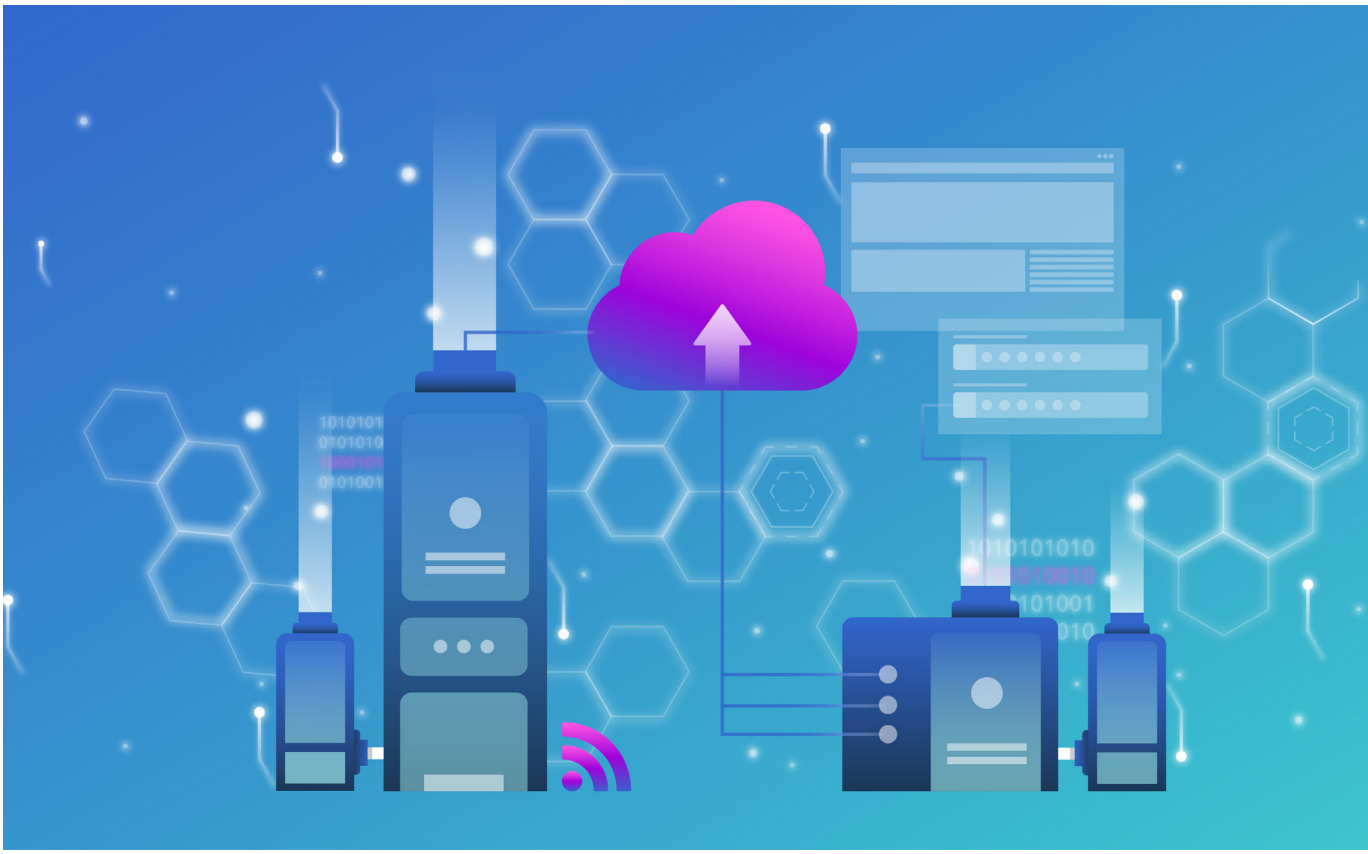
6 maggio 2024 | Ufficio federale della cibersicurezza UFCS



Strategia dell'Ufficio federale della cibersicurezza UFCS

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale della difesa,
della protezione della popolazione e dello sport DDPS
Ufficio federale della cibersicurezza UFCS

