# Incident handler's journal

| **Date:**<br>20/11/2025 | **Entry:**<br>1 |
|---|---|
| Description | L'incidente è iniziato con **email di phishing** inviate ai dipendenti, contenenti allegati dannosi. Una volta aperti, questi hanno installato **malware** sui computer, dando agli aggressori l'accesso alla rete aziendale.<br>Successivamente, gli hacker hanno **distribuito ransomware**, crittografando i file critici e bloccando l'accesso dei dipendenti a cartelle cliniche e software essenziali. L'azienda ha subito **interruzioni operative significative**, ha dovuto spegnere i sistemi e contattare enti esterni per assistenza tecnica e gestione dell'incidente. |
| Tool(s) used | Le email di phishing con allegati dannosi contengono codice progettato per installare malware.<br>Il malware stesso è uno strumento informatico utilizzato dagli aggressori per ottenere accesso alla rete aziendale.<br>Il ransomware è un software malevolo che crittografa i file, bloccando l'accesso ai sistemi e richiedendo un riscatto. |
| The 5 W's | **1.Chi ha causato l'incidente?**<br>Un gruppo organizzato di hacker che utilizza tecniche di phishing e ransomware.<br><br>**2.Che cosa è successo?**<br>I dipendenti hanno ricevuto email di phishing con allegati malevoli. Una volta |

| | |
|---|---|
| | aperti, il malware ha dato agli aggressori accesso alla rete, **permettendo loro** di distribuire ransomware che ha crittografato i file e bloccato le attività della clinica.<br><br>**3.Quando è avvenuto l'incidente?**<br>Martedì mattina, intorno alle 9:00.<br><br>**4.Dove è avvenuto l'incidente?**<br>Presso una piccola clinica sanitaria statunitense, all'interno dei suoi sistemi informatici.<br><br>**5.Perché è accaduto l'incidente?**<br>Perché alcuni dipendenti sono stati ingannati dal phishing, la rete non ha bloccato l'installazione del malware e non erano presenti (o non erano sufficienti) controlli di sicurezza in grado di prevenire o limitare l'attacco. |
| Additional notes | Mi chiedo se la clinica avesse implementato misure di sicurezza come formazione antifishing, backup regolari dei dati o sistemi di rilevamento delle intrusioni. Sarebbe utile capire anche quanto tempo è stato necessario per ripristinare le operazioni e se esisteva un piano di risposta agli incidenti adeguato. |

---

Andrea Vitale

| **Date:**<br>20/11/2025 | **Entry:**<br>2 |
| --- | --- |
| Description | Il problema è l'eccessivo volume di avvisi di sicurezza (alert) generati dai sistemi (come il SIEM), dovuto principalmente a regole mal configurate e un alto tasso di falsi positivi.Questo sovraccarico causa affaticamento negli analisti (Alert Fatigue) e rende difficile identificare rapidamente le vere minacce che si perdono nel "rumore". La soluzione è il continuo affinamento delle regole. |
| Tool(s) used | **SIEM (Security Information and Event Management):** Lo strumento centrale che **genera** gli alert in eccesso.<br>**Sorgenti di Log (Firewall, EDR, Server):** I dispositivi che alimentano il SIEM con dati (log) che possono essere rumorosi. |
| The 5 W's | **1.Chi ha causato l'incidente?**<br>Un certo "Clyne West", che si evince dalla mail.<br><br>**2.Che cosa è successo?** |

| | |
|---|---|
| | Si è verificato un tentativo di attacco di phishing ai danni di un dipendente .<br><br>**3.Quando è avvenuto l'incidente?**<br>Mercoledì 20 luglio 2022 alle 9:30:14<br><br>**4.Dove è avvenuto l'incidente?**<br>L'incidente di phishing ha avuto come bersaglio l'indirizzo email<br><hr@inergy.com><br><br>**5.Perché è accaduto l'incidente?**<br>Perché un dipendente è stato ingannato dal phishing. |
| Additional notes | L' incidente, identificato con il **Ticket ID A-2703** , è un chiaro esempio di attacco di phishing mirato che sfrutta l'ingegneria sociale (richiesta di lavoro) per distribuire malware. |

---

Andrea Vitale