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)

Rapporto esplicativo relativo all'ordinanza sulla cibersicurezza (OCS)

22 maggio 2024

Indice

1 Situazione iniziale

L'11 dicembre 2020 il Consiglio federale ha incaricato il Dipartimento federale delle finanze (DFF) di creare le basi legali per introdurre l'obbligo di segnalare ciberattacchi a infrastrutture critiche. Pertanto il 2 dicembre 2022 il Consiglio federale ha adottato il progetto per queste basi legali e ha licenziato il messaggio concernente la modifica della legge federale del 18 dicembre 2020[1] sulla sicurezza delle informazioni in seno alla Confederazione (legge sulla sicurezza delle informazioni, LSIn) all'attenzione del Parlamento. Successivamente, il 29 settembre 2023, il Parlamento ha approvato la modifica della LSIn[2]. Il termine di referendum è scaduto inutilizzato il 18 gennaio 2024.

Il progetto di ordinanza sulla cibersicurezza contiene, da un lato, le disposizioni d'esecuzione concernenti il capitolo 5 della modifica della LSIn concernenti l'obbligo di segnalare ciberattacchi a infrastrutture critiche e, dall'altro lato, disciplina aspetti organizzativi in relazione con la cibersicurezza. L'ordinanza dovrà entrare in vigore con effetto dal 1° gennaio 2025 assieme al capitolo 5 riveduto della LSIn.

La legge sulla sicurezza delle informazioni è entrata in vigore già il 1° gennaio 2024, senza il citato capitolo 5 riveduto concernente i compiti del nuovo Ufficio federale della cibersicurezza (UFCS) e l'obbligo di segnalare ciberattacchi a infrastrutture critiche. Per la stessa data è inoltre stata abrogata[3] l'ordinanza del 27 maggio 2020[4] sulla protezione contro i ciber-rischi nell'Amministrazione federale (ordinanza sui ciber-rischi, OCiber). Le disposizioni dell'OCiber sono state in parte integrate nella modifica della LSIn (in particolare le definizioni). Le disposizioni che nell'OCiber disciplinavano la sicurezza informatica della Confederazione sono state riprese nell'ordinanza dell'8 novembre 2023[5] sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito (ordinanza sulla sicurezza delle informazioni, OSIn). I compiti del Centro nazionale per la cibersicurezza (NCSC) definiti nell'OCiber, in particolare i suoi compiti nei confronti del settore economico e della popolazione, non sono disciplinati nell'OSIn poiché con la modifica della LSIn sono stati dotati di una nuova base legale. Inoltre il 1° gennaio 2024 il NCSC è stato trasferito nell'UFCS in seno al Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS). Per questo motivo si trovano quindi disposizioni organizzative relative all'UFCS nell'articolo 15*a* capoversi 1 e 2 lettere a–g dell'ordinanza del 7 marzo 2003[6] sull'organizzazione del Dipartimento federale della difesa, della protezione della popolazione e dello sport (OOrg-DDPS).

I compiti dell'UFCS, unitamente all'obbligo di segnalare ciberattacchi a infrastrutture critiche, vengono precisati e descritti in modo più concreto nell'OCS. La futura ordinanza sulla cibersicurezza (OCS) disciplina pertanto, a complemento dell'OSIn, i compiti dell'UFCS e l'obbligo di segnalare ciberattacchi a infrastrutture critiche. Princi-

1 RS **128**
2 FF **2023** 2296
3 RU **2023** 735 (all. 2 n. I).
4 RS **120.73**
5 RS **128.1**
6 RS **172.214.1**

palmente disciplina quindi il rapporto tra l'UFCS e i destinatari al di fuori dell'Amministrazione federale, mentre l'OSIn i compiti e le competenze per la sicurezza delle informazioni all'interno dell'Amministrazione federale.

2 Commento alle singole disposizioni

Sezione 1: Oggetto

Art. 1

Questa disposizione si fonda sulle basi legali del «Capitolo 5: Misure della Confederazione per la protezione della Svizzera dalle ciberminacce» della legge sulla sicurezza delle informazioni (art. 73*a* segg. LSIn) e si rifà inoltre anche all'articolo 15a capoversi 1 e 2 lettere a–g OOrg-DDPS.

L'articolo 1 descrive l'oggetto della regolamentazione dell'ordinanza e le lettere a–d rispecchiano la struttura dell'ordinanza che corrisponde anche ai rispettivi titoli delle relative sezioni:

Lett. a: *Ciberstrategia nazionale e il suo Comitato direttivo*

Negli articoli 2–5 l'ordinanza stabilisce che, d'intesa con i Cantoni, la Confederazione definisca una Ciberstrategia nazionale (CSN) e istituisca un comitato direttivo incaricato della sua attuazione, definendone la composizione, l'organizzazione e i compiti.

Lett. b: *Compiti dell'UFCS*

L'OCS disciplina a titolo complementare negli articoli 6–10 i compiti dell'UFCS secondo l'articolo 73*a* capoverso 2 LSIn. Fino alla fine del 2023 i compiti del NCSC, l'unità amministrativa precedente all'UFCS, erano disciplinati nell'OCiber ora abrogata. Con la revisione complementare della LSIn questi compiti sono stati inseriti in una legge formale gerarchicamente sovraordinata.

Lett. c: *Scambio di informazioni tra l'UFCS e le autorità nonché le organizzazioni per la protezione dai ciberincidenti e dalle ciberminacce*

Ai fini della protezione dai ciberincidenti e dalle ciberminacce, l'ordinanza definisce negli articoli 11–15 lo scambio di informazioni tra l'UFCS e le autorità nonché le organizzazioni riguardante gli incidenti, le minacce e gli attacchi attuali nel settore della cibersicurezza. In questo ambito vengono definite le prescrizioni, le competenze e le responsabilità sia per il sistema di comunicazione per lo scambio sicuro di informazioni, sia per il sistema di informazione per lo scambio automatico in modo da garantire che informazioni rilevanti possano essere trasmesse rapidamente ed efficacemente al servizio giusto.

Lett. d: *Obbligo di segnalare ciberattacchi*

In occasione della procedura di consultazione relativa alla revisione complementare della LSIn è stato più volte ribadito che le disposizioni sull'obbligo di segnalare ciberattacchi a infrastrutture critiche debbano essere concretizzate a livello di ordinanza. Gli articoli 16–21 dell'ordinanza intendono concretizzare questa richiesta, cui si era già ripetutamente accennato nel messaggio concernente la modifica della legge sulla sicurezza delle informazioni[7]. Pertanto sono disciplinati i dettagli sull'obbligo di segnalazione, vale a dire le autorità e organizzazioni esentate dall'obbligo di segnalazione, i ciberattacchi che devono essere segnalati, il contenuto e il volume della segnalazione e lo svolgimento del processo di segnalazione.

Occorre precisare che, in considerazione dell'elencazione esaustiva dell'oggetto della regolamentazione contenuto in questo articolo, tutte le direttive in materia cibersicurezza dell'Amministrazione federale, le competenze e i compiti del Servizio specializzato della Confederazione per la sicurezza delle informazioni e le relative interfacce con i compiti dell'UFCS sono disciplinati nell'OSIn.

Anche le misure della ciberdifesa non sono disciplinate nell'OCS. Queste misure si riferiscono alle misure relative alle attività informative e militari e comprendono in particolare le misure attive previste all'articolo 37 della legge del 25 settembre 2015[8] sulle attività informative (LAIn) per perturbare o rallentare i ciberattacchi. Inoltre concernono anche le misure dell'esercito volte a garantire la prontezza all'impiego in ogni situazione e a mettere a disposizione le competenze per fornire un supporto sussidiario alle autorità civili. Queste misure sono disciplinate nella LAIn e nella legge militare nonché nelle relative ordinanze.

Sezione 2: Ciberstrategia nazionale e Comitato direttivo

Art. 2 Ciberstrategia nazionale

Sino alla fine del 2023 le disposizioni concernenti la Ciberstrategia nazionale erano contenute nell'articolo 5 dell'OCiber ora abrogata. Questo articolo si rifà alla regolamentazione di allora e obbliga il Consiglio federale a definire obiettivi e misure nell'ambito della protezione contro i ciber-rischi nella Ciberstrategia nazionale (CSN). All'interno dell'Amministrazione federale, in base all'articolo 15*a* capoverso 2 lettera g OOrg-DDPS, l'UFCS è competente per l'elaborazione della CSN all'attenzione del Consiglio federale e per il coordinamento della sua attuazione.

