Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF

Centro nazionale per la cibersicurezza NCSC
Sicurezza informatica della Confederazione

9 giugno 2023

Rapporto sulla sicurezza informatica della Confederazione nel 2022

Indice

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 rapidamente i ciberincidenti. Per ciberincidente si intende un evento non intenzionale o provocato intenzionalmente da persone non autorizzate, che compromette la confidenzialità, l'integrità, l'accessibilità o la tracciabilità di dati o che può causare disfunzioni[1].
Affinché le misure necessarie per la sicurezza informatica vengano attuate nell'intera Amministrazione federale, il Consiglio federale emana le pertinenti ordinanze e istruzioni. L'Esecutivo ha inoltre trasferito al delegato alla cibersicurezza la competenza di emanare direttive in materia di sicurezza informatica[2]. Queste direttive sono elaborate dal Centro nazionale per la cibersicurezza (NCSC) con il sostegno del comitato per la sicurezza informatica (C-SI), ovvero l'organo consultivo per tutte le questioni inerenti alla sicurezza informatica nell'Amministrazione federale.
Le unità amministrative sono responsabili della sicurezza dei propri oggetti informatici da proteggere[3]. A tal fine verificano regolarmente i loro oggetti informatici 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 sui ciber-rischi (OCiber; RS *120.73*), il delegato federale 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, l'NCSC redige annualmente il «rapporto sulla sicurezza informatica della Confederazione».
Il rapporto si basa sulle informazioni che i dipartimenti e la Cancelleria federale riportano all'NCSC in merito allo stato della sicurezza informatica. A tale scopo l'NCSC ha condotto un sondaggio strutturato presso tutti gli incaricati della sicurezza informatica dei dipartimenti e della Cancelleria federale. Nel rapporto sono inoltre considerati i risultati e le esperienze dell'NCSC come pure gli avvisi e i rapporti in materia di sicurezza dei fornitori di prestazioni interni all'Amministrazione.
In sintesi, sulla base di queste informazioni l'NCSC giunge alla conclusione che al momento la sicurezza informatica nell'Amministrazione federale è nel complesso adeguata all'attuale situazione di minaccia. Nel caso degli incidenti constatati sono state prese immediatamente tutte le misure necessarie. Tuttavia, occorre osservare che, nonostante le onerose misure di sicurezza adottate nel settore informatico, qualsiasi impresa deve partire dal presupposto che subirà un ciberattacco. Quest'affermazione vale anche per l'Amministrazione federale.
L'NCSC ha integralmente rielaborato e ristrutturato la direttiva in materia di sicurezza informatica «Si001 – Protezione IT di base nell'Amministrazione federale», in vigore dal 1° marzo 2022. Sulla base delle esperienze maturate finora e dei cambiamenti previsti con

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

[2] Art. 11 OCiber

[3] 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. c OCiber).

l'entrata in vigore della legge sulla sicurezza delle informazioni (LSIn)[4], anche i processi «P041 – Analisi del bisogno di protezione» e «P042 – Piano SIPD» sono attualmente in fase di adattamento.
Affinché l'implementazione delle misure di sicurezza richieste nella protezione IT di base e nei piani di sicurezza possa essere dimostrata correttamente, i documenti sulla sicurezza devono essere aggiornati (possono risalire al massimo a 5 anni prima). Tali documenti sono disponibili per l'80 per cento degli oggetti da proteggere dell'Amministrazione federale. Tale valore è sceso rispetto all'anno precedente (90 %) perché, nel quadro delle revisioni dell'inventario, in diverse unità amministrative sono stati identificati ulteriori oggetti da proteggere per i quali è ora necessario redigere una documentazione di sicurezza. La gestione corrente dell'inventario fa sì che si rilevino le fluttuazioni del grado di conformità della documentazione di sicurezza all'obbligo di aggiornarla. Tuttavia, il valore dell'80 per cento dimostra che le unità amministrative continuano a prendere sul serio tale obbligo. Nel 2022 l'attuazione delle misure di sicurezza e la relativa verifica (misure di protezione di base e misure derivanti dai piani per la sicurezza dell'informazione e la protezione dei dati, SIPD) era garantita per il 73 per cento di tutti gli oggetti da proteggere (anno precedente: 70 %). Questo leggero miglioramento è riconducibile ai maggiori controlli da parte dei dipartimenti e delle unità amministrative.

