Ordinanza sulla cibersicurezza (OCS)

del 7 marzo 2025 (Stato 1° aprile 2025)

Il Consiglio federale svizzero,

visti gli articoli 74*c* e 84 capoverso 1 della legge del 18 dicembre 2020[1] sulla sicurezza delle informazioni (LSIn),

ordina:

Sezione 1: Oggetto

Art. 1

La presente ordinanza disciplina:

a. i principi e l'elaborazione della Ciberstrategia nazionale (CSN);
b. i compiti dell'Ufficio federale della cibersicurezza (UFCS);
c. lo scambio di informazioni per la protezione dai ciberincidenti e dalle ciberminacce tra l'UFCS e le autorità nonché le organizzazioni;
d. l'obbligo di segnalazione in caso di ciberattacchi.

Sezione 2: Ciberstrategia nazionale

Art. 2

[1] La CSN definisce i punti seguenti:

a. il quadro strategico per la prevenzione nell'ambito della cibersicurezza;
b. l'individuazione tempestiva delle ciberminacce;
c. le possibilità di reazione e la resilienza in caso di incidenti;
d. la lotta alla cibercriminalità;
e. la cooperazione internazionale.

[2] L'UFCS elabora la CSN unitamente ai rappresentanti dei Cantoni, del settore economico, della società, dei gestori di infrastrutture critiche, del mondo scientifico, della società, dei dipartimenti e della Cancelleria federale.

RU **2025** 169
1 RS **128**

Sezione 3: Compiti dell'UFCS

Art. 3 Richieste sui titolari

Per avvisare autorità, organizzazioni e persone interessate nel caso di una ciberminaccia imminente o di un ciberattacco in corso, l'UFCS può richiedere ai gestori dei registri dei nomi di dominio che rientrano nella competenza della Confederazione i dati di contatto dei titolari dei nomi di dominio.

Art. 4 Analisi tecnica di ciberincidenti e ciberminacce

1 L'UFCS gestisce un team nazionale di risposta alle emergenze informatiche; quest'ultimo svolge in particolare i seguenti compiti:

a. sostegno nella gestione tecnica di ciberincidenti;

b. analisi di questioni tecniche;

c. identificazione e valutazione di ciberminacce.

2 Per l'analisi dei ciberincidenti e delle ciberminacce, gestisce un'infrastruttura resiliente, indipendente dal resto dell'informatica della Confederazione.

Art. 5 Priorizzazione della consulenza e del sostegno in caso di ciberattacchi

1 Se la richiesta di consulenza e sostegno in caso di ciberattacco supera le capacità dell'UFCS, quest'ultimo può stabilire priorità per quanto riguarda la consulenza e il sostegno in relazione ai tempi e all'entità.

2 A tale riguardo tiene conto della sicurezza e dell'ordine pubblici, del benessere della popolazione e del funzionamento dell'economia.

Art. 6 Comunicazione delle vulnerabilità

1 L'UFCS garantisce che le vulnerabilità a livello di hardware e di software siano comunicate in modo coordinato; al riguardo tiene conto degli standard riconosciuti a livello internazionale.

2 Fissa al produttore dell'hardware o del software interessato un termine di 90 giorni per eliminare le vulnerabilità.

3 Può accorciare questo termine se una vulnerabilità:

a. mette a rischio il corretto funzionamento di infrastrutture critiche;

b. concerne sistemi molto diffusi; o

c. è impiegata per un ciberattacco o può essere sfruttata in modo particolarmente semplice per un ciberattacco.

4 Può prolungare il termine fissato se l'eliminazione della vulnerabilità si rivela particolarmente complessa.

5 Può già informare i gestori di infrastrutture critiche prima che le vulnerabilità vengano comunicate o eliminate.

6 Informa immediatamente l'Ufficio federale delle comunicazioni (UFCOM) delle vulnerabilità rilevate negli impianti di telecomunicazione di cui all'articolo 3 lettera d della legge del 30 aprile 1997[2] sulle telecomunicazioni.