Secondo il *capoverso 1* la CSN costituisce 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 al fine di proteggere la Svizzera dai ciberincidenti e dalle ciberminacce. Questo significa che la CSN persegue un

[7] Messaggio del 2 dicembre 2022 concernente la modifica della legge sulla sicurezza delle informazioni (Introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche), FF 2023 84.

[8] RS **121**

approccio globale per la gestione dei ciberincidenti e delle ciberminacce, che comprende diversi aspetti della cibersicurezza:

- *prevenzione nell'ambito della cibersicurezza:* si riferisce a misure che vengono adottate per identificare e minimizzare vulnerabilità e metodi di attacco. Questo può avvenire anche per il tramite di direttive in materia di sicurezza, formazioni per i collaboratori, audit sulla sicurezza e attraverso l'impiego di tecnologie in materia di sicurezza;

- *individuazione tempestiva delle ciberminacce*: questo aspetto comprende le capacità di individuare precocemente i segnali relativi a ciberincidenti e ciberminacce. Si tratta di controllare le attività sospette in reti e sistemi e di implementare tecnologie che permettono di individuare per tempo incidenti e minacce;

- *possibilità di reazione in caso di incidenti:* si tratta della capacità di reagire correttamente ai ciberincidenti e alle ciberminacce non appena vengono individuati. Questo può comportare l'attivazione del gruppo Computer Emergency Response Team (CERT), l'avvio di contromisure e la collaborazione con altre autorità e organizzazioni competenti per la gestione dell'incidente o della minaccia;

- *resilienza in caso di ciberincidenti*: si riferisce alla rapidità con cui è possibile ripristinare un sistema dopo un ciberattacco. Comprende ad esempio l'implementazione di sistemi di backup, piani di emergenza e altre misure volte a minimizzare le ripercussioni di un attacco.

- *lotta e perseguimento penale efficaci in materia di cibercriminalità*: le infrastrutture digitali disponibili in Internet offrono nuove possibilità a potenziali delinquenti idonee a creare danni ingenti a livello sociale ed economico. La cibercriminalità oltrepassa qualsiasi limite territoriale, e lo fa nell'ambito di un processo estremamente dinamico con cicli d'innovazione brevi. Quanto più è forte l'interconnessione digitale tanto maggiore è il rischio che i ciberincidenti, pur prendendo avvio nel mondo virtuale, possano sortire i loro effetti dannosi nel mondo reale. Alla luce di questa evoluzione è importante continuare a migliorare l'interoperabilità e la capacità di reazione in tutta la Svizzera e in collaborazione con i partner internazionali nonché coordinare in maniera efficace le competenze a livello specialistico, tecnico e di personale senza spostare le competenze tra le diverse autorità e i diversi livelli statali.

La CSN definisce il quadro per questi diversi aspetti e coordina gli sforzi sul piano nazionale secondo il capoverso 2 in stretta collaborazione con i Cantoni. Con una strategia esaustiva si vuole garantire che la Svizzera sia complessivamente meglio protetta contro i ciberincidenti e le ciberminacce e sia in grado di reagire in modo efficace.

Art. 3 Istituzione e organizzazione del CD CSN

Sino alla fine del 2023, la funzione e la composizione del Comitato direttivo della Strategia nazionale (CD CSN), erano regolamentate nell'articolo 9 dell'OCiber ora abrogata.

Capoverso 1: Istituzione del CD CSN da parte del Consiglio federale

Il capoverso 1 stabilisce che il CD CSN sia istituito dal Consiglio federale, in modo da conferirgli la debita considerazione a livello politico. Gestisce e sorveglia l'attuazione della CSN e coordina le misure volte a rafforzare la cibersicurezza sul piano nazionale. Il CD CSN riveste un ruolo importante nella creazione di un approccio globale per la gestione di ciberincidenti e ciberminacce in Svizzera. Grazie al coordinamento e alla sorveglianza delle misure di attuazione della CSN, il CD CSN contribuisce a una migliore protezione della Svizzera dai ciberincidenti e dalle ciberminacce e a rendere più efficace la sua reazione di fronte ai pericoli attuali.

Capoverso 2: Organizzazione del CD CSN

Secondo il *capoverso 2* l'UFCS designa la segreteria del CD CSN, che ricopre quindi una funzione di sostegno amministrativa e organizzativa nei confronti del comitato e aiuta a coordinare le attività del comitato, a preparare riunioni, a redigere verbali e rapporti e ad assicurare la comunicazione con i membri e con altri attori rilevanti. Con la messa a disposizione della segreteria, l'UFCS permette al CD CSN di lavorare in modo efficace e sostiene in questo modo anche l'attuazione della CSN. In tale ambito l'UFCS fornisce le proprie conoscenze specialistiche nel settore della cibersicurezza e favorisce una collaborazione efficiente tra i diversi membri del comitato.

Art. 4 Composizione del CD CSN

Capoverso 1: Cerchia dei membri del CD CSN

Per quanto riguarda la composizione del CD CSN occorre osservare che la CSN è una strategia nazionale che non si limita alle attività della Confederazione. È quindi importante che anche i Cantoni, il settore economico, la società e le scuole universitarie siano rappresentate nel CD CSN. Pertanto la sua composizione riflette la necessità di un'attuazione della CSN basata su una partecipazione ampia e variata:

- *i rappresentanti dei dipartimenti e della Cancelleria federale* forniscono la prospettiva dell'Amministrazione federale e sono responsabili del coordinamento e dell'attuazione di misure a livello di Confederazione;

- *i rappresentanti dei Cantoni* garantiscono che gli interessi e le esigenze dei Cantoni relativi alla cibersicurezza siano presi in considerazione. Poiché diversi aspetti della cibersicurezza sono rilevanti anche a livello cantonale, il coinvolgimento dei Cantoni è importante per una strategia nazionale efficace;

- *i rappresentanti del settore economico, della società e delle scuole universitarie* forniscono diverse conoscenze specialistiche e prospettive. Spesso il

settore economico è un obiettivo principale di ciberincidenti e ciberminacce e può offrire visioni preziose in questo contesto. La società rappresenta gli interessi dei cittadini in relazione alla sicurezza digitale e al funzionamento di infrastrutture critiche. Le scuole universitarie possono fornire conoscenze specialistiche a livello di ricerca e innovazione nel settore della cibersicurezza.

Complessivamente questa ampia composizione del CD CSN permette di osservare in modo esaustivo molteplici aspetti della cibersicurezza e richiede una collaborazione coordinata tra i differenti attori sul piano nazionale. Ciò contribuisce ad attuare in modo efficace la CSN e a meglio proteggere la Svizzera contro i ciberincidenti e le ciberminacce.

Capoversi 2 e 3: Nomina dei membri del CD CSN e designazione del presidente da parte del Consiglio federale

Il Consiglio federale nomina ogni cinque anni i membri del CD CSN, ad eccezione dei rappresentati dei Cantoni che vengono designati dalla Conferenza dei Governi cantonali. La nomina regolare di membri ogni cinque anni permette al Consiglio federale di garantire che il CD CSN venga occupato da rappresentanti preparati e competenti dotati delle conoscenze specialistiche necessarie ad attuare la CSN in modo efficace. Ciò contribuisce a mantenere al passo coi tempi il comitato e alla sua rilevanza.
La designazione del presidente tra i rappresentanti del settore economico, della società o delle scuole universitarie sottolinea l'importanza di una direzione equilibrata del comitato. Il presidente può così fornire un'ampia prospettiva e garantire che gli interessi di diversi settori vengano presi in considerazione nella giusta misura. Nel complesso questa struttura permette un adeguamento costante ai nuovi sviluppi nel settore della cibersicurezza e promuove una partecipazione equilibrata di diversi gruppi d'interesse all'attuazione della CSN. Questo contribuisce ad implementare in modo efficace la strategia e a meglio proteggere la Svizzera dai ciberincidenti e dalle ciberminacce.