3 Garanzia della sicurezza informatica – il fattore umano

I collaboratori di tutti i livelli rivestono un ruolo fondamentale nell'ambito della sicurezza informatica. Pertanto, il personale dell'Amministrazione federale viene regolarmente sensibilizzato e istruito su questo tema.
I corsi svolti dall'NCSC sul tema della sicurezza informatica, integrati nell'offerta del Centro di formazione dell'Amministrazione federale (CFAF), sono stati molto frequentati. Nel 2022 questi corsi si sono tenuti spesso in loco anziché esclusivamente online come nell'anno precedente. Considerata l'elevata domanda, nel 2023 si prevede di svolgere i corsi quattro anziché tre volte.
Inoltre, l'NCSC ha regolarmente organizzato corsi e campagne di sensibilizzazione volti a sviluppare e ampliare le conoscenze specialistiche in materia di cibersicurezza degli incaricati della sicurezza informatica dei dipartimenti e delle unità amministrative (ISID e ISIU) e di altre persone interessate. Nel 2022 si sono svolti online diversi corsi per esperti sui temi quali la crittografia (in media 100 partecipanti), le blockchain e i Bitcoin (in media 90 partecipanti), l'informatica forense (in media 140 partecipanti), Tor e Darknet (in media 140 partecipanti) e Kubernetes (in media 130 partecipanti).

[4] Legge federale del 18.12.2020 sulla sicurezza delle informazioni in seno alla Confederazione (legge sulla sicurezza delle informazioni, LSIn), FF **2020** 8755

Sia nel 2021 che nel 2022 l'NCSC ha realizzato, in collaborazione con Prevenzione Svizzera della Criminalità, una campagna nazionale di sensibilizzazione per la popolazione, la cui visibilità è stata promossa anche presso il personale federale. La campagna del 2022 era incentrata sul tema dell'uso consapevole di Internet. Sono stati trattati in particolare il phishing e la truffa, argomenti di centrale importanza anche per l'Amministrazione federale. Nel 2022, complessivamente 40 uffici federali dei dipartimenti DFI, DFAE, DFF, DFGP, DATEC, DDPS, DEFR hanno contribuito a rafforzare la visibilità della campagna.
Al fine di promuovere ulteriormente la consapevolezza dei pericoli, delle minacce e dell'uso degli strumenti digitali e mobili, nel 2022 l'Amministrazione federale ha elaborato un corso di formazione basato sul web sul tema della sicurezza informatica nell'Amministrazione federale, inizialmente introdotto come progetto pilota e dal 2023 dichiarato obbligatorio per tutti i collaboratori neoassunti. Questo modulo consentirà a tutti i collaboratori dell'Amministrazione federale, indipendentemente dalla loro funzione e posizione, di affrontare in modo approfondito il tema della sicurezza informatica.
Per rispondere direttamente alle domande dei collaboratori delle unità amministrative in merito alla sicurezza informatica, l'Amministrazione federale dispone inoltre di otto ISID a livello di dipartimento e Cancelleria federale e di oltre 80 ISIU per i vari uffici.
Sotto la direzione degli ISID e degli ISIU, nel 2022 circa il 94 per cento dei nuovi collaboratori è stato introdotto alle tematiche della sicurezza informatica (anno precedente: 95 %).
Nell'attuale mondo del lavoro, il personale federale lavora sempre più spesso in mobilità rispetto a prima della pandemia di COVID-19. Per questo motivo, l'informatica della Confederazione comprende sempre più strumenti digitali. Tuttavia, grazie a connessioni VPN sicure per accedere ai sistemi dell'Amministrazione federale, molti rischi possono essere eliminati già alla fonte.

4 Incidenti legati alla sicurezza e vulnerabilità

4.1 Incidenti legati alla sicurezza

L'infrastruttura informatica dell'Amministrazione federale è costantemente esposta a ciberattacchi di varia complessità. Tuttavia, nel 2022 non si sono verificati incidenti che hanno messo a repentaglio il corretto funzionamento dell'Amministrazione federale. Grazie a una serie di misure, i team di sicurezza dei fornitori di prestazioni dell'Amministrazione federale sono stati in grado di respingere con successo i ciberattacchi. A scopo illustrativo, di seguito sono esposte le attività intraprese nel 2022 dal Computer Security Incident Response Team (CSIRT) dell'Ufficio federale dell'informatica e della telecomunicazione (UFIT) e dal Cyber Fusion Center (CFC) della Base d'aiuto alla condotta (BAC) per prevenire gli attacchi informatici ai loro sistemi.

