UNIVERSITÀ
DEGLI STUDI
DI MILANO

La gestione tecnica di un incidente informatico

Filippo Berto

Università degli Studi di Milano
29 Jul 2025

Indice

- Introduzione
- Il piano di Risposta agli Incidenti
- Mettiamo in Pratica la Teoria
- Scenario 1: Portale Prenotazioni Ospedale
- Scenario 2: Banca
- Il Giorno Dopo
- Per il Futuro

Link alle slide

Introduzione

Cos'è un Incidente e Perché Dovrebbe Interessarvi?

- **ASP di Palermo**: Nel giugno 2025, l'Azienda Sanitaria Provinciale di Palermo ha confermato di essere stata colpita da un attacco informatico che ha causato notevoli disservizi e leak di informazioni personali.
- **Comune di Brescia**: Nel 2021, il Comune ha subito un grave attacco ransomware che ha bloccato per settimane gran parte dei servizi digitali, dalla gestione delle pratiche anagrafiche al pagamento delle multe.
- **Luxottica**: Il colosso dell'occhialeria è stato vittima di un attacco ransomware nel 2020 che ha causato l'interruzione della produzione in alcuni stabilimenti.

Cos'è un Incidente e Perché Dovrebbe Interessarvi?

Definizione di Incidente Informatico

Definizione

Un incidente è qualsiasi evento che minaccia la **riservatezza**, l'**integrità** o la **disponibilità** dei **dati** e dei **sistemi**.

Cos’è un Incidente e Perché Dovrebbe Interessarvi?

Definizione: Riservatezza

La riservatezza si riferisce alla **protezione delle informazioni** dall’accesso e dalla divulgazione non autorizzata.

Cos'è un Incidente e Perché Dovrebbe Interessarvi?

Definizione: Integrità

L'integrità garantisce che i dati siano **accurati**, **completi** e **non siano stati alterati in modo non autorizzato**.

Cos'è un Incidente e Perché Dovrebbe Interessarvi?

Definizione: Disponibilità

La disponibilità assicura che i sistemi informatici, i dati e le risorse siano **accessibili** e **utilizzabili** dagli utenti autorizzati quando ne hanno bisogno.

Esempi pratici

Evento	Effetto
Un attacco ransomware	*Integrità*
Una fuga di dati (data breach)	*Riservatezza*
Un dipendente che perde il portatile aziendale	*Riservatezza*, *Disponibilità*
Un sito e-commerce che va offline durante il Black Friday	*Disponibilità*
Un errore umano che cancella un database	*Integrità*, *Disponibilità*

Aspetti di un attacco informatico

L’attacco informatico visto come un incendio.

Non si decide come spegnerlo mentre le fiamme divampano.

Serve un piano di prevenzione e d’azione.

Pericolo

È la causa potenziale di un danno. È ciò che potrebbe causare il problema.

Esempio

- Un virus
- Un hacker
- Un dipendente sbadato
- Un hard disk che si rompe.

Rischio

È la probabilità che un pericolo si trasformi in un danno reale, tenendo conto della gravità di tale danno.

Esempio

Il rischio che un virus (pericolo) infetti un PC è alto se il PC non ha un antivirus e l'utente apre allegati sospetti.

Impatto

È la conseguenza negativa di un incidente, ovvero l'entità del danno subito quando un rischio si concretizza.

Esempio

- Impatto Finanziario: Perdita di ricavi, costo del ripristino, multe (es. GDPR).
- Impatto Operativo: Fermo della produzione, impossibilità di erogare servizi.
- Impatto Reputazionale: Perdita di fiducia da parte di clienti e partner.

Prevenzione

Sono tutte le misure e le attività messe in atto prima che un incidente si verifichi, con l'obiettivo di eliminare i pericoli o ridurne il rischio.

Esempio

- Installare antivirus e firewall
- Aggiornare regolarmente i software
- Fare formazione ai dipendenti
- Usare password complesse
- Eseguire backup

Risposta all'emergenza

Sono le azioni specifiche e coordinate che si intraprendono durante e subito dopo un incidente per gestirne le conseguenze e limitarne l'impatto.

Si attiva quando la prevenzione ha fallito.

Esempio

- Isolare i sistemi infetti dalla rete (contenimento)
- Rimuovere il virus (eradicazione)
- Ripristinare i dati dai backup (ripristino)

L'Impatto sul Business

Un incidente non è un «problema dell'IT», ma un **problema di business**.

USD 4.9M: Il costo medio globale di una violazione dei dati nel 2024.

