[Nome della società]

Cybersecurity Incident Response Plan

[Sottotitolo del documento]

Cybersecurity Incident Response Plan

Controllo Documentale

Titolo	Cybersecurity Incident Response Plan
Tipo Documento	Policy
Contatto SimplyIT	E-mail: michele@simplyit.it Tel: +39 049 099 1394

Lista di Distribuzione

Società	Nome Cognome
[Società]	Michele Salvalaggio

Tabella delle Revisioni

Rev	Descrizione	Autori	Verificata	Approvata
[Oggetto]	Released	Michele Salvalaggio		

Sommario

Introduzione

Tutti gli incidenti di cybersecurity e/o le violazioni di dati personali devono essere gestiti in modo efficiente ed efficace, così da contenere l'impatto dell'evento e limitare le conseguenze per l'azienda e per i suoi stakeholder.
Lo scopo di questo documento è fornire indicazioni per la segnalazione e la gestione di qualsiasi incidente causato da un attacco informatico e/o di qualsiasi violazione di dati personali. Il contenuto si basa, tra le altre fonti, sulle buone pratiche del National Institute of Standards and Technology (NIST) del governo statunitense, sulla Direttiva (UE) 2022/2555 (Direttiva NIS 2) e sul Regolamento Generale sulla Protezione dei Dati (GDPR)

Scopo

Questo documento fornisce linee guida per la gestione degli incidenti di cybersecurity all'interno dell'azienda. Tuttavia, ogni evento sarà trattato adottando l'approccio più appropriato in base alle circostanze specifiche del caso.
In caso di violazione di dati personali, tali linee guida devono essere seguite per garantire la conformità ai requisiti legali applicabili. Lo scopo di questo documento è fornire all'azienda una linea guida completa da seguire durante gli incidenti di cybersecurity, indipendentemente dal fatto che incidano sulla continuità operativa, comportino una violazione di dati, abbiano natura criminale. Questo documento è conforme alla Policy di Cybersecurity aziendale ed è inteso a fornire una specificazione ulteriore dei requisiti in materia di sicurezza informatica definiti nel regolamento interno.

Riferimenti esterni e stakeholder

Questa Politica di Gestione degli Incidenti è stata redatta seguendo le linee guida della Direttiva europea NIS2 e degli standard correlati applicabili nei paesi in cui l'azienda opera. Per una corretta gestione degli incidenti di cybersecurity, l'azienda collabora con diversi attori esterni fondamentali. Di seguito è riportata una breve panoramica degli stakeholder chiave, come definiti dalla Direttiva NIS2, e delle loro responsabilità nella gestione degli incidenti:

- Autorità nazionale competente NIS:
  - Garantisce la cooperazione con altre autorità nazionali e stakeholder rilevanti.
  - Coordina lo scambio di informazioni su incidenti significativi e minacce informatiche.
  - Collabora con l'Autorità di Protezione dei Dati in caso di violazioni di dati personali.
- Punto di contatto unico NIS
  - Agisce come punto centrale di coordinamento per la comunicazione con l'UE e gli altri Stati membri riguardo agli incidenti di cybersecurity.

  - Trasmette a ENISA rapporti trimestrali anonimizzati e aggregati sugli incidenti significativi.
  - Facilita la tempestiva notifica degli incidenti transfrontalieri.
- Autorità di Protezione dei Dati
  - Collabora con l'Autorità nazionale competente NIS negli incidenti che coinvolgono violazioni di dati personali.
  - Garantisce il rispetto delle normative sulla protezione dei dati durante la gestione degli incidenti.
  - Funziona come principale punto di contatto per le autorità di controllo e per gli interessati in relazione alle violazioni di dati personali.
- CSIRT nazionale (Computer Security Incident Response Team)
  - Gestisce la risposta agli incidenti per i settori e le entità previsti dalle normative nazionali ed europee.
  - Monitora e analizza minacce, vulnerabilità e incidenti informatici.
  - Fornisce avvisi, bollettini e informazioni rilevanti a entità essenziali e importanti.
  - Collabora a livello nazionale e internazionale per rafforzare le capacità di risposta agli incidenti.

Per i paesi non appartenenti all'UE, esistono organismi equivalenti ai CSIRT nazionali.

