Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS

Ufficio federale della cibersicurezza UFCS

Versione 1.0

Guida sull'analisi della necessità di protezione

del 14 ottobre 2024

1 Introduzione

Questa guida si rivolge alle aziende e alle autorità che desiderano implementare la procedura di sicurezza dell'Amministrazione federale. Il testo in blu è particolarmente rilevante per le unità amministrative dell'Amministrazione federale e per altre organizzazioni soggette alla legge sulla sicurezza delle informazioni (LSIn) o all'ordinanza sulla sicurezza delle informazioni (OSIn).

Secondo l'articolo 16 capoverso 1 LSIn le autorità assoggettate stabiliscono una procedura per garantire la sicurezza delle informazioni nell'impiego di mezzi informatici, che secondo l'articolo 16 capoverso 2 lettera a LSIn comprende la valutazione della necessità di protezione. Questa guida descrive una procedura che può essere utilizzata per determinare la necessità di protezione di un oggetto informatico da proteggere (possibilmente aggregato) prima della messa in servizio. La procedura viene definita sommariamente «analisi della necessità di protezione».

L'infrastruttura informatica di cui ci si assume la responsabilità deve prima essere suddivisa in una serie di oggetti informatici da proteggere. Un oggetto informatico da proteggere può essere e sarà composto da diversi mezzi informatici (ad es. componenti hardware e software nonché dati in essi salvati, modificati e trasmessi), che hanno tutti uno scopo comune definito e sono quindi collegati anche a livello logico (ad es. applicazione specialistica per il disbrigo di un determinato processo operativo). Gli oggetti informatici da proteggere che mettono le loro prestazioni a disposizione di altri oggetti informatici da proteggere sono considerati una piattaforma e sono a loro volta oggetti informatici da proteggere. Alcuni esempi sono eIAM, infrastrutture di server virtualizzate e offerte Software as a Service (SaaS).

Di norma, un oggetto informatico da proteggere non è composto solo dalle informazioni, perché non sarebbe utile creare una propria analisi della necessità di protezione per ogni tipo di documento.

In linea di principio, nella procedura di sicurezza dell'Amministrazione federale la necessità di protezione deve essere determinata e documentata per ogni oggetto informatico da proteggere. Nella valutazione della necessità di protezione vengono considerate solo le possibili conseguenze in caso di compromissione. Il tipo di minaccia che può portare a questa compromissione non viene considerato.[1] L'analisi della necessità di protezione valuta se c'è

[1] Ad esempio nel caso di una perdita di dati è irrilevante se la causa è la mancanza di un backup, un attacco hacker o un collaboratore con cattive intenzioni (in ogni caso i dati sono stati persi).

un rischio che deve essere ridotto.

La necessità di protezione di informazioni viene documentata come «elevata» o «non elevata» per ogni obiettivo di protezione (confidenzialità, integrità, disponibilità, verificabilità e protezione dei dati). Oltre alla necessità di protezione vengono documentati anche i livelli di sicurezza secondo l'articolo 17 LSIn. Ciò ha lo scopo di semplificare la successiva scelta di misure appropriate da utilizzare in caso di necessità di protezione elevata.

2 Procedura per determinare la necessità di protezione

Con la procedura descritta di seguito[2] è possibile determinare la necessità di protezione e il livello di sicurezza di un oggetto informatico da proteggere e stabilire se la necessità di protezione è elevata oppure no. La procedura è composta da due fasi. Nella fase 1 viene descritto l'oggetto informatico da proteggere e viene creato un elenco delle informazioni. Nella fase 2, invece, vengono valutate le possibili conseguenze in caso di violazione degli obiettivi di protezione (confidenzialità, disponibilità, integrità, verificabilità e protezione dei dati[3]).

Fase 1

L'oggetto informatico da proteggere e la sua configurazione tecnica devono essere descritti nel modo più dettagliato possibile. Le seguenti indicazioni sono raccomandate, ma possono essere completate in qualsiasi momento (anche più avanti):

a) oggetto e obiettivi dell'oggetto informatico da proteggere, con indicazione dei processi operativi interessati e degli identificatori[4];

b) beneficiari e fornitori di prestazioni coinvolti (se noti) e persone con indicazione concreta dei ruoli (ad es. ISIU, responsabile dell'oggetto da proteggere, capoprogetto, …);

c) configurazione tecnica (compreso l'ambiente di sviluppo ed eventuali servizi delle piattaforme utilizzati) con schizzi della struttura il più precisi possibile, in particolare anche per quanto riguarda la situazione della rete;

d) diritto d'accesso (per persone, gruppi di persone, ruoli e processi);

e) eventuali condizioni quadro geografiche disponibili (ad es. in quali Paesi vengono salvate le informazioni e da dove vi si accede).