1 in 3: La percentuale di violazioni di dati che coinvolgono dati ombra (shadow data).[1]

[1] Source: https://www.ibm.com/reports/data-breach

L'Impatto sul Business

Costi diretti

Esempio

- Risarcimenti
- Multe (GDPR)
- Costi per i consulenti esterni

Costi indiretti

Esempio

- Danno reputazionale
- Perdita di fiducia dei clienti
- Interruzione dell'operatività (fermo produzione)
- Calo del valore delle azioni

Il piano di Risposta agli Incidenti

Il Piano di Risposta agli Incidenti (Incident Response Plan - IRP)

Definizione: Incident Response Plan

È un documento formale che stabilisce esattamente cosa deve fare un'organizzazione per reagire in modo rapido, coordinato ed efficace quando si verifica un incidente di sicurezza informatica.

Obiettivo: minimizzare l'impatto dell'incidente, riducendo i tempi di inattività, i costi e il danno alla reputazione.

Perché è Fondamentale Avere un Piano?

Riduce il Caos e il Panico Fornisce una guida chiara e passaggi definiti, trasformando l'incertezza in un processo strutturato.

Risparmia Tempo Prezioso In un attacco, ogni secondo conta. Il piano elimina il tempo perso a decidere «chi fa cosa».

Definisce Ruoli e Responsabilità Evita che troppe persone diano ordini o, al contrario, che nessuno prenda l'iniziativa.

Garantisce la Conformità Legale (Compliance) Aiuta a rispettare obblighi di legge, come la notifica di un data breach al Garante per la Privacy entro 72 ore, come richiesto dal GDPR.

Facilita la Comunicazione Assicura che le comunicazioni a clienti, partner e media siano controllate, coerenti e approvate, prevenendo danni reputazionali.

Perché è Fondamentale Avere un Piano?

Un buon IRP non è solo un documento tecnico.

È una guida strategica e operativa.

Perché è Fondamentale Avere un Piano?

Scopo e Obiettivi

Una dichiarazione chiara della finalità del piano.

Esempio

- Proteggere i dati dei clienti
- Garantire la continuità operativa
- Ridurre le perdite finanziarie

Struttura: Preparazione (Preparation)

Identificazione degli asset critici Determinare quali sistemi, dati e servizi sono essenziali all'organizzazione e vulnerabili a minacce informatiche.

Valutazione del threat landscape Valuta le potenziali minacce e vulnerabilità specifiche dell'organizzazione e di ambienti simili.

Analisi dell'impatto Comprensione del potenziale impatto dei possibili incidenti informatici sulle operazioni, la reputazione e la conformità legale.

Sviluppo di policy e procedure Stabilire line guida chiare per la gestione di incidenti, la raccolta dei dati e la comunicazione.

Indicare contatti designati Identificare individui responsabili per la risposta agli incidenti e la comunicazione.

Mantenere una lista di contatti Mantenere aggiornata una lista di contatti interni ed esterni, incluse le autorità legali rilevanti ed eventuali provider di servizi.

Preparare la strumentazione per la gestione della crisi Verificare la disponibilità degli strumenti e le risorse necessarie a rispondere all'emergenza.

Struttura: Preparazione (Preparation)

Definizione di strategie di recovery Indicare i passaggi necessari per ripristinare le normali operazioni dopo un incidente.

Realizzazione di un piano di comunicazoine Definire come l'informazione verrà condivisa internamente ed esternamente all'organizzazione durante e dopo un incidente.

Struttura: Rilevamento e Analisi (Detection & Analysis)

Implementazione del monitoraggio continuo Utilizzo di strumenti come SIEM, IDS e altri sistemi per l'identificazione di anomalie o segni di attacchi di sicurezza.

Analisi delle segnalazioni Investigare le segnalazioni ricevute dai sistemi di identificazione (e dal personale).

Comprensione dell'impatto dell'incidente Verficare la misura (lo scope) e la gravità dell'incidente.

Classificazione dell'incidente Classificare gli incidenti in base alla loro gravità e impatto.

Analisi delle vulnerabilità Indentificare e analizzare le vulnerabilità scoperte tramite risorse interne ed esterne.

Struttura: Contenimento (Containment)

Isolamento dei sistemi compromessi Prevenzione di ulteriori danni isolando i sistemi e le reti compromessi.

Interruzione del malware Fermare la diffusione del malware.

Disabilitare gli account colpiti Mettere in sicurezza gli account utente compromessi.

Implementazione di misure temporanee Applicare misure di sicurezza temporanee per minimizzare l'impatto dell'incidente.

