Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC
Sicurezza informatica della Confederazione

21 aprile 2021

Stato della sicurezza informatica nell'Amministrazione federale nel 2020

1 Sicurezza informatica nell'Amministrazione federale

La sicurezza informatica nell'Amministrazione federale comprende tutte le misure necessarie per evitare i 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 sulla protezione dell'Amministrazione federale contro i ciber-rischi. 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 (uffici) sono responsabili della 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.

Il presente rapporto sullo stato della sicurezza non fornisce indicazioni su singoli attacchi o lacune di sicurezza specifiche. Queste ultime potrebbero favorire direttamente i potenziali aggressori e quindi mettere in pericolo l'intero settore informatico dell'Amministrazione federale. Pertanto, nel presente rapporto non vengono nemmeno menzionati singoli dipartimenti o uffici.

2 Stato attuale della sicurezza informatica nell'Amministrazione federale

Alla fine dell'anno i dipartimenti, la Cancelleria federale e i Servizi del Parlamento riferiscono all'NCSC sullo stato della sicurezza informatica (autodichiarazione basata su un sondaggio strutturato). La plausibilità dei dati viene verificata dall'NCSC.

In sintesi, sulla base dei dati relativi al 2020 l'NCSC ha potuto constatare che al momento la sicurezza informatica nell'Amministrazione federale è nel complesso adeguata all'attuale situazione di minaccia.
Tuttavia, al riguardo occorre osservare che, nonostante le importanti misure di sicurezza prese nel settore informatico, qualsiasi impresa deve partire dal presupposto che cadrà vittima di un ciberattacco (approccio «assume breach[2]»). Quest'affermazione vale anche per l'Amministrazione federale.

Affinché la protezione di base delle TIC e le misure di sicurezza richieste nei piani di sicurezza siano implementate con successo, i documenti sulla sicurezza necessari 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) di tutti gli oggetti da proteggere sono disponibili i relativi documenti sulla sicurezza. Si tratta di un valore fondamentalmente positivo.

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

[2] Secondo l'approccio «assume breach» qualsiasi impresa deve partire dal presupposto che prima o poi cadrà vittima di un ciberattacco nonostante le importanti misure di sicurezza prese nel settore informatico.

Nell'Amministrazione federale, in media il 96 per cento dei documenti sulla sicurezza disponibili è aggiornato (anno precedente: 82 %). Questo netto incremento è riconducibile a misure di correzione e aggiornamento (basate anche sulla decisione del Consiglio federale relativa al rapporto dello scorso anno).

Nel 2020 l'attuazione delle misure di sicurezza (protezione di base e misure derivanti dai piani per la sicurezza dell'informazione e la protezione dei dati, SIPD) era garantita per il 78 per cento circa di tutti gli oggetti da proteggere. Per circa ¾ delle relative applicazioni, l'attuazione delle misure di sicurezza è stata verificata successivamente.
Tuttavia, i controlli richiesti riguardo all'attuazione non raggiungono ancora il livello auspicato.
Sono stati quindi ordinati i provvedimenti necessari per migliorare ulteriormente lo stato di attuazione delle misure di sicurezza richieste e i relativi controlli.

Per quanto riguarda il lavoro a domicilio svolto a seguito delle misure disposte per arginare l'epidemia di coronavirus, sono emersi problemi – soprattutto all'inizio – con le capacità di accesso remoto alla rete della Confederazione (le richieste di accesso sono decuplicate). Tuttavia, i vari fornitori di prestazioni sono stati in grado di aumentare rapidamente tali capacità. Il lavoro a domicilio ha quindi funzionato e continua a funzionare bene.
Finora non sono stati individuati incidenti legati alla sicurezza riconducibili al lavoro a domicilio. I tentativi di alcuni collaboratori di installare propri software sui dispositivi della Confederazione sono stati bloccati grazie alle misure di sicurezza adottate dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT). Inoltre, per questioni di sicurezza è stato necessario ritirare alcuni prodotti offerti dall'UFIT.

Una problematica ancora da risolvere consiste nell'impossibilità di effettuare chiamate (videoconferenze) con contenuti sensibili tramite un apposito sistema. È stato avviato un progetto per rimediare a tale situazione.

L'NCSC ritiene che i rischi risiedano anche nell'errata configurazione dell'infrastruttura IT e nell'utilizzo di software con vulnerabilità che non vengono corrette immediatamente.

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 istruiti regolarmente su questo tema.
Sotto la direzione degli incaricati della sicurezza informatica delle unità amministrative (ISIU), quasi tutti i nuovi collaboratori vengono introdotti alle tematiche della sicurezza informatica. Mentre nel 2019 è stato istruito il 95 per cento circa dei nuovi collaboratori, questo valore è sceso all'87 per cento nel 2020. Tale risultato è stato motivato dall'impossibilità di svolgere corsi in presenza. Sussistono inoltre lacune nella formazione dei collaboratori esterni.
L'Ufficio federale del personale (UFPER) sta valutando la possibilità di elaborare un pacchetto introduttivo a livello federale che contenga le istruzioni di base per i nuovi collaboratori e dirigenti. In questo modo saranno incluse anche le tematiche della sicurezza informatica.
A complemento delle campagne di sensibilizzazione condotte a livello centrale dall'ex Organo direzione informatica della Confederazione (ODIC) e ora dall'NCSC, molte unità amministrative applicano misure di sensibilizzazione specifiche. Ad esempio, alcuni dipartimenti hanno adottato diverse misure di sensibilizzazione con test sulle e-mail di phishing.