7 I capoversi 1–4 non si applicano alle vulnerabilità che l'UFCOM constata e segnala all'UFCS nell'ambito dei suoi controlli di vigilanza (art. 36–40 dell'ordinanza del 25 novembre 2015[3] sugli impianti di telecomunicazione).

Art. 7 Sostegno alle autorità

L'UFCS fornisce sostegno alle autorità della Confederazione e dei Cantoni nello sviluppo, nell'attuazione e nella verifica degli standard e delle regolamentazioni in materia di cibersicurezza.

Sezione 4: Scambio di informazioni

Art. 8 Sistema di comunicazione per lo scambio sicuro delle informazioni e sistemi d'informazione per lo scambio automatico

1 Hanno accesso al sistema di comunicazione dell'UFCS per lo scambio sicuro delle informazioni tutti i gestori di infrastrutture critiche assoggettati all'obbligo di segnalazione nonché le organizzazioni con sede in Svizzera e le autorità.

2 L'UFCS mette a disposizione dei gestori di infrastrutture critiche le informazioni tecniche secondo l'articolo 74 capoverso 2 lettera b LSIn su ciberminacce e ciberincidenti attraverso sistemi di informazione per lo scambio automatico.

3 L'UFCS è responsabile della sicurezza del sistema di comunicazione come pure dei sistemi d'informazione e della liceità del trattamento dei dati.

Art. 9 Registrazione

1 Per utilizzare il sistema di comunicazione le organizzazioni e le autorità devono registrarsi. Devono comunicare immediatamente qualsiasi cambiamento nei dati registrati.

2 La registrazione deve contenere almeno i dati seguenti:

a. ragione sociale, nome o designazione nonché indirizzo;

b. persona di contatto.

2 RS **784.10**
3 RS **784.101.2**

Art. 10 Fornitori di servizi

1 I gestori di infrastrutture critiche possono notificare all'UFCS eventuali fornitori di servizi che forniscono prestazioni nel settore della cibersicurezza per conto di tali gestori e che vogliono partecipare allo scambio di informazioni.

2 I fornitori di servizi devono registrarsi indicando la ragione sociale o il nome come pure i dati della persona di contatto.

Art. 11 Trasmissione e utilizzo delle informazioni

1 In occasione della trasmissione di informazioni le organizzazioni e le autorità registrate stabiliscono a chi l'UFCS può a sua volta trasmettere le informazioni sul sistema di comunicazione per lo scambio sicuro di informazioni, sempreché la trasmissione delle informazioni sia contemplata dalla legge.

2 L'UFCS decide in merito alla pubblicazione delle informazioni autorizzate.

3 I destinatari delle informazioni devono garantire la protezione delle informazioni.

4 I fornitori di servizi registrati di gestori di infrastrutture critiche possono utilizzare le informazioni che ricevono esclusivamente per la protezione delle infrastrutture critiche.

Sezione 5: Obbligo di segnalazione

Art. 12 Eccezioni all'obbligo di segnalazione

1 Le seguenti autorità e organizzazioni sono esentate dall'obbligo di segnalazione alle seguenti condizioni:

a. le scuole universitarie di cui all'articolo 74*b* capoverso 1 lettera a LSIn: con meno di 2000 studenti;

b. le imprese di cui all'articolo 74*b* capoverso 1 lettera d LSIn, a condizione che:
   1. in qualità di gestori di rete, produttori di energia elettrica, gestori di impianti elettrici di stoccaggio o di fornitori di servizi nell'ambito dell'elettricità secondo l'articolo 5*a* capoverso 1 e l'allegato 1*a* dell'ordinanza del 14 marzo 2008[4] sull'approvvigionamento elettrico (OAEl) non siano tenute a rispettare né il livello di protezione A né il livello di protezione B, o
   2. in qualità di esercenti di gasdotti secondo l'articolo 2 capoverso 3 dell'ordinanza del 4 giugno 2021[5] sulla sicurezza degli impianti di trasporto in condotta presentino negli ultimi cinque anni una media di energia trasportata inferiore a 400 GWh all'anno;