Struttura: Eradicazione (Eradication)

Rimozione Codice Malevolo Eliminare qualsiasi software o codice dannoso dai sistemi interessati.

Patch delle Vulnerabilità Applicare le patch o mitigare le vulnerabilità identificate.

Verifica della Sicurezza del Sistema Assicurarsi che la minaccia non sia più presente.

Struttura: Recupero (Recovery)

Ripristino dei Sistemi Riportare i sistemi interessati al loro normale stato operativo.

Ripristino Dati Recuperare i dati dai backup o da altre fonti.

Riparazione delle vulnerabilità Risolvere eventuali vulnerabilità che potrebbero essere state sfruttate.

Convalidare la sicurezza del sistema Verificare che i sistemi siano sicuri prima di riportarli online.

Struttura: Attività successive (Post-Incident Activity)

Ricerca Forense Condurre indagini approfondite per comprendere la causa principale dell'incidente.

Revisione e aggiornamento del piano di risposta Incorporare le lezioni apprese dall'incidente nel piano di risposta all'incidente.

Aggiornare le strategie di recupero Adattare le strategie di recupero in base alle lezioni apprese.

Documentare le attività Tenere un registro dettagliato di tutte le attività relative all'incidente.

Fine prima parte

Domande?

Mettiamo in Pratica la Teoria

Ruoli e Responsabilità

Computer Security Incident Response Team (CSIRT)

Definisce chi fa parte del team di risposta e cosa fa.

Ruolo	Competenza
Incident Commander	Il leader che coordina tutto e prende le decisioni finali
Team Tecnico	Gli specialisti che «combattono l'incendio» sul campo
Responsabile Comunicazione	L'unica persona autorizzata a parlare con l'esterno
Rappresentante Legale	L'esperto di leggi e normative
Management	Il supporto strategico che approva le decisioni con un forte impatto sul business

Ruoli e Responsabilità

Cosa succede se i ruoli non vengono rispettati?

Esempio

- Team tecnico prende l'iniziativa in modo non coordinato
- Comunicazioni affrettate o non corrette trapelano, danneggiando il business
- Il framework di regolamenti legali non viene rispettato correttamente

Definizione e Classificazione degli Incidenti

Un sistema per etichettare la gravità di un incidente (es. Basso, Medio, Alto, Critico).
Questo aiuta a decidere il livello di urgenza e le risorse da allocare.

Esempio

- Un singolo PC con un virus è un incidente Basso
- Un attacco ransomware che blocca tutti i server è Alto
- Un data breach rilascia dati sensibili degli utenti è Critico

Rilevamento e Segnalazione

Come un dipendente segnala un problema? A chi? Quali sistemi automatici generano allarmi?

Esempio: Sorgenti

Intrusion Detection Systems raccolgono informazioni sul comportamento di sistemi, reti ed utenti. La violazione di policy di sicurezza viene segnalato.

- Email da/a domini esterni con allegati o link sospetti
- Collegamento a siti sospetti
- Esecuzione di applicazioni sospette
- Tentativo di accesso a servizi senza autorizzazione
- Honeypot

Personale non sottovalutate l'utilità di queste segnalazioni. Una persona attenta ai dettagli è più efficace di un sistema di sicurezza generico.

Esempio: Destinazioni

Intrusion Prevention Systems sistemi automatici che applicano policy di sicurezza per difendere l'organizzazione.

- Disattivare account a rischio
- Firewall di rete
- Termina applicazioni o sistemi

Team tecnico il personale tecnico è in grado di reagire in modo accurato, ma riesce a gestire un numero limitato di richieste.

Analisi e Triage

I primi passi per capire: «Cosa sta succedendo? Quanto è grave? Chi è colpito?».

Esempio

- Raccolgo informazioni dai log (errori, traffico, accessi, ...)
- Identifico eventuali incidenti
- Classifico gli incidenti per gravità
- Mantengo un «diario» delle informazioni raccolte

Contenimento

Applico azioni immediate per limitare i danni.

Esempio

- Rallento le risposte a certi indirizzi
- Bloccare l'account utente compromesso
- Scollegare il server dalla rete
- Ban indirizzi IP attaccanti
- Risposte con dati falsi
- Scaling delle risorse
- Contatto le forze dell'ordine

Eradicazione

Procedure per rimuovere la causa principale dell'incidente.

Esempio

- Eliminare il malware
- Installare la patch di sicurezza mancante
- Rotazione delle chiavi di accesso
- Aggiungere regole specifiche al firewall

Ripristino (Recovery)

Passi per tornare alla normale operatività in sicurezza.

