28 marzo 2025 | Ufficio federale della cibersicurezza UFCS

Relazione annuale 2024

Ufficio federale della cibersicurezza UFCS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
Protezione civile e sport DDPS
Ufficio federale della cibersicurezza UFCS

Contenuto

Prefazione

L'Ufficio federale della cibersicurezza (UFCS) traccia un bilancio del suo primo anno di vita. Grazie alla sua nuova struttura di ufficio federale, è stato in grado di ottimizzare e stabilizzare i servizi forniti come Centro nazionale di sicurezza informatica (NCSC) all'interno del Dipartimento federale delle finanze (DFF). Come in passato, siamo un piccolo ufficio federale e spesso ci troviamo di fronte alla sfida di dover svolgere numerosi compiti con risorse limitate. Tuttavia, grazie ad approcci innovativi, all'impegno di tutto il nostro personale e agli investimenti nella digitalizzazione, siamo riusciti ad aumentare ulteriormente la nostra produttività e a mettere i nostri servizi a disposizione di un pubblico più ampio.

Ora abbiamo posto le basi per l'adempimento della nostra missione legale e possiamo sviluppare ulteriormente i nostri servizi. Questo è importante, perché le richieste poste all'Ufficio dalla società, dall'economia e dalla politica continuano a crescere. Le minacce informatiche continuano ad aumentare. La transizione dalla globalizzazione alla regionalizzazione, la frammentazione della regolamentazione tra le aree economiche e il crescente utilizzo delle tecnologie dell'informazione e della comunicazione (TIC) come strumenti per la difesa degli interessi hanno un'influenza diretta sulla sicurezza informatica dell'economia e della società.

Il dialogo con altri Paesi dimostra che la Svizzera può svolgere un ruolo importante in questo settore. La strategia dell'UFCS è considerata un buon esempio e il lavoro dell'UFCS e del suo personale gode di grande stima. Il modo in cui portiamo avanti operazioni complesse nei nostri affari nazionali e internazionali suscita interesse oltre i confini nazionali.

Ciononostante, rimane difficile affrontare la moltitudine di sfide e rispondere adeguatamente alle aspettative e alle idee espresse dalla comunità economica, dalle università, dai cantoni e dai politici. Dobbiamo fare attenzione a non perdere la concentrazione e a garantire che le nostre attività operative quotidiane continuino a essere svolte secondo gli standard elevati che ci aspettiamo. Inoltre, dobbiamo essere pronti ad ampliare i nostri servizi, se ciò è desiderato e finanziato.

Sono orgoglioso del fatto che siamo riusciti a offrire un'ampia gamma di servizi mantenendo un alto livello di qualità. Questo si riflette nel feedback positivo che riceviamo sia dai nostri partner che dal pubblico. I prossimi due o tre anni saranno decisivi per il nostro sviluppo. Non vedo l'ora di dare forma alla sicurezza informatica della Svizzera insieme al personale dell'UFCS e a tutte le nostre organizzazioni partner. Spero anche che le autorità politiche siano il più chiare possibile sui servizi che dovremo fornire, sulla loro portata e sulle risorse a cui potremo ricorrere per realizzarli.

L'UFCS è motivato a cogliere le opportunità affinché la Svizzera possa continuare a posizionarsi come attore affidabile nel dominio cibernetico, a beneficio dell'economia, della società e delle autorità.

Florian Schütz, Direttore dell'Ufficio federale della cibersicurezza

Cifre chiave per il 2024

13,3 franchi
spese

63
dipendenti

62'954
segnalazioni volontarie di incidenti informatici

616
contatti con i media

1'100
le aziende sul CSH

991'309
Analisi delle segnalazioni di dispositivi infettati da malware

371
segnalazioni di vulnerabilità da parte di hacker etici

38
briefing settimanali sulla situazione informatica

7
campagne di sensibilizzazione

8'116
sistemi di comando e controllo degli aggressori identificati e bloccati

Situazione nel dicembre 2024

Obiettivi dell'UFCS

Visione

La cibersicurezza è un compito congiunto della politica, dell'economia, delle scuole universitarie e della società. Molte organizzazioni e numerosi singoli privati provano difficoltà a valutare e a gestire i ciber-rischi. La mancanza di trasparenza sulla sicurezza dei prodotti digitali genera insicurezza tra i consumatori e vulnerabilità. A causa della crescente interconnessione, i sistemi non sufficientemente protetti possono provocare danni su vasta scala.

L'UFCS si prefigge di incrementare la cibersicurezza in Svizzera in stretta collaborazione con tutti gli attori determinanti:

L'UFCS pone le basi per un'utilizzazione sicura delle prestazioni e delle infrastrutture digitali nel nostro Paese, nell'ottica di rendere la Svizzera uno dei Paesi leader nella sicurezza della digitalizzazione.

Missione

Il compito fondamentale dell'UFCS è rafforzare la cibersicurezza in seno alle infrastrutture critiche, nei settori dell'economia e della formazione nonché presso la popolazione e le autorità, provvedendo a coordinare l'attuazione della ciberstrategia nazionale (CSN).

A tal fine l'UFCS orienta le sue prestazioni a quattro pilastri strategici:

I quattro pilastri strategici

1 Rendere intelligibili le ciberminacce

Mediante una comunicazione adeguata ai diversi gruppi di destinatari, l'UFCS rende intelligibili le complesse interrelazioni che aprono la via alle ciberminacce. In tal modo consente agli ambienti politici, ai rappresentanti dell'economia e ai membri della società civile di discutere con cognizione di causa in merito alla cibersicurezza e consente a tutti gli interessati di assumere le proprie responsabilità in modo da ridurre i rischi sistemici.

2 Mettere a disposizione strumenti di prevenzione da ciberattacchi

L'UFCS consente ai privati e alle organizzazioni svizzere di ridurre la superficie d'attacco nel ciberspazio. Allerta in merito a possibili attacchi, fornisce informazioni e se del caso mette a disposizione strumenti tecnici volti a facilitare la prevenzione.

