GESTIONE INCIDENTI SULLA SICUREZZA DELLE INFORMAZIONI

Matrice delle Revisioni

Rev.	Data	Descrizione Modifica	Motivo Modifica
00	10.12.18	Prima Emissione	
01	11.12.19	Revisione documento	Aggiornamento della procedura per ampliamento scopo e nuove certificazioni ISO 22301, 27001, 27017, 27018.
02	14.02.20	Revisione documento	Adeguamento documento per NC
03			

INDICE

1. RIFERIMENTI

- Norma UNI EN ISO 9001
- Norma UNI EN ISO 22301
- Norma UNI CEI ISO/IEC 27001
- Norme UNI CEI ISO/IEC 27017 e 27018
- Ulteriore normativa di settore applicabile come da Elenco Documentazione di Origine Esterna

2. SCOPO E APPLICABILITA' DELLA PROCEDURA OPERATIVA

Scopo della presente Procedura Operativa è regolamentare il processo di trattamento degli incidenti sulla sicurezza delle informazioni, dall'individuazione degli eventi e degli incidenti che possono verificarsi, alla loro analisi e valutazione, alla definizione di azioni finalizzate alla riduzione del verificarsi degli incidenti stessi e dei rischi conseguenti.

Tutto il personale è chiamato a segnalare eventi e debolezze relativi alla sicurezza delle informazioni seguendo la presente procedura. Eventi o debolezze identificati attraverso le attività di monitoraggio e valutazione di vulnerabilità rientrano nello scopo della presente procedura. Essa si applica agli incidenti sulla sicurezza delle informazioni che possono verificarsi a qualunque assets rientrante nel perimetro di applicazione della Norma 27001.

3. MODALITA' OPERATIVE

3.1. Definizioni

Per **evento sulla sicurezza delle informazioni** si intende un identificato accadimento relativo allo stato di un sistema, servizio o rete, che, a una prima analisi, presenta bassa importanza per la sicurezza delle informazioni ma che può costituire una possibile violazione della politica per la sicurezza delle informazioni, un malfunzionamento delle contromisure o una situazione mai osservata in precedenza.

Per **incidente relativo alla sicurezza delle informazioni** si intende l'evento o serie di eventi relativi alla sicurezza delle informazioni, non voluti o inattesi, che hanno una probabilità significativa di compromettere le operazioni relative al business e di minacciare la sicurezza delle informazioni. Non sempre un evento costituisce un incidente. Valutando l'impatto o il danno che tale evento potrebbe provocare, la criticità degli asset interessati e la correlazione con altri eventi è possibile determinare se l'evento è un incidente.

Per **gestione degli incidenti sulla sicurezza delle informazioni** si intende l'individuazione delle responsabilità e delle modalità attraverso le quali si identificano, valutano e trattano gli eventi sulla sicurezza delle informazioni

Per **vulnerabilità** si intendono le debolezze esistenti che, se sfruttate, potrebbero compromettere la sicurezza delle informazioni.

Per **gestione delle vulnerabilità** si intende la ricezione di informazioni e rapporti concernenti le vulnerabilità hardware e software, l'analisi della natura e degli effetti delle vulnerabilità e lo sviluppo di strategie di risposta.

Per "**non classificato**" si intende un evento, una debolezza segnalati che, ad una prima analisi, non si riesce ad inserire in una delle categorie precedenti. I "non classificati" sono oggetto di ulteriori analisi per poterli categorizzare prima possibile.

3.2. Segnalazione e Registrazione degli Incidenti

Tutto il personale aziendale, durante lo svolgimento delle proprie attività, può rilevare incidenti relativi alla sicurezza delle informazioni ed ha il compito di segnalarli.

Di seguito sono riportati gli eventi/incidenti che possono impattare sulla continuità del servizio:

1. disastri naturali (terremoto, incendio, etc.);
2. disastro umano (errore, sabotaggio, attacco alla rete, attacchi terroristici)
3. disastro ambientale (rottura delle attrezzature, errori SW, blocco telecomunicazioni, blackout elettrico)
4. interruzione di elettricità oltre l'autonomia degli UPS;
5. interruzione della connettività fonia e dati;
6. rottura dei server.

Al verificarsi di un evento/incidente:

1. interrompere le attività strettamente connesse all'evento o alla debolezza individuati;
2. compilare il modulo Mod. SE_I "Segnalazione eventi e incidenti" da inviare a mezzo mail all'Amministratore di Sistema e per copia conoscenza al Responsabile del Sistema;
3. identificare il problema verificatosi mediante l'attribuzione di una delle categorie riportate negli elenchi seguenti:

Evento/debolezza/incidente relativi a Sistemi, Reti e Comunicazioni

- Accesso non autorizzato a: computers, reti, servizi, informazioni, processi, software
- Modifiche non autorizzate a: informazioni, software, configurazioni, processi
- Indisponibilità di risorse, sistemi e servizi
- Hacking
- Compromissioni relative a: trattamento e gestione delle informazioni
- Malicious software code: virus, worm, Trojan, etc.
- Spyware e Adware
- Spam e Phishing
- Furto di informazioni
- Furto di software
- Errori di configurazione
- altri attacchi, eventi o incidenti