Esempio

- Ripristinare i dati dal backup
- Ripristinare le configurazioni delle applicazioni
- Monitorare i sistemi per verificare che l'attaccante sia stato eliminato

Lezioni Apprese (Post-Mortem)

Stabilisce l'obbligo di condurre un'analisi post-incidente per capire cosa ha funzionato, cosa no, e come migliorare.

Esempio

Struttura tipica di un Post-Mortem:

1. Comportamento atteso
2. Timeline
    1. Origine dell'errore
    2. Analisi degli effetti dell'attacco
    3. Tentativi eseguiti per limitare il danno e recuperare le operazioni
    4. Disaster recovery
3. Lezioni apprese e miglioramenti

Piano di comunicazione

Questa sezione è vitale per i manager e definisce chi avvisare, cosa dire e quando.

Comunicazione Interna Chi informare all'interno dell'azienda (CEO, capi dipartimento, HR) e con quale livello di dettaglio.

Esempio

1. Viene comunicato l'incidente risalendo l'organigramma
2. Poi viene contattato il personale addetto ai processi specializzati
3. Si propaga la notizia seguendo le policy aziendali

Piano di comunicazione

Comunicazione Esterna Quando e come informare clienti, partner, media e il pubblico. Include modelli di comunicazione pre-approvati.

Esempio

- Incidente database GitLab: https://about.gitlab.com/blog/postmortem-of-database-outage-of-january-31/
- Incidente DNS Cloudflare: https://blog.cloudflare.com/cloudflare-1-1-1-1-incident-on-july-14-2025/

Obblighi di Notifica Una lista chiara delle autorità da contattare in base al tipo di incidente e alla giurisdizione (Garante Privacy, Banca d'Italia, Polizia Postale, etc.).

Contact List 24/7 Una lista aggiornata con i contatti telefonici e email di tutto il personale chiave (interno ed esterno).

> Includere contatti di terze parti come l'assicurazione informatica, consulenti esterni, avvocati, forze dell'ordine

Checklist Operative Semplici checklist «passo-passo» per scenari specifici.

Esempio

- Checklist Attacco Ransomware
- Checklist Fuga di Dati

Inventario degli Asset Critici Una mappa dei sistemi e dei dati più importanti dell'azienda.

Un documento non aggiornato è controproducente

Un IRP non è un documento da lasciare a prendere polvere in un cassetto.

È uno strumento vivo, che deve essere costantemente aggiornato e testato, per trasformare un potenziale disastro in un problema gestibile.

Usare strumenti per la gestione degli asset e l'automazione semplifica le operazioni in caso di incidente.

Il Fattore Umano

Le persone sono spesso considerate l'anello più debole della catena della sicurezza, ma con la giusta preparazione possono diventare la prima e più efficace linea di difesa.

Formazione e Consapevolezza (Security Awareness)

Far capire l'importanza della sicurezza all'interno dell'ambito operativo

Esempio

- Riconoscere email di phishing (tentativi di frode)
- Creare e gestire password sicure
- Navigare in sicurezza sul web e non scaricare software sospetto
- Identificare persone o comportamenti sospetti
- Comprendere i pattern tipici degli attacchi

La formazione deve avere un feedback-loop positivo, o non verrà recepita

Esempio

Gamification adottare meccaniche di gioco per spingere alla formazione

Riscontro economico costa meno un bonus al personale rispetto ad un attacco ben riuscito

Il Dilemma del Manager

Le decisioni non sono solo tecniche, ma di business.

> «Dobbiamo spegnere il nostro e-commerce per contenere l'attacco, anche se perdiamo migliaia di euro di vendite ogni ora?»

Questa è una domanda difficile che richiede una valutazione tra rischio e impatto economico.

I processi Aziendali

I processi sono le regole e le procedure che l'organizzazione segue per operare in modo sicuro e coerente.

Policy di Sicurezza

Documenti che stabiliscono cosa si può e non si può fare.

Esempio

- Policy sull'uso accettabile di Internet
- Policy per il lavoro da remoto

Gestione delle Vulnerabilità (Vulnerability Management)

Un processo costante per:

- Identificare le «crepe» nei sistemi (software da aggiornare).
- Valutare la loro gravità.
- Rimediare installando gli aggiornamenti (patch) prima che un aggressore le sfrutti.

Principio del Minimo Privilegio (Least Privilege)

Dare a ogni utente e sistema solo le autorizzazioni strettamente necessarie per svolgere il proprio lavoro.

