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

26 giugno 2024

Rapporto sulla sicurezza informatica della Confederazione nel 2023

Indice

1 Introduzione

In virtù dell'ordinanza sui ciber-rischi (OCiber, art. 11 cpv. 2)[1], determinante per il periodo in esame, all'Ufficio federale della cibersicurezza (UFCS) spetta informare il Consiglio federale sullo stato della sicurezza informatica della Confederazione a fine 2023. In seguito all'entrata in vigore della nuova legge sulla sicurezza delle informazioni, a partire dal periodo di riferimento 2024 tale compito passa alla Segreteria di Stato della politica di sicurezza (SEPOS) (cfr. al punto 5.2.2).[2]

Il rapporto si basa su un sondaggio strutturato sullo stato della sicurezza informatica condotto tra tutti gli incaricati della sicurezza delle informazioni dei dipartimenti e della Cancelleria federale, di cui si è tenuto conto unitamente agli avvisi e ai rapporti in materia di sicurezza dei fornitori di prestazioni interni all'Amministrazione. Alla luce di questi dati l'UFCS valuta la sicurezza delle informazioni in seno alla Confederazione.

Il 2023 è stato caratterizzato da ciberincidenti che hanno avuto un forte impatto sull'Amministrazione federale. Tra i principali si annoverano gli attacchi del gruppo hacktivista filorusso «NoName057(16)» contro la disponibilità dei mezzi informatici dell'Amministrazione federale, le fughe di dati presso alcuni fornitori di servizi della Confederazione (in particolare presso la società Xplain AG) e vari incidenti legati alla sicurezza ai danni di provider di servizi cloud della Confederazione. Per fare luce sulla fuga di dati nel caso Xplain AG, il Consiglio federale ha avviato un'inchiesta amministrativa, da cui sono scaturite varie raccomandazioni su come evitare simili incidenti in futuro. Il presente rapporto non contiene un'analisi delle possibili misure in tale ambito, essendo la pubblicazione della suddetta inchiesta amministrativa antecedente alla sua stesura.

Il secondo capitolo illustra la situazione attuale della sicurezza informatica nell'Amministrazione federale nel 2023, l'organizzazione della sicurezza informatica in seno all'Amministrazione federale e i risultati del sondaggio sui requisiti di compliance relativi alle documentazioni di sicurezza.

Il terzo capitolo presenta i principali incidenti legati alla sicurezza subiti dall'Amministrazione federale nel corso dell'ultimo anno.

Nel quarto capitolo vengono riportate le principali attività e misure sia all'interno che all'esterno dell'Amministrazione federale.

Il quinto e ultimo capitolo contiene un riepilogo dei principali risultati emersi dal rapporto e un breve sguardo alle prospettive future.

2 Stato della sicurezza informatica nell'Amministrazione federale

I rischi e i conseguenti tentativi di attacco ai danni dei sistemi informatici dell'Amministrazione federale, nonché di quelli dei fornitori esterni, sono in costante aumento, anche e soprattutto a causa della situazione geopolitica attuale.

Gli incidenti avvenuti nel 2023 hanno evidenziato, tra i vari aspetti, quanto la gestione dei fornitori sia importante ai fini della cibersicurezza: la governance dei dati a livello federale è

[1] Ordinanza del 27 maggio 2020 sulla protezione contro i ciber-rischi nell'Amministrazione federale (ordinanza sui ciber-rischi, OCiber), RU 2023 735, sostituita il 1° gennaio 2024 dall'ordinanza sulla sicurezza delle informazioni (OSIn; RS 128.1),.

[2] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-98807.html

deficitaria e vi sono lacune nella mappatura dei rapporti commerciali con i partner esterni. In passato era solo limitatamente possibile verificare la cibersicurezza dei fornitori e dei loro rispettivi software. Per entrambi la responsabilità dell'allestimento dei contratti e del collaudo dei prodotti è decentralizzata nelle mani dell'unità amministrativa appaltante, per cui manca uno standard uniforme in materia di sicurezza.