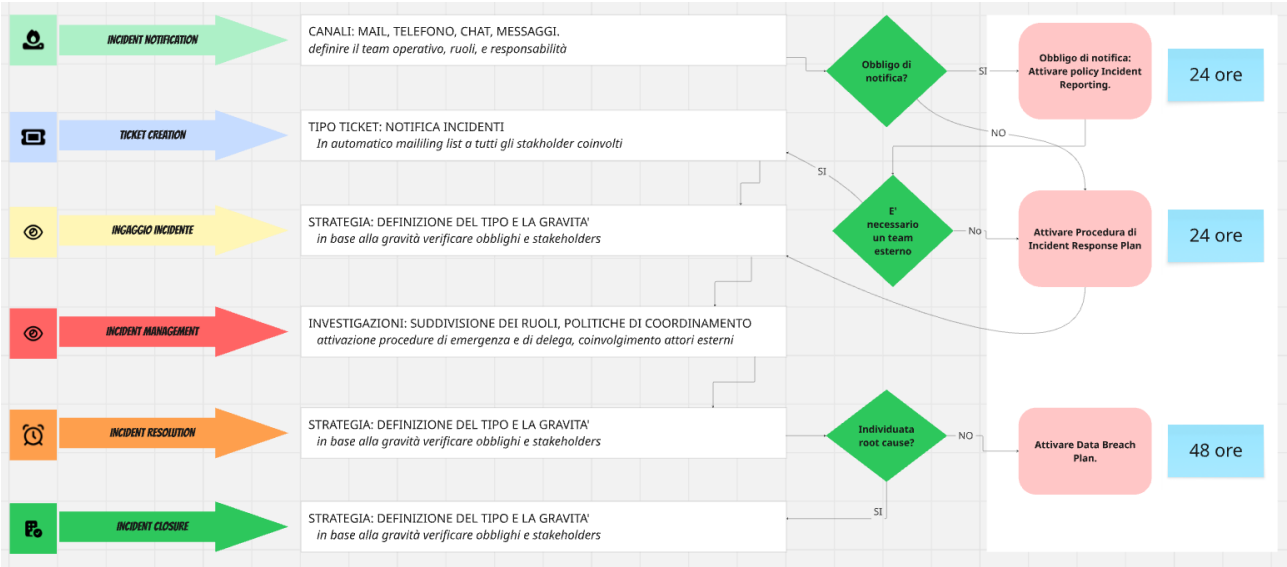
Gestione degli incidenti

Di seguito è riportato un riepilogo dei principali argomenti. Questo riepilogo è progettato per offrire una visione d'insieme e facilitare la lettura e la comprensione del documento completo:

- Notifiche esterne: Spiega come informare le autorità competenti in caso di incidenti significativi e/o violazioni di dati e i modelli di notifica. Descrive inoltre le modalità per segnalare potenziali incidenti informatici e/o violazioni di dati al gruppo responsabile;
- Gestione degli incidenti di cybersecurity: Illustra l'intero processo di gestione degli incidenti informatici secondo le migliori pratiche definite dal NIST. Segue le quattro fasi: Preparazione, Rilevazione e Analisi, Risposta (Contenimento, Eradicazione, Ripristino) e Attività post-incidente;

Workflow

Di seguito è riportato il flusso di lavoro che descrive tutte le fasi per la gestione degli incidenti informatici, incluse le violazioni di dati, gli incidenti significativi e quelli di natura criminale.



Metodi di segnalazione degli incidenti

Per definizione una violazione informatica è una violazione di sicurezza che comporta la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso non autorizzato a dati personali trasmessi, conservati o comunque trattati. Come previsto dall'Articolo 23 della Direttiva NIS2, gli organi amministrativi e di gestione delle entità essenziali e importanti devono essere informati periodicamente o, quando necessario, immediatamente sugli incidenti e sulle relative notifiche.

Reporting

La fase di reporting segue le modalità e i passaggi definiti nella Procedura ufficiale di "Incident Reporting".

Categorizzazione degli incidenti

Per migliorare la gestione degli incidenti e ottenere una visione più chiara delle diverse tipologie di incidenti informatici, l'azienda adotta la classificazione degli incidenti definita da ENISA, basata sulla tassonomia elaborata in conformità con ACN. La specifica completa è riportata nella tabella sottostante.