3 Ridurre i danni dei ciberincidenti

L'UFCS aiuta chi è stato colpito da un ciberincidente a ridurre i danni e a limitare il rischio che l'incidente si diffonda provocando ulteriori vittime.

4 Incrementare la sicurezza dei prodotti e dei servizi digitali

L'UFCS promuove modelli economici e crea incentivi necessari a consentire ai produttori di offrire prodotti e servizi sicuri ed economicamente accessibili. A favore degli utenti, promuove la trasparenza affinché dispongano delle informazioni necessarie per scegliere prodotti e servizi sicuri da ciberattacchi.

Risorse finanziarie

Per l'UFCS, l'anno 2024 è stato segnato finanziariamente dalla trasformazione in ufficio federale e dall'imminente introduzione dell'obbligo di segnalazione. Le assunzioni scaglionate e il rinvio dei progetti informatici previsti hanno portato a un'eccedenza di bilancio. Da queste saranno create delle riserve per gli anni futuri, che aiuteranno a portare avanti i progetti più importanti nonostante il budget limitato.

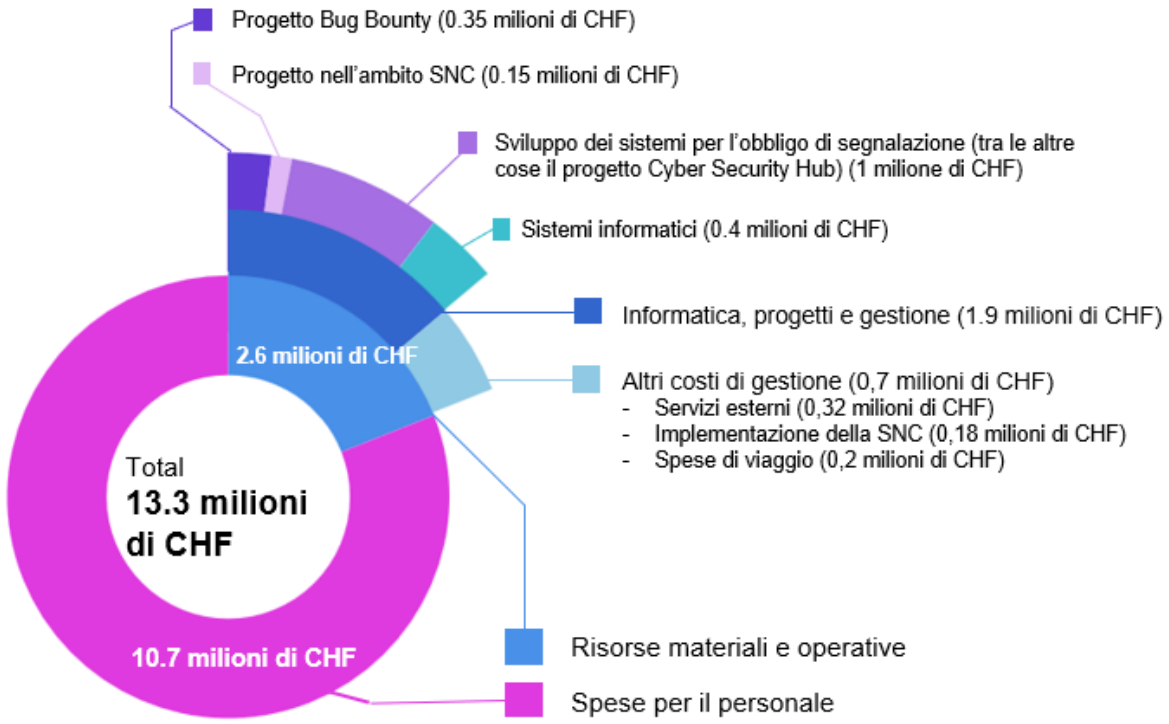


Illustrazione 1: Risorse finanziarie UFCS - Conto 2024

Spesa nel 2024

Nel 2024, i conti finali dell'UFCS erano di 13,3 milioni di franchi. Le spese materiali e operative ammontano a 2,6 milioni di franchi. Degli 1,9 milioni di franchi spesi per l'informatica, 0,4 milioni sono stati destinati alle operazioni e 1,5 milioni agli sviluppi futuri. Una parte significativa della spesa IT è stata dedicata alla creazione del nuovo punto di contatto per la segnalazione di attacchi informatici alle infrastrutture critiche. Un milione di franchi è stato speso per lo sviluppo del Cyber Security Hub (CSH). Non sono inclusi i costi dei fornitori di servizi per la Confederazione, sostenuti dalla Segreteria generale del Dipartimento federale della difesa, della protezione della popolazione e dello sport (GS-DDPS). Circa 0,35 milioni di franchi sono stati utilizzati per programmi di bug bounty volti a individuare e correggere le vulnerabilità nei sistemi informatici dell'Amministrazione federale. 0,33 milioni di franchi sono stati spesi per progetti nell'ambito del CSN, tra cui lo sviluppo di una piattaforma per l'analisi degli incidenti informatici e misure di sensibilizzazione.

Utilizzo delle risorse finanziarie di

La maggior parte delle risorse materiali e operative è dedicata alla prevenzione, al trattamento e al monitoraggio degli incidenti informatici (88%). Sono quindi utilizzate per la missione principale dell'UFCS. Le spese amministrative sono ridotte al minimo, pari all'8% nel 2024.

