsa cultura della sicurezza e una gestione negligente del lavoro da remoto.

# Man-in-the-Middle

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Uso Obbligatorio di una VPN:* Stabilire come policy aziendale che tutto il traffico internet, quando si è connessi a reti non fidate come quelle pubbliche, debba obbligatoriamente passare attraverso una VPN (Virtual Private Network). La VPN crea un "tunnel" criptato che rende il traffico illeggibile per chiunque tenti di intercettarlo.

*Formazione dei Dipendenti:* Addestrare i dipendenti a riconoscere i rischi delle reti Wi-Fi pubbliche, a non connettersi mai a reti sospette e a verificare sempre la presenza di HTTPS (il lucchetto) nel browser prima di inserire qualsiasi dato.

*Configurazione dei Dispositivi:* Disabilitare la funzione di connessione automatica a reti Wi-Fi aperte sui dispositivi aziendali (laptop e smartphone).

**Mitigazione e Risposta:**

*Criptazione End-to-End:* Utilizzare sempre applicazioni che offrono la criptazione end-to-end per le comunicazioni sensibili (chat, email, ecc.).

*Monitoraggio degli Accessi:* Monitorare costantemente i log di accesso alla rete aziendale per individuare connessioni da indirizzi IP sospetti o in orari insoliti, che potrebbero essere un segnale di furto di credenziali.

*Procedura di Emergenza:* Se un dipendente sospetta di aver compromesso le proprie credenziali, deve avere una procedura chiara per segnalarlo immediatamente all'IT, che procederà al cambio della password e alla verifica di eventuali accessi anomali.

.

# Malware Mobile

## Furto di Dati tramite Malware su Dispositivi Rimovibili (USB)

**Target tipico/esempio: azienda con ambiente di ufficio dove i dipendenti utilizzano o sono autorizzati a utilizzare chiavette USB per trasferire file.**

### Come è avvenuto l'attacco

**Fase 1:** *Preparazione e Distribuzione.* Un hacker lascia deliberatamente una o più chiavette USB infette in aree comuni frequentate dai dipendenti dell'azienda target (parcheggi, bar, aree ristoro). Questa tecnica è nota come "USB drop attack".

**Fase 2:** *L'Errore Umano.* Un dipendente, spinto dalla curiosità, raccoglie una delle chiavette e la inserisce in un computer aziendale per vedere cosa contiene. Studi hanno dimostrato che la probabilità che ciò accada è molto alta.

**Fase 3:** *Infezione Automatica.* Il malware presente sulla chiavetta si installa automaticamente sul computer. Questo può avvenire sfruttando la funzione di esecuzione automatica (autorun) del sistema operativo o ingannando l'utente con file dai nomi allettanti (es. "Stipendi_Dirigenti.xlsx").

**Fase 4:** *Propagazione e Furto di Dati.* Una volta installato, il malware (che può essere un ransomware, uno spyware che registra tutto ciò che viene digitato, o un altro tipo di virus) si propaga nella rete aziendale, ruba dati sensibili e li invia a un server controllato dall'hacker.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi molto elevati per la bonifica dell'intera infrastruttura IT. Perdite economiche dirette in caso di attacco ransomware o di frodi basate sui dati rubati.

**Operative:** Interruzione delle attività a causa dell'infezione da malware. Compromissione di interi segmenti di rete e necessità di ripristinare i sistemi da zero.

**Legali:** Se vengono rubati dati personali, l'azienda deve adempiere agli obblighi del GDPR, inclusa la notifica della violazione al Garante della Privacy e agli interessati.

**Reputazionali:** Grave danno d'immagine per non aver implementato policy di sicurezza di base e per la conseguente perdita di dati, che dimostra una cultura della sicurezza carente.

# Malware Mobile

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Policy Aziendale Chiara:* Stabilire e applicare una policy che vieti o limiti severamente l'uso di dispositivi USB non autorizzati e non controllati dall'azienda.