Art. 5 Compiti del CD CSN

L'elenco dei compiti del CD CSN di cui all'*articolo 5* è orientato a un'attuazione e a una sorveglianza efficaci della CSN e comprende quanto segue:

- *lett. a:* la verifica regolare della CSN almeno ogni cinque anni permette al comitato di garantire che la strategia venga adeguata agli sviluppi e alle minacce più recenti e debitamente sviluppata. In caso di necessità il comitato formula raccomandazioni o piani concreti, che mirano ad adeguare l'attuale CSN;

- *lett. b:* la definizione di priorità e tempistiche per l'attuazione delle misure garantisce un impiego efficace delle risorse e il conseguimento degli obiettivi della strategia;

– *lett. c:* la valutazione costante dell'avanzamento relativo all'attuazione delle misure permette al comitato di individuare tempestivamente strozzature e problemi, di reagire adeguatamente e di informare il Consiglio federale nonché i Cantoni in merito a ritardi;

– *lett. d:* il fatto di presentare proposte per misure complementari all'attenzione del Consiglio federale contribuisce a eliminare rapidamente gli ostacoli;

– *lett. e:* il rapporto annuale sull'attuazione della CSN garantisce trasparenza e permette a tutti gli attori rilevanti di seguire i progressi fatti e, se del caso, di effettuare adeguamenti.

Sezione 3: Compiti dell'UFCS

Art. 6 Richieste sui titolari

Questa disposizione si fonda sugli articoli 73*a* capoversi 1 e 2 lettera a nonché 74 capoversi 1 e 2 lettera a LSIn.

Fino alla fine del 2023 il compito dell'UFCS concernente la sensibilizzazione del pubblico era disciplinato nell'articolo 12 capoverso 1 lettera h OCiber, ora abrogata. Dal 1° gennaio 2024 è contenuto nell'articolo 15*a* capoverso 2 lettere d ed e OOrg-DDPS.

Dal 2010 la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI), che nel 2020 è stata sostituita dall'NCSC e infine dall'inizio di quest'anno dall'UFSC, è considerata dall'Ufficio federale delle comunicazioni (UFCOM), secondo l'articolo 15 capoverso 3 ODIn[9], «un ente per la lotta contro la cibercriminalità riconosciuto dall'UFCOM»[10]. Tuttavia, poiché l'UFCS non ha competenze o compiti di diritto penale, si occupa soltanto indirettamente della cibercriminalità. Per chiarire la competenza dell'UFCS a richiedere informazioni di contatto dei titolari dei nomi di dominio ai gestori dei registri dei nomi di dominio, queste competenze sono esplicitamente disciplinate nell'*articolo 6* (cfr. art. 28*e* lett. b LTC e art. 7 segg. ODIn)[11]. La possibilità di richiedere informazioni di contatto dei titolari dei nomi di dominio permette all'UFCS, ad esempio nel caso di ciberminacce o ciberattacchi acuti, di avvisare rapidamente e in modo mirato le parti potenzialmente interessate ed eventualmente di supportarle nell'attuazione di contromisure. Questa competenza è un importante strumento per combattere le ciberminacce e i ciberattacchi e per rafforzare la cibersicurezza in Svizzera.

---

9 Ordinanza del 5 novembre 2014 sui domini Internet (ODIn; RS 784.104.2).

10 Cfr. Pagina Internet dell'UFCOM «Lotta contro la cibercriminalità» (vista l'ultima volta il 29 marzo 2024).

11 L'UFCOM ha delegato alla fondazione SWITCH l'attribuzione e la gestione dei nomi di dominio .ch (cfr. art. 28*a* cpv. 1 della legge del 30 aprile 1997 [LTC; RS 784.10] e art. 8 cpv. 2 in combinato disposto con l'art. 33 ODIn del 5 novembre 2014), che SWITCH gestiscono in una banca dati RDDS (WHOIS). L'UFCS ha concluso un accordo con SWITCH che regola la comunicazione dei titolari dei nomi di dominio nella banca dati RDDS (WHOIS) tramite procedura di richiamo attraverso l'accesso RDAP.

Art. 7 Analisi tecnica di ciberincidenti e ciberminacce

Questa disposizione si fonda sull'articolo 73*a* capoverso 1 e capoverso 2 lettere a ed e nonché sull'articolo 74 capoverso 3 in combinato disposto con l'articolo 74*a* capoverso 3 LSIn.

Fino alla fine del 2023 i compiti del Computer Emergency Response Team (CERT) erano disciplinati dall'articolo 12 capoverso 1 lettera c dell'OCiber, abrogata il 1°gennaio 2024. A partire da quella data il CERT è indicato nell'articolo 15*a* capoverso 2 lettera f OOrg-DDPS.

Capoverso 1: Computer Emergency Response Team (CERT)

L'UFCS gestisce il Computer Emergency Response Team (CERT) nazionale che svolge un ruolo centrale nella gestione dei ciberincidenti e delle ciberminacce in Svizzera. Il CERT è specializzato nella gestione tecnica degli incidenti, nell'analisi di questioni tecniche come pure nell'identificazione e nella valutazione delle ciberminacce dal punto di vista tecnico.

Gli elementi chiave dell'analisi delle questioni tecniche sono il confronto dei dati derivanti da ciberattacchi e la ricerca di anomalie (lett. a). A tale scopo il CERT sviluppa propri strumenti di analisi e utilizza strumenti di analisi di terzi. Inoltre ha un fitto scambio di opinioni con gli specialisti dei team di sicurezza provenienti dall'economia privata e da altri Paesi.

Il sostegno da parte dell'UFCS nella gestione degli incidenti consiste nell'analisi tecnica dell'attacco (lett. b). L'obiettivo dell'analisi è quello di comprendere il più rapidamente possibile quali sono i metodi di attacco impiegati dagli aggressori, quali sono le strategie e le tattiche utilizzate e quali sono le finalità perseguite. Queste informazioni consentono di definire e di attuare opportune contromisure. In tale contesto l'UFCS collabora strettamente con le autorità e le organizzazioni interessate e con i servizi di sicurezza di cui eventualmente dispongono. Contribuisce inoltre al coordinamento tra i diversi attori che partecipano alla gestione tecnica. In caso di necessità, può anche fornire sostegno direttamente sul posto all'autorità o all'organizzazione interessata. L'UFCS fornisce il suo sostegno in caso d'emergenza sotto forma di aiuto immediato. Nel quadro dei lavori necessari a ripristinare i dati e a ricostruire i sistemi dopo la gestione dell'incidente l'UFCS fornisce soltanto un sostegno di consulenza.

Il CERT sostiene le autorità e le organizzazioni anche in modo preventivo. Analizza costantemente le nuove minacce tecniche e i nuovi metodi di attacco e identifica le opportune contromisure (lett. c). Le valutazioni tecniche della situazione di minaccia richiedono la combinazione di diversi elementi ovvero strumenti automatizzati per l'analisi di ciberincidenti e ciberminacce, lo scambio di informazioni con servizi specializzati nazionali e internazionali come pure competenze umane per l'interpretazione dei risultati. L'esecuzione continua di queste valutazioni permette di reagire in modo proattivo ai pericoli, di colmare le lacune in materia di sicurezza e di adeguare le strategie di difesa per proteggersi dalle ciberminacce e dai ciberincidenti attuali e futuri.

Capoverso 2: Infrastruttura resiliente

L'UFCS gestisce un'infrastruttura resiliente che deve funzionare indipendentemente dal resto dell'informatica della Confederazione. Ciò significa che l'UFCS è un fornitore di prestazioni per questa specifica infrastruttura e pertanto dispone di speciali risorse e sistemi tecnici per analizzare i ciberincidenti e le ciberminacce.

La necessità di disporre di un'infrastruttura indipendente deriva dalla complessità e dall'urgenza dei ciberincidenti e delle ciberminacce. In quanto servizio nazionale di contatto per la cibersicurezza, l'UFCS deve essere in grado di analizzare in maniera affidabile i ciberincidenti e le ciberminacce anche nel caso in cui l'informatica della Confederazione fosse compromessa.