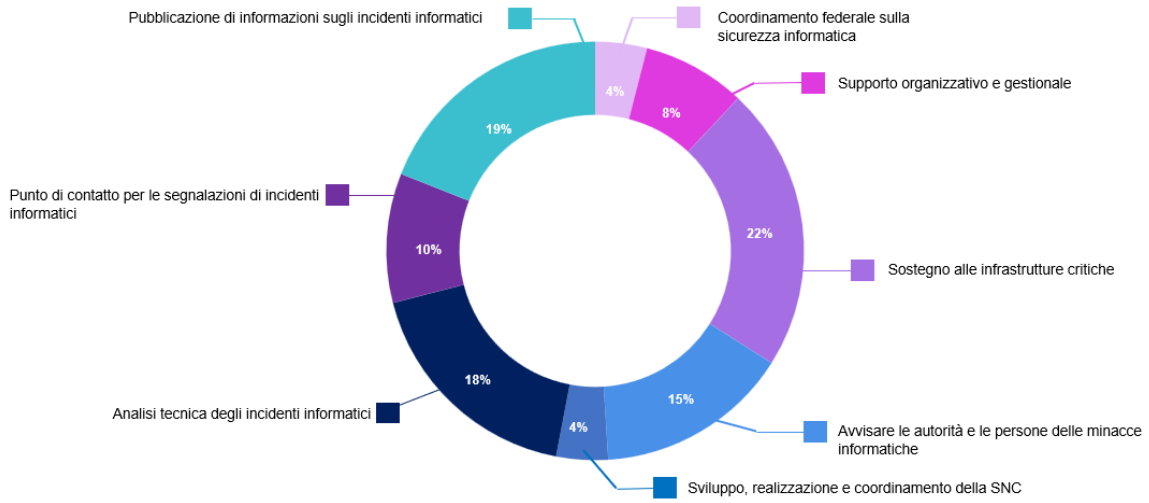


Illustrazione 2: Ripartizione delle risorse finanziarie per compito

Struttura del personale

La spesa per le risorse umane è stata di 10,7 milioni di franchi svizzeri. Nel corso dell'anno, l'UFCS ha potuto assumere 24 nuovi membri del personale. In particolare, il team di reazione agli incidenti è stato notevolmente rafforzato. L'aumento del personale era già stato pianificato al momento della trasformazione in ufficio federale ed è stato utilizzato anche per prepararsi all'introduzione dell'obbligo di segnalare gli attacchi informatici contro le infrastrutture critiche. Per incoraggiare i giovani talenti e offrire loro un'esperienza preziosa nel campo della sicurezza informatica, l'UFCS ha reclutato appositamente dei tirocinanti universitari per contribuire ai nostri progetti.

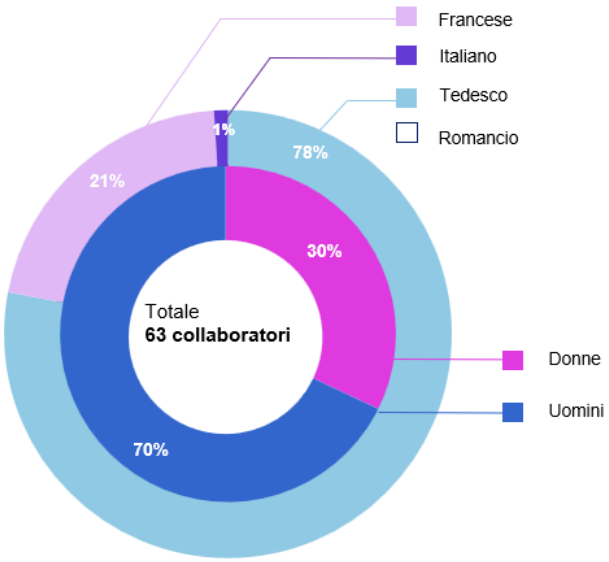


Illustrazione 3: Collaboratori dell'UFSC nel dicembre 2024

Metodo di gestione

Obiettivi e risultati chiave

Dal quarto trimestre del 2024, l'UFCS lavora secondo la metodologia OKR (Objectives & Key Results). L'introduzione o la transizione al quadro OKR adattato all'UFCS è stata graduale, basata sulle esigenze e sulla struttura amministrativa e le basi organizzative dell'UFCS.

Lo strumento di pianificazione e direzione garantisce che tutti i settori di competenza dell'UFCS lavorino in modo coordinato e mirato ogni trimestre per attuare i temi strategici e i compiti statutari dell'Ufficio. L'applicazione della metodologia rafforza l'autonomia dei team, coinvolge i dipendenti a tutti i livelli gerarchici, sia nella fase di pianificazione che in quella di attuazione, e fornisce un quadro chiaro. Stabilendo trasparenza e tracciabilità, nonché un flusso fluido di informazioni all'interno dell'organizzazione, la metodologia contribuisce anche allo sviluppo della cultura aziendale dell'UFCS.

Dopo la fase pilota, si è già osservato un primo effetto positivo. La fase di introduzione è stata completata e la metodologia è parte integrante degli strumenti di gestione dell'UFCS dal 2025. Lo di pianificazione e gestione continua a richiedere particolare attenzione per essere integrato in modo ottimale nelle strutture e nei processi dell'Ufficio nel contesto generale dell'amministrazione federale.

Obiettivi T4 2024

- O1 - Le persone e le organizzazioni interessate sono informate sui servizi offerti dall'UFCS.
- O2 - L'UFCS sta creando le condizioni iniziali per posizionarsi a livello internazionale.
- O3 - L'UFCS dimostra l'utilità del suo lavoro.
- O4 - I settori di importanza sistemica della Svizzera sono sostenuti dall'UFCS nella loro sicurezza informatica.

Illustrazione 4: Obiettivi illustrati Q4

Compiti dell'UFCS secondo i suoi quattro pilastri strategici

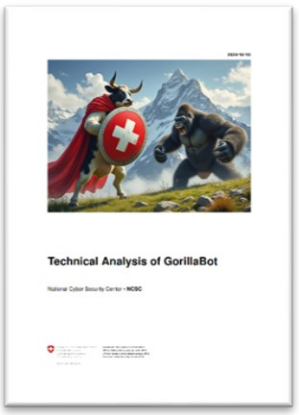
1 Rendere intelligibile le ciberminacce

Nel 2024 l'UFCS ha diffuso costantemente informazioni mirate sulle minacce informatiche alle imprese, alle autorità e al pubblico in generale. Queste informazioni contribuiscono a rafforzare la protezione contro le minacce informatiche in modo mirato. L'UFCS utilizza il suo come canale di comunicazione per il pubblico, pubblicando avvisi attuali, revisioni settimanali e brevi analisi tecniche. Inoltre, i rapporti semestrali hanno contribuito a fornire una panoramica completa dei principali eventi e sviluppi in materia di sicurezza informatica, oltre a raccomandare azioni strategiche.