*Disabilitazione delle Porte USB:* Disabilitare fisicamente o tramite software le porte USB sui computer che non necessitano di tale funzionalità, specialmente quelli che gestiscono dati critici.

*Formazione dei Dipendenti:* Sensibilizzare i dipendenti sui pericoli degli "USB drop attack" e sull'importanza di non collegare mai dispositivi di origine sconosciuta ai computer aziendali.

**Mitigazione e Risposta:**

*Software di Sicurezza degli Endpoint:* Utilizzare soluzioni antivirus/EDR avanzate che scansionano automaticamente qualsiasi dispositivo esterno collegato e bloccano l'esecuzione di malware.

*Controllo dei Dispositivi:* Implementare software di "Device Control" che permetta di creare una lista di dispositivi USB autorizzati (ad esempio, solo quelli forniti dall'azienda e criptati) e di bloccare tutti gli altri.

*Isolamento:* In caso di infezione, la prima e più importante azione è isolare immediatamente il computer colpito dalla rete per contenere la diffusione del malware.

.

# IP Camera Attack

## Compromissione di Telecamere IP tramite Credenziali di Default

**Target tipico/esempio: azienda che utilizza telecamere di sorveglianza IP connesse alla rete aziendale, ma che non ha modificato le credenziali di amministrazione impostate di fabbrica o non ha aggiornato regolarmente il software interno (firmware).**

### Come è avvenuto l'attacco

**Fase 1:** *Scansione e Scoperta.* Gli hacker utilizzano strumenti automatici che perlustrano costantemente Internet alla ricerca di dispositivi IoT, come le telecamere IP, che sono visibili online e rispondono su porte di gestione standard.

**Fase 2:** *Sfruttamento delle Credenziali di Default.* Una volta individuata una telecamera, l'hacker tenta di accedervi utilizzando una lista di combinazioni di username e password di default molto comuni (es. "admin/admin", "root/password"). Poiché moltissimi dispositivi non vengono mai riconfigurati dopo l'installazione, l'accesso riesce con estrema facilità.

**Fase 3:** *Presa di Controllo e Punto d'Ingresso.* L'hacker ottiene il pieno controllo della telecamera. A questo punto, non solo può visualizzare e registrare i flussi video, ma, cosa ancora più grave, la telecamera diventa un punto d'ingresso ("foothold") all'interno della rete aziendale, bypassando le difese perimetrali come i firewall.

**Fase 4:** *Movimento Laterale e Attacco.* Dalla telecamera compromessa, l'hacker inizia a esplorare la rete interna alla ricerca di altri sistemi vulnerabili (computer, server, archivi di dati) per lanciare attacchi più gravi, come il furto di dati sensibili o l'installazione di un ransomware.

---

### Conseguenze (Finanziarie, Operative, Legali, Reputazionali)

**Finanziarie:** Costi per la messa in sicurezza dell'intera infrastruttura IT e per la gestione di eventuali attacchi successivi (ad esempio, il pagamento di un riscatto o i costi di ripristino).

**Operative:** Compromissione della sorveglianza fisica e della sicurezza dei locali. Rischio di interruzione delle attività a causa di attacchi propagati dalla telecamera infetta ad altri sistemi critici.

**Legali:** Grave violazione della privacy (GDPR) se le telecamere riprendono aree con dati personali o dipendenti e i flussi video vengono esposti o rubati. Scattano gli obblighi di notifica in caso di furto di dati.

**Reputazionali:** Danno gravissimo alla fiducia di clienti e partner, che vedono l'azienda come negligente nella gestione della sicurezza di base e incapace di proteggere anche le proprie sedi fisiche.

# IP Camera Attack

## Azioni da intraprendere (Prevenzione, Mitigazione, Risposta)

**Prevenzione (Tecnologica e Processi e Persone)**

*Cambiare Sempre le Credenziali di Default:* La prima e più importante azione è cambiare la password di amministrazione di qualsiasi dispositivo IoT (telecamere, router, stampanti) con una password complessa e unica.

