[Nome della società]

Incident Reporting

[Sottotitolo del documento]

Incident Reporting Policy

Controllo Documentale

Titolo	Incident Reporting
Tipo Documento	Public
Contatto SimplyIT	E-mail: michele@simplyit.it Tel: +39 049 099 1394

Lista di Distribuzione

Società	Nome Cognome
SimplyIT	Michele Salvalaggio

Tabella delle Revisioni

Rev	Descrizione	Autori	Verificata	Approvata
[Oggetto]	Released	Michele Salvalaggio		

Sommario

Introduzione

Tutti gli incidenti di cybersecurity 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. 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).

Scopo

Questa procedura descrive come l'organizzazione comunica gli incidenti di sicurezza informatica, in conformità con gli obblighi normativi e le migliori pratiche di gestione della sicurezza. La procedura definisce i metodi e le modalità di segnalazione e notifica a tutte le funzioni coinvolte, al fine di garantire una risposta rapida ed efficace.

Segnalazione di un incidente di sicurezza informatica

Gli incidenti di sicurezza informatica si verificano quando un sistema o una rete viene compromessa, mettendo a rischio la riservatezza, l'integrità o la disponibilità dei dati aziendali. Esempi di incidenti informatici sono:

- Attacchi esterni o interni (hacker, malware, ransomware)
- Accessi non autorizzati a sistemi aziendali
- Malfunzionamenti dovuti a software non autorizzato o difetti tecnici

Quando un incidente di sicurezza informatica sospetto o effettivo viene identificato, sono disponibili i seguenti metodi di segnalazione per il personale:

- E-mail: ...
- Telefono della sede: ...

Segnalazione di un incidente di violazione dei dati personali non legato alla sicurezza informatica

Se la violazione dei dati personali sospetta o effettiva non riguarda una violazione della sicurezza informatica, i seguenti metodi sono disponibili per il personale per segnalare l'incidente:

- Telefono del responsabile DPO
- E-mail del responsabile DPO

Si rimanda alla procedura di Data Breach per maggiori dettagli e guida alla notifica.

Segnalazione di un incidente di violazione dei dati personali legato alla sicurezza informatica

Se la violazione dei dati personali sospetta o effettiva è dovuta a un incidente di sicurezza informatica, l'incidente deve essere segnalato al Dipartimento ICT indicandone i sospetti e le cause, il quale una volta verificato l'evento provvederà a coinvolgere tutti gli stakeholders coinvolti.

Notifiche

Una volta ricevuta la segnalazione di un incidente di sicurezza informatica, la risposta iniziale da parte del dipartimento ICT è quella di notificare ad eventuali stakeholders interni/esterni previsti dalla normativa vigente.
Una terza parte esterna può notificare un incidente che vede coinvolta l'azienda tramite una sezione dedicata al sito web. Un elenco di contatti importanti è ospitato nel sito web della sicurezza informatica: https://energiapuntozero.it/cybersecurity.

Linee guida per le notifiche di incidenti significativi

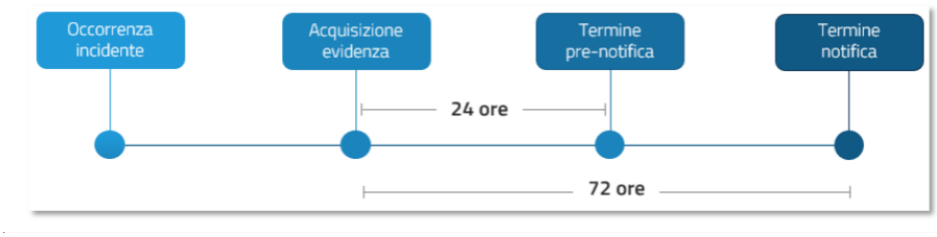
Secondo l'Articolo 23 della Direttiva NIS2, l'organizzazione, come entità essenziale e importante, è obbligata a notificare al CSIRT nazionale senza indugi ogni incidente che abbia un impatto significativo sulla fornitura dei propri servizi. Un incidente è considerato significativo se:

- ha causato o potrebbe causare gravi interruzioni nei servizi operativi o perdite finanziarie significative per la persona coinvolta;

- ha coinvolto o potrebbe coinvolgere altre entità naturali o giuridiche causando perdite tangibili o intangibili sostanziali.