L'UFCS contribuisce anche a una migliore comprensione della sicurezza informatica attraverso campagne di sensibilizzazione. Con la campagna SUPER 2024 e il Mese europeo della sicurezza informatica, l'UFCS si è rivolto al grande pubblico in collaborazione con le organizzazioni partner. Sono state organizzate anche campagne specifiche per alcuni gruppi target, come le autorità locali.

Sicurezza informatica preventiva

Oltre fornire informazioni sulle minacce informatiche, l'UFCS rafforza la prevenzione sviluppando metodi e formazione e producendo pubblicazioni e presentazioni che forniscono un supporto mirato ai decisori economici, amministrativi e politici. Gli standard minimi di sicurezza ICT, le raccomandazioni e le migliori pratiche sono gli elementi chiave di questo lavoro. L'UFCS sviluppa queste basi in stretta collaborazione con organizzazioni di standardizzazione riconosciute a livello internazionale. Nel 2024, l'UFCS si è concentrato sullo sviluppo delle basi per l'integrazione della crittografia post-quantistica e sul miglioramento delle procedure di sicurezza nelle aziende. L'UFCS ha anche pubblicato risultati in riviste specializzate di fama internazionale. Le pubblicazioni dell'UFCS, in particolare sulla messa in discussione critica delle stime di probabilità e degli standard di sicurezza nella gestione del rischio, hanno suscitato interesse a livello internazionale e contribuito a uno scambio trasparente e critico nel campo della cybersecurity.



Cybersecurity nella catena di approvvigionamento

Nel 2024 l'UFCS, in collaborazione con Planzer Transport AG, ha condotto un progetto pilota sulla sicurezza informatica nella catena di fornitura. L'obiettivo era quello di unire le competenze e le risorse dell'industria e della cybersicurezza per sviluppare un approccio strutturato e strumenti pratici per migliorare la cybersicurezza delle aziende lungo tutta la catena di fornitura. Questi strumenti dovrebbero aiutare le aziende a identificare e valutare sistematicamente i rischi di cybersecurity nella catena di fornitura e a gestirli in modo mirato.

Il successo del progetto pilota sottolinea il fatto che la sicurezza informatica non è un progetto una tantum, ma un processo continuo. La stretta collaborazione tra tutte le parti interessate ha permesso di sviluppare una soluzione che contribuirà a migliorare la sicurezza della catena di approvvigionamento a lungo termine.

Sviluppo di un approccio strutturato: il ciclo sviluppato consente di migliorare continuamente la situazione della sicurezza informatica.

Implementazione pragmatica: grazie a un approccio pratico e scalabile, il concetto è stato implementato rapidamente e l'impegno delle associazioni è stato assicurato.

Sfide affrontate: le sfide principali sono state la definizione di un approccio comune, la creazione di un linguaggio armonizzato e la pianificazione delle risorse per attività parallele e sovrapposte.

Trasferimento di conoscenze per le PMI: le conoscenze acquisite nell'ambito del progetto non andranno solo a beneficio del settore della logistica e dei trasporti, ma saranno messe a disposizione di altre PMI in Svizzera a partire dal 2025.

Sviluppo del prodotto: un gruppo di esperti lavorerà costantemente all'ottimizzazione e al miglioramento degli strumenti per incorporare nuovi requisiti di sicurezza informatica.

Illustrazione 5: Misure di protezione dagli attacchi informatici nella catena di fornitura

Attuazione della ciberstrategia nazionale (CSN)

L'attuale CSN è stata approvata dal Consiglio federale e dai Cantoni nell'aprile 2023. Nel 2024 l'UFCS ha continuato a portare avanti e coordinare l'attuazione della CSN con l'obiettivo di rafforzare la resilienza nazionale di fronte alle crescenti minacce informatiche. L'attuazione è monitorata da un comitato direttivo. Il ruolo e la composizione del Comitato direttivo sono stati ampliati per conferirgli maggiore indipendenza e per consentire una maggiore direzione strategica e un più ampio sostegno. Il Comitato direttivo del CSN si è riunito per la prima volta nel giugno 2024. Dopo la sua istituzione, nel 2024 ha istituito cinque gruppi di lavoro lungo i cinque obiettivi strategici del CSN, al fine di approfondire la strategia e valutare e ponderare le priorità future.

Nel settembre 2024 l'UFCS ha organizzato la conferenza nazionale sulla sicurezza informatica in collaborazione con la rete integrata Svizzera per la sicurezza (RSS). La conferenza era incentrata sul tema «Geopolitica e sicurezza operativa». La conferenza ha contribuito ad approfondire lo scambio di conoscenze e la cooperazione nazionale e ha sottolineato l'impegno comune di tutti gli attori nell'attuazione degli obiettivi e delle misure della CSN. Vi hanno preso parte oltre 280 persone provenienti dal mondo economico e scientifico, nonché dai Cantoni e dalla confederazione. Il 93% dei partecipanti ha giudicato l'evento buono o eccellente (valore di raccomandazione (NPS): 59). L'UFSC svolge un ruolo centrale nell'attuazione della CSN e, grazie al lavoro presentato in questo rapporto, sta dando un contributo fondamentale all'attuazione dei cinque obiettivi strategici e, in particolare, a 15 delle 17 misure. Ulteriori informazioni sull'attuazione del CSN saranno pubblicate nel primo rapporto di attuazione del CSN del 2025.

