Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC
Sicurezza informatica della Confederazione

13 aprile 2022

Rapporto sulla sicurezza informatica della Confederazione nel 2021

Indice

1 Organizzazione della sicurezza informatica nell'Amministrazione federale

La sicurezza informatica nell'Amministrazione federale comprende tutte le misure necessarie per evitare ciberincidenti. Si tratta di eventi non intenzionali o provocati intenzionalmente da persone non autorizzate che compromettono la confidenzialità, l'integrità, l'accessibilità o la tracciabilità di dati o che possono causare disfunzioni.[1]
A tal fine il Consiglio federale emana ordinanze e istruzioni concernenti la protezione dell'Amministrazione federale contro i ciber-rischi, mentre il delegato alla cibersicurezza emana direttive in materia di sicurezza informatica.
Inoltre, il Comitato per la sicurezza informatica (C-SI) è l'organo consultivo del Centro nazionale per la cibersicurezza (NCSC) per tutte le questioni inerenti alla sicurezza informatica nell'Amministrazione federale.

Le unità amministrative devono provvedere alla protezione dei loro sistemi informatici, delle loro applicazioni e dei loro dati (oggetti da proteggere). Esse esaminano regolarmente gli oggetti da proteggere e adottano le necessarie misure di sicurezza. Garantiscono inoltre il rispetto e l'attuazione delle direttive in materia di sicurezza informatica, delle procedure di sicurezza nonché delle decisioni del Consiglio federale, dell'NCSC e dei dipartimenti o della Cancelleria federale nel loro settore di competenza.

2 Stato attuale della sicurezza informatica nell'Amministrazione federale

In virtù dell'articolo 11 capoverso 2 dell'ordinanza del 27 maggio 2020 sulla protezione contro i ciber-rischi nell'Amministrazione federale (ordinanza sui ciber-rischi, OCiber; RS *120.73*), il delegato alla cibersicurezza informa regolarmente il Dipartimento federale delle finanze (DFF), all'attenzione del Consiglio federale, sullo stato della sicurezza informatica nei dipartimenti e nella Cancelleria federale. A tal fine, redige annualmente il «rapporto sulla sicurezza informatica della Confederazione».
Vi fungono da base i rapporti dei dipartimenti, dei Servizi del Parlamento e della Cancelleria federale (art. 13 cpv. 1 OCiber; autodichiarazione basata su un sondaggio strutturato), le esperienze e i risultati dell'NCSC, come pure le notifiche e i rapporti sulla sicurezza del fornitore di prestazioni interno all'Amministrazione federale.

In sintesi, fondandosi sui dati relativi al 2021, l'NCSC ha potuto constatare che al momento la sicurezza informatica nell'Amministrazione federale è nel complesso conforme all'attuale situazione di minaccia e che in caso di incidenti vengono prese immediatamente tutte le misure necessarie.
Tuttavia, al riguardo occorre osservare che, nonostante le importanti misure di sicurezza prese nel settore informatico, qualsiasi impresa deve partire dal presupposto che subirà un ciberattacco (approccio «assume breach»[2]). Quest'affermazione vale anche per l'Amministrazione federale.

Affinché l'implementazione delle misure di sicurezza richieste nella protezione di base delle TIC e nei piani di sicurezza possa essere provata correttamente, i documenti sulla sicurezza

[1] Ordinanza del 27.5.2020 sui ciber-rischi (OCiber, RS **120.73**)

[2] L'espressione «assume breach» è composta dai due vocaboli inglesi «assume» (= presupporre, ipotizzare) e «breach» (= lacuna, vulnerabilità).

devono essere aggiornati (possono risalire al massimo a 5 anni prima). Nella media dell'Amministrazione federale, per il 90 per cento (valore identico a quello dell'anno precedente) degli oggetti da proteggere sono disponibili i relativi documenti sulla sicurezza. Si tratta di un valore fondamentalmente positivo.
Nell'Amministrazione federale, in media il 95 per cento dei documenti sulla sicurezza disponibili è aggiornato (anno precedente: 96 %). Se mancano documenti sulla sicurezza, questi vengono elaborati tempestivamente e aggiornati laddove necessario.

