Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

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

**Segreteria di Stato della politica di sicurezza SEPOS
Servizio specializzato Servizi per la sicurezza delle informazioni
Confederazione**

**Pacchetto di misure per evitare future fughe di dati
Identificata ulteriore necessità di intervento**

Risultati del workshop sulle raccomandazioni in materia di sicurezza delle informazioni del 20 marzo 2024

Sulla base delle raccomandazioni formulate nel rapporto d'inchiesta del 28 marzo 2024 legato all'inchiesta amministrativa sulla fuga di dati, gli incaricati della sicurezza delle informazioni (ISD) della CaF e dei dipartimenti, i fornitori interni di prestazioni dell'Amministrazione federale e i rappresentanti dell'UFCS, dell'UFCL e di armasuisse hanno valutato la necessità di intervento per evitare future fughe di dati, in particolare in relazione ai fornitori, e insieme hanno elaborato delle misure. Il workshop è stato moderato dal servizio specializzato della Confederazione per la sicurezza delle informazioni in seno alla Segreteria di Stato della politica di sicurezza (SEPOS).

Subito dopo quanto accaduto alla società Xplain AG i dipartimenti e le unità amministrative hanno adottato e attuato misure immediate. Inoltre il Consiglio federale ha posto in vigore la nuova legge sulla sicurezza delle informazioni (LSIn) dal 1° gennaio 2024, grazie alla quale sono già state avviate numerose misure che comporteranno un miglioramento sistemico e duraturo in termini di sicurezza. Le misure descritte in seguito rispecchiano la necessità di intervento, individuata in aggiunta ai provvedimenti già adottati o previsti dalla nuova legge.

Attualmente l'Amministrazione federale civile e l'esercito stanno lavorando sull'attuazione della nuova legislazione. Dato che ciò comporta cambiamenti profondi e sistemici nell'attuale gestione della sicurezza della Confederazione, nella fase iniziale il dispendio è notevole. Nei dipartimenti e negli uffici il margine di manovra per adottare misure supplementari senza che vengano messe a disposizione risorse aggiuntive è scarso. Gli ISD dei dipartimenti e della CaF sono concordi nell'affermare che all'attuazione della LSIn vada attribuita la massima priorità.

Le misure vengono suddivise in tre categorie: gestione della sicurezza, formazione e sensibilizzazione nonché comunicazione sicura con terzi.

1.1 Clausole contrattuali standardizzate nei contratti con fornitori

Spesso nella pratica le condizioni generali della Confederazione e le clausole standard relative a minacce in materia di cibersicurezza sono troppo poco specifiche per consentire di definire insieme ai fornitori le esigenze di sicurezza concrete riferite a un mandato specifico. Per questa ragione il DDPS (SG) già nel 2022 ha incaricato di elaborare clausole dettagliate in materia di sicurezza delle informazioni, composte da clausole contrattuali imperative per tutti gli acquisti del DDPS (prescrizioni imperative) e da clausole definite su misura che trovano applicazione a seconda del mandato specifico e delle esigenze in materia di protezione dei dati (prescrizioni potestative). La SEPOS (servizio specializzato della Confederazione per la sicurezza delle informazioni) raccomanderà clausole corrispondenti in conformità all'articolo 10 capoverso 3 OSIn.

Definire queste clausole contrattuali standardizzate si è rivelato difficile poiché ad oggi mancano direttive tecniche in materia di sicurezza necessarie a questo scopo oppure perché talvolta queste direttive sono difficili da attuare per esterni (ad es. protezione di base TIC della Confederazione). Le nuove direttive della Confederazione devono essere definite in maniera tale da essere attuabili nella pratica in linea di principio sia per i fornitori di prestazioni interni della Confederazione sia per fornitori di prestazioni esterni e da poter essere concordate all'interno di contratti. Questa esigenza del resto riguarda anche i Cantoni che sono tenuti ad attuare la protezione IT di base della Confederazione quando accedono a sistemi della Confederazione.

Misura 1:

Il DDPS (SEPOS) è incaricato di elaborare clausole contrattuali standardizzate in materia di sicurezza delle informazioni secondo l'articolo 10 capoverso 3 OSIn entro la fine del 2024.

Misura 2:

Il DDPS (SEPOS) è incaricato di elaborare direttive in materia di sicurezza relative alla collaborazione con i fornitori entro la fine del 2024. Occorre disciplinare ad esempio la conferma della consegna dei dati a organi esterni alla Confederazione nonché la cancellazione regolare e documentata di dati operativi della Confederazione presso i fornitori.