Categoria di incidente	**Esempi di incidente**	**Descrizione / Spiegazione**
Contenuti abusivi	Spam	Messaggi inviati senza che il destinatario abbia fornito un consenso verificabile, spediti come parte

Categoria di incidente	Esempi di incidente	Descrizione / Spiegazione
		di un insieme più ampio di comunicazioni con contenuti sostanzialmente simili.
	Linguaggio offensivo o dannoso	Contenuti che discreditano o discriminano qualcuno (ad esempio cyberstalking, razzismo, minacce contro uno o più individui).
	Contenuti relativi a minori, sessuali, violenti, ecc.	Materiali come pornografia minorile, contenuti che glorificano la violenza o simili.
Codice malevolo	Virus	Software inserito intenzionalmente in un sistema per scopi dannosi. In genere richiede un'interazione dell'utente per essere attivato.
	Worm, Trojan, Spyware, Dialer, Rootkit	Diverse tipologie di software malevolo progettate per infettare, spiare, compromettere o controllare un sistema.
Raccolta di informazioni	Scansione	Attacchi che inviano richieste a un sistema per individuare punti deboli. Includono attività di test per raccogliere informazioni su host, servizi e account (es. finger, interrogazioni DNS, ICMP, SMTP, scansioni di porte).
	Sniffing	Osservazione e registrazione del traffico di rete (intercettazione).
	Social engineering	Raccolta di informazioni attraverso interazioni non tecniche con persone (ad esempio menzogne, trucchi, corruzione o minacce).
Tentativi di intrusione	Sfruttamento di vulnerabilità note	Tentativi di compromettere un sistema o interrompere un servizio sfruttando vulnerabilità identificate con codici standardizzati (es. CVE), come buffer overflow, backdoor, cross-site scripting, ecc.

Categoria di incidente	**Esempi di incidente**	**Descrizione / Spiegazione**
	Tentativi di accesso	Molteplici tentativi di accesso (es. guessing o cracking delle password, attacchi brute force).
	Tentativo con exploit sconosciuto	Tentativo di compromesso usando una vulnerabilità non ancora conosciuta.
Nuova firma di attacco	Tentativo con exploit sconosciuto	Tentativo di compromesso usando una vulnerabilità non ancora conosciuta.
Intrusioni	Compromesso di account privilegiato	Compromesso riuscito di un sistema o applicazione (servizio). Può essere avvenuto da remoto tramite una vulnerabilità nota o nuova, oppure tramite accesso locale non autorizzato. Include anche la partecipazione a una botnet.
	Compromesso di account non privilegiato	Accesso non autorizzato a un account standard.
	Compromesso di applicazione	Accesso non autorizzato o manipolazione di un'applicazione.
Bot	-	Inclusione di sistemi in botnet.
Disponibilità	DoS	Un sistema è bombardato con pacchetti fino a rallentare le operazioni o causare crash. Esempi: ICMP e SYN floods, Teardrop attacks, mail-bombing.
	DDoS	Attacchi DoS provenienti da botnet o altre sorgenti, es. DNS amplification.
	Sabotaggio / Interruzione (senza malizia)	Disponibilità compromessa da azioni locali (distruzione, interruzione di alimentazione) o da cause naturali, guasti spontanei o errori umani, senza dolo o negligenza grave.

Categoria di incidente	Esempi di incidente	Descrizione / Spiegazione
Sicurezza delle informazioni	Accesso non autorizzato alle informazioni	Rischi dovuti a abuso locale di dati o sistemi, compromesso di account/applicazioni o intercettazione di dati in trasmissione (spoofing, hijacking). Errori umani, di configurazione o software possono essere causa.
	Modifica non autorizzata delle informazioni	Alterazioni di dati senza autorizzazione.
Frodi	Uso non autorizzato di risorse	Utilizzo di risorse per scopi non autorizzati, inclusi profitti illeciti (es. email per catene di lettere o schemi piramidali).
Copyright	Offerta o installazione di software non autorizzato	Copie di software commerciale senza licenza o altri materiali protetti da copyright.
Mascheramento	Mascheramento	Attacchi in cui un'entità assume l'identità di un'altra per ottenere vantaggi.
	Phishing	Fingere di essere un'altra entità per convincere l'utente a rivelare credenziali private.
Vulnerabile	Apertura ad abusi	Sistemi aperti a rischi: resolver aperti, stampanti leggibili da chiunque, vulnerabilità individuabili tramite scansioni (es. Nessus), firme virus non aggiornate, ecc.
Altri	Altri incidenti	Tutti gli incidenti che non rientrano nelle categorie precedenti. Un aumento degli incidenti in questa categoria indica che il sistema di classificazione deve essere rivisto.

