Ordinanza sulla cibersicurezza (OCS)

del XX.XX.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,
ordina:

Sezione 1: Oggetto

Art. 1

La presente ordinanza disciplina:

a. la Ciberstrategia nazionale e il suo Comitato direttivo;
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 segnalare ciberattacchi.

Sezione 2: Ciberstrategia nazionale e Comitato direttivo

Art. 2 Ciberstrategia nazionale

[1] La Ciberstrategia nazionale (CSN) stabilisce il quadro strategico per la prevenzione nell'ambito della cibersicurezza, l'individuazione tempestiva delle ciberminacce, le possibilità di reazione e la resilienza in caso di incidenti come pure la lotta alla cibercriminalità..

[2] Viene definita d'intesa con i Cantoni.

Art. 3 Istituzione e organizzazione del CD CSN

[1] Il Consiglio federale istituisce un Comitato direttivo della Ciberstrategia nazionale (CD CSN).

1 RS **128**

[2] Il CD CSN dispone di una segreteria che viene gestita dall'Ufficio federale della cibersicurezza (UFCS).

Art. 4 Composizione del CD CSN

[1] Il CD CSN si compone di rappresentanti dei dipartimenti, della Cancelleria federale, dei Cantoni, del settore economico, della società e delle scuole universitarie.

[2] Il Consiglio federale nomina ogni cinque anni i membri del CD CSN, ad eccezione dei rappresentanti dei Cantoni che vengono designati dalla Conferenza dei Governi cantonali.

[3] Nomina il presidente tra i rappresentanti del settore economico, della società o delle scuole universitarie.

Art. 5 Compiti del CD CSN

Il CD CSN ha i seguenti compiti:

a. verificare la CSN almeno ogni cinque anni, contribuire al suo ulteriore sviluppo ed elaborare, se necessario, proposte di adeguamento;

b. elaborare le proposte relative alle priorità e alle tempistiche per l'attuazione delle misure della CSN d'intesa con gli attori indicati nella CSN;

c. valutare costantemente l'attuazione delle misure e informare il Consiglio federale e i Cantoni su eventuali ritardi;

d. presentare se necessario al Consiglio federale proposte per misure complementari;

e. presentare ogni anno al Consiglio federale, ai Cantoni e al pubblico un rapporto sull'attuazione della CSN.

Sezione 3: Compiti dell'UFCS

Art. 6 Richieste sui titolari

Per avvisare le autorità, le organizzazioni e le persone interessate in caso di ciberminacce imminenti o di ciberattacchi in corso, l'UFCS può richiedere i dati di contatto dei titolari dei nomi di dominio ai gestori dei registri dei nomi di dominio che rientrano nella competenza della Confederazione o sono subordinati a tali nomi di dominio.

Art. 7 Analisi tecnica di ciberincidenti e ciberminacce

[1] L'UFCS gestisce il team nazionale di risposta alle emergenze informatiche *(Computer Emergency Response Team [CERT])*, che svolge in particolare i seguenti compiti:

a. gestione tecnica degli incidenti;

b. analisi di questioni tecniche;

c. identificazione e valutazione di ciberminacce.

[2] Per l'analisi dei ciberincidenti e delle ciberminacce l'UFCS gestisce un'infrastruttura resiliente che deve funzionare indipendentemente dal resto dell'informatica della Confederazione.

Art. 8 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, questo può stabilire delle priorità per quanto riguarda i tempi e l'entità della consulenza e del sostegno forniti.

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

Art. 9 Divulgazione coordinata delle vulnerabilità

[1] L'UFCS assicura la divulgazione coordinata delle vulnerabilità secondo gli 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. può essere sfruttata in modo particolarmente semplice per un ciberattacco; o

c. riguarda sistemi molto diffusi.

[4] Può prolungare il termine fissato se eliminare la vulnerabilità si rivela particolarmente complesso.

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

[6] I capoversi 1–4 non si applicano alle vulnerabilità scoperte dall'Ufficio federale delle comunicazioni (UFCOM) nell'ambito dei suoi controlli

(art. 36 segg. dell'ordinanza del 25 novembre 2015[2] sugli impianti di telecomunicazione). In tali casi, l'UFCOM informa l'UFCS.

[7] L'UFCS informa immediatamente l'UFCOM delle vulnerabilità scoperte negli impianti di telecomunicazione di cui all'articolo 3 lettera d della legge del 30 aprile 1997[3] sulle telecomunicazioni.

Art. 10 Sostegno alle autorità

L'UFC 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. 11 Sistema di comunicazione per lo scambio sicuro delle informazioni

[1] Hanno accesso al sistema di comunicazione dell'UFCS per lo scambio sicuro delle informazioni (art. 74 cpv. 2 lett. a) le organizzazioni e le autorità con sede in Svizzera.

[2] L'UFCS è responsabile della sicurezza del sistema di comunicazione e della liceità del trattamento dei dati.

Art. 12 Sistemi d'informazione per lo scambio automatico

[1] L'UFCS mette a disposizione dei gestori di infrastrutture critiche sistemi d'informazione per lo scambio automatico di informazioni tecniche su ciberminacce e ciberincidenti.

[2] L'UFCS è responsabile della sicurezza dei sistemi d'informazione e della liceità del trattamento dei dati.

Art. 13 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 le seguenti informazioni:

a. ragione sociale, nome o designazione nonché indirizzo;

b. dati di contatto della persona registrata.