Nel 2021 l'attuazione delle misure di sicurezza e la relativa verifica (protezione di base e misure derivanti dai piani per la sicurezza dell'informazione e la protezione dei dati, SIPD) era garantita per il 70 per cento circa di tutti gli oggetti da proteggere (anno precedente: 57 %). Questo miglioramento è riconducibile agli sforzi compiuti dai dipartimenti nell'aggiornare i documenti sulla sicurezza, nell'elaborare quelli mancanti nonché nel verificare l'attuazione delle misure.

Gli incaricati della sicurezza informatica dei dipartimenti (ISID) e delle unità amministrative (ISIU) dirigono l'attuazione delle misure di sicurezza informatica su incarico dei responsabili delle unità amministrative.
Tutte le posizioni di ISID e di ISIU sono occupate. Tuttavia, al Dipartimento federale dell'interno (DFI), al Dipartimento federale dell'economia, della formazione e della ricerca (DEFR) e al Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) la funzione di ISID è svolta soltanto a un tasso di occupazione del 60 per cento, a fronte dell'80 per cento richiesto a livello di dipartimento.

Per quanto riguarda il telelavoro svolto a seguito delle misure disposte per arginare la pandemia da coronavirus, nel gennaio 2021 si è verificato un numero sempre maggiore di problemi di disponibilità (larghezza di banda della connessione Internet della Confederazione). Il ricorso al telelavoro da parte degli utenti ha sovraccaricato la connessione alla rete, causando talvolta problemi di performance, come nelle chiamate via Skype e, in particolare, nelle videoconferenze.
L'Ufficio federale dell'informatica e della telecomunicazione (UFIT), d'intesa con il settore Trasformazione digitale e governance delle TIC (TDT) della Cancelleria federale, ha aumentato la larghezza di banda e bloccato alcuni servizi in streaming. In questo modo, da un lato, è stato alleggerito il carico sulla rete, permettendo di svolgere nuovamente le videoconferenze. D'altro lato, però, non è stato più possibile visualizzare video in Internet. Anche questo problema è stato in seguito risolto grazie a ulteriori misure.
Si può affermare che in linea di principio il telelavoro funziona bene e finora non sono stati individuati incidenti legati alla sicurezza riconducibili a tale forma di lavoro.

3 Garanzia della sicurezza informatica – fattore umano

I collaboratori di tutti i livelli rivestono un ruolo fondamentale nell'ambito della sicurezza informatica. Pertanto, i collaboratori dell'Amministrazione federale vengono sensibilizzati e istruiti regolarmente su questo tema.
Sotto la direzione degli ISID e degli ISIU, nel 2021 quasi il 95 per cento dei nuovi collaboratori è stato introdotto alle tematiche della sicurezza informatica (anno precedente: 87 %). Questo miglioramento è stato ottenuto grazie alla maggiore digitalizzazione della formazione durante la pandemia da coronavirus.
Nell'ambito di un pacchetto introduttivo a livello federale rivolto ai nuovi collaboratori, l'NCSC sta elaborando un modulo che tratta le questioni legate alla sicurezza informatica. Il modulo dovrebbe essere disponibile per tutti i collaboratori dell'Amministrazione federale a metà del

2022.

Diversi dipartimenti e unità amministrative hanno adottato misure di sensibilizzazione individuali, ad esempio per quanto concerne le e-mail di phishing.

I corsi svolti dall'NCSC sul tema della sicurezza informatica, integrati nell'offerta del Centro di formazione dell'Amministrazione federale (CFAF), sono stati frequentati da molti collaboratori. Nel 2021 sono stati svolti per la maggior parte online e giudicati in modo molto positivo dai partecipanti.