Linee guida per la notifica di incidenti significativi

Secondo quanto previsto dall'Articolo 23 della Direttiva NIS2, le entità essenziali e importanti devono notificare, senza ingiustificato ritardo, il CSIRT nazionale di qualsiasi incidente che abbia un impatto significativo sul servizio fornito. Procedure analoghe devono essere applicate nei Paesi extra-UE secondo la legislazione locale, notificando gli incidenti significativi alle autorità competenti.

Un incidente è considerato significativo se:

- ha causato o è in grado di causare gravi interruzioni operative dei servizi o perdite finanziarie per l'entità interessata;
- ha interessato o è probabile che interessi altre persone fisiche o giuridiche causando danni materiali o immateriali considerevoli.

La procedura da seguire prevede tre passaggi:

1. **Pre-notifica:**
   Le entità devono pre-notificare il CSIRT nazionale entro 24 ore dal momento in cui vengono a conoscenza di un incidente significativo, indicando se l'incidente potrebbe derivare da atti illegittimi o malevoli o avere un impatto transfrontaliero.
2. **Notifica completa:**
   Entro 72 ore, le entità devono inviare una notifica dettagliata al CSIRT nazionale, fornendo una prima valutazione della gravità e dell'impatto dell'incidente, inclusi eventuali indicatori di compromissione disponibili.
3. **Rapporti intermedi e finali:**
   Le entità possono essere tenute a inviare rapporti intermedi sugli aggiornamenti e un rapporto finale entro un mese. Il rapporto finale deve includere:
   - Una descrizione dettagliata dell'incidente, compresa la gravità e l'impatto;
   - Il tipo di minaccia o la causa originale (root cause) che probabilmente ha innescato l'incidente;
   - Le misure di mitigazione adottate e in corso;

Se un incidente significativo influisce negativamente sulla fornitura del servizio essenziale, sarà responsabilità dell'entità informare i destinatari del servizio, indicando eventuali minacce informatiche significative e le azioni di mitigazione raccomandate, previa consultazione con il CSIRT nazionale.

Notifiche volontarie

Oltre alle notifiche obbligatorie, le entità possono inviare notifiche volontarie al CSIRT nazionale o all'ente nazionale corrispondente, come riportato dall'Articolo 30 della Direttiva NIS2. Tali notifiche possono includere informazioni su:

- Incidenti non significativi ma comunque rilevanti;
- Minacce informatiche rilevate;
- Incidenti sfiorati (near-miss) che non hanno causato interruzioni significative.

I CSIRT nazionali gestiscono le notifiche volontarie seguendo le stesse procedure delle notifiche obbligatorie, assicurandosi che non comportino un onere eccessivo. Le notifiche volontarie hanno priorità inferiore rispetto agli incidenti obbligatori, ma vengono comunque elaborate per contribuire a migliorare la resilienza complessiva della cybersecurity.

Gestione degli Incidenti di Cybersecurity

Per una gestione efficace degli incidenti informatici, è essenziale avere un piano ben definito. Le migliori pratiche si basano sul framework NIST, che prevede i seguenti passaggi:

1. **Preparazione**
2. **Rilevamento e Analisi**
3. **Contenimento, Eradicazione e Recupero**
4. **Attività Post-Incidente**