- Nel 2022 il team CSIRT UFIT ha bloccato su mandato complessivamente 116 domini. Questi blocchi sono stati praticamente sempre causati dall'uso improprio di siti web per la diffusione di malware o per campagne di phishing. I siti sono stati bloccati dal team CSIRT UFIT, in collaborazione con il Computer Emergency Response Team (GovCERT) dell'NCSC. L'UFIT ha inoltre segnalato che alcuni firewall hanno consentito a determinate reti di connettersi direttamente a Internet. Dopo essere state rese note, le regole dei firewall che ne consentivano la connessione sono state rapidamente modificate in modo che le falle di sicurezza potessero essere immediatamente eliminate. Inoltre, su alcuni server (soprattutto Linux) si è constatata una protezione insufficiente contro i malware. I gestori ne sono stati informati e hanno così provveduto a risolvere tempestivamente il problema.

- Nel 2022 il CFC della BAC ha trattato complessivamente 559 eventi che spaziano da sospetti di malware a tentativi di phishing. In generale, però, non si sono verificati incidenti critici legati alla sicurezza, per cui la situazione complessiva può essere descritta come piuttosto tranquilla. Questo stato di calma si riflette anche nel numero di incidenti segnalati e sembra perdurare.

Nel periodo in esame si sono verificati diversi attacchi «Distributed Denial of Service»[5] (DDoS), dimostrando agli incaricati della sicurezza informatica della Confederazione che questo problema rimane di attualità. Gli attacchi DDos mirano a sovraccaricare e quindi a rendere indisponibili server web, servizi online o intere reti attraverso numerosi accessi simultanei. Per contrastare questi attacchi, è stata installata una Web Application Firewall (WAF) su cui è stato configurato un limite di accesso («Rate Limiting»). Restringendo il numero di richieste per ogni indirizzo IP, la WAF protegge l'Amministrazione federale dagli attacchi DDoS.

4.2 Vulnerabilità

Il 29 settembre 2021 l'NCSC è stato riconosciuto dall'organizzazione indipendente statunitense MITRE[6] come servizio autorizzato ad assegnare numeri CVE[7] («Common Vulnerabilities and Exposures»). In questo ruolo, l'NCSC è responsabile dell'elaborazione e della pubblicazione delle informazioni sulle vulnerabilità che gli vengono segnalate e delle registrazioni CVE corrispondenti. Quindi l'NCSC non è solo il servizio ufficiale di contatto per segnalare le falle nella sicurezza in Svizzera, ma gestisce anche i rispettivi numeri CVE per lo scambio internazionale. Da che ha ottenuto questo riconoscimento, l'NCSC ha pubblicato 30 numeri CVE di cui 15 nel 2022.
Oltre alla pubblicazione dei numeri CVE, l'NCSC tratta anche le segnalazioni concernenti i sistemi vulnerabili dell'Amministrazione federale e di organi esterni (Cantoni, Comuni, gestori di infrastrutture critiche e imprese svizzere). Le vulnerabilità nelle applicazioni e nei sistemi sono una delle cause principali degli incidenti legati alla sicurezza, motivo per cui una rapida identificazione e risoluzione è di grande importanza anche per l'Amministrazione federale. Nel 2022 l'NCSC ha pubblicato complessivamente 27 segnalazioni di vulnerabilità altamente critiche. Nell'anno in esame sono state trattate, tra l'altro, le vulnerabilità ad alta criticità riportate qui di seguito.