4 RS **734.71**
5 RS **746.12**

c. le imprese ferroviarie come pure le imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli di cui all'articolo 74*b* capoverso 1 lettera m LSIn, a condizione che:
   1. non siano incaricate di assumere compiti sistemici (art. 37 della legge federale del 20 dicembre 1957[6] sulle ferrovie [Lferr]),
   2. siano titolari di una concessione per il trasporto di viaggiatori secondo l'articolo 6 legge del 20 marzo 2009[7] sul trasporto di viaggiatori (LTV), ma non forniscono alcuna offerta di trasporto ordinata congiuntamente dalla Confederazione e dai Cantoni (art. 28–31*c* LTV),
   3. dispongano di una concessione d'infrastruttura di cui all'articolo 5 Lferr che però non è stata rilasciata poiché sussiste un interesse pubblico alla costruzione e all'esercizio dell'infrastruttura (art. 6 cpv. 1 lett. a Lferr);

d. le imprese di cui all'articolo 74*b* capoverso 1 lettera n LSIn, a condizione che:
   1. secondo gli articoli 2 e 4 e l'allegato II del regolamento di esecuzione (UE) 2023/203[8] oppure secondo l'articolo 2 e l'allegato del regolamento delegato (UE) 2022/1645[9], non debbano realizzare alcun sistema di gestione della sicurezza delle informazioni,

6 RS **742.101**
7 RS **745.1**
8 Regolamento di esecuzione (UE) 2023/203 della Commissione del 27 ottobre 2022 che stabilisce le regole per l'applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti relativi alla gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le organizzazioni di cui ai regolamenti (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011 e (UE) 2015/340 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e per le autorità competenti di cui ai regolamenti (UE) n. 748/2012, (UE) n. 1321/2014, (UE) n. 965/2012, (UE) n. 1178/2011, (UE) 2015/340 e (UE) n. 139/2014 della Commissione e ai regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, e che modifica i regolamenti (UE) n. 1178/2011, (UE) n. 748/2012, (UE) n. 965/2012, (UE) n. 139/2014, (UE) n. 1321/2014 e (UE) 2015/340 della Commissione e i regolamenti di esecuzione (UE) 2017/373 e (UE) 2021/664 della Commissione, nella versione vincolante per la Svizzera secondo il punto 3 dell'allegato all'accordo del 21 giugno 1999 tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo (RS **0.748.127.192.68**).
9 Regolamento delegato (UE) 2022/1645 della Commissione del 14 luglio 2022 recante modalità di applicazione del regolamento (UE) 2018/1139 del Parlamento europeo e del Consiglio per quanto riguarda i requisiti per la gestione dei rischi per la sicurezza delle informazioni con un potenziale impatto sulla sicurezza aerea per le imprese disciplinate dai regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione e che modifica i regolamenti (UE) n. 748/2012 e (UE) n. 139/2014 della Commissione, nella versione vincolante per la Svizzera secondo il punto 3 dell'allegato all'accordo del 21 giugno 1999 tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo (RS **0.748.127.192.68**).

2. non debbano applicare le direttive di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998[10] nel loro programma di sicurezza secondo gli articoli 2, 12, 13 o 14 del regolamento (CE) n. 300/2008[11];

e. i fornitori e i gestori di servizi di cui all'articolo 74*b* capoverso 1 lettera t LSIn, a condizione che non forniscano le loro prestazioni in parte o interamente dietro compenso a favore di terzi.

[2] Le autorità e le organizzazioni di cui all'articolo 74*b* capoverso 1 lettere g, h, l e p LSIn sono esentate dall'obbligo di segnalazione se nel settore interessato occupano meno di 50 persone e se la loro cifra d'affari annua o il loro totale di bilancio annuo non supera i 10 milioni di franchi.

Art. 13 Trasmissione di documentazione per l'accertamento dell'obbligo di segnalazione

Le autorità e le organizzazioni interessate devono mettere a disposizione dell'UFCS tutti i documenti necessari per fornire informazioni in merito all'assoggettamento all'obbligo di segnalazione.

Art. 14 Ciberattacchi da segnalare

[1] Il funzionamento di un'infrastruttura critica è considerato compromesso se:

a. i collaboratori o terzi sono interessati da interruzioni del sistema; o

b. l'organizzazione o l'autorità interessata può mantenere le proprie attività soltanto con l'aiuto di piani d'emergenza.