Nel caso di un incidente da gestire a più livelli statali – come nel caso Xplain AG – si è inoltre constatato che a livello di Amministrazione federale i processi necessari erano più o meno rodati, mentre a livello cantonale dovevano ancora essere consolidati.

Gli incidenti che hanno caratterizzato l'anno in esame 2023 hanno evidenziato come la compliance, da sola, non possa garantire la cibersicurezza. I responsabili degli oggetti da proteggere devono acquisire ulteriori competenze in materia di cibersicurezza, affinché siano in grado anche di valutare e implementare correttamente le misure necessarie ai fini della compliance (cfr. capitolo 4.3.2).

2.1 Organizzazione della sicurezza informatica nell'Amministrazione federale

La sicurezza informatica nell'Amministrazione federale comprende tutte le misure necessarie per impedire nonché individuare e gestire il più rapidamente possibile i ciberincidenti. Per ciberincidente s'intende, ai sensi dell'articolo 5 lettera d della revisione del 29 settembre 2023[3] della legge sulla sicurezza delle informazioni (LSIn), un «evento che si verifica nell'utilizzo di mezzi informatici e che compromette la confidenzialità, la disponibilità o l'integrità delle informazioni o la tracciabilità del loro trattamento».

Affinché le misure necessarie a garantire la sicurezza informatica vengano attuate nell'intera Amministrazione federale, il Consiglio federale emana le pertinenti ordinanze e istruzioni. Sinora l'elaborazione delle direttive in materia di sicurezza informatica è stata di responsabilità del Centro nazionale per la cibersicurezza (NCSC), che in data 1° gennaio 2024 è stato trasferito all'Ufficio federale della cibersicurezza (UFCS) in seno al DDPS. L'elaborazione delle direttive in materia di protezione delle informazioni, invece, era sinora di competenza della Segreteria generale del DDPS (SG-DDPS). In futuro tali direttive saranno riunite ed emanate dal servizio specializzato per la sicurezza delle informazioni in seno alla Segreteria di Stato della politica di sicurezza (SEPOS).[4]

Le unità amministrative sono responsabili del rispetto e dell'attuazione delle direttive in materia di sicurezza informatica nella loro rispettiva sfera di competenza. A tal fine verificano regolarmente i loro oggetti informatici da proteggere[5], definiscono le misure di sicurezza necessarie e le adottano.

[3] FF 2023 2296 (testi sottoposti a referendum)

[4] https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-98807.html

[5] Si tratta di applicazioni, servizi, sistemi, reti, collezioni di dati, infrastrutture e prodotti informatici; più oggetti identici o connessi tra loro possono essere raggruppati in un solo oggetto informatico da proteggere (art. 3 lett. h OCiber).

2.2 Risultati relativi ai requisiti di compliance delle documentazioni di sicurezza

Per l'81,8 per cento dei 2176 oggetti da proteggere complessivamente censiti sono presenti documentazioni di sicurezza valide. Nel 2023 le misure di sicurezza risultanti e i relativi controlli sono stati documentati per il 74,4 per cento degli oggetti da proteggere (anno precedente: 72,5%).

Affinché le misure di sicurezza possano essere implementate con efficacia, i documenti sulla sicurezza necessari devono essere aggiornati (possono risalire al massimo a cinque anni prima). Ciò è stato accertato per il 92 per cento dell'81,8 per cento delle documentazioni di sicurezza valide sopraccitate. Questo valore è calato solo marginalmente rispetto al 92,6 per cento dello scorso anno, dal momento che – rispetto al 2022 – nel 2023 molti documenti sono giunti al termine del periodo di validità di cinque anni. Entrati in vigore nel 2018, i dipartimenti hanno ora difficoltà ad aggiornarli contemporaneamente. Ciò nonostante i numeri confermano all'UFCS che il censimento degli oggetti da proteggere e l'adozione delle misure di sicurezza da parte delle unità amministrative sono rimasti a un livello comparabile a quello dell'anno precedente.