Analisi delle app per smartphone
Nel mese di novembre 2022, in occasione dei Mondiali di calcio in Qatar, il settore Trasformazione digitale e governance delle TIC (Settore TDT) della Cancelleria federale, responsabile dei cellulari aziendali – d'intesa con l'NCSC e l'UFIT – ha bloccato due app sui cellulari aziendali per proteggere i collaboratori e i dati della Confederazione.
Le app «Ehteraz» e «Hayya to Qatar 2022», necessarie per entrare nel Paese, richiedevano un ampio accesso ai dati. Di conseguenza, in collaborazione con i servizi specializzati della Confederazione, l'NCSC ha sottoposto le due app a verifiche tecniche. In via precauzionale ha infine deciso di bloccarle sui cellulari aziendali.
Atlassian Confluence Server
Poco dopo che la vulnerabilità critica nel prodotto «Atlassian Confluence Server»[8] è stata resa nota a inizio giugno 2022, l'Amministrazione federale l'ha immediatamente eliminata tramite

[5] Nelle tecnologie dell'informazione, il concetto «Denial of Service» si riferisce all'indisponibilità di un servizio Internet che in realtà dovrebbe essere disponibile. Spesso questa indisponibilità è dovuta a un sovraccarico della rete di dati. La differenza principale tra gli attacchi DDoS e gli attacchi DoS è che i primi utilizzano più sistemi e possono quindi sovraccaricare le reti e i sistemi con un volume di dati maggiore.

[6] La MITRE Corporation è un'organizzazione senza scopo di lucro che gestisce istituti di ricerca su mandato degli Stati Uniti. È nata dallo scorporo del Massachusetts Institute of Technology (MIT).

[7] Il «Common Vulnerabilities and Exposures» è un sistema di riferimento per la denominazione e la designazione della criticità delle vulnerabilità riscontrate nei sistemi informatici.

[8] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-26134

vari aggiornamenti. Gli aggressori avrebbero potuto sfruttarla ed eseguire qualsiasi codice sui server Confluence come utenti non autenticati. I sistemi sono stati successivamente controllati per individuare eventuali indicatori di compromissione. Poiché non sono stati rilevati segni di compromissione, i server hanno potuto essere rimessi in funzione subito dopo.

Server Microsoft Exchange

A fine settembre 2022 un'impresa vietnamita[9] attiva nel settore della cibersicurezza ha segnalato per la prima volta due vulnerabilità «zero-day»[10] nei server di Microsoft Exchange. Queste vulnerabilità sono denominate «ProxyNotShell» e possono essere sfruttate in combinazione. Esse sono state attivamente sfruttate in tutto il mondo prima che fosse disponibile una patch ufficiale. In questi casi è particolarmente importante reagire rapidamente e seguire le raccomandazioni che possono prevedere addirittura la disattivazione del sistema infetto fino alla risoluzione del problema (ad es. con una patch ufficiale).

Sfruttando queste falle di sicurezza[11], gli aggressori avrebbero potuto, ad esempio, ottenere l'accesso a sistemi vulnerabili ed eseguire da remoto codici dannosi via Internet. Era pertanto necessario intervenire in tempi brevi sia presso l'Amministrazione federale che presso le altre imprese.

Tuttavia, secondo le informazioni fornite dal produttore, le vulnerabilità potevano essere sfruttate solo con un account già autenticato sul server, il che riduceva la probabilità di un attacco.

L'8 novembre 2022 Microsoft ha pubblicato gli aggiornamenti pertinenti per eliminare la vulnerabilità. Questi sono stati immediatamente eseguiti presso l'Amministrazione federale. Inoltre, tutti i sistemi vulnerabili sono stati sottoposti a un esame approfondito, in cui però non sono emersi indicatori di compromissione.

Vulnerabilità nella VPN di FortiOS

Il 13 dicembre 2022 il produttore di prodotti di sicurezza Fortinet ha segnalato una vulnerabilità critica[12] nella VPN di FortiOS. Sfruttando questa lacuna di sicurezza, gli utenti non autenticati avrebbero potuto provocare il crollo da remoto dei dispositivi vulnerabili o eventualmente anche eseguire codici dannosi. Subito dopo la segnalazione di questa vulnerabilità, l'Amministrazione federale ha reagito aggiornando nel giro di due giorni i sistemi interessati e sottoponendoli a un esame per individuare eventuali indicatori di compromissione. Nemmeno in questo caso sono emersi indizi sospetti.

Possibili falle nella sicurezza degli strumenti ausiliari utilizzati per le videoconferenze

Il telelavoro è diventato parte integrante del mondo professionale e, di conseguenze, le riunioni e i workshop si svolgono spesso online. L'Amministrazione federale ha regolamentato le soluzioni di videoconferenza consentite. Tuttavia, per le videoconferenze vengono utilizzati anche altri strumenti ausiliari elettronici commerciali e gratuiti, disponibili su Internet, ad esempio lavagne digitali, strumenti di indagine o di pianificazione e bacheche virtuali.