Evento/debolezza/incidente relativi Personale, Collaboratori, Parti Esterne

- Errori operatore
- Abusi e coercizioni
- Comportamenti inaccettabili o sospetti
- Attività fraudolente
- Uso errato o inaccettabile di risorse
- Violazione di privilegi e/o diritti di accesso
- Furto di attrezzature
- Furto di informazioni e/o identità
- Attrezzature non presidiate, materiale sensibile lasciato incustodito
- Carenza di addestramento
- altro

Evento/debolezza/incidente relativi a failures di sistemi, crash e malfunzionamenti

- Hardware failures
- Software failures
- Communications failures
- altro

Evento/debolezza/incidente relativi a compliance relativa alle prescrizioni legali

- Non-compliance rispetto al Codice sulla Privacy (D.Lgs. 196/03 e Regolamento Europeo 2016/679) e a provvedimenti del Garante
- Non-compliance rispetto alla legislazione riguardante accessi non autorizzati, hacking, violazioni e reati informatici
- Violazioni delle norme sul diritto d'autore, sul software licensing e pirateria informatica
- Downloading di software illegale e/o materiale inappropriate (pornografico, ecc.)
- Frode
- Violazione di accordi contrattuali
- Compromissioni derivanti da non- compliance rispetto alle politiche a alle procedure aziendali
- altro

L'Amministratore di Sistema verifica la natura dell'incidente segnalato e, con il supporto del Responsabile del Sistema e del Responsabile dell'Amministrazione, che si ritiene opportuno coinvolgere, procede all'analisi delle cause e alla identificazione di azioni idonee. Una volta definite le azioni, l'Amministratore di Sistema invia al Personale che ha fatto la segnalazione (e per copia conoscenza al Responsabile del Sistema), la risposta relativa alla chiusura della stessa.

Laddove si verifichino problemi nell'uso della posta elettronica, le modalità di segnalazione a cui si ricorre sono comunicazioni a mezzo telefono o anche comunicazioni scritte.

Per eventi relativi a disastri naturali (terremoto, incendio, etc.) si rimanda agli specifici piani di continuità operativa.

3.3. Risposta

In seguito alla segnalazione ricevuta dal Personale, l'Amministratore di Sistema ed il Responsabile del Sistema per la Sicurezza Informatica, provvedono a classificare l'incidente definendolo come:

- evento;
- vulnerabilità;
- incidente;
- non classificato.

Al riguardo, l'ordine di priorità nella gestione delle risposte agli eventi segnalati, è il seguente:

- incidenti;
- non classificati;
- vulnerabilità;
- eventi.

In seguito alla classificazione dell'incidente, RSGSI e AMM richiedono ulteriori supporti a personale tecnico qualificato, quando necessario, al fine di analizzare e meglio comprendere la natura degli incidenti, per identificare azioni appropriate di contenimento e per l'implementazione di piani di emergenza.

Laddove l'incidente rilevato coinvolga sistemi di alto valore per il business o valutati come critici o altamente critici, sono immediatamente segnalati dall'Amministratore di Sistema alla Direzione. Spetta all'Amministratore di Sistema fornire conferma dell'avvenuto recupero e ripristino dei sistemi interessati da incidenti e che i controlli richiesti siano nuovamente operativi, prima che sia autorizzato il ritorno alla normale operatività. Tale conferma viene fornita a mezzo mail inviata al personale che ha fatto la segnalazione con indicazione nell'oggetto della mail della classificazione attribuita al problema segnalato.

I processi di business interessati dal presente piano sono i seguenti, disposti in ordini di criticità:

- Sviluppo software;
- Assistenza e Manutenzione;
- Gestione della documentazione;
- Amministrazione;
- Call Center Assistenza.

Per ogni processo individuato vengono stabilite le risorse utilizzate e il tempo massimo accettato di indisponibilità del servizio.

3.4. Contatti con le Autorità

US Srl mantiene appropriati contatti con le autorità pertinenti. L'Amministratore di Sistema e la Direzione identificano le autorità con le quali essere in contatto a supporto della gestione degli incidenti relativi alla sicurezza delle informazioni, della gestione della business continuity e del miglioramento continuo. A titolo esemplificativo, sono individuate quali Autorità pertinenti:

- Garante Privacy in caso di Data Breach in merito a incidenti che coinvolgono la protezione dei dati personali;
- Autorità Regionali, per le modifiche di leggi e/o decreti regionali con potenziale impatto sulle attività;
- MEF;
- Vigili del Fuoco;
- Polizia Postale;
- Fornitori di telecomunicazioni;
- Agid, Owasp, etc.

3.5. Contatti con Gruppi Specialistici

Per quanto riguarda i contatti con gruppi specialistici, il Responsabile del Sistema e l'Amministratore Delegato sono iscritti a newsletter relative a temi specifici dell'erogazione del servizio:

- AssoSoftware che invia aggiornamenti e informazioni su tutti gli aspetti di interesse delle società di sviluppo software
- Confindustria
- Owasp
- Altri gruppi e/o associazioni di categoria.

Sulla base del contenuto delle informazioni delle varie newsletter i suddetti responsabili provvedono a smistarle alle competenze interessate.

4. ALLEGATI

MOD SE_I – Segnalazione eventi e incidenti