In generale, le cifre comunicate erano e sono tuttora troppo basse e segnalano la presenza di un problema a livello di compliance. Da esse, inoltre, non è possibile stabilire a livello globale se la qualità dei documenti di sicurezza informatica sia stata sufficientemente controllata e se i medesimi siano anche stati realmente sottoposti a un'analisi critica. Anche una documentazione aggiornata, infatti, non garantisce che le misure di sicurezza siano state implementate e controllate a dovere. L'UFCS non ha alcuna opportunità di verifica in merito. Occorrerà considerare eventuali nuove possibilità nell'ambito della legge sulla sicurezza delle informazioni.

3 Incidenti legati alla sicurezza

Gli incidenti legati alla sicurezza possono avere gravi conseguenze, come la diffusione di informazioni riservate, sabotaggi, ricatti o guasti a sistemi critici. Qui di seguito vengono riportati gli incidenti che nell'anno in esame 2023 hanno avuto una grande rilevanza per l'Amministrazione federale.

3.1 Attacchi DDoS

Gli attacchi DDoS (Distributed Denial of Service) sono attacchi ai danni delle risorse di rete, fino a raggiungere il server bersaglio, in cui criminali o attori statali sfruttano i limiti di capacità intrinseci a ciascuna di esse. L'obiettivo è di compromettere la disponibilità della risorsa attaccata, inviandole un gran numero di richieste al fine di sovraccaricarne la capacità di elaborazione. Nel momento in cui il numero di richieste supera il limite di capacità della risorsa in questione, le reazioni si fanno molto più lente del solito o alcune richieste degli utenti rimangono senza risposta.

3.1.1 Attacco DDoS del gruppo «NoName057(16)» ai danni dell'Amministrazione federale

A partire dal 7 giugno 2023 un gruppo di hacktivisti filorussi chiamato «NoName057(16)» ha sferrato una serie di attacchi DDoS ai danni di vari obiettivi selezionati della Svizzera. Il primo a essere colpito è stato il sito web del Parlamento (www.parlament.ch). Il gruppo ha motivato

gli attacchi con l'imminente discorso del Presidente ucraino Volodymyr Zelensky e il dibattito sulle esportazioni di armi nel Parlamento svizzero.

Gli attacchi sono continuati per circa due settimane colpendo diversi obiettivi, dopodiché il 19 giugno il gruppo ha rivolto la sua attenzione all'estero.

Obiettivi	Data						
	12.06.2023	13.06.2023	14.06.2023	15.06.2023	16.06.2023	17.06.2023	18.06.2023
Amministrazione federale	4	1		1		2	
Cantoni			2		3		
Città			6				6
Servizio pubblico	2		1	1			1
Aeroporti		8				6	
Settore finanziario				5		2	1
Altro				1	3		
Armamenti				1			
Totale 57	**6**	**9**	**9**	**9**	**6**	**10**	**8**

Tabella: Elenco degli attacchi DDoS andati a buon fine al giorno

La portata degli attacchi è stata tale da mettere in difficoltà tutte le organizzazioni colpite. Per debellarli, è stata necessaria una notevole mole di lavoro da parte dell'Amministrazione federale.

L'Amministrazione federale si adopera per garantire che, in caso di attacco DDoS, le applicazioni interne continuino a funzionare anche se i sistemi accessibili dall'esterno sono sovraccarichi e non riescono più a rispondere correttamente alle richieste. In questo caso non è stato così. Sistemi interni importanti dipendevano da servizi di sistemi esterni, il che alla fine ha comportato una limitazione del lavoro per alcune ore. Nel mese di novembre del 2023 l'NCSC ha pubblicato un rapporto di analisi dettagliato sugli attacchi DDoS (cfr. allegato).[6]

Ad avere conseguenze decisamente più gravi degli attacchi DDoS, tuttavia, sono gli attacchi ransomware ai danni di aziende e autorità, di cui si parlerà più in dettaglio al capitolo 3.2 successivo.