Esempio

Non si danno le chiavi dell'intero edificio a ogni dipendente, ma solo quelle del suo ufficio.

La Tecnologia (Gli Strumenti di Difesa)

La tecnologia fornisce gli scudi e le armi per difendere il perimetro digitale.

Firewall Controlla il traffico di rete in entrata e in uscita, bloccando le connessioni sospette o non autorizzate.

Esempio

- Bloccare tutto il traffico che non è strettamente necessario
- Individua tentativi di accesso malevoli

Antivirus / Antimalware analizza i file per trovare e bloccare codice maligno.

Esempio

- Identifica comportamenti anomali di utenti e sistemi
- Limita l'estensione dei danni
- Fornisce informazioni sull'origine dell'attacco

La Tecnologia (Gli Strumenti di Difesa)

Intrusion Detection System monitora il comportamento dei computer connessi alla rete interna, identificando comportamenti anomali.

Sistemi di Backup avere copie sicure e aggiornate dei dati è una misura preventiva contro il danno permanente di un attacco ransomware o di un guasto.

Esempio

- Backup giornalieri
- Regola del 3-2-1
- Test di ripristino

Crittografia rende i dati illeggibili a chiunque non possieda la chiave corretta, proteggendoli anche in caso di furto del dispositivo.

Secrets leak checker controlla automaticamente che non vengano rilasciati accidentalmente secret.

Esercitazioni e Simulazioni (Drills)

Le esercitazioni e le simulazioni sono test controllati e sicuri che mettono alla prova il piano, le persone e le tecnologie per vedere come si comporterebbero durante un vero attacco.

Perché Sono Assolutamente Indispensabili?

Scoprire i Buchi nel Piano È il motivo principale. Durante una simulazione, ci si accorge subito di cosa manca o cosa non funziona.

Esempio

- Il numero di telefono del nostro consulente legale è sbagliato.
- La procedura per isolare un server non è chiara e nessuno sa come applicarla.
- Ci vogliono due ore per avere l'approvazione del management, un tempo inaccettabile.

Allenare il Team (e Creare Memoria Muscolare) In una crisi, le persone non hanno il tempo di pensare: reagiscono d'istinto. Le esercitazioni allenano il team a seguire le procedure in modo quasi automatico, riducendo il panico e gli errori.

Perché Sono Assolutamente Indispensabili?

Testare la Tecnologia Si scopre se gli strumenti di sicurezza funzionano come previsto.

> «Pensavamo che il nostro sistema di backup fosse funzionante, ma durante il test abbiamo scoperto che il ripristino fallisce.»

Migliorare la Comunicazione e il Coordinamento Le simulazioni forzano i diversi reparti (IT, Legale, Comunicazione, Management) a collaborare, mettendo in luce problemi di comunicazione e di catena di comando.

Aumentare la Fiducia Un team che si è esercitato è un team più sicuro di sé e più preparato ad affrontare una vera crisi con calma e professionalità.

Esercitazione «Gioco da Tavolo» («Tabletop»)

Il team di risposta si riunisce attorno a un tavolo (fisico o virtuale) e un moderatore presenta uno scenario di incidente.

Esempio

Avete appena ricevuto una richiesta di riscatto da un gruppo ransomware. Cosa fate?

Come funziona Il team discute a parole i passaggi che seguirebbe, consultando il piano di risposta. Non si toccano i sistemi reali.

Obiettivo Verificare la logica del piano, i ruoli e i processi decisionali. È un esercizio a basso costo e a basso impatto, perfetto per identificare le lacune strategiche.

Tipi di Simulazione

Simulazione Funzionale («Walkthrough»)

I membri del team eseguono realmente alcune delle azioni previste, ma in un ambiente di test isolato.

Come funziona Un analista potrebbe provare a isolare un finto server infetto, oppure il responsabile della comunicazione potrebbe scrivere una bozza di comunicato stampa basata sullo scenario.

Obiettivo Testare non solo la logica del piano, ma anche la capacità pratica del team di eseguire compiti specifici.

Tipi di Simulazione

Simulazione Completa («Full-Scale Simulation»)

È la simulazione più realistica e complessa, una vera e propria «prova generale». Simula un attacco reale nel modo più fedele possibile, spesso senza preavviso per la maggior parte dei partecipanti.

Red Team (gli «Attaccanti») Un team di esperti (interni o esterni) che tenta attivamente di violare le difese dell'azienda, usando le stesse tecniche degli hacker.

Blue Team (i «Difensori») Il team di sicurezza interno dell'azienda, che deve rilevare l'attacco e rispondere in tempo reale.

