POLITICA DI GESTIONE DEGLI INCIDENTI DI SICUREZZA IT

Approvazione
Data: **03/11/2021**
Dirigente ASI: **Dott.ssa Francesca Pruneti**
Firmato digitalmente ai sensi del D.Lgs. n. 82/2005

Informazioni sul documento		
Redazione a cura di: *U.O. Sicurezza IT*	**Destinatari:** *Utenti dell'Università di Parma*	**Deposito del documento:** *www.unipr.it/regolamento-sicurezza-IT*

Sommario

1. Scopo del documento

Lo scopo di questo documento è definire la corretta gestione degli incidenti di sicurezza IT. Una buona gestione degli incidenti IT è utile a proteggere i dati personali di cui l'Ateneo è titolare, garantire la sicurezza delle informazioni e dei sistemi impiegati per il loro trattamento, oltre che minimizzare l'impatto sui servizi erogati e sull'operatività degli utenti. In particolare il documento indica le linee guida affinché gli incidenti di sicurezza IT:

- vengano rilevati e analizzati tempestivamente;
- vengano gestiti adeguatamente;
- abbiano un impatto ridotto al minimo;
- vengano intraprese le azioni di contenimento necessarie per prevenire ulteriori danni;
- gli incidenti e le corrispettive azioni di mitigazione vengano registrate e documentate;
- le autorità competenti o gli interessati siano informati tempestivamente come richiesto dalle normative vigenti.

2. Ambito di applicazione

La politica descritta in questo documento si applica al perimetro informatico dell'Ateneo. Questo perimetro ha dei contorni mutevoli che nel corso del tempo tendono ad assumere caratteristiche e dimensioni sempre meno circoscritte. Il perimetro informatico dell'Ateneo è costituito da: sistemi IT, servizi, processi e procedure che utilizzano software e hardware, ma anche da utenti con prassi e consuetudini diverse. Tutte le componenti di questo perimetro informatico, da quelle più fisiche a quelle immateriali, possono subire o generare un incidente informatico, o comunque esserne coinvolte almeno in parte.

3. Cosa sono gli incidenti di sicurezza IT

Un incidente di sicurezza IT è un evento che tende o può compromette i principi di integrità, riservatezza e disponibilità di informazioni gestite dall'Ateneo tramite strumenti informatici. Un evento che non abbia queste caratteristiche, benché possa creare disagio agli utenti o danno economico all'Ateneo, non deve essere considerato un incidente di sicurezza IT. Viene classificato come incidente di sicurezza IT anche un evento che non consenta di adempiere gli obblighi di legge o espone l'organizzazione al rischio di incorrere in sanzioni o dover procedere a risarcimenti per eventuali danni cagionati. Di seguito un elenco non esaustivo di eventi che costituiscono un incidente di sicurezza IT:

- accesso non autorizzato a banche dati, sistemi informatici, reti aziendali o relativi apparati;
- accesso non autorizzato al perimetro dell'organizzazione dove si trovano strumentazioni o apparati informatici ad accesso limitato;
- diffusione o divulgazione non autorizzata di informazioni;
- compromissione dell'integrità dei sistemi o delle informazioni;
- impossibilità di accesso ad informazioni trattate dall'organizzazione;
- malfunzionamento di qualsiasi natura dei sistemi di controllo, accesso e sorveglianza;
- danneggiamento fisico o logico delle risorse contenenti informazioni, o necessarie alla loro elaborazione, con conseguente perdita o riduzione di integrità, riservatezza e disponibilità delle informazioni;
- diffusione di malware all'interno dell'infrastruttura IT, etc.

4. Cosa sono le violazioni di dati personali (Data Breach)

La violazione dei dati personali trattati dall'Ateneo, detto anche "Data Breach", è un particolare tipo di incidente di sicurezza IT che determina - accidentalmente o in modo illecito - la distruzione, la perdita, la modifica, la divulgazione non autorizzata o l'accesso a dati personali trasmessi, conservati o comunque trattati dal titolare del trattamento dell'Ateneo (come definito nel Regolamento UE 679/2016 - GDPR). Una violazione dei dati personali può compromettere la riservatezza, l'integrità o la disponibilità di dati personali. Per una definizione precisa di dato personale si rimanda al documento ***"Politica di classificazione dei dati personali"***. A titolo semplificativo, per dato personale si intende qualsiasi informazione riguardante una persona fisica identificata o identificabile (interessato). Si considera identificabile la persona fisica che può essere riconosciuta, direttamente o indirettamente, attraverso dei dati che lo caratterizzano, per esempio nome e cognome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online, uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale (GDPR, art. 4). Le violazioni di dati personali possono verificarsi in un ampio numero di casi, a titolo di esempio riportiamo:

- smarrimento o furto di attrezzature informatiche aziendali (o non aziendali) che contengono dati personali (es.: pc portatili, chiavette etc.);
- invio di messaggi contenenti dati personali a un destinatario sbagliato;
- pubblicazione di dati personali su risorse informatiche accessibili al pubblico (es.: pubblicazione su siti web dell'Ateneo di dati personali).
- divulgazione di dati confidenziali a persone non autorizzate;
- accesso abusivo (es.: data breach causato da un accesso non autorizzato ai sistemi);
- l'impossibilità di accedere ai dati per cause accidentali o per attacchi esterni, virus, malware, ecc
- banche dati alterate o distrutte senza autorizzazione rilasciata dal relativo proprietario;
- violazione di misure di sicurezza fisica (ad esempio, forzatura di porte o finestre di stanze di sicurezza o archivi, contenenti informazioni riservate);

5. Classificazione degli incidenti di sicurezza IT

Una classificazione degli incidenti di sicurezza IT, insieme a un'adeguata analisi e documentazione delle informazioni relative all'incidente, è di fondamentale importanza per una risposta tempestiva ed efficace. A seconda dell'impatto che un incidente ha sull'organizzazione e sulle capacità degli utenti di adempiere alle loro mansioni viene adottata la seguente valutazione.

Impatto	Descrizione
Basso	- Non causa danni significativi a operatività, produttività, amministrazione e gestione - Causa una perdita di fiducia trascurabile - Coinvolge solo dati non classificati - L'Impatto sulla integrità delle informazioni è trascurabile o secondario con scarso effetto sul business - Comporta una perdita di disponibilità delle informazioni che può essere tollerata fino a due/tre giorni - Causa perdite economiche e commerciali trascurabili

	- Non causa danni significativi in merito a obblighi contrattuali e rischi di conformità
Medio	- Potrebbe causare interruzioni di attività interne all'organizzazione - Potrebbe degradare l'effettiva operatività in una parte dell'organizzazione - Può causare una limitata pubblicità negativa - Comporta una perdita di disponibilità delle informazioni che può essere tollerata fino a un giorno - Vi sono interessi economici e commerciali di basso interesse per la concorrenza e di basso valore commerciale - Potrebbe causare una violazione minore o tecnica di obblighi legali o normativi
Alto	- Può causare interruzioni delle attività proprie dell'organizzazione con qualche ripercussione anche in altre organizzazioni - Può compromettere l'effettiva operatività in diverse parti dell'organizzazione - Può causare una limitata pubblicità negativa tale da influenzare le relazioni con altre organizzazioni o le relazioni con il pubblico - Coinvolge dati classificati come interni - Le modifiche non autorizzate, o la perdita di accuratezza, sono moderatamente critiche. L'impatto è notevole e comincia ad avere gravi ripercussioni sul business e le sue operazioni - La perdita di disponibilità può essere tollerata fino a una/due ore - Vi sono interessi economici e commerciali di moderato interesse per la concorrenza e di moderato valore commerciale - Può causare la violazione di obblighi legali o normativi
Molto alto	- Può causare violazioni e ostacolare una eventuale attività investigativa - Può causare interruzioni gravi delle attività proprie dell'Organizzazione con ripercussioni consistenti anche in altre organizzazioni - Può impedire l'effettiva operatività dell'organizzazione - Può causare un'ampia pubblicità negativa tale da influenzare le relazioni con altre organizzazioni, con il pubblico o con altri paesi - Coinvolge dati classificati come Confidenziali - Le modifiche non autorizzate, o la perdita di accuratezza, sono fondamentali per i processi e le applicazioni di business - Gli asset devono essere pienamente disponibili durante il normale orario di lavoro - Vi sono Interessi economici e commerciali di elevato interesse per la concorrenza, valore commerciale - Causa di perdite finanziarie elevate - Costituisce una violazione grave degli obblighi contrattuali relativi alla sicurezza delle informazioni fornita da terze parti - Può causare una violazione grave di obblighi legali o normativi
Critico	- Può causare violazioni eccezionalmente gravi - Può causare danni eccezionalmente gravi all'efficacia di attività operative o logistiche - Può causare interruzioni eccezionalmente gravi delle attività proprie dell'organizzazione con gravi ripercussioni anche in altre organizzazioni - Può impedire seriamente l'effettiva operatività dell'organizzazione, arrivando eventualmente a causarne la chiusura - Può causare un'ampia pubblicità negativa tale da influenzare negativamente le relazioni con altre organizzazioni, con il pubblico o con altri Paesi - Coinvolge dati classificati come riservati