Indice

1 Situazione iniziale: le sfide in materia di cibersicurezza in Svizzera

Sul piano della cibersicurezza, in Svizzera si riscontrano attualmente le seguenti sfide principali[1]:

- elevata vulnerabilità dell'economia, delle autorità, degli istituti di formazione e della popolazione nel ciberspazio;
- insufficiente capacità di reazione in caso di ciberincidenti e crisi di rilevanza sistemica;
- scarsa maturità dei prodotti e dei servizi digitali in termini di cibersicurezza e assenza di meccanismi di controllo della qualità;
- comprensione non abbastanza avanzata della problematica della cibersicurezza da parte degli ambienti economici, in seno alla società e a livello politico;
- mancanza di trasparenza e insufficienza di dati per una corretta valutazione delle dichiarazioni in materia di cibersicurezza e per la definizione di corrispondenti misure politiche ed economiche;
- scarsa protezione degli attori non contemplati tra le infrastrutture critiche;
- zone grigie giuridiche e coordinamento lacunoso degli strumenti per la cibersicurezza tra autorità e operatori privati.

In presenza di tali sfide, i ciberattacchi sono spesso condotti con successo provocando gravi danni economici ed elevati rischi di perturbazione delle infrastrutture critiche nazionali.

Negli ultimi anni il numero di segnalazioni di ciberincidenti che hanno provocato danni è aumentato di circa il 30 per cento l'anno. Il numero di segnalazioni provenienti da infrastrutture non critiche è quasi triplicato negli ultimi dodici mesi. Nel 2023 l'UFCS ha elaborato 187 000 segnalazioni di phishing e ha identificato e chiuso in Svizzera 8223 siti web utilizzati per operazioni di phishing. Nel quadro di diverse centinaia di segnalazioni, l'UFCS ha individuato la presenza di malware presso infrastrutture critiche, provvedendo alla loro eliminazione in collaborazione con le aziende colpite. In media ogni 40 ore l'UFCS riceve una segnalazione concernente un'infezione da malware e una relativa richiesta di supporto per la gestione dell'incidente.

In particolare le PMI si ritrovano sempre più spesso nel mirino dei criminali informatici. I dati vengono criptati e rubati mediante attacchi ransomware. In seguito i criminali esigono un riscatto per il decriptaggio dei dati e per evitarne la pubblicazione. Gli attacchi sono in larga misura automatizzati, per cui possono essere attaccate con un minimo dispendio anche imprese di piccole dimensioni. In Svizzera, circa il 75 per cento di tutte le aziende genera un fatturato inferiore a 500'000 franchi l'anno. Per queste aziende è particolarmente difficile investire nella cibersicurezza. Devono pertanto poter fare affidamento su modalità sicure di sviluppo e manutenzione di prodotti e servizi digitali oppure su prestazioni di sicurezza economicamente accessibili.

[1] Elenco elaborato in base alle verifiche dell'efficacia della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (cfr. Verifica dell'efficacia della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022), sulla scorta della Ciberstrategia nazionale (CSN) nonché in base ai rapporti settimanali e alle statistiche dei casi del Servizio di contatto, di GovCERT e dell'OIC.

I ciberattacchi non risparmiano nemmeno la popolazione. A questo livello è diffuso soprattutto il fenomeno delle truffe informatiche. In seno alla popolazione sono chiaramente individuabili un crescente senso di insicurezza e l'esigenza di informazioni e servizi di supporto.

Nel contempo, presso le scuole universitarie svizzere e aziende innovative, sono in fase di elaborazione soluzioni interessanti nel campo della cibersicurezza. Il loro piazzamento sul mercato o addirittura la creazione di standard globali si stanno tuttavia rivelando obiettivi ardui da raggiungere.

2 Visione dell'UFCS

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.

3 Missione: i quattro pilastri strategici dell'UFCS

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:

1. **rendere intelligibili le ciberminacce**
2. **mettere a disposizione strumenti di prevenzione da ciberattacchi**
3. **ridurre i danni dei ciberincidenti**
4. **incrementare la sicurezza dei prodotti e dei servizi digitali**

3.1 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.