Illustrazione 6: Obiettivi e misure CSN

2 Mettere a disposizione strumenti di prevenzione

Lo scambio di informazioni sulle minacce attuali, sui modelli di attacco e sulle possibili contromisure è un elemento chiave nella prevenzione degli attacchi informatici. L'UFCS si considera quindi una piattaforma per questo scambio di informazioni e sta lavorando per garantire che le informazioni rilevanti sugli attacchi informatici siano centralizzate e analizzate, e che i risultati di queste analisi siano poi messi a disposizione di tutte le organizzazioni interessate sotto forma di raccomandazioni per l'azione.

Scambio di informazioni su CSH

Dall'autunno del 2022, l'UFCS gestisce il Cyber Security Hub (CSH) per lo scambio di informazioni sulle minacce e sulle misure informatiche tra le autorità e le imprese. Questa piattaforma funge da strumento per lo scambio e la gestione di informazioni su minacce informatiche, incidenti informatici, vulnerabilità e pratiche di sicurezza informatica.

Nel 2024, il CSH si è evoluto in una piattaforma più potente, facile da usare ed efficiente. Questi miglioramenti contribuiscono a garantire alle organizzazioni svizzere una migliore protezione contro le minacce informatiche. Ciò si riflette anche nel fatto che il numero di utenti del CSH è passato da 1.000 nel 2023 a 3.300 nel 2024.

Le aziende iscritte al CSH ricevono aggiornamenti settimanali sulla situazione attuale delle minacce informatiche tramite scambi online. Ogni settimana, circa 350 specialisti di sicurezza informatica partecipano a questi eventi. (NPS: 60).

Iniziative di settore

Lo scambio di informazioni avviene anche attraverso la fornitura di servizi elettronici specifici per il settore**.** A tal fine, l'UFCS sostiene la creazione di «centri di cibersicurezza» (CSC) in vari settori e comunità. I CSC sono centri di competenza settoriali per le misure preventive della cibersicurezza, lo scambio di informazioni, l'analisi delle minacce e le misure di sensibilizzazione, nonché la gestione degli incidenti. Lavorano in stretta collaborazione con l'UFCS, ma tengono anche conto delle esigenze degli attori settoriali nel campo della cybersecurity. In particolare, l'UFCS agisce come coordinatore centrale e operatore del CSH nazionale. La visione dell'UFCS è quella di organizzare tutti i settori critici in CSC settoriali. I CSC già istituiti sono il FS-CSC con il settore finanziario e la «Swiss Industry Cybersecurity Association» (SWICYBA - CSC). Attualmente sono in fase di sviluppo il Healthcare-CSC, la cui fase pilota si è conclusa nel febbraio 2025, e il Rail-ISAC con il settore ferroviario. Il concetto di IG-CSC con le organizzazioni non governative della Ginevra internazionale è pronto e sarà implementato a seconda delle risorse disponibili.

Altre iniziative prevedono l'organizzazione di tavole rotonde settoriali con le infrastrutture critiche.

Informazioni sulle minacce informatiche

L'UFCS fornisce agli operatori delle infrastrutture critiche informazioni tecniche sulle attuali minacce informatiche (note anche come «Cyber Threat Intelligence») e mantiene uno scambio regolare con loro.

Attraverso la piattaforma antiphising.ch l'UFCS ha ricevuto 975.309 segnalazioni di siti web sospetti, da cui sono stati identificati più di 20.000 siti di phishing. Inoltre, l'UFCS ha ricevuto quasi un milione di segnalazioni relative a dispositivi infetti come smartphone, computer o oggetti connessi (IoT) situati in Svizzera, e le ha trasmesse agli operatori interessati o ai relativi fornitori di servizi Internet. Infine, l'UFCS è stato in grado di identificare 8.116 server utilizzati dai criminali informatici per controllare i dispositivi infettati da software maligni (noti come «malware»).

Lo scambio di informazioni tecniche sulle minacce informatiche attraversa anche le frontiere. Ciò consente di monitorare rapidamente la situazione delle minacce informatiche. Le informazioni tecniche possono essere condivise in modo rapido e appropriato, facilitando una risposta rapida ed efficace alle nuove minacce informatiche. Nel 2024, utilizzando analisi tecniche, l'UFCS è stato in grado di identificare gli elementi chiave di un sofisticato attacco di «spear phishing» rivolto agli Stati europei e di allertare rapidamente gli Stati interessati attraverso i canali stabiliti.

Nell'ambito di un «Proof of Concept» e di un partenariato pubblico-privato, è stata sviluppata anche una piattaforma di analisi. Questa consente di scambiare e analizzare informazioni sui rischi informatici sistemici. Quattro fornitori di informazioni del settore privato mettono a disposizione dati sugli incidenti informatici a vari livelli - organizzativo, umano e tecnico - che vengono analizzati dall'UFCS. In futuro, l'UFCS utilizzerà queste informazioni per sviluppare prodotti che contribuiranno a migliorare la resilienza informatica in Svizzera.