3.2 Attacchi ransomware

Un attacco ransomware è un ciberincidente in cui i dati e i file della vittima vengono rubati e crittografati. Successivamente gli aggressori chiedono un riscatto sia per decriptare i dati sia per rinunciare alla divulgazione degli stessi («double extorsion», in italiano doppia estorsione). Se non viene pagato il riscatto, la vittima rischia che i dati che le sono stati trafugati vengano pubblicati sul darknet. Gli attacchi ransomware possono colpire non solo aziende o autorità, ma anche privati, i cui dati rientrano spesso tra i danni collaterali di questi attacchi.

3.2.1 Incidente ai danni della società Xplain AG

L'attacco ransomware ai danni della società Xplain AG, un importante fornitore di servizi di

[6] https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte/fachberichte/ddos-bericht-6-2023.html

varie unità amministrative e Cantoni, ha causato la fuga di ingenti quantità di informazioni, per un totale di 431 GB. In essi erano contenuti 146 623 file e 19 863 cartelle. Coinvolti nell'attacco vi erano anche dati personali e classificati, provenienti in particolare dall'area della sicurezza interna. Gli aggressori hanno divulgato i dati sul darknet, per cui sono diventati di dominio pubblico. La pubblicazione di dati riservati e rilevanti per la sicurezza ha gravi conseguenze e comporta un enorme dispendio di lavoro e di costi. Oltre alla necessità di individuare e attuare misure d'urgenza per contenere i rischi immediati e informare le persone interessate, si è dovuto anche valutare se i sistemi e i database dell'Amministrazione federale fossero stati compromessi.

L'incidente ha impedito l'utilizzo temporaneo di sistemi importanti. Si è inoltre reso imprescindibile un grande dispiego di personale per individuare in via definitiva quali uffici fossero clienti di Xplain AG, quale fosse la natura dei rapporti contrattuali, quali diritti di verifica fossero stati definiti e quale fosse la durata dei contratti.

Il primo passo consiste in un'analisi a 360 gradi dell'incidente. In data 1° maggio 2024 il Consiglio federale ha pubblicato gli esiti dell'inchiesta amministrativa, a cui ha fatto seguito lo stesso giorno il rapporto a cura dell'incaricato federale della protezione dei dati.
Nel rapporto dell'inchiesta amministrativa si afferma che negli ultimi anni sono stati pochi i casi in cui dati produttivi della Confederazione sono stati trasferiti attivamente all'ambiente informatico di Xplain AG. Ciò avveniva durante le fasi di test e integrazione di un software o nell'ambito di servizi di manutenzione o supporto, sia ad opera del personale di Xplain AG in possesso di un account di posta elettronica della Confederazione che da parte di dipendenti della Confederazione. Inoltre, una funzione di supporto presente in alcune applicazioni di Xplain, e nel frattempo disattivata, ha provocato il trasferimento di grandi volumi di dati dall'ambiente informatico della Confederazione a quello della società. Alla luce del rapporto il Consiglio federale ha definito una serie di misure per impedire future fughe di dati, le quali sono state inserite in un apposito pacchetto di misure (cfr. capitolo 5.2.1).

Il Centro nazionale per la cibersicurezza (NCSC) ha coordinato la gestione dell'incidente, definito le misure di ripristino della sicurezza dei sistemi ed effettuato, con il supporto di risorse interne ed esterne all'Amministrazione federale, un'analisi completa di tutti i dati pubblicati. Quale contributo all'elaborazione dell'incidente e alla creazione della massima trasparenza possibile, ha pubblicato un rapporto sulla procedura e sui risultati dell'analisi dei dati.[7]

Questo attacco ransomware ai danni della società Xplain AG è un caso esemplare di come la quantificazione del danno causato da una fuga di dati possa in brevissimo tempo diventare molto complessa. Questo enorme impegno, tuttavia, si sarebbe potuto evitare se si fosse saputo sin dall'inizio quali dati fossero in possesso del fornitore e chi fosse cliente di Xplain AG. Ci si è resi conto, inoltre, che la gestione degli incidenti su più livelli statali non è standardizzata: se nell'Amministrazione federale i processi erano più o meno rodati, a livello dei Cantoni li si doveva ancora consolidare. Alla luce di questa esperienza si sta ora definendo una procedura standard e una classificazione uniforme della gravità degli incidenti. I controlli effettuati in fase di collaudo al software fornito, inoltre, erano stati insufficienti. Nessuno si era reso conto, ad esempio, che la funzione di segnalazione degli errori inviava dati sensibili a Xplain AG.