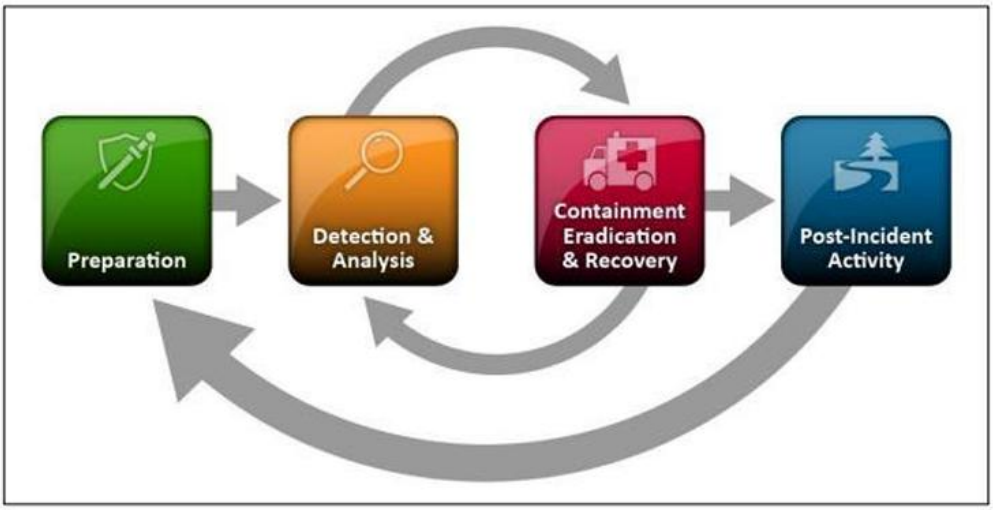


Figure 1: Incident Response Life Cycle. Source: NIST SP 800-61 Rev. 2 - Computer Security Incident Handling Guide

In caso di incidente significativo, come richiesto da NIS2, dal GDPR, le autorità nazionali competenti devono essere informate prima, durante e dopo il processo di gestione dell'incidente.

Preparazione

I membri rilevanti del gruppo di risposta agli incidenti informatici devono essere coinvolti in tutte le attività di pianificazione pre-incidente. Queste attività includono:

- Aggiornare e testare regolarmente il piano di risposta agli incidenti per garantirne la pertinenza ed efficacia.

Rilevamento e analisi

I membri rilevanti del team di risposta agli incidenti devono seguire i passaggi indicati di seguito per raccogliere informazioni, determinare la causa dell'incidente e valutare i rischi potenziali. Tutte le informazioni devono essere incluse nel registro degli incidenti.

Rilevamento dei Segnali di Incidente

Il processo inizia identificando potenziali segnali di incidente sui principali vettori di attacco, distinguendo tra:

- Segnali precursori, che indicano che un incidente potrebbe essere in corso (ad esempio attività di uno scanner di vulnerabilità).
- Segnali indicatori, che indicano che un incidente è in corso o è già avvenuto (ad esempio alert antivirus o voci di log anomale).

Analisi dell'Incidente

Questa è la fase cruciale nella gestione di un incidente informatico. Una volta rilevato un possibile incidente o ricevuta una segnalazione, il team di risposta agli incidenti deve condurre un'analisi completa, che comprende:

- Confermare l'autenticità dell'incidente
- Assegnare un responsabile iniziale e registrare i dettagli nei sistemi dedicati (es ticket management system, registro incidenti etc.).
- Raccogliere i file di log
- Determinare, se possibile, la causa principale che ha permesso il verificarsi dell'incidente.
- Individuare strategie appropriate per combattere e contenere l'incidente.
- Valutare il livello di rischio e identificare il responsabile del rischio.
- Pianificare le azioni di trattamento del rischio, comprese le misure di mitigazione.

Notifica dell'Incidente

All'inizio di questa fase, non appena viene rilevato un incidente significativo, deve essere effettuata la pre-notifica al CSIRT nazionale o all'ente nazionale competente entro 24 ore.

Contenimento, Eradicazione e Ripristino

Contenimento

Lo scopo di questa fase è limitare i danni e prevenire ulteriori conseguenze.

- Se necessario, il contenimento a breve termine può includere l'isolamento della rete, lo spegnimento di workstation infette o la disattivazione di server compromessi.
- Configurazioni ad hoc dei sistemi di difesa dell'infrastruttura di rete (firewall, IPS/IDS, proxy, ecc.).
- Evitare di modificare dati o lo stato del sistema fino alla raccolta delle informazioni necessarie.
- Valutare se interrompere immediatamente una connessione o se raccogliere ulteriori evidenze (e con quale metodo).
- Interrompere l'azione dell'attaccante attraverso il controllo degli accessi, ad esempio disabilitando account o isolando segmenti di rete.
- Informare le funzioni che devono essere messe al corrente (Direzione, Legale, HR, Comunicazione, ecc.).
- Sviluppare strategie di contenimento predefinite per ciascuna tipologia di incidente, considerando fattori quali potenziali danni, necessità di preservare le prove, disponibilità dei servizi, tempi e risorse richieste, efficacia e durata della soluzione.