2 RS 784.101.2
3 RS 784.10

Art. 14 Fornitori di servizi

[1] I gestori di infrastrutture critiche possono notificare all'UFCS eventuali fornitori di servizi 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 di contatto della persona registrata.

Art. 15 Trasmissione e utilizzo delle informazioni

[1] Le aziende e le autorità registrate trasmettono informazioni all'UFCS e stabiliscono se e a chi l'UFCS può a sua volta trasmettere le informazioni, qualora la trasmissione delle informazioni non fosse contemplata dalla legge.

[2] L'UFCS decide in merito alla pubblicazione delle informazioni autorizzate alla trasmissione sul sistema di comunicazione come pure sui sistemi d'informazione per lo scambio automatico.

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

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

Sezione 5: Obbligo di segnalazione

Art. 16 Eccezioni all'obbligo di segnalazione

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

a. gli organi di cui all'articolo 74*b* capoverso 1 lettere b e c LSIn: se sono responsabili di meno di 1000 abitanti; è determinante la popolazione stabilmente risiedente;

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,

4 RS **734.71**

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 (OSITC) presentino negli ultimi cinque anni una media di energia trasportata inferiore a 400 GWh all'anno;

c. le imprese di cui all'articolo 74*b* capoverso 1 lettera n LSIn, a condizione che:

1. non debbano realizzare alcun sistema di gestione della sicurezza delle informazioni secondo gli articoli 2 e 4 e l'allegato II del regolamento (UE) 2023/203[6] oppure secondo l'articolo 2 e l'allegato del regolamento (UE) 2022/1645[7],

2. non debbano applicare le direttive di cui al punto 1.7 dell'allegato del regolamento di esecuzione (UE) 2015/1998[8] nel loro programma di sicurezza secondo gli articoli 2, 12, 13 o 14 del regolamento (CE) 300/2008[9];

d. le imprese ferroviarie come pure le imprese che gestiscono impianti di trasporto a fune, linee filoviarie, autobus e battelli di

5 RS **746.12**

6 Regolamento di esecuzione (UE) n. 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.

7 Regolamento delegato (UE) n. 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.

8 Regolamento di esecuzione (UE) n. 2015/1998 della Commissione del 5 novembre 2015 che stabilisce disposizioni particolareggiate per l'attuazione delle norme fondamentali comuni sulla sicurezza aerea.

9 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.

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[10] sulle ferrovie [Lferr]),
2. siano titolari di una concessione per il trasporto di viaggiatori secondo l'articolo 6 legge del 20 marzo 2009[11] 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);

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

[2] Le imprese di cui all'articolo 74*b* capoverso 1 lettere f, g, h, l e p LSIn, alle quali il capoverso 1 non è applicabile, 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. 17 Obbligo di documentazione delle richieste di informazioni sull'assoggettamento all'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. 18 Ciberattacchi da segnalare

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

a. i collaboratori o i 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:

10 RS **742.101**
11 RS **745.1**

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

b. si è verificata una violazione della sicurezza dei dati secondo l'articolo 24 della legge federale del 25 settembre 2020[12] sulla protezione dei dati (LPD).

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

[4] Un ciberattacco è considerato connesso ai reati di estorsione, minaccia o coazione se suddetti reati sono rivolti contro le autorità o le organizzazioni assoggettate all'obbligo di segnalazione, o contro i loro responsabili o i loro collaboratori, compresi gli ex responsabili o gli ex collaboratori, oppure contro persone che lavorano per le autorità o le organizzazioni assoggettate all'obbligo di segnalazione.

Art. 19 Contenuto della segnalazione

[1] 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;

c. tipo di attacco;

d. metodo di attacco; e

e. indicazioni sull'autore.

[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. unità dell'organizzazione o dell'autorità interessate;

b. grado di compromissione della disponibilità, dell'integrità e della confidenzialità delle proprie informazioni e delle informazioni di terzi; e

c. ripercussioni del ciberattacco sul funzionamento delle unità dell'organizzazione o dell'autorità interessate.

[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.

12 RS **235.1**

Art. 20 Trasmissione della segnalazione

Se la segnalazione non viene effettuata tramite il sistema di comunicazione dell'UFCS, questo informa la persona di contatto di cui all'articolo 13 capoverso 2 lettera b di aver ricevuto la segnalazione e del suo contenuto.

Art. 21 Termine per registrare la segnalazione

[1] Se entro il termine di segnalazione di 24 ore 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.

Sezione 6: Disposizioni finali

Art. 22 Modifica di altri atti normativi

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

Art. 23 Entrata in vigore

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

Allegato
(art. 22)

Modifica di altri atti normativi

Le ordinanze qui appresso sono modificate come segue:

1. Ordinanza del 7 marzo 2003 [13]sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport

Art 15a cpv. 2 frase introduttiva nonché lett. f e h

[2] Assume in particolare le seguenti funzioni:

f. gestisce il team nazionale di risposta alle emergenze informatiche *(Computer Emergency Response Team [CERT]);*

h. rappresenta la Svizzera in organi internazionali per l'analisi tecnica di ciberminacce e per la gestione di ciberincidenti.

2. Ordinanza del 31 agosto 2022[14] sulla protezione dei dati

Art. 41 cpv. 1

Abrogato

13 RS **172.214.1**
14 RS **235.11**