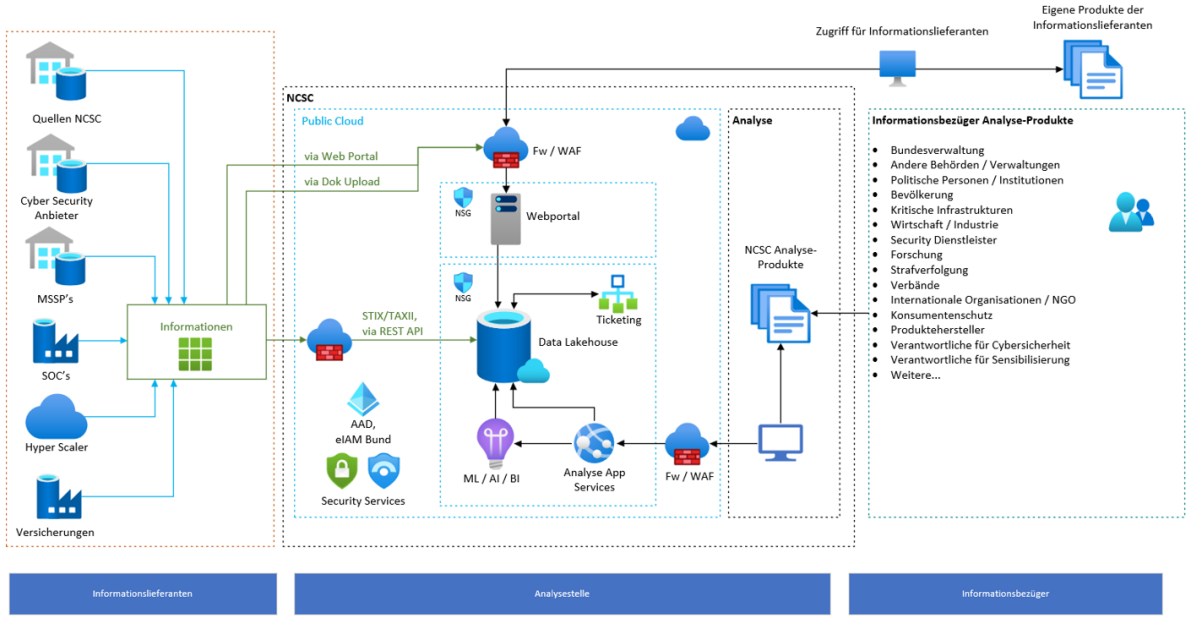


Illustrazione 7: Architettura logica del Cyber Analysis, Research & Collaboration (CyARC)

Sportello unico svizzero per gli incidenti informatici

Oltre a scambiare informazioni sulle minacce informatiche alle infrastrutture critiche, l'UFCS gestisce lo sportello unico svizzero per gli incidenti informatici, rivolto al grande pubblico e alle piccole e medie imprese. Grazie a queste segnalazioni volontarie, l'UFCS identifica le tendenze emergenti in materia di minacce informatiche e può lanciare allarmi di conseguenza. L'UFCS rende inoltre disponibili sul proprio sito web le statistiche sugli incidenti informatici segnalati e presenta i casi più significativi in una sintesi settimanale.

Tra i reati fraudolenti più frequentemente segnalati dalle aziende, si è registrato un forte aumento del caso della «truffa del presidente», con un totale di 716 segnalazioni. D'altra parte, le segnalazioni di incidenti di ransomware sono leggermente diminuite nel 2024: mentre l'anno precedente erano stati segnalati 109 incidenti, nell'anno in esame ne sono stati registrati 92.

Il modulo di segnalazione è stato rivisto nell'aprile 2024, in parte per far fronte al costante aumento delle segnalazioni che utilizzano le stesse risorse, ma anche per offrire un servizio migliore alle persone che segnalano.

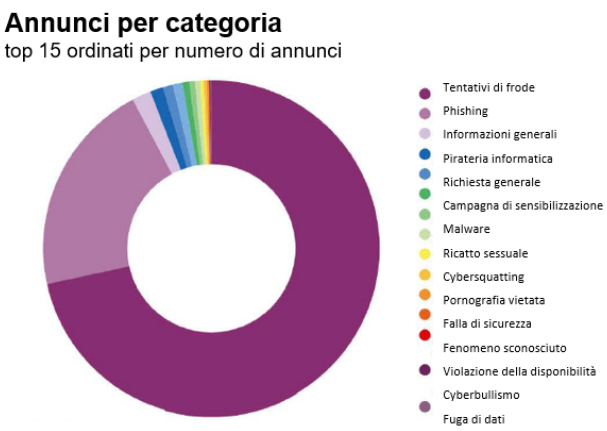


Illustrazione 8: Dichiarazioni volontarie

3 Ridurre i danni dei ciberattacchi

L'UFCS non solo ha analizzato le minacce, ma ha anche supportato gli operatori delle infrastrutture critiche, l'amministrazione e la Svizzera come piazza economica nella gestione degli incidenti informatici. In caso di incidenti informatici che interessano l'Amministrazione federale, l'UFSC è responsabile della gestione operativa. A tal fine, l'UFCS ha istituito un'organizzazione di reperibilità per garantire la disponibilità telefonica di esperti tecnici 24 ore su 24, 7 giorni su 7. Questo supporto ha permesso di limitare il numero di incidenti informatici e di ridurre i costi di gestione. Questo supporto ha permesso di limitare i danni e di evitare che gli incidenti si aggravassero. Tuttavia, i lavori necessari dopo l'attacco - come la reinstallazione dei sistemi informatici - hanno dovuto essere eseguiti dalle aziende interessate, senza l'aiuto della Confederazione, in conformità con il principio di sussidiarietà.

Nel 2024, gli sforzi dell'UFCS per la gestione degli incidenti si sono concentrati in particolare sulla protezione degli incidenti in occasione di eventi particolarmente esposti alle minacce informatiche. Si sono svolti diversi eventi di questo tipo, tra cui l'incontro annuale del World Economic Forum (WEF) e la conferenza di alto livello sulla pace in Ucraina il 15 e 16 giugno 2024. Durante questi eventi si sono verificati diversi attacchi informatici, ma grazie a una buona preparazione sono stati rapidamente messi sotto controllo. Oltre coordinamento generale delle contromisure, l'UFCS è stato responsabile dello sviluppo dell'analisi dei rischi, dell'esame delle vulnerabilità delle principali infrastrutture (Attack Surface Management), della sensibilizzazione di tutti gli stakeholder, dello sviluppo di analisi di «Threat Intelligence» e della difesa - in stretta collaborazione con tutti i partner coinvolti. Questi eventi hanno evidenziato la qualità della collaborazione interistituzionale. In effetti, la Svizzera ha ricevuto diverse richieste dall'estero per capire come proteggersi efficacemente da tali eventi in tempi così brevi.