Questa infrastruttura indipendente e resiliente permette all'UFCS di adempiere i propri compiti in modo efficace e di garantire che la Svizzera possa reagire adeguatamente ai ciberincidenti e alle ciberminacce.

Art. 8 Priorizzazione della consulenza e del sostegno in caso di ciberattacchi

Questa disposizione si fonda sull'articolo 74 capoverso 3 e sull'articolo 74*a* capoverso 3 LSIn.

In generale

L'articolo 74 capoverso 3 LSIn prevede che l'UFCS possa fornire consulenza e sostegno ai gestori di infrastrutture critiche nel far fronte a ciberincidenti e a ciberminacce come pure nell'eliminare vulnerabilità. Questo a condizione che il funzionamento dell'infrastruttura critica interessata rischi di essere compromesso e, nel caso si tratti di gestori privati, non sia possibile procurarsi per tempo un sostegno equivalente sul mercato. I gestori interessati decidono autonomamente se vogliono avvalersi del sostegno da parte dell'UFCS.

La consulenza e il sostegno vengono forniti principalmente sotto forma di analisi tecniche e informazioni in merito alle misure tecniche e organizzative. Le analisi tecniche hanno lo scopo di identificare la causa dell'incidente, comprendere l'entità della compromissione e riconoscere le potenziali vulnerabilità negli strumenti informatici e nel sistema di sicurezza. Possono comprendere ad esempio l'esame dei protocolli di sistema, le analisi dei malware come pure le valutazioni della sorveglianza della rete. Oltre alle analisi tecniche, l'UFCS offre anche consulenza sulle misure organizzative per far fronte in modo più efficace all'incidente. Dal momento che l'UFCS è coinvolto in molti incidenti, è in grado ad esempio di fornire indicazioni sulle modalità di comunicazione dell'incidente o sull'organizzazione d'emergenza necessaria.

Capoverso 1: Priorizzazione delle prestazioni di consulenza e di sostegno

Il capoverso 1 prende in esame la situazione in cui l'UFCS nel caso di un ciberattacco si trova ad affrontare un numero di richieste di consulenza e sostegno superiore a

quello che è in grado di gestire con le proprie risorse e capacità in termini di personale e di mezzi tecnici disponibili. In uno scenario del genere l'UFCS si riserva il diritto di decidere a quali richieste dare la priorità e quale sarà l'entità del sostegno fornito. In altri casi meno urgenti la consulenza e il sostegno vengono forniti di conseguenza con un certo ritardo. Oltre alla tempistica può variare anche il grado di aiuto fornito. Alcuni casi possono richiedere un esame completo e un sostegno complessivo, mentre altri ricevono forse soltanto una consulenza di base. Questa disposizione permette all'UFCS nei periodi di maggior carico lavorativo di prendere decisioni strategiche su come impiegare al meglio le proprie risorse per fornire il maggior aiuto possibile.

Capoverso 2: Priorizzazione tenendo conto degli interessi pubblici

In presenza di un numero elevato di ciberincidenti e di ciberminacce simultanei, l'UFCS fornisce sostegno in modo prioritario alle organizzazioni e alle autorità assoggettate all'obbligo di segnalazione per le quali l'evento ha le maggiori ripercussioni sulla sicurezza, sull'ordine pubblico, sul benessere della popolazione e sul funzionamento dell'economia. Ciò significa che l'UFCS impiega le proprie risorse e fornisce il proprio sostegno in modo mirato laddove le ripercussioni di un evento sono particolarmente gravi. Ciò può voler dire ad esempio che viene data la priorità alle infrastrutture critiche, alle istituzioni pubbliche o ad altre importanti organizzazioni per garantire che siano adeguatamente protette e che ricevano rapidamente sostegno in caso di attacco. Grazie a questa priorizzazione l'UFCS può garantire che le istituzioni e le organizzazioni più importanti per il funzionamento della società e dell'economia siano adeguatamente protette nel caso di ciberincidenti e ciberminacce. Ciò contribuisce ad assicurare la resilienza e la stabilità del Paese nel caso di un evento su larga scala che colpisse molti obiettivi in Svizzera.

Art. 9 Divulgazione coordinata delle vulnerabilità

Questa disposizione si fonda sull'articolo *73a* capoverso 2 lettera c come pure sull'articolo 73*b* capoverso 3 in combinato disposto con l'articolo 73*c* capoverso 2 LSIn.

I compiti dell'UFCS in relazione al coordinamento delle vulnerabilità non erano esplicitamente disciplinati nell'OCiber, ma erano compresi nei compiti generali dell'UFCS che dal 1° gennaio 2024 sono elencati nell'articolo 15*a* capoverso 2 lettera b OOrg-DDPS. Inoltre dal 1° gennaio 2024 l'articolo 43 capoverso 1 lettera c OSIn prevede una base giuridica per la ricerca di vulnerabilità nell'infrastruttura informatica dell'Amministrazione federale e dell'esercito. Questa disposizione prevede che l'UFCS informi di tanto in tanto la Cancelleria federale, le segreterie generali, i dipartimenti e gli uffici federali in merito alle minacce e alle vulnerabilità attuali come pure in merito ai rischi che li riguardano e se necessario raccomandi misure per ridurre i rischi.

L'importanza di una gestione attiva delle vulnerabilità e il ruolo dell'UFCS nella ricerca e nella divulgazione coordinata delle stesse vulnerabilità vengono descritti in modo

più esauriente nel rapporto del Consiglio federale sulla promozione dell'hackeraggio etico in Svizzera (disponibile in tedesco e francese).[12]

Capoverso 1: Divulgazione coordinata delle vulnerabilità

La divulgazione coordinata delle vulnerabilità è un elemento importante degli sforzi complessivi in materia di cibersicurezza dal momento che permette di analizzare, valutare e colmare potenziali lacune in materia di sicurezza prima che possano essere sfruttate da eventuali aggressori. L'obiettivo del processo di divulgazione coordinata è quello di consentire la maggiore trasparenza possibile in merito alle vulnerabilità senza generare rischi per la sicurezza. L'elemento chiave di questo processo è che dopo aver scoperto una vulnerabilità vengono informati prima di tutto i produttori. Gli hacker concordano con loro un embargo prima del quale non può essere divulgata alcuna informazione sulla vulnerabilità. Ciò dà ai produttori tempo sufficiente per eliminare la vulnerabilità prima che venga resa pubblica. Questo processo è consolidato a livello internazionale e viene sancito anche nell'UE ad esempio dalla direttiva NIS 2 (art. 12 e 13).[13]

Le regole per la divulgazione coordinata delle vulnerabilità sono stabilite nella norma ISO/IEC 29147:2018-10.[14] L'UFCS è tenuto a divulgare le vulnerabilità segnalate conformemente alle regole stabilite nella suddetta norma. Ciò significa che l'UFCS non tiene segreta o non trasmette ad altre autorità alcuna vulnerabilità senza prima informare i produttori. L'UFCS è invece tenuto ad attuare determinate misure attraverso il processo di divulgazione coordinata in modo tale da garantire che la vulnerabilità non possa più essere sfruttata.

Attraverso la cooperazione con servizi specializzati esteri e internazionali l'UFCS può garantire che le vulnerabilità a livello internazionale vengano identificate ed eliminate. Nel settembre 2021 l'UFCS è stato riconosciuto dall'organizzazione statunitense MITRE come servizio specializzato in materia di vulnerabilità ed è stato autorizzato ad assegnare alle vulnerabilità scoperte un numero CVE in conformità allo standard «Common Vulnerabilities and Exposure (CVE)» per la loro contrassegnazione e identificazione, in modo che le vulnerabilità note ricevano una designazione univoca. Ciò permette agli esperti in materia di sicurezza, ai produttori, agli utenti e alle autorità di fare riferimento a una determinata vulnerabilità in modo uniforme. L'utilizzo dei numeri CVE consente inoltre di comunicare, documentare ed eliminare in maniera più efficace le lacune in materia di sicurezza. L'utilizzo di uno schema di denominazione standardizzato facilita anche la cooperazione tra i diversi attori nell'ambito della cibersicurezza e contribuisce a migliorare la trasparenza e l'efficacia nel trattamento delle lacune in materia di sicurezza.

