Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Organo direzione informatica della Confederazione ODIC
Sicurezza TIC Confederazione

Stato della sicurezza informatica nell'Amministrazione federale nel 2019

1 Sicurezza informatica nell'Amministrazione federale

La sicurezza informatica nell'Amministrazione federale comprende misure di protezione dell'integrità e dell'accessibilità dei sistemi delle tecnologie dell'informazione e della comunicazione (TIC), nonché misure di protezione del carattere confidenziale, dell'integrità, dell'accessibilità e della tracciabilità dei dati memorizzati, elaborati e trasferiti in questi sistemi[1]. A tal fine, il Consiglio federale emana le istruzioni sulla sicurezza TIC nell'Amministrazione federale[2].
Sulla base di queste istruzioni l'Organo direzione informatica della Confederazione (ODIC) definisce le direttive TIC in materia per l'Amministrazione federale.
Le misure di sicurezza TIC si orientano agli attuali standard internazionali, in particolare agli standard ISO concernenti le procedure di sicurezza TIC, nonché alla valutazione della situazione di minaccia.

Le unità amministrative sono responsabili della protezione dei loro sistemi e applicazioni TIC e dei loro dati (oggetti da proteggere). Esse esaminano regolarmente gli oggetti da proteggere e adottano le necessarie misure di sicurezza.

Per valutare la situazione attuale – e l'eventuale necessità di emanare misure urgenti – il settore Sicurezza TIC Confederazione dell'ODIC collabora strettamente con la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e con altri servizi competenti per la sicurezza TIC[3].

Per quanto concerne la sicurezza informatica, in linea di principio l'Amministrazione federale non si differenzia da altre autorità e imprese o dai privati: tutti sono sottoposti ad attacchi continui e devono proteggersi di conseguenza. Va tuttavia rilevato che le organizzazioni statali come l'Amministrazione federale sono spesso più esposte agli attacchi di altre organizzazioni statali rispetto ai privati o alle PMI.

---

[1] Ordinanza del 9 dicembre 2011 concernente l'informatica e la telecomunicazione nell'Amministrazione federale (ordinanza sull'informatica nell'Amministrazione federale, OIAF) RS **172.010.58**

[2] https://www.isb.admin.ch/isb/it/home/ikt-vorgaben/grundlagen/w002-weisungen_bundesrat_ikt-sicherheit_bundesverwaltung_wisb.html

[3] Ad es. il Computer Emergency Response Team dell'ODIC (GovCERT.ch), il Computer Security Incident Response Team dell'UFIT (CSIRT) o il Computer Emergency Response Team del DDPS (BAC MilCERT).

Il presente documento 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 sullo stato della sicurezza 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'ODIC sullo stato d'attuazione delle misure di sicurezza (autodichiarazione basata su un sondaggio strutturato). La plausibilità dei dati viene verificata dall'ODIC, in particolare mediante gli eventuali risultati della revisione informatica di cui all'articolo 28 OIAF.
In sintesi, sulla base dei dati relativi al 2019 l'ODIC ha potuto constatare che al momento la sicurezza informatica nell'Amministrazione federale è nel complesso adeguata all'attuale situazione di minaccia e raggiunge un livello paragonabile a quello di organizzazioni analoghe e dell'economia privata.

Ai fini dell'attuazione delle misure di sicurezza richieste, la documentazione sulla sicurezza deve essere disponibile e aggiornata.
Nel 2019 l'attuazione delle misure di sicurezza era garantita per il 90 per cento circa di tutti gli oggetti da proteggere. Si tratta di un valore fondamentalmente positivo, dal momento che una parte della documentazione è in fase di rielaborazione.
Tuttavia, i controlli richiesti riguardo all'attuazione non hanno ancora raggiunto il livello auspicato, nonostante la situazione sia migliorata rispetto all'anno precedente (controlli per il 70 % degli oggetti da proteggere contro il 66 % del 2018).
Grazie all'attuazione e al controllo delle misure di sicurezza richieste, lo stato della sicurezza informatica può essere mantenuto e garantito durevolmente in tutta l'Amministrazione federale.