[7] https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte/fachberichte/bericht-datenanalyse-xplain.html

3.2.2 Altri incidenti analoghi a quello di Xplain AG

3.2.2.1 Attacco ransomware ai danni di arb Architekten AG

In data 21 luglio 2023 l'Ufficio federale delle costruzioni e della logistica (UFCL) è stato informato di un attacco ai danni del suo fornitore arb Architekten AG. Il collettivo ransomware «Abyss» aveva sottratto circa 220 GB di dati non compressi, tra cui piani edilizi di ambasciate e residenze svizzere all'estero, e li aveva pubblicati in forma crittografata sul darknet. L'azienda è riuscita a ripristinare i dati criptati e ha sporto denuncia. Scaduto il termine di pagamento del riscatto il 1° settembre 2023, è stata pubblicata la chiave per decriptare i documenti trafugati.

3.2.2.2 Incidente ai danni della società Concevis AG

In data 14 novembre 2023 un'altra software house svizzera, Concevis AG, è caduta vittima di un attacco ransomware. Gli aggressori hanno crittografato tutti i server dell'azienda e rubato i dati, tra cui presumibilmente anche dati operativi dell'Amministrazione federale. Informati rapidamente i servizi interessati, si sono adottate le prime misure per minimizzare il rischio di sicurezza per l'Amministrazione federale. Le applicazioni sviluppate da Concevis sono gestite da fornitori di prestazioni dell'Amministrazione federale. Attualmente è improbabile che possa esservi una compromissione dei sistemi della Confederazione. Ad oggi le conseguenze dell'attacco non sono ancora del tutto note.

3.3 Problemi di sicurezza ai danni di provider di servizi cloud

Errori di configurazione e lacune di sicurezza presso i provider di servizi cloud possono essere causa di fughe di dati e attacchi. La presenza di lacune di sicurezza non colmate e di configurazioni errate negli ambienti cloud, infatti, può essere sfruttata dagli aggressori per infiltrarsi nei sistemi. Sebbene i due problemi di sicurezza illustrati in questo capitolo non abbiano ancora avuto conseguenze dirette sull'Amministrazione federale, potrebbero potenzialmente minare la fiducia della popolazione nei confronti delle soluzioni cloud utilizzate dalla Confederazione. È imperativo che si faccia tesoro di quanto appreso da questi incidenti quando si concepiscono le misure di sicurezza per le soluzioni cloud.

3.3.1 Diffusione di malware tramite Microsoft Teams

L'Amministrazione federale ha constatato che in Microsoft Teams gli utenti esterni possono inviare via chat ai dipendenti della Confederazione degli allegati, per i quali Microsoft Teams non verifica automaticamente l'assenza di codici nocivi. In un test il Computer Security Incident Response Team (CSIRT) dell'Ufficio federale dell'informatica (UFIT) ha riscontrato che il file viene riconosciuto e cancellato dall'antivirus presente sui dispositivi della Confederazione soltanto al momento del salvataggio. Ciò significa che, a differenza della prassi odierna, quando i dipendenti federali utilizzano Teams non hanno una seconda linea di difesa contro i malware. Pertanto, in questi casi, la protezione dei dispositivi della Confederazione dipende esclusivamente dall'antimalware locale.