Inoltre, l'NCSC ha proposto nuovi corsi per acquisire conoscenze specialistiche nel campo della cibersicurezza allo scopo di sviluppare e ampliare le conoscenze dei collaboratori dell'NCSC, degli ISID e degli ISIU e di altre persone interessate dell'Amministrazione federale che si occupano di questioni legate a questo tema.

Occorre inoltre sottolineare che molti collaboratori reagiscono correttamente alle e-mail di spam e di phishing, cancellandole immediatamente o segnalandole al fornitore di prestazioni tramite il pulsante «Segnala Spam» presente nel programma di posta elettronica Outlook affinché possano essere analizzate.
Per compiere attacchi di phishing mirati (e anche per altri tentativi di truffa), spesso vengono manipolate e-mail di servizi esterni (ad es. fornitori). I destinatari difficilmente riescono a riconoscerle come fasulle. Poiché in diversi casi inizialmente gli aggressori sono riusciti nel loro intento, è ancora necessario organizzare campagne di sensibilizzazione.

4 Incidenti legati alla sicurezza e vulnerabilità

4.1 Sintesi dei fornitori di prestazioni interni

Nel 2021 l'UFIT, il maggiore fornitore di prestazioni interno della Confederazione, ha trattato un totale di 434 incidenti legati alla sicurezza[3] (anno precedente: 834). Al riguardo occorre evidenziare che non tutti gli incidenti legati alla sicurezza causano danni diretti all'Amministrazione federale: nell'elaborazione di tali incidenti, ad esempio, si esaminano a scopo preventivo anche le vulnerabilità critiche.
In qualità di fornitore di prestazioni per il servizio standard TIC «Comunicazione di dati», l'UFIT, insieme al Computer Security Incident Response Team (CSIRT), è responsabile del monitoraggio della rete, ad eccezione di poche reti specifiche[4]. Di conseguenza, gli incidenti menzionati nei rapporti del CSIRT/dell'UFIT possono essere considerati rappresentativi dell'intera Amministrazione federale civile.
Inoltre, nell'anno in rassegna, il Cyber Fusion Center (CFC) del fornitore di prestazioni DDPS ha trattato circa 400 segnalazioni interne. La maggior parte delle segnalazioni è stata classificata come non critica.
Le altre unità amministrative non hanno segnalato eventi particolari.

[3] L'espressione «incidente legato alla sicurezza» comprende tutti gli avvisi di sicurezza in entrata. Tra questi rientrano anche i casi sospetti che dopo essere stati analizzati si rivelano innocui o falsi allarmi, oppure i casi di phishing che non concernono direttamente l'Amministrazione federale.

[4] Fa eccezione, ad esempio, la comunicazione di dati garantita sulle reti centrali dell'esercito (segnatamente sulle reti destinate all'Aggruppamento Difesa), che deve essere fornita mediante un'infrastruttura della Confederazione e internamente dalla Base d'aiuto alla condotta (BAC), al fine di soddisfare le esigenze volte a garantire la disponibilità e a rendere possibile una degradazione graduale dei sistemi (Modello di mercato per il servizio standard TIC «Comunicazione di dati» del 19.6.2020).

4.2 Incidenti legati alla sicurezza

L'Amministrazione federale è costantemente presa di mira, sia con attacchi molto diffusi via e-mail sia con attacchi mirati all'infrastruttura IT della Confederazione o a singoli collaboratori.
La tipologia degli aggressori spazia da distributori di spam di massa a organizzazioni criminali o «hacktivisti», fino a presunti attori statali.

e-mail in entrata
L'UFIT analizza costantemente tutte le e-mail in entrata e provvede affinché quelle che non appaiono sicure non vengano recapitate ai destinatari.

Nel 2021, il 34,5 per cento (anno precedente: 48 %) delle e-mail in entrata è stato **eliminato** ancor prima di essere recapitato al destinatario:

e-mail in entrata nell'Amministrazione federale:	138 872 079 (anno precedente: ca. 160 mio.)
di cui eliminate a livello centrale[5]	47 955 038
e-mail inoltrate ai destinatari	90 917 041

Questo calo delle e-mail eliminate è dovuto principalmente allo smantellamento dell'infrastruttura Emotet[6] (per i dettagli v. «Blocco di URL e domini)».