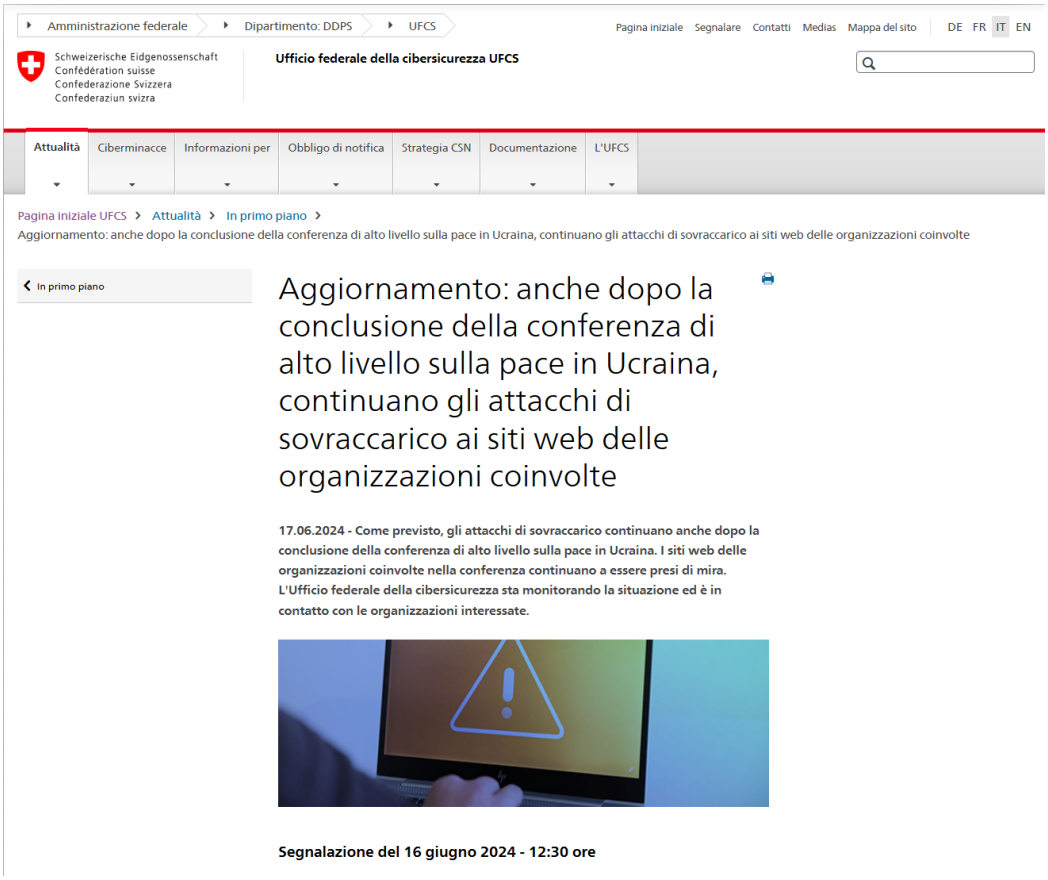


Illustrazione 9: Aggiornamento sulla situazione durante la conferenza di alto livello sulla pace in Ucraina

4 Incrementare la sicurezza dei prodotti e dei servizi digitali

Le vulnerabilità nei dispositivi tecnici, nell'hardware e nel software sono ancora uno dei principali punti di ingresso per gli incidenti informatici. Per sostenere l'economia e il pubblico in generale, l'UFSC ha concentrato i suoi sforzi su due aree. Da un lato, l'UFCS funge da autorità ufficiale svizzera per la numerazione dei CVE, dove i ricercatori possono segnalare le vulnerabilità scoperte nei prodotti. L'UFCS funge da intermediario tra le persone che hanno identificato la vulnerabilità e i produttori di prodotti, per consentire una rapida correzione delle vulnerabilità, assegnando al contempo un identificatore unico che renda la vulnerabilità riconoscibile su scala globale. Inoltre, l'UFCS sta sperimentando il programma bug bounty dell'amministrazione federale, volto a rafforzare la sicurezza informatica della sua infrastruttura IT. L'UFCS ha anche rafforzato la sua collaborazione con il National Test Centre for Cybersecurity (NTC), un'iniziativa del Cantone di Zugo. Questo centro testa i prodotti informatici per individuare le falle di sicurezza quando nessun altro lo fa.

Bug Bounty

L'implementazione di programmi di bug bounty all'interno dell'amministrazione federale contribuisce a rafforzare la sicurezza informatica dell'infrastruttura IT e a ridurre i rischi informatici in modo efficiente ed economico. Nel 2024 l'UFCS ha ricevuto un totale di 371 segnalazioni di vulnerabilità da parte di hacker etici. Dopo un'analisi tecnica, 239 di queste sono state ritenute valide e, di conseguenza, è stato versato un totale di 250.900 franchi svizzeri in taglie. Tutti i dipartimenti e la Cancelleria federale sono stati colpiti dalle violazioni della sicurezza. Il 12% delle vulnerabilità di sicurezza valide, ossia un totale di 45 segnalazioni, è stato classificato come «critico» e quindi doveva essere trattato come priorità assoluta all'interno dell'Amministrazione federale e corretto senza indebiti ritardi. Altre 51 vulnerabilità sono state valutate come «alte» e rappresentano un rischio significativo per l'Amministrazione federale. È quindi essenziale che vengano affrontate rapidamente, poiché il loro potenziale di danno è paragonabile a quello delle vulnerabilità critiche. Anche in questi casi, quindi, il processo di patching deve essere avviato il più rapidamente possibile, al fine di ridurre la superficie di attacco per i criminali informatici. Altre 102 vulnerabilità sono state classificate come medie. Infine, le restanti 41 vulnerabilità sono state classificate come «basse», cioè non molto critiche.

Il programma Bug Bounty ha dovuto essere sospeso nel settembre 2024, poiché il budget disponibile era stato completamente utilizzato. La maggior parte dei finanziamenti per il programma Bug Bounty è stata fornita dal settore trasformazione digitale e governance IT della Cancelleria federale.