Obiettivo Testare l'intera catena di difesa (persone, processi e tecnologie) sotto pressione reale. È l'esercizio più costoso e impegnativo, ma quello che fornisce i risultati più preziosi.

Altri Aspetti di Preparazione

Gestione degli Asset e dei Dati È il processo di mappare, classificare e dare una priorità a tutti gli asset aziendali (dati, software, sistemi). Significa rispondere alla domanda: «Cosa dobbiamo proteggere prima di tutto?».

Gestione della Sicurezza della Catena di Fornitura È il processo di valutare e gestire i rischi di sicurezza che provengono da terze parti (fornitori di software, consulenti, servizi cloud, etc.) che hanno accesso ai tuoi dati o sistemi.

Contratti e Accordi con Terze Parti Avere accordi e contratti pre-negoziati (spesso chiamati «retainer») con esperti esterni che possono essere chiamati in causa immediatamente. Garantisce l'accesso immediato a competenze specialistiche che l'azienda potrebbe non avere internamente.

Assicurazione Cyber Una polizza assicurativa specificamente pensata per coprire le perdite finanziarie derivanti da un incidente informatico. Trasferisce una parte del rischio finanziario a una compagnia di assicurazione.

Fine seconda parte

Domande?

Passiamo a degli esempi pratici

Scenario 1: Portale Prenotazioni Ospedale

Scenario 1: Portale Prenotazioni Ospedale

Consideriamo lo scenario di un CUP online di un ospedale.

Preparazione

Asset critici: servizi, dati, server

Threat landscape: ransomware, data breaches, supply chain attacks, DDoS attacks, insider threats

Analisi dell'impatto: temporaneo disservizio, danni economici, perdita reputazione, ripercussioni legali

Policy e Procedure:

- Backup giornalieri
- Isolamento dei server
- Accesso solo a personale fidato
- Verifica vulnerabilità dei sistemi
- IDS e logging

Attacco

Logging del traffico:

- I nostri servizi ricevono moltissime richieste
- Non è un problema di configurazione interno
- Il traffico arriva da indirizzi diversi

Identificazione: Attacco DDoS al portale prenotazioni

Parte la comunicazione interna

Livello di rischio: Medio

Contenimento

- Verifichiamo la sorgente delle richieste: Logging
- Blocchiamo gli IP che ci stanno contattando: Firewall
- Aumentiamo le risorse del sistema: Scaling verticale

Eradicazione

- Verifichiamo che le nuove regole del firewall abbiamo bloccato l'attaccante

Recupero

Il traffico al portale si riduce, l'attacco è finito

- Downscaling delle risorse, non più necessarie
- Verifica di aggiornamenti e patch di sicurezza

Attività successive

- Forensic: indagini sull'origine dell'incidente
- Revisione IRP: è stato efficace? Cosa poteva essere gestito meglio?
- Documentazione: cosa è stato fatto per rispondere all'emergenza?
- Comunicazione esterna

Scenario 2: Banca

Scenario 2: Banca

Consideriamo lo scenario di una banca.

Preparazione

Asset critici: servizi, dati, server

Threat landscape: ransomware, phising, data breaches, supply chain attacks, DDoS attacks, online fraud, insider threats

Analisi dell'impatto: temporaneo disservizio, danni economici, perdita reputazione, ripercussioni legali

Policy e Procedure:

- Backup giornalieri
- Fallback site (HA)
- Isolamento rete server
- Verifica vulnerabilità dei sistemi
- IDS e logging
- Least privilege principle
- Accesso fisico limitato

Attacco

I servizi stanno fallendo:

- I log ci mostrano molti errori nelle operazioni
- Gli errori sono legati ai dati nel database
- Accedendo ai server, i dati non sono più leggibili

Identificazione: Attacco ransomware all'infrastruttura

Parte la comunicazione interna

Livello di rischio: Alto

Contenimento

- Spegnimento di tutti i server: fermiamo il ransomware
- Isolamento della rete: evitiamo che si diffonda

Eradicazione

- Verifichiamo la sorgente dell'attacco
- Eliminiamo il codice malevolo

Recupero

- Verifichiamo di aver fermato l'attacco sul sistema pulito
- Recupero dei dati da backup
- Rafforzamento delle policy di sicurezza

Attività successive

- Conformità legale: riportare l'accaduto alle autorità seguendo il framework legislativo
- Forensic: indagini sull'origine dell'incidente
- Revisione IRP: è stato efficace? Cosa poteva essere gestito meglio?
- Documentazione: cosa è stato fatto per rispondere all'emergenza?
- Comunicazione esterna: comunicare agli stakeholder l'accaduto

Il Giorno Dopo

Attività Successive all'Incidente (Post-Incident Activity)

La gestione di un incidente non finisce quando l'attacco è terminato.