	- Le modifiche non autorizzate, o la perdita di accuratezza sono molto critiche. L'impatto è molto grave e le conseguenze possano portare al fallimento totale di alcuni o di tutti i processi/applicazione di business. - Gli asset coinvolti devono essere SEMPRE disponibili - Vi sono Interessi economici e commerciali di altissimo interesse per la concorrenza, di altissimo valore commerciale - Causa di perdite finanziarie eccezionalmente elevate - Costituisce una violazione eccezionalmente grave degli obblighi contrattuali relativi alla sicurezza delle informazioni fornita da terze parti - Può causare una violazione eccezionalmente grave di obblighi legali o normativi

6. Gestione degli eventi di sicurezza IT

Gli incidenti vengono gestiti attraverso una sequenza di fasi distinte:

- preparazione all'incidente;
- rilevazione, identificazione e analisi;
- contenimento, eradicamento e recupero;
- attività post-incidente.

6.1. Attività pre-incidente

Le metodologie di risposta agli incidenti enfatizzano l'uso proattivo e continuo di strumenti, formazione e processi necessari per prevenire gli incidenti garantendo che sistemi, reti e applicazioni siano sufficientemente sicuri. La preparazione include tutte le attività che consentono di rispondere a un incidente: politiche, strumenti, procedure, efficaci piani di azione e comunicazione, e implica che i gruppi interessati abbiano istituito i controlli necessari per recuperare e continuare le operazioni dopo che un incidente è stato scoperto. Le analisi post-mortem di incidenti precedenti devono costituire la base per il miglioramento continuo.

6.2. Rilevazione, identificazione e analisi

I primi passi per rilevare, verificare, investigare e analizzare un incidente sono importanti per lo sviluppo di una strategia efficace di contenimento ed eradicazione. Una volta confermato un incidente, è possibile assegnare risorse per indagare l'ambito, l'impatto e la risposta necessari. Le fasi di rilevamento e analisi determinano la fonte dell'incidente e preservano le prove; tali informazioni devono essere comunicate alla U.O. Sicurezza IT che detiene ed aggiorna il "Registro degli incidenti di sicurezza IT dell'Ateneo".

6.3. Contenimento, eradicamento e recupero

Il contenimento è la fase di triage in cui il sistema o servizio compromesso viene identificato, isolato o comunque mitigato e quando le parti interessate vengono avvisate. Le procedure di contenimento tentano di limitare attivamente la portata e l'entità dell'attacco. Il contenimento implica l'acquisizione, la conservazione, la messa in sicurezza e la documentazione di tutte le prove. Il contenimento deve impedire ai dati di lasciare la rete attraverso le macchine interessate e impedire che l'attaccante causi ulteriori danni alle risorse aziendali.

L'eradicazione è la rimozione di codice dannoso, o di un profilo o accesso inappropriato. L'eradicazione include anche la gestione delle vulnerabilità che potrebbero essere state la causa principale della compromissione.

6.4. Attività post-incidente

Tutte le attività di risposta agli incidenti saranno documentate e esaminate post-mortem per valutare se il processo di indagine è stato efficace. Successive correzioni possono essere apportate ai metodi e alle procedure utilizzate per migliorare il processo di risposta agli incidenti.

La documentazione offre l'opportunità di migliorare i processi di risposta agli incidenti e identificare problemi ricorrenti. Questa fase consente anche l'analisi dell'incidente per le sue implicazioni procedurali, la raccolta di metriche e l'incorporazione di buone pratiche nelle attività di risposta e formazione future.

Revisioni del documento

Ver.	Descrizione modifiche	Autore	Data modifica
1.0	*Versione iniziale*	*U.O. Sicurezza IT*	*21/05/2021*