Deve essere creato un elenco delle informazioni che contiene tutte le informazioni generate, salvate, elaborate e/o trasmesse dall'oggetto informatico da proteggere oppure necessarie per mettere a disposizione l'oggetto informatico da proteggere. Le informazioni devono essere raggruppate adeguatamente. Per ogni gruppo di informazioni devono essere fornite e documentate le seguenti indicazioni:

a) descrivere il gruppo di informazioni;

b) eventuali classificazioni e/o classificazioni necessarie secondo gli articoli 18, 19 e 20 OSIn[5];

c) indicare se un gruppo di informazioni contiene anche dati personali e di quali dati

[2] La procedura si ispira al Rapid Risk Assessment di Mozilla (https://infosec.mozilla.org/guidelines/risk/rapid_risk_assessment).

[3] https://www.bj.admin.ch/bj/it/home/staat/datenschutz/info-bundesbehoerden.html

[4] Ad esempio nome del progetto, numero/ID del progetto ecc.

[5] Per le informazioni classificate «ad uso interno», «confidenziale» o «segreto» deve essere specificato anche il gruppo delle persone autorizzate. Questo passaggio è importante per riconoscere i rischi e successivamente per scegliere le misure adeguate.

personali si tratta.

Fase 2

Per ogni elenco delle informazioni creato nella fase 1 per tutti i gruppi di informazioni è necessario chiarire quali conseguenze avrebbe una compromissione dell'oggetto informatico da proteggere. A tal fine, bisogna rispondere almeno alle seguenti quattro domande:

a) Cosa succederebbe se le informazioni venissero rivelate oppure ascoltate da servizi informazioni o organizzazioni simili[6]? (violazione della confidenzialità)

b) Cosa succederebbe se le informazioni non fossero disponibili per un periodo prolungato? (violazione della disponibilità)

c) Cosa succederebbe se le informazioni venissero modificate senza autorizzazione? (violazione dell'integrità)

d) Cosa succederebbe se non fosse completamente chiaro chi ha modificato le informazioni dopo il primo inserimento? (violazione della verificabilità)

Per la classificazione ora è necessario verificare se

a) queste conseguenze potrebbero comportare un pregiudizio della sicurezza delle informazioni o un potenziale danno finanziario secondo i criteri dell'articolo 28 OSIn;

b) leggi e ordinanze (ad es. la legge sugli agenti terapeutici, segreti aziendali ecc.) giustificano o richiedono una necessità di protezione elevata;

c) il/la responsabile della protezione dei dati arriva alla conclusione che esiste un rischio elevato per i diritti fondamentali delle persone interessate secondo l'articolo 22 capoverso 1 LPD[7];

d) le conseguenze per l'organizzazione non sono accettabili[8].

3 Risultati dell'analisi della necessità di protezione

La procedura descritta nel capitolo 2 fornisce un elenco di gruppi di informazioni e possibili conseguenze rilevanti per l'oggetto da proteggere, in cui le possibili conseguenze sono documentate e valutate secondo gli obiettivi di protezione (cioè confidenzialità, integrità, disponibilità, verificabilità, e protezione dei dati).

Il livello di sicurezza (di un oggetto informatico da proteggere) secondo l'articolo 17 LSIn viene valutato sulla base dei seguenti criteri:

a) il livello di sicurezza «protezione di base» si applica se l'oggetto informatico da proteggere non deve essere attribuito a un livello di sicurezza più elevato;

b) il livello di sicurezza «protezione elevata» si applica se almeno in un punto vengono documentate conseguenze notevoli secondo l'articolo 28 capoverso 1 OSIn o vengono trattate informazioni classificate «confidenziale»;

a) il livello di sicurezza «protezione molto elevata» si applica se almeno in un punto vengono documentate conseguenze gravi secondo l'articolo 28 capoverso 2 OSIn o vengono trattate informazioni classificate «segreto».

L'oggetto informatico da proteggere e la sua necessità di protezione vengono inventariati

[6] Per le informazioni classificate si può rispondere alla domanda con l'aiuto del catalogo di classificazione.

[7] Nell'Amministrazione federale per la valutazione viene usato lo strumento per la verifica preliminare dei rischi dell'Ufficio federale di giustizia.