Un incidente è un'opportunità di miglioramento costosissima.

È important trasformarlo in un'opportunità di miglioramento misurabile

L'Analisi Post-Mortem

La «Lezione Appresa» (Lessons Learned) un'attività estremamente importante.

Analizzare l'incidente in dettaglio per ricavarne spunti di miglioramento.

Blameless (Senza colpevoli)

Non cerchiamo chi ha sbagliato, ma perché il sistema (umano, procedurale e tecnologico) ha permesso che l'errore succedesse.

Cosa è successo? Si ricostruisce una cronologia precisa degli eventi.

Qual è stato l'impatto reale? Si quantificano i danni (finanziari, operativi, reputazionali).

Cosa ha funzionato bene? Si identificano i punti di forza della risposta (es. «Il team ha comunicato in modo efficace», «Il backup ha funzionato perfettamente»).

Cosa non ha funzionato? Si analizzano onestamente le debolezze (es. «Ci abbiamo messo troppo tempo a rilevare l'attacco», «Il piano di comunicazione non era chiaro»).

Come possiamo migliorare? Questa è la domanda finale, che porta all'azione.

Piano di azione

Il risultato non è un semplice report da archiviare. È un piano d'azione concreto con azioni specifiche, scadenze precise e responsabili assegnati.

Esempio

Entro 30 giorni, il reparto IT dovrà implementare l'autenticazione a due fattori su tutti i sistemi critici

Gestione delle Conseguenze

L'incidente lascia una scia di conseguenze che vanno gestite attivamente.

Comunicazione Continua Non basta un solo comunicato stampa. Bisogna continuare a informare gli stakeholder (clienti, partner, dipendenti) sui progressi, per ricostruire la fiducia. La trasparenza (controllata) è fondamentale.

Supporto Legale e di Conformità Inizia il dialogo con le autorità (es. Garante Privacy), si gestiscono eventuali richieste di risarcimento o azioni legali. È un processo che può durare mesi.

Valutazione dell'Impatto Finanziario Si fa la conta dei danni.

- **Costi Diretti** Fatture dei consulenti, straordinari del personale, acquisto di nuovo hardware/software, eventuali multe.
- **Costi Indiretti (spesso più alti)** Perdita di clienti, danno al marchio, calo di produttività, tempo del management distolto dalle normali attività.

Rafforzare le Difese

Un incidente fornisce la spinta (e la giustificazione di budget) per fare cambiamenti che prima venivano rimandati.

Aggiornamento del Piano di Risposta (IRP)

Il piano viene modificato sulla base di ciò che non ha funzionato.

Implementazione delle Azioni Correttive

Il piano d'azione del post-mortem viene eseguito. Questo può includere:

- Miglioramenti Tecnologici: Acquistare un nuovo firewall, implementare un sistema di monitoraggio più avanzato (SIEM).
- Miglioramenti dei Processi: Semplificare la catena di approvazione, migliorare le procedure di backup.
- Miglioramenti delle Competenze: Organizzare nuova formazione per i dipendenti sulle aree risultate più deboli (es. phishing).

Condivisione della Conoscenza

Le lezioni apprese non devono rimanere confinate al team di sicurezza. Devono essere condivise con tutta l'organizzazione per aumentare la cultura della sicurezza a tutti i livelli.

Per il Futuro

Tracciabilitià e Log (Traceability)

È la «scatola nera» dell'organizzazione:

- Come sono entrati? (Il punto di origine)
- Cosa hanno fatto una volta dentro? (Il movimento laterale)
- Quali dati hanno visto, rubato o modificato? (L'impatto sui dati)
- Quando è successo esattamente? (La cronologia)

Senza la capacità di tracciare le attività in tempo reale, non si può mai essere sicuri di aver espulso completamente l'intruso.

Tracciabilitià e Log (Traceability)

Quali Log Raccogliere? Non si può registrare tutto, il volume sarebbe ingestibile. Bisogna decidere quali eventi sono importanti per la sicurezza.

Centralizzazione (SIEM) I log sono generati da migliaia di dispositivi diversi. Lasciarli su ogni singolo dispositivo è inutile. Devono essere raccolti, aggregati e correlati in un unico sistema centrale, chiamato SIEM (Security Information and Event Management). Un SIEM è un «motore di ricerca» per i log che può identificare schemi sospetti.