Analizzando e filtrando le e-mail in entrata, l'UFIT fornisce un contributo fondamentale alla sicurezza dell'intera Amministrazione federale.

Phishing
Il phishing è un tentativo di accedere ai dati personali degli utenti tramite siti web, e-mail o brevi messaggi falsificati per commettere un furto di identità oppure per installare sul sistema software dannosi che vengono scaricati tramite documenti allegati.
I collaboratori dell'Amministrazione federale non ne sono risparmiati: nel 2021 sono stati trattati 11 attacchi di phishing riusciti (anno precedente: 34).
Come dimostra il gran numero di segnalazioni di e-mail spam, questo metodo è ancora molto diffuso tra i cibercriminali.
I collaboratori di tutta l'Amministrazione federale vengono sensibilizzati costantemente riguardo agli attacchi di phishing. In tale contesto viene mostrato anche quanto siano sofisticati i metodi utilizzati.

Malware
Si può menzionare con soddisfazione che nel 2021 si è verificato soltanto **un** incidente causato da malware che ha infettato **un** dispositivo dell'Amministrazione (anno precedente: 15).
Sebbene si trattasse di un attacco mirato, l'intervento immediato del fornitore di prestazioni ha permesso di evitare danni maggiori.
Nonostante quest'unico incidente nel 2021, non si può prescindere da ulteriori miglioramenti nella protezione contro i malware.

[5] Vengono eliminate a livello centrale – e quindi rese innocue – le e-mail di mittenti già noti per l'invio di spam e malware nonché le e-mail in cui vengono rilevati direttamente virus e malware.

[6] Emotet è un software dannoso che viene inviato soprattutto tramite e-mail di spam. Originariamente, Emotet era un trojan esclusivamente bancario. Gli aggressori miravano a penetrare nel sistema informatico della vittima per ottenere i dati di accesso ai conti bancari. Adesso Emotet funziona come un «dropper» ed è utilizzato per scaricare altri malware.

Skype for Business
Nell'ottobre 2021 in un dipartimento sono stati rilevati tentativi di attacco contro Skype for Business. Gli aggressori hanno cercato di accedere a numerosi account in Skype provando a inserire varie password. In tre casi sono riusciti nel loro intento. I collaboratori interessati sono stati contattati immediatamente e invitati a modificare la password. Inoltre, sono state intraprese altre misure immediate.

Learning Management System (LMS) dell'Esercito svizzero
In occasione dell'inizio delle scuole reclute in modalità di telelavoro a causa della pandemia da coronavirus, si sono verificate carenze nella disponibilità della piattaforma di apprendimento LMS dell'esercito. Un servizio esterno ha inoltre individuato una vulnerabilità nella protezione dei dati. Entrambi i problemi sono stati risolti tempestivamente.

Blocco di URL e domini (siti web esterni)
A seguito di 11 mandati sono stati bloccati 90 domini[7] (anno precedente: 217). Sebbene la ragione principale di tale blocco fosse ancora la presenza di malware, il numero basso è anche dovuto allo smantellamento dell'infrastruttura Emotet, da parte di Europol e di altre autorità di perseguimento penale, che è stato reso noto a fine gennaio. Fino al mese di marzo è stato registrato un numero nettamente inferiore di tentativi di attacco tramite malware contenuti nello spam. In seguito si sono verificati nuovi attacchi con il malware IcedID, che ha preso il posto di Emotet. Nonostante queste ondate di attacchi, soltanto un client è stato infettato (v. paragrafo «Malware»).