3.3.2 Incidente Storm-0558 nel cloud di Microsoft

In data 11 luglio 2023 Microsoft ha pubblicato sul blog due post in cui comunicava che un'autorità federale statunitense aveva rilevato una serie di attacchi andati a buon fine ai danni delle caselle di posta elettronica di Exchange Online e Outlook.com, nel frattempo comunque bloccati. Tali attacchi sono stati attribuiti a un gruppo di hacker cinesi, presumibilmente di stampo governativo, noto come «Storm-0558». Dall'11 maggio 2023 gli aggressori avevano avuto accesso alle e-mail di circa 25 autorità, perlopiù europee, ed erano anche riusciti ad

infiltrarsi in vari account di posta elettronica privati appartenenti al personale di queste autorità. Servendosi di una chiave di firma rubata, gli hacker erano riusciti a contraffare i token di autenticazione[8] utilizzati per l'accesso. Con questo sistema avrebbero potuto compromettere anche altri servizi del cloud M365[9]. Questi attacchi sono stati scoperti il 16 giugno 2023, dopodiché Microsoft ha provveduto a eliminare le vulnerabilità sfruttate. L'Amministrazione federale non è stata interessata dall'attacco.
L'incidente mette tuttavia in luce quanto sia complesso, anche per una grande azienda, garantire una gestione sicura delle chiavi, e ha confermato la decisione dell'Amministrazione federale di non utilizzare le soluzioni di crittografia offerte da Microsoft Cloud.

4 Attività e misure

4.1 Programmi «bug bounty»

Nel periodo di riferimento 2023, l'NCSC ha svolto programmi «bug bounty» per singoli servizi e applicazioni per conto di svariate unità amministrative. Nell'estate del 2023, inoltre, l'NCSC ha lanciato e a mano a mano messo a punto il proprio programma «bug bounty» che, a partire da settembre 2023, ha consentito agli hacker etici di cercare e segnalare le vulnerabilità di tutti i sistemi pubblicamente esposti (*.admin.ch) dell'Amministrazione federale.

Nei mesi di settembre e ottobre 2023, l'NCSC ha ricevuto nell'arco di dieci giorni ben 134 segnalazioni di vulnerabilità individuate nei sistemi pubblicamente esposti dell'Amministrazione federale. A seguito di un'analisi tecnica, 98 di esse sono state classificate come vulnerabilità valide. Le lacune in materia di sicurezza hanno riguardato tutti i dipartimenti e la Cancelleria federale.

I risultati ottenuti sinora con il programma «bug bounty» dell'NCSC dimostrano che non tutte le lacune di sicurezza presenti in sistemi e applicazioni hanno potuto essere identificate mediante le misure di sicurezza esistenti. Le oltre 100 vulnerabilità segnalate nell'arco di dieci giorni dimostrano quanto sia urgente che in futuro l'Amministrazione federale continui a investire nel programma «bug bounty» dell'NCSC (oggi UFCS), ampliandolo ulteriormente. Così facendo, la Confederazione avrà la possibilità di agire in maniera proattiva, eliminando i potenziali rischi per la sicurezza dei propri sistemi informatici prima che i medesimi vengano sfruttati dagli aggressori. Il programma «bug bounty» dell'UFCS, inoltre, contribuisce in maniera determinante a incrementare la ciberresilienza dell'Amministrazione federale. Le conseguenze derivanti da componenti informatici dell'Amministrazione federale configurati in modo errato o non adeguato possono ripercuotersi gravemente sulla sicurezza e sull'integrità di sistemi, applicazioni o reti.

4.2 Misure di formazione

4.2.1 Campagna nazionale di sensibilizzazione alla cibersicurezza S-U-P-E-R

Nel 2023 la Prevenzione Svizzera della Criminalità (PSC) e l'NCSC, insieme ai corpi di polizia

[8] L'autenticazione basata su token è un modo per confermare l'identità di un utente o di un dispositivo.

[9] Microsoft 365 (M365) è un servizio cloud di Microsoft comprendente una serie di applicazioni di produttività e strumenti di collaborazione per le aziende.

cantonali e comunali, hanno organizzato la terza campagna nazionale di sensibilizzazione S-U-P-E-R (www.s-u-p-e-r.ch) sul tema della cibersicurezza. Oltre ai corpi di polizia cantonali e comunali, anche l'Amministrazione federale con i dipartimenti DFI, DFF, DFAE e DEFR ha contribuito alla divulgazione dei contenuti della campagna. Internamente ai dipartimenti le campagne sono state pubblicizzate tramite intranet, e-mail e manifesti.