Periodo di Conservazione (Retention) Per quanto tempo bisogna conservare i log? Un giorno? Un mese? Un anno? La legge può imporre dei minimi (es. 6 mesi), ma conservare i log ha un costo di archiviazione.

Protezione dei Log La prima cosa che un hacker esperto fa dopo essere entrato è cancellare i log per coprire le proprie tracce. I sistemi di log devono essere protetti e resi «immutabili».

Controlli continui

Verifica (Assessment)

Processo fondamentale durante tutta la vita dell'organizzazione.

Controlla che le **policy interne** (aziendali) ed **esterne** (legislative) vengano rispettate.

- Fornisce prove oggettive sullo stato dell'azienda
- Identifica pericoli e valuta rischi
- Automatizzabile con strumenti informatici
- Considera lo human-in-the-loop per il miglioramento

Verifica Continua (Continous Assessment)

Esegue il processo di verifica ad intervalli prefissati, costruendo uno storico.

- Aiuta a capire come evolve la situazione
- Fornisce maggiore fiducia nella qualità

Controlli continui

L'approccio della «fotografia annuale» non funziona più per tre motivi principali:

Ambienti IT Dinamici Le aziende cambiano ogni giorno. Nuovi dipendenti arrivano, nuovi software vengono installati, nuovi servizi cloud vengono attivati. Una valutazione fatta a gennaio è già obsoleta a febbraio.

Minacce in Continua Evoluzione Gli hacker non aspettano il vostro audit annuale. Sviluppano nuove tecniche di attacco ogni giorno.

Velocità degli Attacchi Un attacco può avvenire e concludersi in pochi minuti o ore. Una verifica annuale è troppo lenta per essere utile.

Controlli continui

Che cosa si verifica continuamente?

- Verifica delle Vulnerabilità
- Verifica delle Configurazioni
- Verifica di Identità e Accessi
- Verifica del Comportamento (Anomaly Detection)
- Verifica della Conformità (Compliance)

Certificazione

La certificazione è una verifica esterna da parte di un ente fidato (Certification Authority).

Garantisce qualità ai propri utenti con oggettività e aderenza agli standard.

In alcuni ambiti è legalmente richiesta per operare.

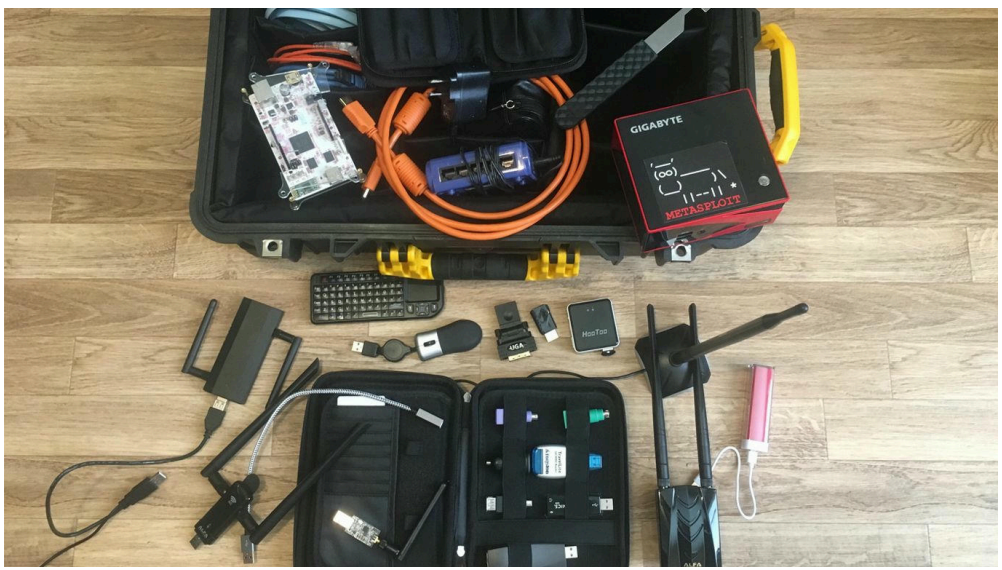
Attacchi fisici

Un'organizzazione non è solamente software.

È anche persone, edifici, hardware.

Ci sono molti modi per superare la sicurezza:

- Social engineering
- Malware su USB (USB Drop Attack)
- Bypass di porte e serrature
- Dump di storage e memoria
- Keylogger
- Wiretapping



Domande?