4 Incidenti legati alla sicurezza

Nel 2020 l'UFIT, il maggiore fornitore di prestazioni interno della Confederazione, ha elaborato un totale di 834[3] incidenti legati alla sicurezza insieme al Computer Security Incident Response Team (CSIRT). 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 linea di principio gli incidenti legati alla sicurezza possono essere suddivisi in tre categorie:

- attacchi contro parte dell'Amministrazione federale;
- incidenti esterni legati alla sicurezza con conseguenze dirette per l'Amministrazione federale;
- eventi e malfunzionamenti interni.

4.1 Attacchi contro l'Amministrazione federale

L'Amministrazione federale è sottoposta ad attacchi continui, che possono essere sia attacchi molto diffusi via e-mail sia attacchi mirati all'infrastruttura TIC della Confederazione. 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 2020, il 48 per cento delle e-mail in entrata è stato eliminato ancor prima di essere recapitato al destinatario:

e-mail in entrata nell'Amministrazione federale:	159 827 600 (anno precedente: 306 687 261)
di cui eliminate a livello centrale[4]:	76 576 865 (anno precedente: 238 548 362)
e-mail inoltrate ai destinatari:	83 250 735 (anno precedente: 68 138 899)

Il forte calo del numero di e-mail in entrata e non eliminate a livello centrale è probabilmente dovuto al fatto che, da un lato, i mittenti di spam noti sono stati resi innocui e, dall'altro, che i filtri antispam e antivirus dei provider di posta elettronica cancellano un numero notevolmente maggiore di e-mail dannose e quindi non le inoltrano.

Analizzando 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

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

software dannosi che vengono scaricati dai documenti allegati. I collaboratori dell'Amministrazione federale non ne sono risparmiati: nel 2020 sono stati rilevati 34 attacchi di phishing riusciti (anno precedente: 58).
Per gli attacchi di phishing vengono utilizzati in maniera illecita anche gli indirizzi e-mail delle unità amministrative dell'Amministrazione federale. I mittenti utilizzati con maggiore frequenza sono la divisione Imposta sul valore aggiunto e l'Amministrazione federale delle dogane. Per accedere ai dati delle vittime vengono ad esempio promessi dei rimborsi d'imposta.
I collaboratori di tutta l'Amministrazione federale vengono sensibilizzati costantemente riguardo agli attacchi di phishing. In tale contesto viene mostrato anche quanto siano sottili i metodi utilizzati.

4.2 Incidenti esterni legati alla sicurezza con conseguenze dirette per l'Amministrazione federale

Siti web infetti
La categoria degli «incidenti esterni legati alla sicurezza» comprende, ad esempio, la consultazione di siti web potenzialmente non sicuri: questi spesso presentano gravi lacune di sicurezza e pertanto possono essere utilizzati per attacchi di phishing o per distribuire malware. Nel 2020 la Confederazione ha bloccato l'accesso a circa 217 di questi siti web (talvolta a titolo preventivo).
Grazie al continuo miglioramento dell'analisi degli accessi a Internet, nel 2020 è stato necessario bloccare ancora solo pochi URL esterni. Da questi URL sono stati perpetrati attacchi contro i siti Internet dell'Amministrazione federale.

4.3 Eventi e malfunzionamenti interni

I malfunzionamenti interni riguardano principalmente l'accessibilità dei sistemi e dei dati. Nell'ultimo anno non si sono registrate gravi interruzioni che abbiano compromesso in maniera sostanziale l'accessibilità richiesta.

Dispositivi infetti
Sono stati individuati 20 dispositivi infetti (anno precedente: 55), di cui 5 (25 %) nella rete WLAN pubblica dell'Amministrazione federale (non dispositivi dell'Amministrazione federale). Anche se i dispositivi dell'Amministrazione federale infettati sono stati «soltanto» 15 (anno precedente: 19), ogni dispositivo infetto avrebbe potuto rappresentare una minaccia per tutta l'Amministrazione federale. I dispositivi in questione sono stati puliti e i collaboratori interessati ne sono stati resi attenti.
La diminuzione costante del numero di dispositivi infetti può essere considerata un aspetto positivo. Questa circostanza è dovuta sia alle misure tecniche approntate sia al comportamento adottato dai collaboratori.

5 Altre misure

In base alla valutazione della situazione corrente e agli incidenti legati alla sicurezza, l'Amministrazione federale adotta misure di sicurezza adeguate. Oltre a eventuali misure urgenti, vengono elaborate e attuate in modo durevole e proporzionato misure giuridiche, organizzative e tecniche.

Le basi per l'NCSC sono disciplinate nell'OCiber, entrata in vigore il 1° luglio 2020. Essa ha attribuito al delegato federale alla cibersicurezza la facoltà di impartire istruzioni in materia di sicurezza informatica. Allo stesso tempo, i settori dell'ODIC Sicurezza informatica, MELANI e GovCERT sono stati integrati nell'NCSC.

Per sostenere i collaboratori dell'Amministrazione federale, nel maggio 2019 l'ODIC ha lanciato una campagna di sensibilizzazione sulla sicurezza informatica che è stata portata avanti sino alla fine del 2020. I contenuti di questa campagna sono accessibili anche per le PMI e la collettività[5].

Centro nazionale per la cibersicurezza NCSC

[5] www.sicurezza-informatica.admin.ch