Una delle domande più frequenti poste da membri di consigli di amministrazione, dirigenti aziendali e singoli privati è: «Che cosa possiamo fare per proteggerci da ciberincidenti?». La cibersicurezza è tema di frequenti discussioni anche a livello politico. I decisori si trovano in continuazione di fronte alla sfida di dover valutare ciberminacce e individuare contromisure.

L'UFCS raccoglie informazioni sulle svariate caratteristiche dei ciberincidenti, mette a punto un quadro delle correlazioni e ne deduce corrispondenti campi d'azione, argomenti di discussione e raccomandazioni. In tal modo l'UFCS contribuisce a far sì che le discussioni sulla tematica delle ciberminacce siano fondate su informazioni sicure e consente a tutti gli interessati di assumere le proprie responsabilità, in modo da ridurre i rischi sistemici. Per sviluppare ulteriormente i rispettivi prodotti e servizi in funzione delle esigenze, i fornitori di soluzioni di cibersicurezza possono basarsi sulle analisi dell'UFCS.

3.2 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.

I ciberattacchi abbisognano di preparazione. I criminali informatici analizzano la vulnerabilità dei possibili obiettivi, acquistano o sviluppano in proprio malware opportuni e svolgono tentativi iniziali d'accesso. Molti autori di ciberattacchi impiegano metodi e procedimenti simili. L'UFCS individua gli schemi d'attacco frequenti e provvede a informare e allertare al riguardo i partner e le potenziali vittime. Le informazioni fornite spaziano da indicazioni tecniche sui vettori d'attacco fino a resoconti sui metodi impiegati da determinati criminali per scegliere i propri obiettivi. Tali informazioni consentono di allertare le organizzazioni interessate affinché aumentino il proprio livello di protezione.

Ancor più importante dell'individuazione tempestiva è ridurre la superficie d'attacco. Tre fattori contribuiscono in maniera determinante ad abbassare il livello di cibersicurezza: 1) punti di vulnerabilità presenti nei sistemi; 2) errori di configurazione dei sistemi; 3) comportamenti errati degli utenti.

Promuovendo l'individuazione tempestiva e l'eliminazione dei punti di vulnerabilità, l'UFCS riduce la superficie d'attacco dei sistemi utilizzati dai privati e dalle organizzazioni svizzere. Allerta gli utenti in caso di attacchi e mette a disposizione le informazioni necessarie per la protezione. Per prevenire attacchi su vasta scala con potenziali ripercussioni sistemiche, l'UFCS impiega in maniera mirata i pertinenti strumenti tecnologici e collabora con le autorità competenti per disciplinare misure di sicurezza vincolanti.

L'UFCS sviluppa tecnologie per l'individuazione e la protezione dalle minacce. Questo servizio è offerto dall'UFCS se i prodotti necessari non sono disponibili sul mercato o se la situazione di minaccia giustifica un intervento sul mercato. I prodotti sviluppati in proprio per l'individuazione e la protezione sono messi a disposizione, ogni qual volta possibile, sotto forma di software open source o mediante procedimenti open source.

3.3 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.

I ciberincidenti provocano diversi generi di danni. I danni concreti originati da un attacco dipendono di volta in volta dal modello aziendale o dalla situazione personale delle vittime. Inoltre, nel quadro di un ciberincidente sussiste spesso il rischio che i danni si diffondano presso altri utenti. I criminali informatici possono per esempio sfruttare le connessioni delle vittime per attaccare ulteriori obiettivi. Oppure le perturbazioni e i guasti causati da un ciberincidente possono estendersi, con danni ingenti, anche a terzi.

È possibile ridurre i danni ponendo degli argini temporali e organizzativi agli effetti dei ciberincidenti. In via prioritaria l'UFCS provvede alla prevenzione di minacce sistemiche in grado di pregiudicare il funzionamento dello Stato. Questa categoria di minacce non provoca soltanto guasti di sistema, bensì anche danni economici considerevoli e tali da incidere sensibilmente sull'andamento del prodotto interno lordo (PIL). L'UFCS assiste le vittime nella gestione degli eventi fornendo loro consulenza tecnica nonché assistenza sul piano organizzativo. A seconda del potenziale di danno, le prestazioni di supporto spaziano dalla semplice consulenza fino alla gestione integrale della crisi informatica (protezione tecnica e ripristino compresi). Vale il principio che le prestazioni dell'UFCS sono fornite ai privati in via sussidiaria. Ciò significa che, per quanto possibile, gli interessati devono gestire un evento autonomamente e con il ricorso a prestazioni offerte sul mercato.