*Aggiornare il Firmware:* Mantenere il firmware dei dispositivi costantemente aggiornato per correggere le vulnerabilità di sicurezza non appena vengono scoperte dal produttore.

*Segmentazione della Rete:* Isolare tutti i dispositivi IoT, incluse le telecamere, in una rete separata (VLAN o rete ospiti) dal resto della rete aziendale. In questo modo, anche se una telecamera viene compromessa, l'hacker non può accedere ai sistemi critici come server e PC.

**Mitigazione e Risposta:**

*Limitare l'Accesso da Internet:* Non esporre mai l'interfaccia di gestione delle telecamere direttamente su Internet. Se è necessario un accesso remoto, utilizzare sempre una VPN sicura.

*Monitoraggio del Traffico:* Monitorare il traffico di rete per individuare comunicazioni anomale provenienti dalle telecamere verso destinazioni sospette su Internet, che potrebbero indicare una compromissione.

*Disabilitare Servizi Non Necessari:* Disabilitare sui dispositivi tutte le funzioni non strettamente necessarie e potenzialmente insicure, come Telnet o UPnP.

.

www.fowhe.com/it/index

# Chi è Fowhe

**Fowhe è dal 2007 fornitore di servizi ed operatore di TLC, focalizzato sul settore business che progetta ed implementa soluzioni IT**, favorendo la transizione digitale delle piccole e medie imprese e delle PA del territorio. Il team di Fowhe è costituito da **Ingegneri informatici, Ingegneri delle telecomunicazioni**, **tecnici specializzati nel settore dei sistemi e delle reti**.
Fowhe dispone di risorse di rete e datacenter sul territorio Pugliese e, secondo l'analisi 2025 di Plimsoll Italia sulle 524 aziende del settore, Fowhe si posiziona 31a tra le imprese del settore con maggior margine di profitto (www.plimsoll.it).
**E' classificato come soggetto importante dall'Agenzia per la Cybersicurezza Nazionale** (ACN), ai sensi della direttiva NIS2 e il Decreto Legislativo 138/2024.

NAMEX ROMA INTERNET EXCHANGE POINT  RIPE NCC RIPE NETWORK COORDINATION CENTRE  ASSOProvider

## 1 E' operatore di TLC

Fowhe è autorizzata dal 2007 ai sensi dell'articolo 25 del Decreto Legislativo n. 259/2003 e ss.mm.ii. del Codice delle comunicazioni elettroniche, è titolare di autorizzazione generale per l'offerta al pubblico di servizi di comunicazione elettronica, è titolare di autorizzazione generale per l'installazione e la fornitura di reti pubbliche di comunicazioni.

## 2 E' Autonomous System

Fowhe è Autonomous System con numero AS60443, presente nei principali Internet Exchange Point nazionali e dispone di risorse IT/TLC sul territorio Pugliese. Questo gli consente di essere un operatore di rete indipendente che implementa ed eroga i migliori servizi disponibili.

## 3 E' parte dell'ecosistema di Internet

Fowhe è socia dei consorzi e delle associazioni che rappresentano l'ecosistema di Internet come il Roma Internet Excenge Point (NAMEX), il Regional Internet Registry for Europe (RIPE), l'Associazione di Provider Internet Indipendenti Italiani (Assoprovider).

## 4 E' costantemente aggiornata

Il Team di Fowhe partecipa ai principali eventi e conferenze che interessano il mondo dell'informatica e delle telecomunicazioni restando sempre al passo con le innovazioni e le tendenze del settore.

fowhe.com

# Contatti


### Website
www.fowhe.com/it/index

### E-mail
business@fowhe.com

### Telefono
+ (39) **06 90285189**

### Social Media
www.linkedin.com/company/fowhe-s-r-l-

### Head quarter
Via A. Salandra 18 - ROMA

### Sedi operative
Via Assunta 19 - MARTANO (LE)

Viale Donato De Leonardis zona ASI - BARI