Incident Response Policy and Procedures

Questo documento definisce la politica e le procedure da seguire in caso di incidenti di sicurezza informatica, al fine di garantire una risposta rapida, efficace e coordinata per mitigare i rischi associati a violazioni della sicurezza, attacchi informatici o altri eventi imprevisti che possano compromettere la protezione dei dati aziendali di G3 s.p.a e dei partner commerciali che si affidano a G3. La politica stabilisce le responsabilità, le azioni da intraprendere e le risorse necessarie per identificare, contenere, risolvere e prevenire incidenti futuri, assicurando al contempo la conformità alle normative di settore e la protezione dell'integrità aziendale.



Documento per uso interno – Utilizzo consentito solo a personale autorizzato. Divulgazione non permessa senza approvazione

Gestione degli incidenti di sicurezza:

- Gli incidenti di sicurezza devono essere segnalati immediatamente al CISO e gestiti tempestivamente secondo le procedure aziendali stabilite all'interno di questo documento e dei documenti complementari allegati all'interno del SGSI (Sistema di Gestione della Sicurezza delle Informazioni);
    1. Handle an Incident
    2. (BCP) - G3 Piano di Continuità Operativa
    3. G3 Disaster Recovery (DR)
    4. Risk Management G3
- Il Team di sicurezza informatica coordinerà la risposta agli incidenti, che include l'analisi dell'incidente, la mitigazione del danno, e la comunicazione con i soggetti interessati (dipendenti, fornitori, clienti, autorità competenti, se necessario).

Ogni incidente di sicurezza deve essere registrato in modo dettagliato, con informazioni sui fatti, le azioni intraprese e le lezioni apprese. Questo aiuta a migliorare le politiche e i processi di sicurezza per prevenire futuri incidenti.

- Vedi: Segnalazione di un incidente - Politica di sicurezza aziendale

Se l'incidente è in corso o è appena stato riscontrato segui le seguenti istruzioni;

Contatta immediatamente:

- Team di Incident Response utilizza i seguenti contatti:
    - E-mail: incident@generaltechcenter.com
    - Telefono fisso: + [0039] 095 3787462
    - Cellulare: 350 059 0978
- Canali aziendali dedicati:
    - Linea telefonica di emergenza:
        - [+0039] 348- 529-4608
    - Indirizzo email dedicato:
        - stefano.gualtieri@g3spa.it
- Partner commerciali:
    - CIRT@Ford.com

Prendi visione del documento di segnalazione di un incidente e invialo compilato.

Recupero dei Dati e Continuità Operativa

In caso di perdita totale dei dati, G3 S.p.a. ha implementato un sistema di backup regolare che consente di ripristinare tutte le informazioni aziendali in modo rapido ed efficiente. I dati vengono archiviati in backup sicuri, e in caso di necessità, il processo di recupero può essere completato entro un periodo massimo di due giorni, garantendo così una rapida ripresa delle attività aziendali. Questo sistema assicura la continuità operativa e la protezione delle risorse aziendali, minimizzando i tempi di inattività. Questa ed altre procedure di recupero dei dati e di tutela della continuità operativa sono contenuti all'interno della Politica di Sicurezza aziendale, all'interno del documento (BCP) Piano di Continuità Operativa.

Gli incidenti devono essere gestiti in conformità con le procedure documentate.
In caso di incidente in corso consultare il Documento Handle an Incident

Raccolta delle prove

L'organizzazione ha stabilito ed implementato procedure per raccogliere prove sugli eventi di sicurezza.
Vedi documento: Segnalazione di un incidente

Gestione degli Incidenti di Sicurezza (Incident Response)

È fondamentale che tutti gli incidenti siano registrati in modo accurato e dettagliato, mantenendo la tracciabilità di ogni fase dell'incidente, dal rilevamento alla risoluzione. Il piano di risposta prevede anche la comunicazione interna ed esterna, inclusa la notifica alle autorità competenti.

Piano per la Raccolta delle Prove

Un'efficace risposta agli incidenti è fondamentale per mitigare i danni, preservare la continuità operativa e proteggere i dati sensibili. La raccolta delle prove, elemento cruciale di questo processo, segue un approccio ben strutturato e documentato, che permette di analizzare l'incidente in modo completo e trarre insegnamenti per prevenire eventi futuri. Di seguito sono delineate le fasi chiave per la raccolta delle prove in caso di incidente.