L'UFCS crea strutture nazionali e internazionali volte a semplificare il coordinamento della gestione di ciberincidenti. Nel quadro di eventi che coinvolgono diverse autorità svizzere, l'UFCS funge da organo direttivo. Mettendo a disposizione pertinenti documentazioni ed emanando raccomandazioni sulle best practices, l'UFCS consente alle organizzazioni e a singoli privati di prepararsi in maniera ottimale alla gestione di un ciberincidente.

3.4 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.

Dalle ricerche svolte sulla tematica della sicurezza risulta che quasi ogni applicazione presenta almeno un punto di vulnerabilità determinante per la sicurezza. Nemmeno gli hardware sono esenti da errori pregiudizievoli per la cibersicurezza. A causa della complessità degli attuali sistemi TIC, non è possibile escludere completamente simili errori. Tuttavia, la maggior parte degli errori può essere evitata oppure individuata ed eliminata in modo rapido: mediante processi di

sviluppo strutturati in modo idoneo e con l'esecuzione di appositi test lungo tutto il ciclo di vita dei prodotti. Maggiori investimenti nella cibersicurezza rendono inevitabilmente più cari i prodotti. Sul mercato, i prodotti elaborati con procedimenti meno costosi concorrenziano sempre i prodotti sicuri. Per i consumatori è quasi impossibile determinare quanto un prodotto sia sicuro e se un prezzo più elevato implichi effettivamente una maggiore sicurezza.

L'UFCS appoggia ed elabora iniziative e modelli che creano trasparenza per quanto concerne la cibersicurezza dei prodotti rendendo il mercato più favorevole ai prodotti sicuri. Tra le iniziative e i modelli possibili figurano per esempio schemi di etichettamento, proposte di regolamentazione, la creazione di incentivi nonché modelli di finanziamento.

4 Modello operativo dell'UFCS

Per fornire le sue prestazioni nel modo più efficiente possibile, l'UFCS consolida e aggrega i contenuti esistenti, ne garantisce la qualità e li comunica, in funzione delle esigenze, ai fornitori di prestazioni e ai beneficiari delle prestazioni.

L'UFCS opera conformemente al modello vincolante di cooperazione definito nella CSN e lavora in stretta collaborazione con i Cantoni, con l'economia e con le scuole universitarie. L'obiettivo della collaborazione è raggruppare le conoscenze specialistiche e far sì che tutte le parti coinvolte si sostengano a vicenda in modo da consentire un'ottimizzazione della protezione dalle ciberminacce.

L'UFCS elabora contenuti propri e fornisce prestazioni proprie soltanto se non sono disponibili contenuti adeguati di terzi, se i contenuti di terzi non sono impiegabili a beneficio di tutti oppure nei casi in cui contenuti e prestazioni devono essere forniti direttamente dalla Confederazione in virtù di prescrizioni legali o per motivi di affidabilità. L'UFCS intende fungere anche da «vivaio» per nuove prestazioni di cui si riscontra un fabbisogno. Quando simili prestazioni hanno raggiunto un certo grado di maturità e possono essere fornite da terzi in maniera più adeguata, l'UFCS le fornisce ad altre organizzazioni.

Se possibile, le prestazioni dell'UFCS sono fornite in forma digitale attraverso una piattaforma. Sono fornite direttamente soltanto laddove assolutamente necessario, segnatamente nell'assistenza per la gestione di incidenti e in determinati ambiti della sensibilizzazione. La concentrazione delle attività su una piattaforma consente di commisurare le prestazioni dell'UFCS, mantenendo l'impiego delle risorse entro limiti gestibili.

A tal fine l'UFCS allestisce e gestisce una piattaforma di self-service che offre informazioni sulle ciberminacce, raccomandazioni specifiche e generali nonché mezzi per la prevenzione e la condivisione di informazioni.