[8] A tal proposito l'organizzazione dovrebbe effettuare una «business impact analysis» e definire i criteri rilevanti per i propri processi operativi.

come «asset».

L'analisi della necessità di protezione deve essere verificata dall'incaricato/a della sicurezza informatica dell'unità amministrativa (ISIU). La verifica comprende, tra l'altro, anche il controllo della plausibilità delle possibili conseguenze documentate e della verificabilità e fondatezza della valutazione. A tale scopo potrebbe essere necessario coinvolgere altri organi rilevanti. Se sono interessati anche dati personali, è necessario coinvolgere il/la responsabile della protezione dei dati. Nell'ambito di progetti e processi operativi è opportuno che l'analisi della necessità di protezione venga approvata dai committenti e dai responsabili dei processi operativi.

4 Ulteriori fasi nella procedura di sicurezza

L'analisi della necessità di protezione valuta se esiste un rischio che deve essere ridotto. Se non vi è una necessità di protezione elevata, per l'organizzazione non vi sono rischi straordinari che richiederebbero un'analisi dei rischi estesa. I requisiti minimi per la sicurezza informatica sono coperti dai requisiti di base (protezione IT di base (Si001)). Questi devono essere attuati per ogni oggetto informatico da proteggere.

Le conseguenze che sono notevoli o gravi per l'organizzazione e portano a una necessità di protezione elevata sono di particolare interesse. Queste devono essere ridotte a un livello accettabile con misure tecniche e organizzative adeguate. Inoltre devono essere attuate le direttive concernenti la necessità di protezione elevata (P042) secondo il piano SIPD. L'interazione tra l'analisi della necessità di protezione, la protezione IT di base e la procedura in caso di necessità di protezione elevata è schematizzata nella figura 1.

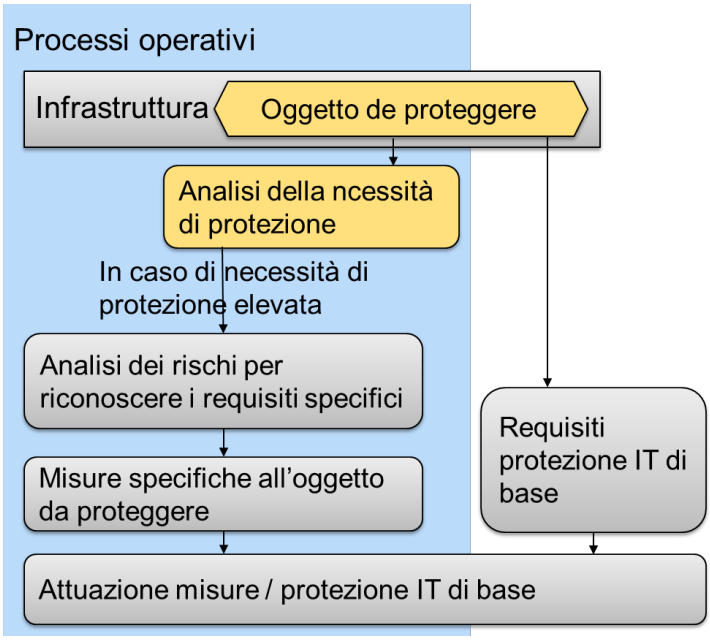

Figura 1: Analisi della necessità di protezione come parte della procedura di sicurezza

Se delle informazioni classificate «confidenziale» o «segreto» vengono trasmesse ad aziende esterne o se delle aziende esterne devono essere coinvolte nello sviluppo, nella gestione, nell'esercizio, nella manutenzione o nella verifica di un oggetto informatico da proteggere con il livello di sicurezza «protezione elevata» o «protezione molto elevata», deve essere avviata una procedura di sicurezza relativa alle aziende secondo l'OPSAz.

Se con l'oggetto informatico da proteggere vengono trattati dati personali, potrebbe essere

necessario creare anche un registro delle attività di trattamento secondo l’articolo 12 LPD e un regolamento sul trattamento secondo l’articolo 6 OPDa (organi federali) o l’articolo 5 OPDa (privati).

Un’analisi della necessità di protezione è un artefatto nei progetti ma anche una parte della documentazione per ogni oggetto informatico da proteggere. Un progetto può contenere vari oggetti informatici da proteggere, quindi non esiste necessariamente una sola analisi della necessità di protezione (di un oggetto informatico da proteggere) per progetto. L’analisi della necessità di protezione deve essere completata già nella prima versione dei progetti. Tuttavia successivamente deve essere portata avanti per la documentazione e deve sempre essere aggiornata.