La procedura da seguire prevede tre fasi:

- Pre-notifica: Le entità devono pre-notificare al CSIRT nazionale entro 24 ore dal momento in cui vengono a conoscenza di un incidente significativo
- Notifica completa: Entro 72 ore, le entità devono inviare una notifica dettagliata al CSIRT, fornendo una valutazione iniziale della gravità e dell'impatto dell'incidente, inclusi eventuali indicatori di compromissione disponibili.
- Rapporti provvisori e finali: Le entità possono essere richieste di inviare rapporti provvisori sugli aggiornamenti e un rapporto finale entro un mese. Quest'ultimo deve includere:
    - Una descrizione dettagliata dell'incidente, inclusa la sua gravità e impatto;
    - Il tipo di minaccia o causa originale (causa principale) che ha probabilmente innescato l'incidente;
    - Le misure di mitigazione adottate e in corso;
    - Dove noto, l'impatto transfrontaliero dell'incidente.



Commentato [MS1]: Valutare se inserirlo

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

Documentazione e Registrazione degli Incidenti

Ogni incidente deve essere documentato in un registro interno degli incidenti, che deve contenere informazioni precise e complete per garantire la corretta gestione, analisi e conformità. Il registro deve includere i seguenti dettagli:

1. Descrizione Dettagliata dell'Incidente

2. Data e Ora di Rilevamento
3. Azioni Adottate
4. Notifiche Effettuate

Una documentazione accurata e tempestiva degli incidenti non solo assicura la conformità alle normative, ma aiuta anche a migliorare le risposte future, prevenire rischi simili e facilitare le analisi post-incidente. Il modello da utilizzare è il seguente: Registro_Incidenti_NIS2 & Incident Response team v1.0.xlsx.

Modalità di reporting

L'ACN riporta le seguenti linee guida:

I soggetti coinvolti in un incidente devono inviare una segnalazione e successivamente una notifica completa tramite la compilazione e l'invio di un apposito modulo online disponibile sul sito web del CSIRT Italia (https://www.csirt.gov.it/segnalazione).

Nella notifica al CSIRT Il soggetto segnalante dovrà fornire le seguenti informazioni:

• data e ora di rilevamento dell'incidente;
• asset impattati;
• vettori d'attacco;
• misure di rientro intraprese e pianificate;
• IoC;
• evidenze rilevanti (es. sample di malware, ransom note).

È possibile inviare un malware o una e-mail malevola (in formato .msg o .eml) utilizzando la casella infected@csirt.gov.it. I contenuti inviati dovranno essere inclusi in un archivio nel formato zip protetto con la password "infectedacn".
E' stato creato un modello di notifica di incidente per velocizzare la comunicazione: Modello Notifica Incidente CSIRT-ACN v1.0.docx.

Nella fase di notifica è necessario utilizzare le tassonomie definite dall'ACN al seguente indirizzo:

https://www.acn.gov.it/portale/documents/20119/552690/ACN_Tassonomia_Cyber_CLEAR.pdf

https://www.acn.gov.it/portale/documents/d/guest/lineeguida_cad_definizioneprocessiproceduregestioneincidenti

Tabella RACI

Uno degli strumenti maggiormente utilizzati per l'assegnazione di ruoli e responsabilità, è la matrice di assegnazione responsabilità (cosiddetta matrice RACI) che permette di definire chiaramente ruoli e responsabilità per le varie attività di un processo. In particolare, RACI è un acronimo le cui lettere indicano la tipologia di responsabilità che un certo ruolo ha nell'ambito di una determinata attività:

- Responsible (R): chi esegue operativamente l'attività.
- Accountable (A): chi ha la responsabilità sul risultato dell'attività.
- Consulted (C): chi viene consultato durante l'esecuzione dell'attività in quanto possiede conoscenze necessarie al completamento dell'attività.
- Informed (I): chi è informato sull'avanzamento e il completamento dell'attività

In fase si segnalazione si consiglia di inserire nel piano di comunicazione al CSIRT il dettaglio e i soggetti responsabili come stabilito dal modello RACI. A seguire è riportato un esempio di matrice RACI per un generico processo costituito da n fasi:

Fase	Attività	Ruolo 1	Ruolo 2	Ruolo m
Fase 1	Attività 1	A, R	C	I
Fase 1	Attività 2	R	A, R	–
Fase 1	Attività ...	A	R	C
Fase 2	Attività 1	A, R	I	C
Fase 2	Attività 2	I	–	A, R
Fase 2	Attività ...	A, R	I	I
Fase n	Attività 1	C	I	A, R
Fase n	Attività 2	R	–	A
Fase n	Attività ...	A, R	C	C

Piano di comunicazione

Comunicazione per Data breach con violazione dati personali

Si chiede di fare riferimento alle linee guida dettate dalla procedura di Data Breach e al responsabile DPO in materia.

Comunicazione per incidenti che non violino i dati personali

Comunicazione rivolta ai dipendenti

Oggetto: Aggiornamento urgente su incidente di sicurezza informatica

[Nome Società] informa tutto il personale che in data [data incidente] è stato rilevato un evento di sicurezza informatica che ha interessato alcuni sistemi aziendali. L'incidente è stato immediatamente gestito attraverso l'attivazione del piano interno di risposta agli incidenti e i sistemi coinvolti sono stati isolati in modo da prevenire ulteriori conseguenze. Sono in corso verifiche tecniche approfondite che consentiranno di definire con precisione l'origine dell'evento, la natura delle attività non autorizzate e l'eventuale coinvolgimento di dati aziendali.