---

12 Cfr. al riguardo: Rapporto del Consiglio federale del 29 novembre 2023, La promozione dell'hackeraggio etico in Svizzera, rapporto del Consiglio federale in adempimento del postulato 20.4594, Bellaiche, del 17 dicembre 2020, n. 4.2.4., pag. 13 seg.

13 Direttiva NIS 2: DIRETTIVA (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2).

14 ISO/IEC 29147:2018-10 (data di pubblicazione 2018-10), pag. 14.

Capoversi 2–4: Termine per eliminare la vulnerabilità

L'UFCS richiede ai produttori dell'hardware o del software interessato da vulnerabilità che una vulnerabilità venga eliminata in linea di massima entro un termine di 90 giorni. Si tratta di una prassi comune nel settore della cibersicurezza.[15] Questo termine, da un lato, concede ai produttori tempo sufficiente per analizzare le vulnerabilità e per sviluppare e attuare contromisure, mentre, dall'altro lato, garantisce anche che le vulnerabilità non persistano troppo a lungo.

A seconda della criticità e della complessità di una vulnerabilità il relativo termine può essere accorciato. Tuttavia in caso di necessità è anche possibile prolungare il termine fissato (p. es. a seguito di un onere elevato per le contromisure o di un'esigenza di coordinamento elevata).

Capoverso 5: Comunicazione della vulnerabilità prima che venga eliminata o pubblicata

Se è a conoscenza di una vulnerabilità che rappresenta una ciberminaccia acuta per altre infrastrutture critiche, l'UFCS informa i relativi gestori prima che la vulnerabilità venga pubblicata oppure eliminata dal produttore dell'hardware o del software interessato. Questa prassi è importante per informare tempestivamente i gestori di infrastrutture critiche riguardo a potenziali rischi per la sicurezza e dare loro la possibilità di adottare opportune misure per proteggere i propri sistemi. Grazie allo scambio di informazioni sulle vulnerabilità i gestori di infrastrutture critiche possono adottare in modo proattivo misure per ridurre i rischi prima che le vulnerabilità siano note pubblicamente. Ciò può contribuire a impedire o ad attenuare potenziali attacchi alle infrastrutture critiche.

Capoverso 6: Regolamentazione speciale per l'UFCOM

Questa disposizione è intesa a evitare conflitti di competenza e doppioni tra l'UFCS e l'UFCOM. L'UFCOM esercita la vigilanza sul mercato per quanto riguarda l'offerta, la messa a disposizione sul mercato, la messa in servizio, l'installazione e l'esercizio degli impianti di telecomunicazione. Inoltre svolge controlli del mercato presso attori economici, in primo luogo presso il produttore svizzero oppure, in assenza di quest'ultimo, presso l'importatore di tali impianti, verifica gli impianti interessati e adotta le misure necessarie se gli impianti controllati non sono conformi alle prescrizioni vigenti (art. 33 legge del 30 aprile 1997[16] sulle telecomunicazioni [LTC]). Tra queste prescrizioni rientrano anche i requisiti in materia di cibersicurezza per determinati impianti di radiocomunicazione conformemente all'articolo 7 capoverso 3 lettere d, e ed f dell'ordinanza del 25 novembre 2015[17] sugli impianti di telecomunicazione (OIT)[18].

---

15 Cfr. Linee guida dell'Ufficio federale tedesco della sicurezza informatica sul processo di divulgazione coordinata delle vulnerabilità (CVD), n. 3.3., pag.10.

16 RS **784.10**

17 RS **784.101.2**

18 Gli impianti di radiocomunicazione interessati non devono danneggiare la rete o il suo funzionamento, né abusare delle risorse della rete arrecando quindi un deterioramento inaccettabile del servizio. Devono contenere elementi di salvaguardia per garantire la protezione dei dati personali e della vita privata degli utilizzatori e degli abbonati. Inoltre devono supportare caratteristiche speciali che consentano di tutelarsi dalle frodi.

Dato che a questo riguardo gli obiettivi dell'UFCS e dell'UFCOM si sovrappongono, non è possibile eseguire una divulgazione coordinata secondo il capoverso 1 se in occasione di un controllo di un attore economico l'UFCOM scopre prima dell'UFCS che i requisiti in materia di cibersicurezza non vengono rispettati per un impianto di radiocomunicazione. Nel corso della procedura del controllo del mercato dopo la verifica effettuata dall'UFCOM, l'attore economico è a conoscenza del fatto che gli impianti interessati presentano una vulnerabilità già prima del fabbricante estero. Per questa ragione vi è bisogno di un meccanismo di coordinamento volto a coordinare le procedure dell'UFCOM e dell'UFCS. Di conseguenza l'UFCOM informa l'UFCS in merito a vulnerabilità e quest'ultimo eventualmente esegue la divulgazione coordinata delle vulnerabilità secondo il capoverso 1.

Capoverso 7: Informazione dell'UFCOM

L'UFCOM necessita senza indugio delle informazioni relative alle vulnerabilità scoperte dall'UFCS in impianti di telecomunicazione. Ciò consente da un lato di garantire che l'UFCOM non avvii una procedura contemporaneamente alla divulgazione coordinata da parte dell'UFCS e d'altro lato grazie a queste informazioni l'UFCOM sarà in grado di definire in che modo procedere ulteriormente in una procedura già in corso nel quadro della sua vigilanza sul mercato contro un produttore svizzero o un importare (vedi spiegazioni relative al capoverso 6).

Se il produttore informato dall'UFCS è stato in grado di eliminare la vulnerabilità entro il termine previsto, successivamente l'UFCOM può verificare se gli adeguamenti da parte dal produttore sono stati effettuati anche per gli impianti disponibili sul mercato. Se la vulnerabilità non è stata eliminata, l'UFCOM può disporre misure corrispondenti nel quadro della procedura contro l'importatore.

Art. 10 Sostegno alle autorità

Questa disposizione si fonda sull'articolo 73*a* capoverso 2 lettera c LSIn.

Quale centro di competenza della Confederazione per la cibersicurezza, l 'UFCS fornisce sostegno alle competenti autorità della Confederazione e dei Cantoni nello sviluppo, nell'attuazione e nella verifica degli standard e delle regolamentazioni in relazione alla cibersicurezza in particolare nel modo seguente:

- *Competenza specialistica*: dispone di specialisti che possono fornire consulenza e sostegno alle autorità nell'attuazione dei suddetti standard e delle suddette regolamentazioni in materia di cibersicurezza.

- *Fornitura di assistenza tecnica*: fornisce assistenza alle autorità nello sviluppo e nell'attuazione di standard e regolamentazioni in materia di cibersicurezza.

- *Coordinamento e cooperazione*: assume il coordinamento per facilitare la cooperazione tra le diverse autorità e garantisce che le regolamentazioni e gli standard sviluppati in materia di cibersicurezza siano coerenti ed efficaci.

– *Scambio di informazioni*: funge da base per lo scambio di informazioni tra le autorità in merito alle prassi consolidate e in materia di cibersicurezza.

Sezione 4: Scambio di informazioni

Art. 11 Sistema di comunicazione per lo scambio sicuro delle informazioni

Questa disposizione si fonda sull'articolo 73*a* capoversi 1 e 2 lettera e nonché sull'articolo 74 capoversi 1 e 2 lettera a LSIn.

Il compito dell'UFCS riguardante lo scambio sicuro delle informazioni è stato disciplinato fino alla fine del 2023 dall'articolo 12 capoverso 1 lettere b e i dell'OCiber, abrogata il 1° gennaio 2024. L'OOrg-DDPS non contiene alcuna regolamentazione specifica a tale riguardo.