Dall'analisi della campagna effettuata a novembre 2023 è risultato che il progetto, con la homepage dedicata ogni volta a nuovo argomento, le pagine interattive[10] e il quiz a video, è stato un successo. Degno di nota, in particolare, è l'ampio sostegno alla campagna da parte dei corpi di polizia, dei singoli dipartimenti dell'Amministrazione federale e dei Comuni. Gli aspetti positivi emersi nel 2023 confluiranno nella progettazione della campagna S-U-P-E-R finale del 2024.

4.2.2 Corsi per esperti

Nel 2023 l'NCSC ha organizzato tre corsi per esperti online sui temi «Tecnologie di sicurezza per il cloud computing», «End-to-End Encrypted (E2EE) Messaging» e «Sicurezza DNS», rivolti al personale dell'Amministrazione federale. Al primo corso hanno partecipato circa 140 dipendenti, al secondo e al terzo circa 110 ciascuno. I corsi per esperti sono facoltativi e offrono ai partecipanti la possibilità di valutare meglio problematiche specifiche di rilievo per la sicurezza e/o condividere le nuove competenze acquisite all'interno dell'Amministrazione federale. Sono un elemento formativo di fondamentale importanza per aumentare in maniera economicamente sostenibile le conoscenze sulla sicurezza degli specialisti informatici.

4.2.3 Corso per il personale sulla sicurezza informatica (compliance)

Per poter affrontare direttamente le domande sulla sicurezza informatica che potrebbero emergere tra i collaboratori delle diverse unità amministrative, l'Amministrazione federale dispone, a livello di dipartimento e di Cancelleria federale, di incaricati della sicurezza delle informazioni dei dipartimenti (ISID) e, a livello di ufficio, di incaricati della sicurezza delle informazioni delle unità amministrative (ISIU). Sotto la loro guida, nel 2023 circa il 94 per cento (stessa percentuale dell'anno precedente) dei nuovi collaboratori è stato istruito in merito alle tematiche di rilevanza per la sicurezza informatica. Questo valore non arriva mai al 100% per cento, perché c'è sempre del personale che viene assunto sul finire dell'anno e che non ha ancora avuto il tempo di completare il modulo «Sicurezza delle informazioni nell'Amministrazione federale». Altri motivi sono le assenze per malattia o gli account utente del personale esterno che non hanno accesso al modulo.

[10] Le pagine interattive vengono utilizzate spesso e volentieri per incrementare la user experience.

4.3 Sfide nel campo della formazione

4.3.1 Corsi per fornitori di servizi esterni

Vari dipartimenti segnalano di avere un problema di fondo a sensibilizzare adeguatamente il personale esterno o i fornitori di servizi in merito alla sicurezza informatica. All'atto dell'assunzione e durante il periodo di prova i dipendenti interni della Confederazione devono obbligatoriamente frequentare corsi di e-learning specifici sulla sicurezza informatica. Questa regola, invece, non vale per i dipendenti esterni e non sempre è applicabile a titolo generale per motivi di ordine tecnico, ad esempio perché i collaboratori esterni non dispongono di un dispositivo della Confederazione e/o di un accesso al Web Based Training (WBT). Alcuni uffici hanno comunicato l'introduzione di processi per poter formare e perfezionare i collaboratori esterni in modo mirato.

Ci si è resi conto, inoltre, che la documentazione di gara e le condizioni contrattuali per i fornitori di servizi esterni devono essere integrate con aspetti relativi alla formazione o al perfezionamento, in modo tale che l'Amministrazione federale possa esigere che i collaboratori esterni dispongano di conoscenze in materia di sicurezza informatica o possano essere istruiti in base alla loro funzione e al loro livello.