1.2 Inventariazione dei rapporti con i fornitori

Un elemento importante emerso dall'inchiesta amministrativa concernente la fuga di dati verificatasi presso Xplain consiste nella necessità di tenere un sistema attivo ed efficace di gestione dei fornitori. In un'ottica di medio termine i dipartimenti e gli uffici potranno collegare i loro oggetti da proteggere con i loro fornitori all'interno dell'applicazione ISMS e quindi saranno in grado di valutare i relativi rischi e i rapporti di dipendenza. L'Amministrazione federale però non può aspettare due anni per avere una panoramica migliore dei suoi rapporti con i fornitori. Già oggi l'UFCL è in grado di creare su richiesta degli elenchi dei rapporti di natura contrattuale e finanziaria con i fornitori delle unità amministrative.

Misura 3:

Le unità amministrative sono incaricate di completare il loro inventario degli oggetti da proteggere con i fornitori coinvolti entro la fine del 2024. Gli elenchi dei fornitori sono messi a disposizione dal DFF (UFCL).

Misura 4:

Nel quadro della rendicontazione ordinaria 2024 la CaF e i dipartimenti sono incaricati di riferire al DDPS (SEPOS) in merito all'attuazione della misura relativa all'inventariazione dei rapporti con i fornitori.

1.3 Controlli e audit

Gli incaricati della sicurezza delle informazioni dei dipartimenti sono concordi nell'affermare che nel settore degli audit vi è urgente necessità di intervento. Tale necessità non riguarda solo la vigilanza sull'attuazione della sicurezza delle informazioni presso i fornitori, ma anche gli audit interni in materia di sicurezza. Secondo l'articolo 13 OSIn tutte le unità amministrative sono tenute a stabilire all'interno di un piano annuale dei controlli e degli audit le modalità con cui verificare l'attuazione della sicurezza delle informazioni nel loro settore nonché presso terzi. I responsabili della sicurezza degli uffici decidono in merito allo svolgimento di audit. Un acquisto centralizzato sarebbe più efficiente rispetto a una situazione in cui ogni singola unità amministrativa si procura sostegno dall'esterno per svolgere gli audit. L'UFCL dovrà essere incaricato di acquistare prestazioni di audit su richiesta per tutte le unità amministrative. Inoltre l'OSIn prevede che il servizio specializzato della Confederazione per la sicurezza delle informazioni (SEPOS) rilevi il fabbisogno di audit di tutta l'Amministrazione federale e possa svolgere audit direttamente. Lo scopo è fare in modo che gli audit vengano svolti in maniera consolidata e prioritaria a livello di Confederazione presso i fornitori di prestazioni interni ed esterni. Questo riguarda in particolare le imprese sensibili sotto il profilo della sicurezza che vengono sottoposte alla procedura di sicurezza relativa alle aziende. Secondo la LSIn è il Servizio specializzato per la procedura di sicurezza relativa alle aziende della SEPOS a fungere da servizio di riferimento centrale.

Misura 5:

Insieme ai servizi d'acquisto della Confederazione e agli incaricati della sicurezza delle informazioni il DDPS (SEPOS) elabora un piano relativo alle capacità di controllo e di audit tra i fornitori in base all'obbligo legale previsto dalla LSIn e attua questo concetto partendo da un approccio basato sui rischi.

Misura 6:

Il DFF (UFCL) è incaricato di acquistare prestazioni di audit su richiesta per tutte le unità amministrative.

1.4 Applicazione SGSI

Per consentire ai dipartimenti e agli uffici di attuare le nuove direttive nel modo più efficace ed efficiente possibile, in particolare le direttive in materia di SGSI previste dall'ordinanza sulla sicurezza delle informazioni (OSIn), il DFF (UFIT) e il DDPS (SG)

collaborano per quanto riguarda l'acquisto e l'introduzione di un'applicazione SGSI standardizzata grazie alla quale digitalizzare i compiti e i processi previsti dall'OSIn. L'applicazione SGSI dovrà essere pronta nel 2025 per essere introdotta e utilizzata dagli uffici. L'aggiudicazione è stata pubblicata su SIMAP in data 20 marzo 2024.

