

# Report IA e Cybersecurity W21D1

In questo esercizio dovremo dare un prompt ad una AI, nel mio caso ho scelto ChatGPT, per simulare un attacco ransomware ad una azienda e implementare misure di sicurezza per la mitigazione l'attacco.

Per favore, simula una situazione in cui un'azienda è colpita da un ransomware, implementa delle misure di sicurezza per mitigare l'attacco.

Certo! Di seguito ti propongo una **simulazione realistica** di un attacco ransomware a un'azienda, seguita da una **strategia di risposta** e misure di mitigazione suddivise in fasi.

## **Simulazione di attacco ransomware e risposta aziendale**

### **Scenario**

**Azienda:** MediTech S.p.A.

**Settore:** Dispositivi medicali

**Dimensioni:** 300 dipendenti

**Infrastruttura IT:** 20 server (Windows/Linux), rete interna, servizi cloud, backup locale e cloud.

## **Fase 1: Attacco ransomware**

### ◆ **Giorno 0 – Compromissione iniziale**

Un dipendente del reparto contabilità apre un'email di phishing con allegato un documento Excel. L'allegato sfrutta una vulnerabilità di macro non aggiornate per eseguire uno script che scarica ed esegue un payload ransomware chiamato **BlackCrypt**.

### ◆ **Giorno 1 – Espansione laterale**

Il ransomware:

- Eleva i privilegi grazie a credenziali salvate nel browser del dipendente.
- Si propaga lateralmente sfruttando la condivisione di rete aperta e la mancanza di segmentazione.
- Cifra file nei file server, database locali e backup connessi.

### ◆ **Giorno 2 – Riscatto e blocco attività**

L'interfaccia del server mostra un messaggio di riscatto:

"I vostri file sono stati criptati. Pagate 5 BTC per riaverli."

## **Fase 2: Risposta immediata all'incidente**

### **1. Isolamento**

- Disconnessione dei sistemi infetti dalla rete.
- Spegnimento sicuro dei server colpiti.
- Blocco delle VPN e disattivazione temporanea dell'accesso esterno.

### **2. Notifica**

- Coinvolgimento immediato del team di risposta agli incidenti (CSIRT).
- Comunicazione all'Autorità Garante Privacy (se coinvolti dati personali).
- Informazione ai dipendenti per evitare la diffusione del malware.

### **3. Analisi forense**

- Identificazione dell'origine (email, IP).
- Raccolta dei log da firewall, endpoint, Active Directory.

### **4. Backup e ripristino**

- Verifica dell'integrità dei backup cloud isolati.
- Ripristino graduale dei sistemi partendo dai più critici.
- Implementazione di una rete temporanea sicura per il ripristino.



## Fase 3: Misure preventive post-attacco

### ◆ Tecniche

- Segmentazione della rete: separare reti utente, server, backup.
- Backup 3-2-1:
  - 3 copie dei dati
  - 2 su supporti diversi
  - 1 offline/off-site
- Endpoint Detection & Response (EDR) su tutte le postazioni.
- Patch management automatizzato e controllato settimanalmente.

### ◆ Utenti e processi

- Formazione anti-phishing obbligatoria ogni 6 mesi.
- Accesso a privilegi minimi (PoLP) per utenti e servizi.
- Multi-Factor Authentication (MFA) per accessi critici (VPN, email, admin).
- Simulazioni periodiche di attacco per testare la risposta.

### ◆ Procedure

- Creazione e test di un Incident Response Plan documentato.
- Redazione di un Business Continuity Plan (BCP).
- Audit annuale della sicurezza IT con esperti esterni.



## Esito

Dopo 5 giorni, MediTech riesce a ripristinare il 90% delle operazioni senza pagare il riscatto. L'evento viene classificato come **Data Breach** ad alto rischio, ma contenuto efficacemente grazie alla reazione rapida e alla disponibilità di backup offline.

# Facoltativo

Dato un report creato da Verizon, dovremo chiedere ad una AI di fornire un riassunto e delle informazioni su phishing e social engineering.

Riassunto



## Dati chiave

- 22.052 incidenti analizzati, di cui 12.195 confermati come violazioni di dati — il numero più alto nella storia del DBIR.
- I dati provengono da 139 paesi, con contributi da fornitori di sicurezza, enti governativi, compagnie assicurative e fonti pubbliche.
- L'elemento umano è stato coinvolto nel 60% delle violazioni.
- La complicità di terze parti è raddoppiata, passando dal 15% al 30% delle violazioni.



## Principali modalità di accesso iniziale

1. Abuso di credenziali (22%) – leggero calo dal 31% dell'anno precedente.
2. Sfruttamento di vulnerabilità (20%) – in crescita del 34%, specialmente su dispositivi edge e VPN.
3. Phishing (15%) – stabile, ma spesso preludio all'abuso di credenziali.



## Tattiche e tecniche emergenti

- Ransomware presente nel 44% delle violazioni, in crescita rispetto al 32% dello scorso anno. Tuttavia, la media dei riscatti pagati è calata a 115.000 dollari.
- Gli attacchi ransomware colpiscono l'88% delle PMI rispetto al 39% delle grandi imprese.
- Malware infostealer ha portato al furto di credenziali aziendali anche da dispositivi personali (BYOD).
- Espionaggio in aumento: rappresenta ora il 17% delle violazioni con una forte incidenza negli attacchi sponsorizzati da stati.



