

W21D1 – Pratica

Epic Education Srl

Prompt AI sicurezza contro Ransomware

Analisi ChatGPT ultimo DBIR

Analisi heartbleed.c

Simone Giordano

29/11/2025



Contatti:

Tel: 3280063044

Email: mynameisimone@gmail.com

Linkedin: <https://www.linkedin.com/in/simone-giordano-91290652/>

Sommario

Prompt AI per misure di sicurezza contro un Ramsomware	3
Traccia.....	3
Esercizio.....	3
Analisi ChatGPT dell'ultimo DBIR	4
Traccia.....	4
Esercizio.....	4
Analisi heartbleed.c	9
Traccia.....	9
Esercizio.....	9

Prompt AI per misure di sicurezza contro un Ransomware

Traccia

Crea un prompt che aiuti la tua organizzazione a implementare delle misure di sicurezza contro il ransomware partendo da una simulazione di attacco.

Esercizio

PROMPT

Implementa delle misure di sicurezza per la seguente simulazione di attacco

1. Phishing Iniziale

Un attore malevolo invia una email fraudolenta contenente un allegato sospetto o un link ingannevole. L'utente, non riconoscendo il pericolo, apre l'allegato o clicca sul link.

2. Attivazione del Payload

Dopo l'interazione dell'utente, il file avvia un finto processo di installazione per mascherare le sue reali intenzioni.

Apparentemente si presenta come un aggiornamento software o un documento legittimo.

3. Escalation di Privilegi

Una volta attivo, il malware acquisisce privilegi elevati sulla macchina compromessa. L'attaccante "ottiene" diritti amministrativi necessari per espandere l'attacco.

4. Movimento Laterale

Con i nuovi privilegi, l'attaccante tenta di accedere ad altri sistemi/host nella rete utilizzando protocolli legittimi come SMB o RDP.

5. Cifratura dei File

Il ransomware avvia la cifratura dei file presenti sulla macchina infetta.

I documenti appaiono rinominati o resi inaccessibili.

6. Nota di Riscatto

Al termine dell'attacco appare una schermata con la richiesta di riscatto, in cui l'attaccante comunica che i dati sono stati bloccati e fornisce istruzioni per la presunta "restituzione".

Risposta Perplexity

Per mitigare un attacco simulato come quello descritto, si possono implementare le seguenti misure di sicurezza corrispondenti alle fasi dell'attacco:

1. Phishing Iniziale

- Usare filtri antispam e gateway di posta elettronica con intelligenza artificiale per bloccare messaggi sospetti prima che raggiungano gli utenti.
- Formare gli utenti all'identificazione di email fraudolente (es. mittenti camuffati, link sospetti, errori di dominio simili).
- Implementare l'autenticazione a più fattori per limitare l'uso di credenziali compromesse.

2. Attivazione del Payload

- Impiegare soluzioni di sandboxing per eseguire in modo sicuro gli allegati e rilevare comportamenti anomali o malware.
- Tenere sempre aggiornati antivirus e sistemi di rilevamento delle minacce.

3. Escalation di Privilegi

- Configurare controlli di accesso basati sul principio del privilegio minimo.
- Utilizzare sistemi di monitoraggio e rilevazione delle anomalie per identificare tentativi di aumento di privilegi.

4. Movimento Laterale

- Segmentare la rete impedendo l'accesso libero tra nodi tramite firewall e regole di accesso restrittive.
- Monitorare il traffico di rete e log degli accessi per individuare movimenti laterali sospetti, soprattutto su protocolli come SMB o RDP.

5. Cifratura dei File

- Implementare backup regolari e sicuri dei dati, conservati offline o in ambienti isolati.
- Utilizzare soluzioni di protezione endpoint con capacità antiransomware.

6. Nota di Riscatto

- Non pagare il riscatto e coinvolgere immediatamente il team di risposta agli incidenti.
- Attivare procedure di ripristino da backup e analisi forense per rimuovere il malware e mitigare l'impatto.

Queste contromisure vanno integrate in un programma di sicurezza a più livelli che includa formazione continua, tecnologie di prevenzione e monitoraggio attivo sulla rete e sugli endpoint, per una difesa efficace contro attacchi ransomware e phishing.