Capoverso 1: Accesso al sistema di comunicazione sicuro

Gli aggressori utilizzano spesso gli stessi metodi e mezzi per portare a termine con successo gli attacchi contro il maggior numero possibile di vittime. Se le vittime di attacchi comunicano rapidamente ad altre organizzazioni e autorità le indicazioni tratte da ciberincidenti e ciberminacce, il loro numero può essere sensibilmente ridotto. Per tale ragione l'UFCS gestisce un sistema di comunicazione per lo scambio sicuro delle informazioni in merito ai ciberincidenti e alle ciberminacce. Attraverso questo sistema di comunicazione l'UFCS può comunicare in modo rapido ed efficiente informazioni su incidenti e minacce alle autorità e alle organizzazioni registrate che hanno sede in Svizzera. Ciò permette alle organizzazioni e alle autorità registrate di reagire più rapidamente alle minacce e di adottare contromisure. Inoltre questo sistema di comunicazione aiuta anche a sviluppare una migliore consapevolezza della natura e della portata dei ciberincidenti e delle ciberminacce.

Capoverso 2: Responsabilità dell'UFCS per la sicurezza e la protezione dei dati

Il sistema di comunicazione per lo scambio sicuro delle informazioni è un sistema d'informazione dell'UFCS. L'UFCS è responsabile della sicurezza e garantisce la liceità del trattamento dei dati.

Art. 12 Sistemi d'informazione per lo scambio automatico

Questa disposizione si fonda sull'articolo 73*a* capoversi 1 e 2 lettera e nonché sull'articolo 74 capoversi 1 e 2 lettera a LSIn.

Capoverso 1: Scambio automatico di informazioni

I sistemi d'informazione messi a disposizione dall'UFCS per lo scambio automatico di informazioni tecniche sono un mezzo molto importante per proteggere le infrastrutture critiche da ciberincidenti e ciberminacce consentendo ai gestori delle infrastrutture critiche di disporre sempre di informazioni aggiornate. L'UFCS utilizza questi sistemi

d'informazione protetti per informare tempestivamente i gestori di infrastrutture critiche su indicatori tecnici e modelli di attacco che non sono ancora noti al pubblico e che non possono nemmeno essere pubblicati dall'UFCS per motivi di sicurezza. Gli indicatori tecnici di ciberincidenti o ciberminacce sono indicazioni o segnali specifici di minacce potenziali o effettive nell'ambito della tecnologia dell'informazione o della cibersicurezza. Questi indicatori possono assumere varie forme come ad esempio le firme di malware, vale a dire caratteristiche inequivocabili di software dannosi che indicano che un sistema è infetto o è stato esposto a un'infezione. Comprendono anche anomalie nel traffico di rete. In questo caso si tratta ad esempio di modelli insoliti nel traffico di dati che possono indicare la presenza di una possibile ciberminaccia, come velocità di trasferimento dei dati insolitamente elevate oppure connessioni sospette a indirizzi IP noti come dannosi. Attraverso questi sistemi d'informazione possono essere scambiati automaticamente con i gestori di infrastrutture critiche anche altri indicatori di analisi forense digitale. Può trattarsi di diversi tipi di tracce digitali che indicano un ciberincidente o una ciberminaccia, come ad esempio insolite modifiche di file, login sospetti o tentativi di accesso non autorizzati. I gestori di infrastrutture critiche sono rilevati come tali al momento della registrazione presso l'UFCS in modo che le informazioni tecniche di cui sopra possano essere distribuite in modo mirato solo all'interno della cerchia delle infrastrutture critiche. Tutti i gestori di infrastrutture critiche registrati vengono attribuiti a uno o più settori in modo che possa aver luogo anche uno scambio di informazioni specifiche per un determinato settore.

Capoverso 2: Responsabilità dell'UFCS per la sicurezza e la protezione dei dati

Analogamente alle disposizioni contenute nell'articolo 11 capoverso 2, l'UFCS è responsabile della sicurezza e della protezione dei dati per quanto riguarda i sistemi d'informazione per lo scambio automatico di informazioni.

Art. 13 Registrazione

Questa disposizione si fonda sull'articolo 73*a* capoversi 1 e 2 lettera e nonché sull'articolo 74 capoversi 1 e 2 lettera a LSIn.

Capoverso 1: Registrazione per partecipare allo scambio di informazioni

Per partecipare allo scambio di informazioni le organizzazioni e le autorità interessate devono registrarsi e comunicare immediatamente all'UFCS qualsiasi cambiamento nei dati registrati.

Capoverso 2: Dati da registrare

La registrazione deve contenere almeno le seguenti informazioni:

- *ragione sociale, nome o designazione e indirizzo dell'autorità o dell'organizzazione (lett. a)*: affinché le autorità e le organizzazioni siano correttamente identificate, al momento della registrazione devono indicare la propria ragione so-

ciale, il proprio nome o la propria denominazione e il proprio indirizzo con i seguenti dati: via, numero civico, numero postale di avviamento e nome del luogo;

- *dati di contatto della persona registrata (lett. b):* la registrazione delle autorità o delle organizzazioni deve contenere almeno il nome e il cognome di una persona di contatto. Inoltre occorre indicare per l'UFCS il numero di telefono come pure l'indirizzo e-mail e la funzione della persona registrata. È possibile registrare più persone di contatto.

In concomitanza con la registrazione, l'autorità o l'organizzazione viene informata in merito ai criteri per partecipare allo scambio di informazioni ai sensi dell'articolo 15 della presente ordinanza e la registrazione può essere completata soltanto se viene confermato attivamente di aver preso atto dei suddetti criteri.

La registrazione per partecipare allo scambio di informazioni non è obbligatoria neanche per le autorità e le organizzazioni assoggettate all'obbligo di segnalazione. Una registrazione tempestiva per le suddette autorità e organizzazioni significa tuttavia un risparmio di tempo in caso di un ciberattacco soggetto all'obbligo di segnalazione.

Art. 14 Fornitori di servizi

Questa disposizione si fonda sull'articolo 73*a* capoversi 1 e 2 lettera e nonché sull'articolo 74 capoversi 1 e 2 lettera a LSIn.

Capoverso 1: Notifica

Al fine di garantire la sicurezza e l'integrità delle infrastrutture critiche in Svizzera, i gestori di tali infrastrutture hanno la possibilità conformemente al *capoverso 1* di notificare all'UFCS i loro fornitori di servizi per la cibersicurezza affinché possano partecipare allo scambio di informazioni.

Capoverso 2: Dati da registrare

I fornitori di servizi eventualmente notificati dai gestori di infrastrutture critiche devono registrarsi conformemente al *capoverso 2* indicando la loro ragione sociale o il nome come pure i dati di contatto della persona registrata (vedi a tale riguardo per analogia quanto esposto in precedenza all'articolo 13 capoverso 2).

Art. 15 Trasmissione e utilizzo delle informazioni

Questa disposizione si fonda sull'articolo 73*a* capoversi 1 e 2 lettera e nonché sull'articolo 74 capoversi 1 e 2 lettera a LSIn.

Lo scambio di informazioni ha luogo su base volontaria e si fonda sulla fiducia che le informazioni fornite vengano utilizzate per gli scopi previsti. È pertanto determinante che i fornitori di informazioni possano decidere, tenendo conto delle disposizioni di

legge, come verranno utilizzate le informazioni condivise e che tutti i partecipanti conoscano e rispettino i criteri per lo scambio di informazioni.

Capoverso 1: Trasmissione delle informazioni condivise soltanto secondo le disposizioni dei fornitori di informazioni

La regolamentazione secondo cui le informazioni condivise possono essere trasmesse secondo quanto disposto dai fornitori di informazioni, qualora la trasmissione delle informazioni non fosse contemplata dalla legge, è importante per garantire che le informazioni non vengano diffuse senza autorizzazione o non vengano utilizzate impropriamente. Le informazioni in merito a ciberincidenti o a ciberminacce devono essere condivise in modo confidenziale. Mostrano quali sono le conoscenze disponibili su un incidente e quali misure di protezione sono state identificate. Gli aggressori potrebbero utilizzare tali informazioni per i loro scopi. Inoltre queste informazioni contengono anche dati sensibili per l'autorità o l'organizzazione interessata, ad esempio perché potrebbero compromettere la sua reputazione. Per tale ragione è importante che in linea di massima i fornitori di informazioni possano determinare autonomamente la cerchia di destinatari. A tale scopo nell'ambito della cibersicurezza si è imposta la classificazione secondo il «Traffic Light Protocol» (protocollo TLP). Questo standard promulgato dal «Forum of Incident Response and Security Teams (FIRST)»[19] distingue i seguenti criteri per l'ulteriore diffusione di informazioni:

- TLP «clear» - nessuna restrizione per la diffusione dell'informazione;
- TLP «green» - i destinatari possono trasmettere informazioni, ma non divulgarle su fonti pubbliche;
- TLP «amber» - i destinatari possono condividere informazioni all'interno della loro organizzazione[20] e con i loro partner, se questo è necessario;
- TLP «amber strict» - i destinatari possono condividere informazioni esclusivamente all'interno della loro organizzazione;
- TLP «red» - l'informazione è destinata soltanto al singolo individuo e non deve essere trasmessa.