## **Minacce legate all'Intelligenza Artificiale**

- Uso crescente di testi generati da GenAI in e-mail malevole (raddoppiato in due anni).
- 14% dei dipendenti accede regolarmente a strumenti GenAI su dispositivi aziendali, spesso con account non aziendali.
- Rischio di perdita di dati sensibili tramite caricamento su piattaforme AI non autorizzate.



## **Coinvolgimento umano**

- L'errore umano, la social engineering (es. phishing, pretexting) e l'abuso interno restano fattori chiave.
- Errore umano = 2x più frequente dell'abuso intenzionale da parte di interni.
- Errori comuni: invio errato di e-mail (misdelivery), perdita o esposizione accidentale di credenziali/API.



## **Ruolo delle terze parti**

- Le violazioni legate a terze parti sono cresciute esponenzialmente.
- Casi emblematici: vulnerabilità MOVEit, compromissioni tramite piattaforme come Snowflake.
- Solo il 54% delle vulnerabilità sui dispositivi edge è stato completamente risolto, con un tempo mediano di 32 giorni.



## **Approfondimenti settoriali**

- Focus su settori: Sanitario, Finanziario, Retail, Istruzione, Manifatturiero.
- Nuova sezione per le PMI e il Settore Pubblico.

## 📌 Conclusioni e raccomandazioni

- Il **patching rapido**, l'**MFA obbligatoria**, la **gestione dei segreti API**, e un **maggiore controllo delle terze parti** sono cruciali.
- La **collaborazione tra organizzazioni** e la **condivisione delle informazioni** sono essenziali per rafforzare la sicurezza.
- Le aziende devono rivalutare il **rischio operativo** connesso ai fornitori SaaS e alle dipendenze digitali critiche.

Informazioni su phishing e social engineering

## ✅ Dati confermati dal report caricato

- Il **phishing** è al 15% tra i vettori di accesso iniziale nei breach non legati a Error o Misuse (fonte: pagina "Summary of findings", grafico Fig. 5 e Fig. 16) .
- Il **social engineering** è una delle categorie principali nel DBIR, insieme a System Intrusion, Error, Web App Attacks, ecc. (vedi introduzione ai "Incident Classification Patterns") .
- Le email scritte con **AI generativa** per scopi malevoli sono raddoppiate in due anni (da ~5% a ~10%) — questo è riportato nella sezione sulle minacce emergenti legate all'AI .
- Il **60% delle violazioni** coinvolge l'**elemento umano**, come l'interazione con phishing, errori o comportamenti ingenui (Fig. 14–15) .
- **Credential harvesting** e l'abuso delle credenziali rubate tramite phishing sono collegati a molte delle violazioni analizzate, con phishing spesso come step iniziale non rilevato .
- Gli attacchi sono sempre più **automatizzati** (es. AI per creare campagne phishing su larga scala) .
- Viene raccomandato l'uso di **MFA**, **segmentazione della rete**, e **formazione degli utenti** come contromisure dirette .

# Pratica Extra

## Introduzione

Le implementazioni TLS e DTLS in OpenSSL 1.0.1 prima della versione 1.0.1g non gestiscono correttamente i pacchetti dell'estensione Heartbeat, il che permette ad attaccanti remoti di ottenere informazioni sensibili dalla memoria del processo attraverso pacchetti appositamente costruiti che causano una lettura oltre i limiti del buffer (buffer over-read), come dimostrato dalla possibilità di leggere chiavi private. Il problema è legato ai file `d1_both.c` e `t1_lib.c`, ed è noto come vulnerabilità Heartbleed.

## Analisi delle vulnerabilità contenute nel codice

Tipo	Descrizione	Gravità
Buffer over-read	Heartbleed: il server legge oltre i limiti del buffer client	Critica
RNG non implementato	Padding non sicuro	Media
Nessun controllo su malloc	Possibili crash	Media
Uso di strlen su buffer binari	Test imprecisi	Bassa

## Analisi attacchi contenuti nei log

Tipo	Vettore	Gravità	Azioni consigliate
SSH brute-force	116.31.116.17	Media	Limitare IP, Fail2ban
PhpMyAdmin scan	190.129.24.154	Media	Nascondere o rimuovere PhpMyAdmin
WebDAV accesso	180.97.106.37	Media	Disabilitare WebDAV se non usato
Binary fuzzing	/	Critica	Controllare logs, memory leaks
WordPress RCE	191.101.x.x etc.	Critica	Aggiornare plugin/vulnerabilità note
Shell injection	nowosely.byl	Critica	Monitorare /tmp, alert intrusioni
XML-RPC abuse	Multipli	Alta	Disabilitare XML-RPC se non usato
FTP scans	110.11.148.226	Media	Limitare accesso FTP
SMTP overload	81.114.251.53	Alta	Limitare connessioni, SPF/DKIM/DMARC