Analisi ChatGPT dell'ultimo DBIR

Traccia

1. Scarica l'ultimo Data Breach Investigations Report (DBIR) di Verizon (non richiede registrazione):
<https://www.verizon.com/business/resources/reports/dbir/>
2. Chiedi a ChatGPT un riassunto del report
3. Chiedi le informazioni su phishing e social engineering contenute nel report

Esercizio

2

Prompt fai un riassunto di questo report: <https://www.verizon.com/business/resources/T939/reports/2025-dbir-data-breach-investigations-report.pdf?FirstName=Ciao&LastName=Ciao&Email=1983giordano%40gmail.com&Company=&Segment=vzw&Country=it&zCSMKTOGDPROptIn=>

RISPOSTA ChatGPT

Ecco un **riassunto strutturato** del 2025 *Data Breach Investigations Report (DBIR)* di Verizon — con i punti principali e le implicazioni più rilevanti.

Dati generali sul report

- Il DBIR 2025 è l'edizione numero 18 del rapporto annuale. [Verizon+1](#)
 - Sono stati analizzati **22.052 incidenti di sicurezza reali**, di cui **12.195 violazioni confermate (data breaches)**. [Verizon+1](#)
 - Le organizzazioni coinvolte provengono da **139 paesi** e includono imprese di tutte le dimensioni e settori. [Verizon+1](#)
-

Principali tendenze e risultati chiave (globale)

- **Sfruttamento di vulnerabilità in aumento:** l’“exploitation of vulnerabilities” come vettore iniziale di attacco è cresciuto del **34%** rispetto all’anno precedente. Ora rappresenta circa il **20% di tutte le violazioni**. [Verizon+2](#)[Verizon+2](#)
 - **Ransomware sempre più diffuso:** gli attacchi ransomware, con o senza cifratura, sono presenti in **44% delle violazioni** analizzate — un aumento del **37%** rispetto al 2024. [Verizon+2](#)[Verizon+2](#)
 - **Coinvolgimento di terze parti in forte crescita:** le violazioni che vedono implicate terze parti si sono **doppiate rispetto all’anno precedente (30%)**. Ciò evidenzia quanto la supply chain e i partner esterni rappresentino oggi un rischio importante. [Verizon+1](#)
 - **“Fattore umano” ancora centrale:** circa il **60% delle violazioni** coinvolge in qualche modo errori umani, abuso di credenziali o social engineering. [Verizon+1](#)
-

Dettagli sulle tecniche e modalità di attacco

- **Credential abuse (abuso di credenziali) e vulnerabilità sfruttate** sono tra le vie d’ingresso più comuni. Nel 2025: credential abuse ~ 22%, exploit vulnerabilità ~ 20%. [Verizon+2](#)[LinkedIn+2](#)
 - Un’importante porzione di exploit riguarda **zero-day e vulnerabilità su dispositivi di perimetro e VPN**, spesso poco o non patchati. [Verizon+1](#)
 - Solo circa il **54% delle vulnerabilità su dispositivi di perimetro/VPN** viene completamente remediato; la mediana del tempo di patching è di **32 giorni**. [Verizon+1](#)
-

Focus su Ransomware e impatto su aziende di dimensioni diverse

- Per le **PMI (piccole e medie imprese)**, il ransomware è particolarmente pericoloso: in questo segmento è presente in **88% delle violazioni**. [Verizon+2](#)[Quisitive+2](#)

- Nonostante la crescita degli attacchi, **la mediana delle riscatti pagati è scesa a 115.000 USD**, probabilmente anche grazie al fatto che molte vittime (circa il 64%) **non pagano** il riscatto — un aumento rispetto al 50% di due anni fa. [Verizon+2Verizon+2](#)
-

Differenze regionali e aspetti settoriali

- Nel report 2025 emerge un forte aumento delle **intrusioni di sistema (system intrusion)** in EMEA: le violazioni di questo tipo quasi raddoppiano, al **53%** del totale regionale. [Verizon+1](#)
 - Sempre in EMEA, un dato preoccupante: **29% dei breach provengono dall'interno dell'organizzazione** (insider), fra errori involontari o uso improprio di dati. [Verizon+1](#)
 - Per settore: il **manufacturing** ha visto un'impennata (quasi sei volte) negli attacchi motivati da **spionaggio industriale**; anche **salute (healthcare)**, istruzione, finanza e retail restano tra i più bersagliati. [Verizon+1](#)
-