Tali strumenti rappresentano un potenziale rischio per i dispositivi dell'Amministrazione federale, in quanto possono essere sfruttati dai cibercriminali come vettore di attacco.

Al fine di contrastare questo rischio di sicurezza, il Settore TDT della Cancelleria federale sta elaborando una linea guida vincolante per gli strumenti destinati alla collaborazione agile nel quadro dell'iniziativa strategica 2 (IS-2) «Focalizzazione sull'utente». Inoltre, gli ISIU e gli ISID sono incaricati di sensibilizzare i collaboratori in proposito.

[9] https://ncsgroup.vn/blog/warning-new-attack-campaign-utilized-a-new-0day-rce-vulnerability-on-microsoft-exchange-server-12715.html

[10] Sono denominate vulnerabilità «zero-day» le vulnerabilità per le quali non esiste ancora una patch che ne impedisca lo sfruttamento.

[11] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41040
https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-41082

[12] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-42475

Vulnerabilità critica nei prodotti di Citrix

Il 13 dicembre 2022 il produttore Citrix ha segnalato una vulnerabilità critica[13] nei prodotti Citrix ADC e Citrix Gateway. Si trattava di una vulnerabilità di autenticazione che avrebbe permesso anche l'esecuzione di codici dannosi via Internet. A causa della criticità, i sistemi dell'Amministrazione federale sono stati aggiornati con le patch necessarie nel giro di pochi giorni. La vulnerabilità ha riguardato anche il sistema Mobile Device Management (MDM) dell'Amministrazione federale.

4.3 Sistemi e protocolli di rete obsoleti

L'NCSC constata che nell'Amministrazione federale si continuano a utilizzare sistemi e protocolli di rete obsoleti che aumentano significativamente il rischio di falle nella sicurezza.

La responsabilità di sostituire i sistemi e i protocolli obsoleti spetta ai responsabili delle applicazioni dei beneficiari di prestazioni che lavorano negli uffici e nei dipartimenti. A causa delle diverse priorità, questi, a loro volta, non sempre dispongono delle risorse necessarie per sostituire i protocolli esistenti e, secondo l'NCSC, non sempre sono consapevoli dei rischi che ne derivano per la sicurezza. Sebbene questi rischi siano indicati nei rapporti sulla sicurezza delle unità amministrative e ben noti 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.

Tuttavia, va osservato che 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.

Soppressione delle versioni obsolete dei protocolli TLS 1.0 e TLS 1.1

Nel quadro di un rilevamento dell'UFIT sono state identificate diverse interfacce che utilizzano il protocollo di autenticazione e crittografia delle versioni obsolete dei protocolli «TLS 1.0 e TLS 1.1». Il TLS[14] è un protocollo che mira a garantire la confidenzialità e l'integrità della trasmissione dei dati nelle reti. Poiché i TLS 1.0 e TLS 1.1 sono versioni di protocollo obsolete e presentano delle vulnerabilità, l'esercizio di sistemi che utilizzano queste versioni non è più ammesso nell'Amministrazione federale. Tuttavia, la maggior parte di questi protocolli non si cela nelle classiche connessioni https[15], ma nei cosiddetti protocolli proprietari che utilizzano i protocolli TLS. L'uso diffuso dei protocolli TLS nei vari prodotti rappresenta quindi una sfida e, per rimediare a questa situazione, bisognerà investire risorse e tempo sufficiente (in alcuni casi la risoluzione del problema può durare fino alla fine del 2026).
In sintesi va detto che allo stato attuale 1786 sistemi con la versione obsoleta dei protocolli sono ancora attivamente in uso nell'Amministrazione federale. Un aspetto positivo è che nel 2022 il numero di versioni obsolete dei protocolli TLS 1.0 e TLS 1.1 che sono state aggiornate equivale a quello delle versioni ancora in uso.