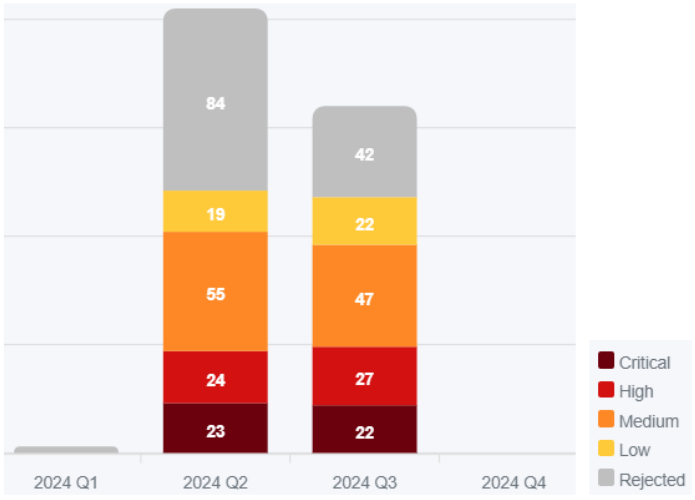


Illustrazione 10: Numero di segnalazioni

Prospettive e obiettivi per l'anno prossimo

Per l'anno 2025, l'UFCS si trova di fronte a grandi opportunità e sfide nel campo della sicurezza informatica. Le richieste in questo settore in rapida evoluzione continuano a crescere, rendendo indispensabile un uso mirato delle risorse disponibili e la definizione di chiare priorità. Con un budget previsto di 16,1 milioni di franchi svizzeri e riserve accantonate che consentono di riportare i fondi all'anno successivo, i progetti attuali possono essere portati avanti nel 2025. Tuttavia, l'attuale pianificazione finanziaria non prevede investimenti significativi nell'UFCS. Allo stesso tempo, si prevede che le minacce informatiche si intensifichino, soprattutto in un contesto geopolitico sempre più teso. L'UFCS intende affrontare queste sfide adottando un duplice approccio:

1. Definizione delle priorità: l'UFSC stabilisce le priorità delle sue missioni in base al rapporto costi/benefici per la sicurezza informatica della Svizzera a breve e medio termine.

2. Piattaforma: l'UFCS agisce principalmente come piattaforma scambio e moltiplicatore dei contributi dei suoi partner. Ove possibile, l'UFCS agisce organo di coordinamento e di facilitazione, colmando, se necessario, le lacune di competenze.

Priorità chiare in un ambiente in espansione

A causa della duplice tattica, nel 2025 l'UFCS si concentrerà su tre aree d'azione centrali:

1. Sviluppo continuo della piattaforma digitale: la piattaforma digitale è la spina dorsale della strategia di sicurezza informatica dell'Ufficio federale. Il miglioramento continuo è essenziale per affrontare efficacemente le minacce in costante evoluzione.

2. Attuazione della ciberstrategia nazionale (CSN): L'attuazione rigorosa della CSN rimane un compito centrale per garantire la sicurezza a lungo termine della Svizzera nello spazio digitale. La pubblicazione del primo rapporto sull'attuazione della CSN offrirà l'opportunità di valutare i progressi compiuti

3. Esecuzione affidabile delle attività operative: la qualità e l'affidabilità delle attività operative sono di fondamentale importanza per l'UFCS. L'attenzione si concentrerà sulle attività operative e tattiche con un impatto immediato o a medio termine, mentre i progetti strategici a più lungo termine saranno inizialmente trattati in modo mirato e ad hoc.

Efficienza attraverso l'ottimizzazione interna

Parallelamente a questa rifocalizzazione sulle principali aree di azione, l'UFCS continuerà a ottimizzare le proprie strutture interne. L'obiettivo è quello di snellire i processi attraverso l'automazione, facilitare ulteriormente la collaborazione con i partner, rafforzare il ruolo di coordinamento dell'UFCS e aumentare l'efficienza complessiva dell'ufficio, in modo da poter rispondere ai crescenti rischi informatici con un livello di qualità costante, almeno nel medio termine.

Prospettive a lungo termine e partnership

L'UFSC continuerà a fare del suo meglio per ottenere i migliori risultati possibili con le risorse disponibili e per rafforzare la sicurezza digitale della Svizzera anche nel 2025. Per farlo, potrà contare sull'ampio sostegno delle istituzioni federali partner e del settore privato. La missione fondamentale rimane invariata: fungere da coordinatore e fornire servizi di alta qualità all'economia, alla società, alle autorità e al mondo accademico.

L'UFSC desidera ringraziare tutti coloro che si impegnano per la cibersicurezza e che contribuiscono all'adempimento del suo mandato.

Pubblicazioni e riferimenti

Pubblicazioni UFCS nel 2024 :

- Relazione semestrale 2023/2
- Relazione semestrale 2024/1
- Rapporto: Truffe telefoniche nel dominio cibernetico
- Analisi tecnica della rete botnet "Gorilla
- Breve analisi tecnica del malware "Poseidon Stealer
- Relazione sull'analisi dei dati a seguito dell'attacco informatico a Xplain
- Rapporto anti-phishing 2023
- Considerazioni tecnologiche, Computer quantistici e crittografia
- Valutazione UFCS, Crittografia post-quantistica e misure da
- Rapporto sulla sicurezza informatica della Confederazione nel 2023
- Raccomandazioni per i controlli di sicurezza sulle persone nelle aziende
- Misure di resilienza informatica per grandi eventi e conferenze internazionali
- Conferenza di alto livello sulla pace in Ucraina: prima valutazione dell'UFCS sul lavoro della rete di monitoraggio della situazione

Articoli

- A. Grünert, J. B. Michael, R. Oppliger e R. Rytz, "Why Probabilities Cannot Be Used in Cyber Risk Management", in *Computer*, vol. 57, n. 10, pp. 86-89, ott. 2024.
- R. Oppliger e A. Grünert, "How to Measure Cybersecurity and Why Heuristics Matter" (Come misurare la sicurezza informatica e perché le euristiche contano), in Computer, vol. 57, n. 2, pp. 111-115, febbraio 2024.