Implicazioni e raccomandazioni

Secondo il report, questi risultati dimostrano l'urgenza di adottare:

- Una **strategia di difesa a più livelli (defense-in-depth)**, non solo tecnologie singole. [GlobeNewswire+1](#)
 - **Patch tempestive**, in particolare su dispositivi di perimetro e VPN. [Verizon+1](#)
 - **Gestione rigorosa della supply chain** e dei fornitori/terze parti. [Verizon+1](#)
 - **Formazione continua del personale** per ridurre il rischio legato a errori umani, phishing e abuso credenziali. [Verizon+1](#)
 - Politiche di resilienza e backup efficaci, tra le tante difese contro ransomware e data breach.
-

A cosa serve questo report — e a chi è utile

Il DBIR 2025 è una risorsa preziosa per:

- Responsabili IT e cybersecurity, per valutare il proprio livello di esposizione.
 - Manager e leadership aziendale, per comprendere l'importanza strategica della sicurezza.
 - PMI, che — dati i numeri — risultano particolarmente vulnerabili.
 - Consultant, auditor e professionisti della compliance, che possono usare il report come benchmark globale.
-

Se vuoi — posso preparare per te un **infografica riassuntiva (in formato testo)** con i dati più importanti (percentuali, trend, vettori di attacco), così è più facile da includere in un report interno o in una presentazione. Vuoi che la faccia subito?

PROMPT Estrai le informazioni su phishing e social engineering contenute nel report

ChatGPT ha detto:

Ecco un estratto con le informazioni rilevanti su phishing e social-engineering contenute nel *2025 DBIR (Verizon)*, con i dati più utili per analisi o formazione.

💡 Principali numeri su phishing & social engineering (2025 DBIR)

- Il report analizza 22.052 incidenti e 12.195 violazioni confermate (data breaches). [Infosecurity Magazine+2Keepnet Labs+2](#)
 - Il pattern “Social Engineering” risulta come il 2º pattern più frequente a livello globale, con un’incidenza di 17% di tutte le violazioni. [Keepnet Labs+2Infosecurity Magazine+2](#)
 - Nel 2025, la “human element” (elemento umano) è ancora coinvolta in circa 60% delle violazioni. [LinkedIn+2PhishingBox+2](#)
 - Quindi, anche se le intrusioni di sistema (system intrusion) sono in aumento, gli attacchi basati su persone (phishing, pretexting, errori umani) restano un vettore critico. [LinkedIn+2Techbusiness+2](#)
-

📌 Dettagli e dinamiche di social engineering

- La classe “Social Engineering” include tecniche come phishing, pretexting, e Business Email Compromise (BEC). [Verizon+2LinkedIn+2](#)
 - Il rapporto segnala che phishing continua a essere la tecnica predominante all’interno di “social actions” (azioni sociali) legate alle violazioni. [GlobeNewswire+2Verizon+2](#)
 - In EMEA (Europa, Medio Oriente, Africa): il phishing è riportato nel 19% delle violazioni per quella regione. [Verizon+2Verizon+2](#)
 - Spesso il phishing non è definito come vettore iniziale del breach, ma può comunque essere la causa indiretta – ad esempio tramite furto di credenziali usate in un secondo momento. Il report stesso nota che “credential abuse” e “social engineering” tendono a sovrapporsi. [LinkedIn+2SOCRadar® Cyber Intelligence Inc.+2](#)
-

⚠️ Implicazioni evidenziate dal report

- L’elemento umano rimane un fattore critico di rischio: nonostante l’aumento di attacchi sofisticati (zero-day, malware, ransomware), persiste una quota importante di attacchi basati su phishing e social engineering. [Techbusiness+2LinkedIn+2](#)