Invitiamo tutto il personale a prestare particolare attenzione a eventuali messaggi di posta elettronica sospetti, a richieste insolite di credenziali o informazioni interne e a qualunque comportamento anomalo dei dispositivi. Raccomandiamo cautela e il rispetto rigoroso delle pratiche aziendali di sicurezza, incluse l'adozione di password robuste, la verifica dell'autenticità delle comunicazioni ricevute e l'immediata segnalazione di eventuali anomalie al reparto ICT. Forniremo aggiornamenti non appena saranno disponibili nuovi elementi.

Comunicazione rivolta ai fornitori o partner

Oggetto: Informazione su incidente di sicurezza informatica e verifica delle integrazioni tecniche

Con la presente [Nome Società] informa che in data [data incidente] è stato individuato un incidente di sicurezza che ha interessato alcuni sistemi aziendali. L'evento è attualmente oggetto di una analisi tecnica approfondita al fine di determinarne con precisione la portata e l'impatto. In via precauzionale, sono state applicate misure di contenimento che includono la sospensione temporanea di specifiche integrazioni, la revisione delle configurazioni condivise e il rafforzamento dei controlli di sicurezza. Invitiamo la vostra squadra tecnica a verificare eventuali interazioni tra i nostri sistemi e i vostri servizi, inclusi i collegamenti API, le VPN dedicate, le sincronizzazioni applicative e le credenziali condivise. Se doveste rilevare comportamenti anomali o attività sospette riconducibili al perimetro di collaborazione, vi chiediamo di segnalarcelo immediatamente. Rimaniamo disponibili a condividere ulteriori informazioni tecniche necessarie per agevolare la vostra analisi.

Comunicazione rivolta all'ACN

Oggetto: Notifica volontaria soggetto NIS2

Spett.le Agenzia per la cybersicurezza nazionale

Desideriamo informare che, a seguito di un evento di sicurezza informatica rilevato in data [data incidente], alcuni servizi potrebbero risultare temporaneamente non disponibili oppure potrebbero funzionare con prestazioni ridotte. L'evento ha reso necessario avviare una serie di interventi tecnici di contenimento e bonifica che comportano, per ragioni di sicurezza, la sospensione o la limitazione dell'accesso a determinate funzioni. Il nostro team tecnico è impegnato nel ripristino delle normali condizioni operative e sta lavorando con la massima priorità per ridurre ogni possibile disagio. I dati dei clienti rimangono oggetto di costante monitoraggio e protezione e, qualora emergessero indicazioni riguardanti un loro possibile coinvolgimento, provvederemo a comunicarlo senza ritardo. Ringraziamo per la comprensione e per la collaborazione in questa fase.

Oggetto: Notifica incidente soggetto NIS2

[Nome Società], in qualità di soggetto rientrante nel perimetro della normativa NIS2, informa che in data [data e ora di rilevazione] è stato individuato un incidente di cybersicurezza che ha comportato un impatto sui sistemi informativi aziendali e che, in ragione delle sue caratteristiche tecniche e del potenziale rischio per la continuità operativa, richiede la segnalazione e la successiva notifica al CSIRT Italia secondo quanto previsto dalle linee guida dell'Agenzia per la Cybersicurezza Nazionale. L'evento è stato rilevato attraverso:

- Attività di monitoraggio;
- Procedure interne di sicurezza;
- Segnalazione terze;

È stata effettuata una autovalutazione preliminare dell'impatto, che indica:

- [Violazione dati personali;
- Perimetro circoscritto a soli [descrivere perimetro];

Le evidenze raccolte fino a questo momento suggeriscono che l'incidente è un attacco di tipo:

- [specificare la categoria, ad esempio malware, phishing mirato, compromissione credenziali, vulnerabilità nota, sfruttamento remoto non autenticato o altro]

Sono stati individuati indicatori di compromissione rilevanti:

- [specificare IoC Hash, email, etc]

Contestualmente alla raccolta delle evidenze, [Nome Società] ha avviato le misure di contenimento e di ripristino necessarie a limitare l'estensione dell'incidente.

[Nome Società] rimane a disposizione dell'Agenzia per la Cybersicurezza Nazionale per ogni ulteriore chiarimento e per fornire tempestivamente ulteriori evidenze tecniche che si rendessero necessarie per approfondire la valutazione dell'incidente, per supportare i processi di prevenzione e risposta e per contribuire alla sicurezza complessiva delle infrastrutture nazionali.