Identificazione delle prove e degli host aggressori

Durante questa fase, l'attenzione è rivolta alla raccolta di prove per comprendere l'incidente e identificare gli host responsabili.

- Raccogliere e conservare le prove nel rispetto dei requisiti legali, garantendo la loro ammissibilità in tribunale se necessario.
- Documentare tutte le azioni e mantenere un registro dettagliato della gestione delle prove.
- Identificare gli host aggressori convalidando gli indirizzi IP, consultando database di incidenti e monitorando potenziali canali di comunicazione, dando priorità al contenimento e al ripristino.

Eradicazione

Questa fase riguarda la rimozione effettiva e il ripristino dei sistemi interessati.

- Discutere il processo utilizzato per rimuovere l'attaccante o gli attaccanti:
  - I backup sono compromessi?
  - È stato rilevato o sospettato un rootkit? Se sì, è necessario ricostruire il sistema o i sistemi?
  - Implementare procedure di hardening, patching o miglioramenti di sicurezza?
  - Account compromessi?

Ripristino

Questa fase serve a riportare i sistemi interessati in produzione in modo sicuro, evitando il verificarsi di nuovi incidenti. Tutte le azioni devono essere documentate.

- Stabilire chi decide il ritorno in produzione.
- Definire tempi e date per il ripristino delle operazioni.
- Coordinare il processo di ripristino, se necessario.
- Implementare un programma di monitoraggio dei sistemi, comprensivo di processi di verifica e criteri di accettazione.
- Valutare il monitoraggio esistente per rilevare o prevenire futuri attacchi.
- Testare e verificare che i sistemi compromessi siano puliti e pienamente operativi.

Attività post incidente

Le attività da seguire sono fondamentali verificare che il perimetro sia sicuro.

- Monitoraggio dei log rafforzato
- Attivazione di alert aggiuntivi
- Ricostruire la root cause e documentarla
- Elaborare e comunicare con gli stakeholder piani di rafforzamento
- Aggiornare password e token
- Patch management
- Vulnerability scanner & penetration test

Revisione e Reporting

Il rapporto finale deve essere inviato al CSIRT o all'ente nazionale competente entro un mese, includendo una descrizione dettagliata dell'incidente, la causa principale, le misure di mitigazione adottate e, se nota, l'eventuale ricaduta transfrontaliera dell'incidente.

Conformità e Sanzioni

Secondo l'Articolo 33 della Direttiva NIS2, l'autorità competente in materia di sicurezza informatica può richiedere audit e scansioni periodiche o mirate condotte da organismi indipendenti nel caso in cui vengano rilevate violazioni gravi della direttiva.

I costi di tali operazioni saranno a carico dell'entità esaminata, salvo diversa indicazione dell'autorità NIS. Ciò si applica in caso di:

- **Violazioni ripetute**: quando la stessa violazione o violazioni simili si verificano più volte.
- **Mancata notifica di incidenti significativi**: non segnalare incidenti significativi o non porvi rimedio è considerato un grave inadempimento.
- **Non conformità a istruzioni vincolanti**: ignorare o non rispettare le istruzioni vincolanti dell'autorità competente costituisce una violazione grave.

Inoltre, secondo l'Articolo 34 della Direttiva NIS2, le sanzioni amministrative specifiche per il mancato rispetto degli obblighi previsti dagli Articoli 21 e 23 della direttiva.

Ulteriori sanzioni in Italia

Secondo il Decreto Legge Italiano n. 65 del 2018, l'Autorità Nazionale per la Sicurezza Informatica può imporre multe da **12.000 a 120.000 euro** in caso di:

- Mancata adozione di misure tecniche e organizzative appropriate e proporzionate per la gestione degli incidenti.
- Mancata implementazione di misure adeguate per prevenire e ridurre l'impatto degli incidenti.

In caso di mancata notifica degli incidenti significativi all'Autorità Nazionale Italiana competente, le multe variano da **25.000 a 125.000 euro**.