Le informazioni condivise sulla piattaforma dell'UFCS sono suddivise in categorie conformemente al protocollo TLP. In tal modo viene indicato in che modo l'informazione può essere ulteriormente diffusa. Questi criteri sono vincolanti per tutti i destinatari, a meno che la trasmissione delle informazioni non sia contemplata dalla legge.

[19] Vedi al riguardo «Forum of Incident Response and Security Teams: Traffic Light Protocol (TLP)», sul sito web Traffic Light Protocol (TLP) (first.org).

[20] Il TLP non specifica che cosa si debba intendere per «la loro organizzazione». Ciò può creare confusione, in particolare nel caso di grandi aziende o di amministrazioni. Nell'Amministrazione federale il protocollo viene applicato intendendo con il termine «organizzazione» un'unità amministrativa, ad esempio un ufficio federale.

Capoverso 2: Decisione dell'UFCS in merito alla pubblicazione di informazioni

L'UFCS ha l'autorità di stabilire se e quando pubblicare le informazioni sulle ciberminacce e sui ciberattacchi di cui è stata autorizzata la trasmissione ed è pertanto responsabile di decidere quali di queste informazioni possono essere trasmesse e a chi. In questo caso si tratta di informazioni che vengono esaminate e trattate internamente. A tale riguardo si tiene conto di quali informazioni sono utili e rilevanti per il pubblico e per determinati gruppi di destinatari nonché come possono essere diffuse al meglio attraverso il sistema di comunicazione disponibile o i sistemi d'informazione.

Capoverso 3: Garanzia della protezione delle informazioni

I destinatari delle informazioni hanno la responsabilità di adottare misure volte a garantire la sicurezza e la confidenzialità delle informazioni ricevute. La protezione di queste informazioni è particolarmente importante poiché possono essere sensibili e la loro divulgazione o compromissione potrebbe avere conseguenze negative. Ad esempio potrebbe favorire ulteriori ciberattacchi o inasprire problemi già esistenti in materia di sicurezza.

Capoverso 4: Criteri per eventuali fornitori di servizi di gestori di infrastrutture critiche

I fornitori di servizi che lavorano per le infrastrutture critiche e che sono stati notificati e registrati dai gestori delle infrastrutture critiche ai sensi dell'articolo 14 della presente ordinanza possono utilizzare le informazioni che ricevono esclusivamente per le attività specifiche che svolgono su incarico della rispettiva infrastruttura critica. Questo serve a garantire la confidenzialità e la gestione appropriata delle informazioni sensibili nonché a ridurre al minimo il rischio di un uso improprio o di un accesso non autorizzato.

Sezione 5: Obbligo di segnalazione

Art. 16 Eccezioni all'obbligo di segnalazione

Questa disposizione si fonda sull'articolo 74*c* LSIn, secondo cui il Consiglio federale esenta le organizzazioni e autorità dall'obbligo di segnalazione di cui all'articolo 74*b* LSIn per quanto riguarda i ciberattacchi che causano guasti funzionali con ripercussioni minime sull'ordine pubblico, sulla sicurezza, sul benessere della popolazione o sul funzionamento dell'economia.

In generale

Se autorità oppure organizzazioni sono assoggettate all'obbligo di segnalazione in diversi settori secondo l'articolo 74*b* LSIn, l'esenzione in un settore non comporta l'esenzione dall'obbligo di segnalazione qualora siano assoggettate all'obbligo di segnalazione anche in uno o più altri settori.

Occorre anche tenere conto del fatto che esistono autorità e organizzazioni assoggettate all'obbligo di segnalazione per le quali non esistono eccezioni all'obbligo di segnalazione conformemente ai capoversi 1 e 2 trattati di seguito. Tra queste rientrano:

- le organizzazioni che forniscono prestazioni volte a coprire le conseguenze di malattie, infortuni, incapacità al lavoro e al guadagno, vecchiaia, invalidità e grande invalidità (art. 74*b* cpv. 1 lett. i LSIn);

- la Società svizzera di radiotelevisione (art. 74*b* cpv. 1 lett. j LSIn); e

- le agenzie di stampa d'importanza nazionale (art. 74*b* cpv. 1 lett. k LSIn).

Capoverso 1: Valori soglia specifici

Si è rinunciato a definire eccezioni specifiche per settore a livello di legge per consentire al Consiglio federale di adeguare i valori soglia stabiliti a livello di ordinanza in tempi brevi e in funzione di nuovi sviluppi. Per quanto possibile i valori soglia sono stati definiti in base alle sfide specifiche nel rispettivo settore.

Lett. a: Organi di cui all'articolo 74b capoverso 1 lettere b e c LSIn

Per «*organi di cui all'articolo 74b capoverso 1 lettere b e c LSIn*» si intendono:

- le autorità federali, cantonali e comunali nonché le organizzazioni intercantonali, cantonali e intercomunali (art. 74*b* cpv. 1 lett. b LSIn) che sono responsabili di meno di 1000 abitanti in termini di popolazione stabilmente risiedente sono esentate dall'obbligo di segnalazione. Le amministrazioni di norma piccole o molto piccole di questi comuni non devono essere gravate in via aggiuntiva dall'obbligo di segnalazione. Dato il valore soglia di 1000 abitanti in termini di popolazione stabilmente risiedente, quasi il 40 per cento dei comuni è escluso dall'obbligo di segnalazione. Complessivamente ciò riguarderebbe circa 430 000 abitanti;

- le organizzazioni cui sono affidati compiti di diritto pubblico nei settori dell'approvvigionamento di acqua potabile, del trattamento delle acque di scarico e dello smaltimento dei rifiuti e le cui attività sono limitate a un comune o a un'organizzazione responsabili di meno di 1000 abitanti in termini di popolazione stabilmente risiedente sono esentate dall'obbligo di segnalazione.

L'eccezione non si applica ai fornitori e ai gestori di servizi e infrastrutture che servono all'esercizio dei diritti politici secondo l'articolo 74*b* capoverso 1 lettera s LSIn. Questi sono assoggettati all'obbligo di segnalazione anche se offrono i loro servizi e le loro infrastrutture a meno di 1000 abitanti.

Lett. b: Imprese di cui all'articolo 74b capoverso 1 lettera d LSIn

I valori soglia definiti in questa sede per l'ambito dell'elettricità si basano sull'ordinanza del 14 marzo 2008 sull'approvvigionamento elettrico (OAEl)[21], con la quale si

[21] RS **734.71**

intendono dichiarare vincolanti le raccomandazioni dello standard minimo per migliorare la resilienza delle TIC[22] per determinati attori del settore dell'elettricità.[23] La raccomandazione prevede che in sede di attuazione dello standard minimo gli attori siano tenuti a raggiungere un determinato livello di protezione dei loro impianti da ciberminacce (livello di protezione A, B o C). Il livello di protezione dipende dalle dimensioni e dall'influenza dell'attore sulla sicurezza dell'approvvigionamento e viene determinato in base a valori soglia corrispondenti. Di conseguenza soltanto le aziende elettriche appartenenti ai due livelli di protezione più elevati A e B dovranno essere assoggettate all'obbligo di segnalazione. Gli attori più piccoli tenuti a soddisfare i requisiti meno elevati del livello di protezione C sono esentati dall'obbligo di segnalazione. Al pari dei gestori di rete, i produttori di energia elettrica e i gestori di impianti elettrici di stoccaggio sono attori previsti dal diritto in materia di approvvigionamento elettrico[24]. Se un'impresa gestisce impianti sia per la produzione sia per lo stoccaggio di energia elettrica e questi impianti possono essere telecomandati ricorrendo allo stesso sistema, le potenze vengono sommate. La regolamentazione speciale riguarda anche i fornitori di servizi dei gestori di rete, dei produttori di energia elettrica e dei gestori di impianti di stoccaggio. Tra i fornitori di servizi non rientrano i produttori di hardware o software di cui all'articolo 74*b* capoverso 1 lettera u LSIn, per i quali non vi è alcuna regolamentazione speciale.