3 Fattore umano

I collaboratori di tutti i livelli rivestono un ruolo fondamentale nell'ambito della sicurezza informatica. Pertanto, anche nel 2019 i collaboratori dell'Amministrazione federale sono stati istruiti su questo tema.
Sotto la direzione degli incaricati della sicurezza informatica delle unità amministrative, quasi tutti i nuovi collaboratori (95 % circa) vengono introdotti alle tematiche della sicurezza informatica. Invece i collaboratori esterni, in particolare, non sono ancora stati opportunamente istruiti.
Inoltre, nell'anno in esame, 130 specialisti come capiprogetto, responsabili di sistema e incaricati della sicurezza informatica hanno ricevuto una formazione specifica sulla sicurezza TIC e sui relativi processi dell'Amministrazione federale.
Tramite il Centro di formazione dell'Amministrazione federale l'ODIC offre corsi di formazione e formazione continua.
L'ODIC tiene inoltre corsi di formazione mirati e personalizzati in alcune unità amministrative e svolge campagne di sensibilizzazione generali in tutta l'Amministrazione federale.
A complemento delle suddette campagne di sensibilizzazione condotte a livello centrale dall'ODIC, molte unità amministrative applicano misure di sensibilizzazione specifiche (riguardanti soprattutto le e-mail di phishing).

4 Incidenti riguardanti la sicurezza

Nel 2019 l'Ufficio federale dell'informatica e della telecomunicazione (UFIT), il maggiore fornitore di prestazioni interno della Confederazione, ha elaborato complessivamente circa 900 incidenti riguardanti la sicurezza[4]. Al riguardo occorre evidenziare che non tutti gli incidenti riguardanti la sicurezza causano danni diretti all'Amministrazione federale. Nell'elaborazione di tali incidenti, ad esempio, si esaminano a scopo preventivo le vulnerabilità critiche.

In linea di principio gli incidenti riguardanti la sicurezza possono essere suddivisi in tre categorie:

- attacchi contro l'Amministrazione federale;
- incidenti esterni riguardanti la 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 mirati all'infrastruttura TIC della Confederazione sia attacchi molto diffusi via e-mail. La tipologia degli aggressori spazia da distributori di spam di massa a organizzazioni criminali o «hacktivisti», fino a presunti attori statali.

E-mail contenenti malware
Gli attacchi mirati vengono perpetrati, ad esempio, tramite l'invio di e-mail contenenti software dannosi (malware) – o link a tali software – a destinatari dell'Amministrazione federale. L'UFIT analizza costantemente le e-mail in entrata e provvede affinché le e-mail che non appaiono sicure non vengano recapitate ai destinatari.

Secondo l'analisi dell'UFIT relativa al 2019, il 78 per cento delle e-mail in entrata è stato eliminato prima di essere recapitato al destinatario:

e-mail in entrata nell'Amministrazione federale:	306 687 261	(100 %)
di cui eliminate a livello centrale (non inoltrate ai destinatari):	238 548 362	(78 %)
e-mail inoltrate ai destinatari:	68 138 899	(22 %)

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.

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 dai documenti allegati.

In 58 casi di phishing i collaboratori dell'Amministrazione federale hanno rivelato i propri dati di accesso a servizi di posta elettronica privati. Non sono però state constatate perdite di dati

[4] L'espressione «incidente riguardante la 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 dei falsi allarme, oppure i casi di phishing che non concernono direttamente l'Amministrazione federale. Poiché l'UFIT fornisce molte prestazioni di base e trasversali per tutta l'Amministrazione federale, la presente statistica fornisce un quadro rappresentativo.

o minacce per l'infrastruttura TIC della Confederazione. I collaboratori interessati vengono sempre informati dagli incaricati della sicurezza informatica della loro unità organizzativa riguardo agli attacchi rilevati e alle misure da adottare. In tal modo essi possono modificare i dati di accesso in questione (password) e migliorare il proprio comportamento.