- Non è sufficiente proteggere solo con tecnologie: firewall, EDR o patch non bastano. È essenziale l'educazione continua degli utenti e una cultura di sicurezza, perché il phishing e le trappole sociali spesso fanno leva su errori umani o fiducia. [GlobeNewswire+2Keepnet Labs+2](#)
 - Attacchi su più fasi: phishing o social engineering iniziale possono preparare il terreno per un accesso posteriori tramite credential reuse, accesso non autorizzato o malware. Questo rende difficile attribuire il breach a un singolo vettore, ma rafforza l'importanza di considerare la catena di attacco completa. [LinkedIn+2PhishingBox+2](#)
-

👤 Cosa significa per un'organizzazione (raccomandazioni)

- Implementare un programma di formazione e consapevolezza che non sia “una tantum”, ma continuo, con simulazioni realistiche di phishing, aggiornamenti e sensibilizzazione.
- Monitorare e analizzare indicatori di comportamento oltre a quelli tecnici: ad esempio, segnalazioni di email sospette, segnalazioni di possibili phishing, cambiamenti nelle credenziali.
- Combinare la difesa tecnica (patch, EDR, MFA, gestione privilegi) con controlli organizzativi e procedurali che riducano la superficie di attacco e la dipendenza dall'utente.
- Considerare la supply chain e terze parti: data la complessità delle catene produttive e la presenza di terze parti, la formazione e le misure di sicurezza dovrebbero estendersi anche a fornitori, partner e consulenti.

Analisi heartbleed.c

Traccia

1 Analizza il codice in cerca di vulnerabilità <https://github.com/patricia-gallardo/insecure-coding-examples/blob/main/vulnerability/heartbleed.c>;

2. Analizza i log della slide seguente in cerca di attacchi.

Esercizio

1

Codice vulnerabile	Vulnerabilità
memcpy(bp, pl, payload);	Copia un numero di byte dichiarato dal client senza controllare se esistono davvero → permette di leggere memoria privata (Heartbleed).
RAND_pseudo_bytes(bp, padding); # funzione vuota	La funzione non riempie il padding, quindi vengono inviati byte casuali presi dalla memoria del server.
strlen(test_case);	strlen si ferma al primo 0x00 e quindi sbaglia la lunghezza reale quando i dati sono binari.
buffer = OPENSSL_malloc(...); # senza controllo	Se malloc fallisce, il programma usa un puntatore NULL → crash.
n2s(p, payload); # senza verificare che ci siano 2 byte	Legge 2 byte anche se il pacchetto potrebbe essere più corto → accesso fuori limite.
n2s(pl, seq); # nel ramo RESPONSE	Legge 2 byte dal payload anche se il payload potrebbe essere troppo corto.
s.s3 = malloc(sizeof(S3)); # senza free	Piccola perdita di memoria: nel test non viene liberata.
dtls1_write_bytes # versione finta	Non gestisce errori e non simula bene l'invio reale, può mascherare problemi.

Di seguito un estratto dell'analisi del codice di ChatGPT.

log_entry	comment
Oct 2	General web scan / suspicious request
Oct 2 06:25:46 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ss	SSH brute force attempt
Oct 2	General web scan / suspicious request
Oct 2 06:25:48 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ss	SSH brute force attempt
Oct 2	General web scan / suspicious request
Oct 2 06:25:51 host-vps sshd[8463]: Failed password for root from 116.31.116.17 port 31142 ss	SSH brute force attempt
Oct 2	General web scan / suspicious request
Oct 2 06:25:51 host-vps sshd[8463]: Received disconnect from 116.31.116.17: 11: [preauth] 191.96.249.97 -	General web scan / suspicious request
1	General web scan / suspicious request
91.96.249.97 -	General web scan / suspicious request
9	General web scan / suspicious request
1.96.249.97 -	General web scan / suspicious request
1.96.249.97 - - [20/Apr/2017:15:45:49 +0200] "GET /phpmyadmin/scripts/setup.php HTTP/1.0"	Scan for phpMyAdmin
190.129.24.154 -	General web scan / suspicious request
1	General web scan / suspicious request
90.129.24.154 -	General web scan / suspicious request
9	General web scan / suspicious request
0.129.24.154 -	General web scan / suspicious request
0.129.24.154 - - [14/Jul/2015:06:41:59 -0400] "GET /phpMyAdmin/index.php HTTP/1.1" 404 162	Scan for phpMyAdmin
190.129.24.154 -	General web scan / suspicious request
1	General web scan / suspicious request