Che cos’è l’Incident Response (IR) e l’Incident Response Plan (IRP)



Che cos’è Incident Response (IR) secondo il Framework NIST

Il compito dell’**Incident Response Framework** è quello di fornire uno strumento efficace al management (incident response teams (CSIRTs), system and network administrators, chief information security officers (CISOs), chief information officers (CIOs), security staff etc..) alla gestione e mitigazione dell’incidente di sicurezza informatico, capace di garantire la continuità operativa e che sia mezzo di difesa oltre che strumento utile alle fasi investigative.

Le linee guida per avere una capability di IR vengono dettagliate dal **National Institute of Standards and Technology (NIST)** attraverso l’Incident Response Framework.

Il NIST è un’agenzia governativa americana che definisce degli standard tecnologici, considerata oggi il più grande fornitore internazionale di materiali utili a prevenire e scongiurare attacchi terroristici, criminali, nonché accessi non autorizzati ai sistemi informatici.

Cos’è l’Incident Response Plan (IRP)?

L’Incident Response Plan è un processo strutturato e ripetibile utile alle organizzazioni a prevedere, prioritizzare e rispondere in maniera tempestiva ed efficace agli incidenti di cybersecurity grazie alla predisposizione di standard, policy, procedure e team adeguati.

L’Incident Response è la capacità operativa dell’Incident Management di minimizzare l’impatto delle violazioni e ripristinare nel più breve tempo possibile le regolari operazioni.

L’IRP prevede diverse fasi che permettono di prevenire o ridurre i danni causati da un incidente di sicurezza informatica grazie ad una anticipata e programmata verifica della capacità dell’organizzazione a rispondere a problemi di sicurezza stabilendo la messa in atto di tool e know-how necessari a prevenire la violazione.

Si tratta quindi di una attività preventiva che si basa sulla valutazione del rischio per rilevare e minimizzare gli incidenti di sicurezza grazie alla mitigazione dei punti deboli del Information Technology (IT) divenuta ormai sempre più soggetta a cyber attacchi che frequentemente compromettono dati personali e business.

Per fare ciò bisogna identificare ed analizzare costantemente le cyber minacce e poiché esse si evolvono e si trasformano costantemente, condividere le informazioni tra le diverse organizzazioni è il modo più efficace e rapido per farlo.

Al fine di garantire un efficace modello di interazione e cooperazione tra tutti gli attori coinvolti nel processo di gestione dell’incidente, è auspicabile che all’interno dell’organizzazione sia identificato un responsabile della Sicurezza Informatica, che possa sovraintendere i processi di gestione della sicurezza costituendo così il punto di contatto con il **Computer Emergency Response Team (CERT)** a cui sono affidate funzioni di responsabilità del monitoraggio degli incidenti a livello nazionale.

Tre modelli di Incident Response Team offerti dal NIST:

1. **Central Incident Response Team**: un singolo team gestisce

tutti gli incidenti. Modello applicabile alle piccole imprese con poca, o nessuna infrastruttura e risorsa IT.
2. **Distributed Incident Response Teams**: molteplici team gestiscono gli incidenti, ognuno responsabile per gli incidenti di uno specifico segmento fisico o logico. Modello efficace per le grandi organizzazioni e per quelle che gestiscono risorse dislocate sul territorio. Tali teams dovrebbero comunque far parte di un'unica entità coordinata in modo che il processo di risposta agli incidenti sia coeso e le informazioni siano condivise all'interno dell'organizzazione.
3. **Coordinating Team**: un team di risposta agli incidenti che fornisce consulenza alle altre squadre senza avere autorità su di loro, ad esempio una squadra del dipartimento può assistere quelle delle singole agenzie. Modello pensato come un **Computer Security Incident Response Team (CSIRT)** o per CSIRTs.

A loro volta i membri che compongono il team, in riferimento all'azienda che usufruisce del servizio, possono essere lavoratori impiegati della ditta, oppure il servizio di IR può essere gestito in parte dal team interno all'organizzazione mentre il restante risultare a carico di una azienda esterna. Esiste poi un terzo modo che prevede la gestione del processo esclusivamente a carico di un'azienda esterna.

Fasi dell'Incident Response

1. Preparation (Preparazione):

E' un processo che coinvolge persone, sistemi, network e applicazioni.

Devono essere individuati e catalogati tutti gli asset sensibili così come le varie possibili minacce, va predisposta quindi una strategia dove si definiscono le priorità sulla base dell'impatto che gli eventi potrebbero avere sull'organizzazione. Affinché non si verifichi e per ridurre

gli eventuali danni, va messa in sicurezza tutta l'infrastruttura IT, realizzando Risk Assessment periodici, policy adeguate, patching continuo, messa in sicurezza del network, vanno quindi applicati tutti gli standard in materia.

Bisogna inoltre rendere disponibili e facilmente utilizzabili tutte le risorse utili alla gestione della crisi: software di crittografia e analisi, così come hardware utili alla mitigazione dell'incidente e al ripristino, documentazione facilmente consultabile degli incidenti, piano di comunicazione tra attori interni ed esterni, accesso facile ad un elenco dei contatti utili, software forense, storage sicuri.

2. Detection & Analysis (Rilevamento e Analisi):

Utili ad effettuare il rilevamento di un incidente sono i precursori, segnali che un incidente potrebbe verificarsi in futuro e gli indicatori, segnali che un incidente potrebbe essersi verificato o potrebbe essere in atto.

I precursori possono essere utilizzati per evitare che si verifichino incidenti, ma è molto raro che questi si verifichino, nella maggior parte dei casi si vedono prima gli indicatori. Questi producono solitamente migliaia di alerts al giorno e molti di questi possono essere dei falsi positivi, è per questo fondamentale realizzare una corretta analisi utile a determinare il verificarsi di un incidente.