[2] Vi è una manipolazione o una fuga di informazioni se:

a. informazioni rilevanti per le attività aziendali vengono consultate, modificate o comunicate da persone non autorizzate; o

b. è stata effettuata una segnalazione di violazioni della sicurezza dei dati secondo l'articolo 24 della legge federale del 25 settembre 2020[12] sulla protezione dei dati.

[3] Un ciberattacco è considerato non identificato per un periodo prolungato se l'incidente si è verificato più di 90 giorni prima.

10 Regolamento di esecuzione (UE) 2015/1998 della Commissione del 5 novembre 2015 che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea, nella versione vincolante per la Svizzera secondo il punto 3 dell'allegato all'accordo del 21 giugno 1999 tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo (RS **0.748.127.192.68**).

11 Regolamento (CE) n. 300/2008 del Parlamento europeo e del Consiglio dell'11 marzo 2008 che istituisce norme comuni per la sicurezza dell'aviazione civile e che abroga il regolamento (CE) n. 2320/2002, nella versione vincolante per la Svizzera secondo il punto 3 dell'allegato all'accordo del 21 giugno 1999 tra la Confederazione Svizzera e la Comunità europea sul trasporto aereo (RS **0.748.127.192.68**).

12 RS **235.1**

4 Un ciberattacco è considerato connesso ai reati di estorsione, minaccia o coazione se suddetti reati sono rivolti contro un'autorità o un'organizzazione assoggettata all'obbligo di segnalazione oppure contro persone che lavorano per tale autorità o organizzazione assoggettata.

Art. 15 Contenuto della segnalazione

1 Oltre alle indicazioni di cui all'articolo 74*e* capoverso 2 LSIn, la segnalazione deve contenere le seguenti informazioni sul ciberattacco:

a. data e ora in cui è stato rilevato l'attacco;

b. data e ora in cui è stato compiuto l'attacco; e

c. indicazioni sull'aggressore.

2 Deve inoltre contenere informazioni che indichino se l'attacco era connesso ai reati di estorsione, minaccia o coazione e se è stata sporta una denuncia penale.

3 Deve contenere le seguenti informazioni sulle ripercussioni del ciberattacco:

a. grado di compromissione della disponibilità, dell'integrità e della confidenzialità delle informazioni; e

b. ripercussioni del ciberattacco sul funzionamento dell'organizzazione o dell'autorità.

4 Se la segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, deve contenere anche le seguenti informazioni sull'autorità o sull'organizzazione assoggettata all'obbligo di segnalazione:

a. ragione sociale, nome o designazione nonché indirizzo; e

b. dati di contatto della persona che effettua la segnalazione.

Art. 16 Termine per registrare la segnalazione

1 Se entro il termine di segnalazione di 24 ore dopo la scoperta del ciberattacco non sono note tutte le informazioni necessarie, l'UFCS concede all'autorità o all'organizzazione interessata un termine di 14 giorni per completare la segnalazione.

2 Se entro la scadenza del termine non sono disponibili tutte le informazioni necessarie, l'UFCS chiede all'autorità o all'organizzazione interessata di completarle immediatamente o di confermare che le informazioni non sono disponibili.

Art. 17 Trasmissione della segnalazione

1 Se la segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, quest'ultimo informa la persona o le persone di contatto di cui all'articolo 9 capoverso 2 lettera b di aver ricevuto la segnalazione e del suo contenuto.

2 Una o più organizzazioni assoggettate all'obbligo di segnalazione possono decidere di affidare la procedura di segnalazione, singolarmente o collettivamente, a una terza organizzazione.

Sezione 6: Disposizioni finali

Art. 18 Modifica di altri atti normativi

La modifica di altri atti normativi è disciplinata nell'allegato.

Art. 19 Entrata in vigore

La presente ordinanza entra in vigore il 1° aprile 2025.

Allegato
(Art. 18)

Modifica di altri atti normativi

...[13]

13 Le mod. possono essere consultate alla RU **2025** 168.