Prevenzione e Preparazione

- **Politiche e procedure di gestione degli incidenti**: E' formalizzata una politica documentata che descriva in dettaglio come affrontare gli incidenti di sicurezza. Questa politica copre tutte le fasi della gestione dell'incidente: dalla segnalazione, alla risposta, fino al recupero.
- **Formazione e consapevolezza**: Tutto il personale deve essere formato periodicamente sulle procedure da seguire in caso di incidente.

Raccolta delle Prove dell'Incidente

- **Identificazione dell'incidente**: Allo scoppio di un incidente, è cruciale identificare tempestivamente la natura e la gravità dell'incidente. I primi dati da raccogliere comprendono la data e l'ora dell'incidente, la tipologia (ad esempio, attacco informatico, perdita di dati, errore umano), e i sistemi coinvolti. La documentazione iniziale deve includere anche informazioni sul personale che ha segnalato l'incidente e le azioni intraprese immediatamente dopo la rilevazione.
    - Vedi documento: Segnalazione di un incidente
- **Log di sistema e registri delle comunicazioni**: I log di sistema (server, applicazioni, firewall, sistemi di monitoraggio) sono una fonte primaria di dati per la ricostruzione dell'incidente. I log sono raccolti e archiviati in modo sicuro, in modo da evitare alterazioni. L'accesso a questi log deve essere limitato e monitorato per evitare la perdita di prove. La documentazione di tutte le comunicazioni interne (e-mail, messaggi istantanei, verbali di riunioni) durante l'incidente è altrettanto cruciale per avere una visione completa degli eventi.

Analisi e Documentazione dell'Incidente

- **Analisi forense**: Se l'incidente è significativo, l'analisi forense deve essere condotta da professionisti qualificati, che utilizzano strumenti specifici per recuperare e preservare le prove digitali. L'analisi forense non si limita alla semplice raccolta di dati, ma implica anche la loro interpretazione, per determinare la causa radice dell'incidente, l'estensione dei danni e il possibile impatto su dati e sistemi. I risultati dell'analisi forense devono essere registrati in report dettagliati, che possono essere utilizzati per la successiva investigazione e come supporto per le azioni correttive.
- **Valutazione dell'impatto**: Oltre alla causa dell'incidente, è valutato l'impatto su operazioni, risorse, reputazione e dati sensibili. Devono essere raccolti dati relativi alla portata del danno, come la perdita di dati, l'interruzione dei servizi o il danneggiamento di infrastrutture critiche. Una documentazione accurata dell'impatto permette di classificare l'incidente secondo la sua gravità e di determinare le priorità nelle azioni correttive.
- **Documentazione delle lezioni apprese**: Un report finale sull'incidente deve essere redatto per raccogliere le conclusioni. Il report redatto deve sintetizzare le cause dell'incidente, le azioni adottate, le lezioni apprese e le raccomandazioni per migliorare la gestione della sicurezza. Le informazioni devono essere condivise con tutte le parti interessate per evitare che si ripetano situazioni simili in futuro.

Miglioramento Continuo

- **Revisione post-incidente**: Dopo ogni incidente, il piano di risposta deve essere revisionato in base all'esperienza accumulata. Un'analisi di ciò che ha funzionato e di ciò che non ha funzionato aiuterà a migliorare le procedure e a rafforzare i controlli esistenti. La raccolta di dati e feedback durante questa fase è fondamentale per ottimizzare il processo di gestione degli incidenti, includendo eventuali nuove minacce identificate o vulnerabilità non precedentemente considerate.

Sicurezza delle informazioni durante le interruzioni

La sicurezza delle informazioni durante le interruzioni è un aspetto cruciale per garantire la protezione dei dati e la continuità operativa, soprattutto in caso di eventi imprevisti come attacchi informatici, disastri naturali o malfunzionamenti hardware.

1. Piani di Continuità Operativa e Disaster Recovery

Leggi: BCP Business Continuity Plan - Politica di Sicurezza aziendale

Esso include:

- **Backup regolari** dei dati e delle informazioni sensibili.
- **Piani di disaster recovery** che dettagliano le procedure per il ripristino dei sistemi e delle applicazioni, garantendo che i dati possano essere recuperati e l'operatività ripresa in tempi rapidi.
- **Rilevamento e risposta agli incidenti**: un sistema di monitoraggio per individuare eventuali anomalie nei sistemi e intervenire tempestivamente per limitare i danni.

Riferimenti alle politiche di sicurezza aziendali:

- Disaster Recovery
- Handle an Incident
- Risk Management