Poiché le informazioni possono essere ambigue, incomplete o contraddittorie i tempi di analisi possono essere lunghi ed è necessario avvalersi di una squadra di esperti che si occupi delle SOP (Standard Operating Procedure), così come di strumenti tecnici quali sistemi IDS/IPS, sniffer di pacchetti, analizzatori di log, software di verifica dell'hash crittografico, software di automazione della sicurezza (es. SIEM).

La fase di Rilevamento e Analisi si struttura in:

- osservare i segnali di un incidente, chiamati precursori e indicatori;
- analizzare i segnali;
- documentare l’incidente;
- prioritizzare gli incidenti;
- notificare l’incidente.

3. Containment, Eradication & Recovery (Contenimento, Sradicamento e Ripristino):

- **Contenimento**: rientrato in questa fase tutte quelle azioni atte ad impedire che l’incidente o l’evento si diffonda all’interno del sistema e del network. Lo scopo principale di questa fase è limitare e prevenire ulteriori danni. Esempi di alcuni passaggi utili sono: isolare il segmento di rete compromesso o le workstation infette, backup del sistema, acquisizione di un’immagine forense, rimuovere gli account e/o le backdoor utilizzati dagli hacker, installare patch di sicurezza, e svolgere tutte quella attività necessarie a limitare l’ulteriore escalation dell’incidente.
- **Sradicamento:** le azioni intraprese per l’eliminazione completa della minaccia dalla rete o dal sistema. Vanno inoltre mitigate tutte le vulnerabilità che hanno consentito o potrebbero consentire una nuova intrusione da parte dell’attaccante.
  Le tecniche di eradicazione potrebbero avere un forte impatto sul business perciò qualsiasi decisione dovrà essere intrapresa dopo una attenta e dettagliata analisi.
  E’ utile in questa fase l’utilizzo delle immagini disco originali per il ripristino del sistema, l’installazione di patch, la scansione dei sistemi e/o dei file interessati con un software anti-malware, la disconnessione per isolare i sistemi compromessi da quelli che non sono stati compromessi evitando così che il resto della rete venga compromessa.

- **Ripristino:** le azioni necessarie a ripristinare la rete o il sistema, portandolo così alla sua normalità. Questo può avvenire solamente se i sistemi sono stati patchati e testati, quindi solo a seguito della verifica che il sistema possa essere ripristinato in sicurezza utilizzando un backup, va inoltre stabilito per quanto tempo questo dovrà essere monitorato affinché si ottenga una convalida del fatto che il piano di ripresa è stato eseguito con successo e che non esistono segni di violazione nell'ambiente.

4. Post-Incident Activity (Attività post incidente):

La fase dell'attività post incidente, spesso indicata come post mortem è utile al miglioramento della postura dell'organizzazione in ambito sicurezza. Le lezioni apprese durante tutte le fasi precedenti vengono applicate per migliorare la preparazione alla gestione di incidenti futuri, grazie all'identificazione degli errori tecnici, procedurali, manuali, difetti di processo, problemi di comunicazione e/o qualsiasi vettore di attacco precedentemente sconosciuto. E' importante a questo scopo creare un documento degli eventi che hanno causato l'incidente che includa prove, attori coinvolti, step di risposta e altri elementi chiave.

Alcune tipologie di incidenti di sicurezza e vettori di attacco

- **Supporti esterni o rimovibili**: cyber attacco eseguito attraverso supporti rimovibili (es. memory card, CD) o unità periferica;
- **Attacco di forza bruta**: cyber attacchi utilizzati per compromettere, degradare o distruggere sistemi, reti o servizi (es. attacco DDoS (Distributed Denial of Service)
- **Web**: cyber attacco eseguito da un sito web o da un'applicazione web-based.
- **E-mail**: cyber attacco eseguito tramite un messaggio e-

mail o un allegato. Il destinatario è invitato dall'hacker a cliccare su un collegamento che reindirizza alla pagina Web infetta o ad aprire un allegato infetto.

- **Uso improprio della tecnologia**: qualsiasi incidente risultante dalla violazione delle policy dell'organizzazione da parte dell'utente;
- **Perdita o furto di apparecchiature**: perdita o il furto di un dispositivo informatico o di un supporto utilizzato o fornito dall'organizzazione, ad es. un laptop o uno smartphone.
- **Uso improprio**: quando l'incidente si verifica a seguito della violazione delle policy, ad esempio quando l'utente installa un software che porta alla perdita di dati sensibili.
- **Falsificazione dell'identità o delle informazioni**: cyber attacco in cui un avversario assume con successo l'identità di una delle parti legittime in un sistema o in un protocollo di comunicazione, ad esempio, spoofing e man in the middle.
- Drive-by download: cyber attacco che avviene all'insaputa dell'utente che attiva il download di un malware aprendo un sito web.
- **Malvertising**: pubblicità online dannose che possono causare infezioni malware oppure tracciare l'attività degli utenti.
- **Hovering of Mouse**: il malware può infettare il dispositivo quando la vittima passa semplicemente il mouse su un collegamento dannoso.
- **Scareware**: attacco malware che afferma di aver rilevato un virus o un altro problema su un dispositivo e indirizza l'utente a scaricare o acquistare software dannoso per risolvere il problema.
- **Altro**: qualsiasi attacco che non rientra in nessuna delle altre categorie sopra descritte

Articolo a cura della Redazione

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/che-cose-lincident-response-ir-e-lincident-response-plan-irp/