L'applicazione SGSI consente di sistematizzare e di standardizzare l'inventariazione di informazioni e di sistemi informativi (cosiddetti «oggetti da proteggere»). Grazie all'applicazione SGSI in futuro la partecipazione di terzi (fornitori o Cantoni) verrà rilevata in modo sistematico, verranno valutati i rischi e verranno documentate eventuali misure di sicurezza. In un'ottica di medio termine, il DDPS e il DFF faranno in modo che i dati concernenti i fornitori vengano raccolti attingendo a collezioni di dati già esistenti (principio «once-only»). Fino a quel momento l'UFCL metterà a disposizione gli elenchi in caso di necessità.

Se tutte le unità amministrative utilizzeranno l'applicazione SGSI standardizzata per la propria gestione della sicurezza, sia i dipartimenti sia la SEPOS con un clic potranno avere tra l'altro una panoramica degli oggetti da proteggere, dei fornitori rilevanti sotto il profilo della sicurezza delle informazioni e dello stato di attuazione di direttive e misure. Per questa ragione gli ISD sono favorevoli a un obbligo di acquisto dell'applicazione SGSI per tutte le unità amministrative della Confederazione. Il diritto in materia di sicurezza delle informazioni della Confederazione dovrà essere integrato con una norma in tal senso in un punto appropriato.

Misura 7:

Il DDPS (SEPOS) è incaricato di verificare entro la metà del 2025 se le unità amministrative (CaF, dipartimenti e uffici) dovranno essere obbligate a utilizzare l'applicazione SGSI standardizzata della Confederazione per la loro gestione della sicurezza, non appena questa sarà disponibile.

2.1 Concetto di formazione per le esigenze in materia di formazione specifiche alla funzione

Durante l'analisi di incidenti legati alla sicurezza si riscontra regolarmente che i collaboratori di tutti i livelli non conoscono le direttive esistenti oppure non le applicano con sistematicità. Un esempio è costituito dall'articolo 11 dell'ordinanza sulla trasformazione digitale e l'informatica che disciplina l'accesso ai dati per i fornitori esterni di prestazioni. Misure di formazione e di sensibilizzazione adottate dopo che si è verificato un incidente spesso sono costose e di solito non comportano un miglioramento duraturo in termini di sicurezza. Per questa ragione le misure di formazione devono far parte di un piano sovraordinato e durevole la cui attuazione ed efficacia devono essere misurate.

Il DDPS dovrà essere incaricato di definire, entro la fine del 2024, le esigenze in materia di formazione per le rispettive categorie di persone (ad es. responsabili di applicazioni, responsabili di progetto, ruoli di progetto come RSIPD, dirigenti, collaboratori in generale, responsabili e incaricati della sicurezza delle informazioni ecc.) all'interno di un concetto di formazione in collaborazione con la CaF e con i dipartimenti e di elaborare uno scadenzario per lo svolgimento delle misure di formazione. In tale contesto assicura che venga verificata l'efficacia delle misure di formazione.

Misura 8:

Il DDPS (SEPOS) è incaricato di definire le esigenze in materia di formazione specifiche alla funzione all'interno di un concetto di formazione entro la fine del 2024 in collaborazione con la CaF e i dipartimenti e di elaborare uno scadenzario per lo svolgimento delle misure di formazione. In tale contesto il servizio specializzato assicura che venga verificata l'efficacia delle misure di formazione.

Per una comunicazione sicura al livello «confidenziale» l'Amministrazione federale ha a disposizione il servizio standard CVC o «Threema». Tuttavia l'Amministrazione federale si trova a fare i conti con la mancanza di strumenti idonei per svolgere in sicurezza videoconferenze di gruppo tra i singoli dipartimenti o con partner al livello «confidenziale» o addirittura «segreto». Durante la pandemia ad esempio è emersa in modo chiaro l'esigenza di disporre di un sistema sicuro per videoconferenze. Le autorità federali devono essere in grado di comunicare in sicurezza tra di loro e con partner dei Cantoni o del settore industriale nonché con partner internazionali (dati, lingua, immagini e video). Per questa ragione, nel quadro dei servizi standard a metà 2024 con il progetto Secure Video Conferencing Service la CaF metterà a disposizione una soluzione basata su Webex per garantire una comunicazione via video sicura (fino al livello dati personali degni di particolare protezione).

Misura 9:

Previa consultazione della Conferenza degli incaricati della sicurezza, la CaF è incaricata di presentare alla Conferenza dei segretari generali (CSG) una panoramica dei mezzi di comunicazione disponibili e del loro utilizzo per i rispettivi livelli di classificazione, in particolare con terzi, entro la fine del 2024.

Berna, 3 aprile 2024