Raccomandazioni per la gestione di versioni obsolete dei protocolli

L'NCSC raccomanda ai fornitori di prestazioni di procedere come segue.
Per eliminare le versioni obsolete dei protocolli sistematicamente e su vasta scala, bisogna bloccarle completamente; se del caso, le versioni assolutamente necessarie possono essere autorizzate in seguito in modo controllato e separato sulla base di un pertinente piano di migrazione. Una possibile soluzione è spostare tali sistemi in un ambiente di rete isolato in

[13] https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2022-27518

[14] Inglese: «Transport Layer Security»

[15] L'acronimo https sta per «Hypertext Transfer Protocol Secure» ed è il protocollo di comunicazione del World Wide Web che permette di trasmettere i dati senza che questi possano essere intercettati.

modo da non generare scambi di dati con altri sistemi informatici dell'Amministrazione federale. Fintantoché le versioni obsolete dei protocolli TLS sono utilizzate soltanto per comunicare all'interno dell'Amministrazione federale e i sistemi in questione non sono pubblicamente accessibili da Internet, il rischio è da considerarsi basso.

5 Sintesi dei fornitori di prestazioni interni

In generale, per i fornitori di prestazioni IT interni il 2022 è stato un anno relativamente tranquillo sul fronte delle ciberminacce. Per contro, a livello globale la cibersicurezza è sempre più al centro dell'attenzione. Le questioni importanti e di attualità sono simili a quelle del 2021. Inoltre, è emerso ancora una volta che cicli di vita funzionanti e una buona gestione delle patch sono molto importanti per la protezione dei sistemi informatici. Moltissimi attacchi prendono di mira componenti per i quali sono disponibili da qualche tempo patch o soluzioni alternative.
Per i fornitori di prestazioni è di fondamentale importanza verificare i diritti d'accesso nei sistemi e garantire la sicurezza informatica negli ambienti di sviluppo, affinché le falle di sicurezza non vengano trasferite nell'ambiente produttivo.
Con il crescente utilizzo di servizi cloud, si pone inoltre la pressante questione di come garantire una collaborazione sicura ed efficace, ad esempio quando si indaga su un incidente che coinvolge diversi fornitori di servizi cloud. Anche alla luce delle attuali tensioni internazionali, i fornitori di prestazioni esprimono timori riguardo alle conseguenze di una crisi di approvvigionamento di elettricità e alla disponibilità dei sistemi informatici.
L'impiego dei cosiddetti «security champion» è stato avviato presso i vari fornitori di servizi nel quadro del consolidamento della metodologia DevSecOps[16], secondo cui l'attuazione dei progetti agili deve integrare la sicurezza informatica. Assumendo il ruolo di «security champion», i collaboratori che si occupano dei progetti supportano i product owner e i capiprogetto affinché l'aspetto della sicurezza sia integrato nella fase di sviluppo dei progetti e diventi così automaticamente parte integrante dei prodotti (approccio «security by design»). Tale approccio è sempre più importante per i progetti agili, poiché i prodotti sono in costante sviluppo. In questo contesto, la sicurezza informatica non è più associata a pietre miliari classiche, ma è parte integrante del processo di sviluppo che deve essere costantemente monitorato.
Nell'anno in esame il programma «Mitigation Credential Theft – MCT» è giunto in fase di «attuazione» presso i fornitori di prestazioni. Si tratta tra l'altro di impedire l'installazione involontaria o indesiderata di software.
Per questo motivo, l'introduzione di un software «Privilege Access Manager» (PAM), conformemente alla nuova protezione IT di base (versione 5) e alla direttiva delle applicazioni E033 concernente la protezione dell'identità, è stata dichiarata necessaria per tutti i sistemi della burotica. A tale scopo, nel 2022 è stato introdotto un adeguato strumento per la gestione di questa infrastruttura ed è stato avviato l'esercizio produttivo per l'amministrazione dei server Windows. È stato inoltre elaborato un «Proof of Concept» (PoC) per i sistemi Linux, affinché nel 2023 possa essere avviato anche l'esercizio produttivo per la gestione dei sistemi Linux.

6 Rafforzamento della sicurezza informatica

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.

[16] Da Dev(elopment), Sec(urity) e Op(eration)s

6.1 Misure 2022

Per rafforzare la sicurezza informatica, nel 2022 tutti i dipartimenti e la Cancelleria federale hanno attuato misure o svolto attività specifiche.