I furti di identità con metodi di phishing aumenteranno. Dato che i metodi utilizzati sono sempre più sofisticati e ideati su misura per le vittime, il pericolo che ne deriva è grande. Anche gli eventi attuali vengono sfruttati direttamente per lanciare attacchi (ad es. crisi causata dal coronavirus, campionati mondiali ecc.).
Oltre ad attuare le misure tecniche di sicurezza necessarie per riconoscere le e-mail di phishing e i siti web contenenti malware, vengono organizzate campagne per la sicurezza nell'ambito delle quali il tema del phishing viene trattato con la massima attenzione.
I primi frutti di questo lavoro si vedono già nel numero nettamente superiore di e-mail di phishing riconosciute dai collaboratori e segnalate all'UFIT.

Dispositivi infettati
Nel 2019 l'UFIT ha individuato complessivamente 107 dispositivi infettati. Di questi, 19 dispositivi delle postazioni di lavoro sono stati effettivamente infettati (2018: 84) e hanno dovuto essere ripristinati (in totale l'UFIT gestisce circa 30 000 postazioni di lavoro).
Siccome il numero di dispositivi infettati può sembrare basso, è opportuno ricordare che ogni dispositivo infettato può rappresentare una minaccia per tutta l'Amministrazione federale.

Attacchi contro i siti Internet dell'Amministrazione federale
Nel 2019 sono stati bloccati 30 aggressori che hanno compiuto attacchi contro i siti Internet dell'Amministrazione federale[5]. Altri attacchi sono stati bloccati per proteggere l'infrastruttura dell'Amministrazione federale da un'eventuale scansione intensiva.

4.2 Incidenti esterni riguardanti la sicurezza con conseguenze dirette per l'Amministrazione federale

Siti web infettati
I siti web non sicuri rappresentano una minaccia anche per l'Amministrazione federale. Spesso presentano gravi lacune di sicurezza e pertanto possono essere utilizzati per attacchi di phishing o per distribuire malware. Nel 2019 la Confederazione ha bloccato, come misura preventiva o reattiva, l'accesso a circa 715 di questi siti web.

Lacune di sicurezza nelle componenti hardware e nei sistemi operativi
Le lacune di sicurezza individuate nelle componenti hardware e/o nei sistemi operativi vengono eliminate immediatamente. Se ciò non è possibile, i settori interessati vengono monitorati da vicino e protetti adottando apposite misure. Finora non sono stati rilevati abusi di tale lacune di sicurezza.

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.

[5] Questi siti Internet sono gestiti internamente all'Amministrazione.

A causa di comportamenti errati dei collaboratori, in alcuni casi sporadici il sistema della postazione di lavoro ha dovuto essere ripristinato. Dopo un incidente, i collaboratori interessati ricevono sempre istruzioni specifiche da parte dell'incaricato della sicurezza informatica competente (vedi più sopra: Phishing).

5 Altre misure

In base alla valutazione della situazione e agli incidenti riguardanti la sicurezza, l'Amministrazione federale adotta misure di sicurezza adeguate. Oltre a eventuali misure urgenti, vengono elaborate misure sul piano giuridico, organizzativo e tecnico, che vengono attuate durevolmente e in maniera proporzionata.

Per rafforzare la sicurezza informatica nell'Amministrazione federale, anche a beneficio del Paese, il Consiglio federale ha deciso di istituire il Centro nazionale per la cibersicurezza. I lavori di realizzazione del Centro sono iniziati nel 2019. Esso garantirà un ulteriore miglioramento sostanziale nell'ambito della sicurezza informatica[6].

Per sostenere i collaboratori dell'Amministrazione federale, nel maggio 2019 l'ODIC ha lanciato una campagna di sensibilizzazione sulla sicurezza informatica. I contenuti di questa campagna sono accessibili anche per le PMI e la collettività[7].

Organo direzione informatica della Confederazione

[6] https://www.melani.admin.ch/melani/it/home/ueber_ncsc/das_ncsc.html

[7] https://www.sicurezza-informatica.admin.ch