Incidenti esterni legati alla sicurezza con conseguenze dirette per l'Amministrazione federale
Quattro vulnerabilità critiche in Microsoft Exchange[8] hanno permesso attacchi da remoto con conseguenti esecuzioni di codici. I sistemi Exchange sono stati corretti in pochi giorni dal fornitore di prestazioni attraverso un cambiamento di emergenza («Emergency Change»).

Inoltre, con PrintNightmare Microsoft ha reso nota una vulnerabilità critica: gli utenti senza privilegi elevati, che potevano installare un driver per la stampante, avrebbero potuto mettere in pericolo l'intero sistema. In generale, l'installazione di software da parte degli utenti presenta un grosso rischio. Tale possibilità è esclusa sui client della Confederazione e quindi il rischio è nettamente inferiore.

Il 10 dicembre 2021 è stata resa nota la vulnerabilità Log4j[9], particolarmente critica. L'Apache Software Foundation ha attribuito a Log4j il livello massimo di criticità, ossia 10. Gli aggressori possono sfruttare questa vulnerabilità per eseguire da remoto un codice dannoso e, in determinati casi, assumere il controllo completo del sistema.
Un aggiornamento per Log4j – volto a correggere la vulnerabilità – è stato pubblicato alcuni giorni prima che il problema fosse reso noto. Sono seguiti ulteriori aggiornamenti per Log4j relativi a questa falla nella sicurezza, perché quelli precedenti non erano stati in grado di eliminare completamente la vulnerabilità, vale a dire che si sarebbe potuta ancora sfruttare in talune configurazioni non standard. Log4j è integrata in molte soluzioni software. In alcuni casi è necessario attendere l'aggiornamento del produttore del software perché non è possibile eseguirlo autonomamente. I tentativi degli aggressori di sfruttare questa vulnerabilità nell'Amministrazione federale sono stati respinti con successo perché i fornitori di prestazioni hanno installato immediatamente gli aggiornamenti disponibili e monitorato attentamente le conseguenze di Log4j.

[7] Il dominio è il nome univoco che identifica un sito web.

[8] Microsoft Exchange è un groupware e server di posta elettronica della ditta Microsoft. Serve ad archiviare e gestire a livello centrale e-mail, appuntamenti, contatti, attività e altri elementi per diversi utenti, agevolando così la collaborazione all'interno di un gruppo di lavoro o di un'impresa.

[9] Nota anche con il nome Log4Shell.

Grazie alla reazione immediata dei fornitori di prestazioni – sotto il coordinamento dell'NCSC – gli incidenti descritti non hanno avuto alcuna conseguenza negativa all'interno dell'Amministrazione federale.

Vulnerabilità nei dipartimenti
I dipartimenti segnalano che in linea di principio le vulnerabilità rilevate hanno avuto soltanto conseguenze di lieve o media entità[10].
Conseguenze di grave entità si sono verificate unicamente in occasione dell'interruzione di servizi trasversali che hanno impedito l'esecuzione di importanti compiti.

4.3 Sistemi / protocolli di rete obsoleti

Ad eccezione dei Servizi del Parlamento e del DATEC, i dipartimenti segnalano che sono ancora in uso sistemi e protocolli di rete obsoleti.

La responsabilità dell'uso di sistemi e protocolli obsoleti ricade sui responsabili delle applicazioni dei beneficiari di prestazioni negli uffici e nei dipartimenti. Questi, a loro volta, hanno poche possibilità di sostituire i protocolli esistenti perché non dispongono di fondi e personale sufficienti e quindi sono costretti ad accettare il rischio che persistano lacune, talvolta importanti, nella sicurezza.

Sebbene queste lacune siano indicate nei rapporti sulla sicurezza e ben note alle direzioni, di fatto, a causa della loro complessità tecnica, pochissimi responsabili sono consapevoli dei reali rischi a cui espongono la sicurezza delle informazioni. Questa situazione può portare a un accumulo di rischi a livello di sicurezza. In quanto responsabile del coordinamento in ambito di cibersicurezza, l'NCSC seguirà da vicino tale problematica.
Per la maggior parte dei sistemi e dei protocolli sono previsti una sostituzione o un aggiornamento (in certi casi entro la fine del 2024).
Alcuni sistemi obsoleti – soprattutto negli ambienti di laboratorio – sono già collegati a reti isolate e non generano quindi scambi di dati con la rete della Confederazione.