Sono state, tra l'altro, attuate le seguenti misure:

- i collaboratori sono stati sensibilizzati attraverso diverse azioni, ad esempio la campagna nazionale di sensibilizzazione S-U-P-E-R[17], le campagne di phishing, le informazioni pubblicate in Intranet su temi concernenti il telelavoro, i viaggi all'estero, la protezione dei dati (in parte a livello interdipartimentale) e la cibersicurezza in generale;
- nel Dipartimento federale degli affari esteri (DFAE) è stato avviato il progetto «Endpoint Detection and Response» (EDR)[18]. L'obiettivo è introdurre una soluzione EDR sul maggior numero possibile di sistemi dell'Amministrazione federale;
- è stato introdotto il programma «Security Champion» per l'attuazione agile dei progetti;
- è stato avviato il progetto «DigiSec» che mira a presentare un'applicazione per l'implementazione di un sistema di gestione della sicurezza delle informazioni («Information Security Management System», ISMS) nell'Amministrazione federale;
- i sistemi ISMS sono stati ulteriormente ampliati in diverse unità amministrative;
- la certificazione esterna secondo la norma ISO 27001, intesa a garantire la sicurezza informatica, è stata portata avanti in alcune unità amministrative;
- l'NCSC ha avviato il programma «Bug Bounty» dell'Amministrazione federale[19];
- è stata avviata la creazione dello standard «securitxt.txt» sui siti web dell'Amministrazione federale allo scopo di migliorare il flusso delle segnalazioni delle vulnerabilità[20];
- le risorse di personale destinate alla sicurezza informatica sono state aumentate ulteriormente;
- è stato proseguito il programma «Mitigation Credential Theft – MCT», inteso a prevenire il furto e l'usurpazione di identità;
- è stato introdotto il servizio di firma delle macro, che riduce i rischi derivanti dalle macro di MS Office.

6.2 Misure 2023

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

- le scansioni web mensili saranno estese a tutti i siti web esposti su Internet, al fine di eliminare le vulnerabilità note;
- il programma «Bug Bounty» integrerà altre applicazioni critiche; in questo modo le applicazioni saranno controllate proattivamente al fine di individuare eventuali vulnerabilità;
- sono previste formazioni per promuovere la consapevolezza della sicurezza informatica («security awareness») nonché campagne di sensibilizzazione;
- i sistemi accessibili via Internet saranno sottoposti ad altri «penetration test» e verranno adottate le misure necessarie;

[17] Campagna di sensibilizzazione S-U-P-E-R: https://www.s-u-p-e-r.ch/it/

[18] La nozione inglese «Endpoint Detection and Response» (EDR) descrive una categoria di strumenti e tecniche che aiutano a rilevare («detection») e rispondere («response») rapidamente alle minacce attive sui terminali («endpoint»).

[19] I programmi «Bug Bounty» hanno lo scopo di potenziare la ciber-resilienza nell'Amministrazione federale (admin.ch) https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/medienmitteilungen/newslist.msg-id-89868.html.

[20] https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte/informatiksicherheitsberichte-bund.html

- si procederà all'implementazione di un sistema ISMS secondo la LSIn e conformemente alla norma ISO 27001;
- il software di crittografia di proprietà della Confederazione «SecureCenter» sarà sostituito dalla soluzione «CHCrypt».

L'NCSC diventerà un ufficio federale

Negli ultimi anni la cibersicurezza è diventata sempre più importante a tutti i livelli. Garantire la cibersicurezza è diventato un compito indispensabile della Confederazione. In considerazione della crescente importanza dell'NCSC, il 2 dicembre 2022 il Consiglio federale ha deciso che l'NCSC diventerà un ufficio federale aggregato al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS). L'NCSC continuerà a svolgere i compiti principali relativi alla cibersicurezza, tra cui il sostegno delle infrastrutture critiche nella gestione dei ciberincidenti, la messa a disposizione di un servizio nazionale di contatto per la popolazione e le imprese, la diffusione di informazioni e avvertimenti riguardanti le ciberminacce e le misure di protezione da adottare, la sensibilizzazione della popolazione, la gestione delle vulnerabilità e la protezione dei sistemi dell'Amministrazione federale[21].

[21] L'NCSC diventerà un ufficio federale: https://www.admin.ch/gov/it/pagina-iniziale/documentazione/comunicati-stampa.msg-id-92048.html