4.3.2 Formazione dei responsabili degli oggetti da proteggere

Dalle segnalazioni emerge che il ruolo del responsabile degli oggetti da proteggere[11] richiede in alcuni casi maggiori competenze specialistiche, in termini di valutazione e attuazione della documentazione di sicurezza informatica, rispetto a quelle che in realtà possiedono le persone designate quali responsabili degli oggetti da proteggere. Per allinearsi, occorre che siano supportati più da vicino dagli incaricati della sicurezza informatica delle unità amministrative (ISIU) oppure, se possibile, formati o sostituiti in maniera opportuna.

5 Conclusioni e prospettive future

5.1 Risultati

Oltre alle misure finalizzate a una gestione sicura dei dati e a una buona «ciberigiene», l'UFCS raccomanda in generale che i dati vengano condivisi con terzi soltanto nella misura minima necessaria, in forma possibilmente anonimizzata. Tutte le divisioni devono verificare il grado di criticità dei loro rapporti di dipendenza da fornitori e servizi e, in base a tale verifica, stabilire tramite contratto – soprattutto in caso di criticità elevata – un diritto di verifica presso fornitori o operatori di servizi e un obbligo di segnalazione degli incidenti. Il contratto deve inoltre contenere indicazioni su come procedere con i dati che non avrebbero dovuto giungere fino al fornitore di servizi.

È altresì fondamentale prevedere ulteriori misure tecniche per la protezione proattiva e il monitoraggio dei propri sistemi, al fine di poter adottare le dovute contromisure in caso di irregolarità. Ciò implica anche il fatto che i canali di collegamento e comunicazione tra i fornitori e le proprie organizzazioni siano protetti al meglio. La pianificazione d'emergenza dev'essere

[11] Per l'oggetto da proteggere dev'essere definita una persona (all'interno dell'UA di competenza) che funga da suo responsabile. Tale persona ha il compito di attuare questa prescrizione. Dev'essere consapevole della propria responsabilità ed essere tecnicamente in grado anche di assumersi tale responsabilità.

costantemente aggiornata e testata. Gli scenari di esercitazione dovrebbero tenere conto anche dei rapporti con i fornitori e degli effetti indiretti delle fughe di dati.

5.2 Prospettive future

5.2.1 Misure annunciate per il 2024

Per il 2024 il Consiglio federale ha deliberato un pacchetto di misure per il rafforzamento della sicurezza informatica, prevedendo di intensificare ulteriormente le attività in tal senso.

Il pacchetto di misure si concentra su tre aree:

- in primo luogo verrà rafforzata la gestione della sicurezza, tra l'altro definendo entro la fine del 2024 ulteriori prescrizioni di sicurezza per la collaborazione con i fornitori. Dovrà inoltre essere rafforzata anche la capacità di controllo e verifica.
- In secondo luogo, entro la fine del 2024 verrà elaborato un piano di formazione specifico per le diverse funzioni con l'obiettivo di istruire e sensibilizzare il personale sulle prescrizioni di sicurezza vigenti.
- In terzo luogo, entro la fine del 2024 verrà stilato un compendio dei mezzi di comunicazione a disposizione delle autorità federali.

In questo modo l'Amministrazione federale risponde agli incidenti legati alla sicurezza avvenuti nel 2023.

Per rafforzare la sicurezza informatica a breve e medio termine, i dipartimenti e la Cancelleria federale continueranno a lavorare per mantenere aggiornata la documentazione di sicurezza e adottare le misure richieste in modo tempestivo. L'UFCS raccomanda di concentrarsi nello specifico sull'implementazione delle misure, essendoci a volte un disallineamento tra la documentazione e l'implementazione effettiva.

5.2.2 Modifica relativa alla redazione dei futuri rapporti

A partire dall'anno di riferimento 2024 spetta al servizio specializzato della Confederazione per la sicurezza delle informazioni in seno alla SEPOS redigere annualmente il rapporto, all'attenzione del Consiglio federale, sullo stato della sicurezza delle informazioni della Confederazione, secondo al capoverso 1 articolo h LSIn[12].

[12] RS 128 - Legge federale del 18 dicembre 2020 concernente... | Fedlex (admin.ch)