5 Rafforzamento della sicurezza informatica

5.1 Misure 2021

Per rafforzare la sicurezza informatica, tutti i dipartimenti, i Servizi del Parlamento e la Cancelleria federale hanno attuato misure o svolto attività specifiche.

Ad esempio:
- sono state svolte regolarmente campagne di sensibilizzazione (talvolta a livello interdipartimentale);
- i diritti di accesso sono stati verificati sistematicamente;

[10] Conseguenze di grave entità = fuga di dati, informazioni/dati degni di particolare protezione accessibili a persone non autorizzate, osservanza delle disposizioni legali fortemente pregiudicata o resa impossibile, prestazioni rese impossibili, intero dipartimento e/o servizi esterni interessati.

Conseguenze di media entità = osservanza delle disposizioni legali pregiudicata od ostacolata, prestazioni limitate, conseguenze sostenibili per i servizi esterni.

Conseguenze di lieve entità = osservanza delle disposizioni legali non pregiudicata né ostacolata, prestazioni interne all'unità amministrativa limitate, nessuna conseguenza per i servizi esterni.

- i cellulari sono stati controllati per individuare possibili malware o il software di spionaggio «Pegasus»;
- sono stati condotti colloqui con la direzione, tra le altre cose sulla sicurezza informatica;
- sono stati organizzati corsi, ad esempio la «Security Academy» (settimana di formazione) del DDPS;
- le risorse di personale destinate alla sicurezza informatica sono state aumentate;
- sono stati eseguiti programmi «bug bounty»[11] e test pubblici per la valutazione della sicurezza;
- i sistemi di gestione della sicurezza delle informazioni (ISMS) sono stati ulteriormente sviluppati;
- sono state realizzate speciali zone tecniche, soprattutto per i sistemi domotici (impiantistica degli edifici);
- sono state svolte verifiche;
- le connessioni VPN permanenti (Always-On VPN) delle postazioni di lavoro sono state implementate;
- sono stati avviati progetti come quello per la firma di macro.

5.2 Misure previste a breve e medio termine

Per rafforzare la sicurezza informatica a breve e medio termine, i dipartimenti, i Servizi del Parlamento e la Cancelleria federale hanno previsto, tra le altre, le seguenti misure:

- introduzione di una strategia in materia di digitalizzazione;
- campagne di sensibilizzazione;
- corsi per il trattamento delle informazioni classificate;
- realizzazione di un ISMS dipartimentale;
- potenziamento delle risorse di personale;
- svolgimento di verifiche tecniche;
- aggiornamento delle istruzioni interne sulla sicurezza delle informazioni;
- prosecuzione e completamento del programma «Mitigation Credential Theft – MTC», volto a ridurre il furto di dati di accesso, e del progetto per la firma di macro nonché sostituzione del software di crittografia di proprietà della Confederazione «SecureCenter».

Per quanto riguarda l'NCSC, oltre a garantire sostegno agli ISID e agli ISIU in tutti gli ambiti della sicurezza informatica, l'attività si concentra sull'ulteriore sviluppo delle direttive in materia di sicurezza, sul potenziamento della gestione delle vulnerabilità, sull'adozione di misure per l'ulteriore formazione dei collaboratori dell'Amministrazione federale nonché sull'attuazione della legge sulla sicurezza delle informazioni (LSIn).

[11] Nei programmi bug bounty, i cosiddetti «hacker etici» – che operano in un quadro definito e nel rispetto della legge – sono incaricati di individuare eventuali vulnerabilità nei sistemi informatici di un'organizzazione. Per ciascuna vulnerabilità trovata e convalidata («bug») vengono ricompensati («bounty») in base alla gravità della vulnerabilità trovata.