Il valore soglia di 400 GWh all'anno definito nell'articolo 16 capoverso 1 lettera b numero 2 dell'ordinanza in oggetto per esercenti di gasdotti è stato determinato in collaborazione con l'Associazione svizzera dell'industria del gas (ASIG). È determinante l'energia complessiva trasportata tramite la loro rete (ai consumatori finali o verso altre reti). La regolamentazione speciale riguarda soltanto esercenti di gasdotti la cui attività commerciale consiste nella vendita di gas a consumatori finali (la disposizione speciale quindi non riguarderebbe ad es. la Transitgas AG).

Con l'articolo 74*b* capoverso 1 lettera d LSIn, oltre a imprese di approvvigionamento di energia elettrica e di gas, sono assoggettate all'obbligo di segnalazione anche altre imprese attive nel settore dell'energia, ad esempio i gestori di condotte per il trasporto di petrolio, centrali di riscaldamento a distanza, raffinerie o imprese attive nei settori dell'energia da legno e del carbone. In linea di principio queste imprese sono assoggettate all'obbligo di segnalazione, a meno che non raggiungano i valori soglia definiti nell'articolo 16 capoverso 2 lettera b dell'ordinanza in oggetto. Le imprese attive sia nel settore dell'approvvigionamento di energia elettrica o di gas sia in un altro settore

---

22 Ufficio federale per l'approvvigionamento economico del Paese, «Standard minimo per migliorare la resilienza delle TIC», Berna, 2018.

23 In data 21 settembre 2023 il Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni (DATEC) ha avviato la consultazione concernente le revisioni parziali di diverse ordinanze nel settore dell'energia. Ad esempio è previsto che attraverso la revisione dell'ordinanza sull'approvvigionamento elettrico (OAEl) venga rafforzata la protezione da ciberminacce nell'approvvigionamento elettrico. Inoltre lo standard minimo TIC viene dichiarato vincolante per gli attori più importanti, ossia per i gestori di rete, i produttori e i gestori di impianti di stoccaggio. A tale scopo vengono assegnati a un determinato livello di protezione (profilo di protezione) con requisiti graduali che sono tenuti a raggiungere.

24 Riguardo ai produttori di energia elettrica cfr. l'art. 5 cpv. 2 della legge del 23 marzo 2007 sull'approvvigionamento elettrico (RS 734.7). Riguardo ai gestori di impianti elettrici di stoccaggio cfr. ad es. l'art. 17*a* cpv. 1 LAEl o l'art. 8*a* cpv. 1 lett. a n. 3 OAEl.

dell'energia (petrolio, calore a distanza ecc.) possono avvalersi di una regolamentazione speciale solo se il ciberattacco o le conseguenze di quest'ultimo si limitano a questo settore energetico.

Ai sensi dell'articolo 74*b* capoverso 1 lettera d LSIn sono già esentati dall'obbligo di segnalazione i titolari di licenze conformemente alla legge federale del 21 marzo 2003[25] sull'energia nucleare. Di conseguenza una regolamentazione a livello di ordinanza è superflua.

Lett. c: Imprese di cui all'articolo 74b capoverso 1 lettera n LSIn

Le imprese che sono definite secondo l'articolo 74*b* capoverso 1 lettera n LSIn e che non sono tenute ad adempiere requisiti specifici in materia di gestione della sicurezza o di programmi di sicurezza secondo i regolamenti UE indicati, sono esentate dall'obbligo di segnalare all'UFCS ciberattacchi rivolti contro i loro sistemi informatici. Questo si applica alle imprese che:

- non sono obbligate a realizzare un sistema di gestione della sicurezza delle informazioni (ISMS) conformemente agli articoli 2 e 4 e all'allegato II del regolamento (UE) 2023/203 del 5 ottobre 2023 o all'articolo 2 e all'allegato del regolamento (UE) 2022/1645 del 14 luglio 2022. Sono esentate anche dall'obbligo di segnalazione nei confronti dell'UFCS in caso di ciberattacchi. Un ISMS è un approccio sistematico per l'amministrazione di informazioni aziendali sensibili finalizzato a garantirne la sicurezza. Comprende persone, processi e sistemi informatici applicando un processo di gestione dei rischi. I regolamenti UE indicati stabiliscono standard e requisiti per la realizzazione di un tale sistema;

- non sono tenute ad attuare le direttive di cui al punto 1.7 dell'allegato del regolamento (UE) 2015/1998: tale regolamento riguarda norme per la sicurezza dell'aviazione civile. Il punto 1.7 dell'allegato potrebbe contenere misure o standard di sicurezza specifici che devono essere realizzati all'interno di un programma di sicurezza. Se l'impresa interessata non è tenuta ad attuare queste direttive nel suo programma di sicurezza – cosa che avviene sulla base degli articoli 2, 12, 13 o 14 del regolamento (CE) 300/2008 – è esentata anche dall'obbligo di segnalazione in caso di ciberattacchi.

Lett. d: Imprese ferroviarie di cui all'articolo 74b capoverso 1 lettera m LSIn

L'obbligo di segnalazione si limita alle imprese di trasporto con compiti sistemici di interesse pubblico sottoposte alla vigilanza dell'UFT, la cui attività sicura e affidabile è indispensabile per il benessere della popolazione e il funzionamento dell'economia. Di conseguenza le altre imprese sono escluse dall'obbligo di segnalazione.

Lett. e: Fornitori e gestori secondo l'articolo 74b capoverso 1 lettera t LSIn

I fornitori e i gestori di servizi di «cloud computing» e motori di ricerca come pure centri di calcolo che hanno sede in Svizzera sono assoggettati all'obbligo di segnalazione

[25] RS **732.1**

solo se forniscono le loro prestazioni in parte o interamente a favore di terzi e dietro compenso. In base al nuovo criterio della fornitura commerciale di prestazioni l'obbligo di segnalazione non riguarda nemmeno i centri di calcolo che forniscono le loro prestazioni esclusivamente per uso proprio.

Anche tutti i servizi di sicurezza e fiduciari digitali che vengono offerti a terzi sono assoggettati all'obbligo di segnalazione per ciberattacchi (senza un valore soglia medio) indipendentemente dal loro giro d'affari o dalla loro clientela. Invece i servizi che una persona ha sviluppato e utilizza esclusivamente per sé non sono assoggettati all'obbligo di segnalazione.

Capoverso 2: Valori soglia intersettoriali

Come eccezione generale, ai fini dell'obbligo di segnalazione a carico delle imprese, si è fatto riferimento al valore soglia della categoria delle «piccole imprese» in conformità alla raccomandazione della Commissione UE[26]. Di conseguenza le autorità e organizzazioni assoggettate all'obbligo di segnalazione di cui all'articolo 74*b* LSIn sono escluse dall'obbligo di segnalazione se 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. Si è rinunciato a convertire gli importi da euro in franchi svizzeri, dato che la norma europea si applica anche in Paesi UE economicamente più deboli dove la cifra d'affari o il totale di bilancio annuo di 10 milioni dovrebbe essere più difficile da raggiungere.

L'eccezione di cui al capoverso 2 si applica soltanto a imprese assoggettate all'obbligo di segnalazione per le quali non sono stati definiti valori soglia specifici secondo il capoverso 1. Vi rientrano:

- gli stabilimenti che figurano nell'elenco cantonale di cui all'articolo 39 capoverso 1 lettera e della legge federale del 18 marzo 1994[27] sull'assicurazione malattie (art. 74*b* cpv. 1 lett. f LSIn);

- i laboratori medici che dispongono di un'autorizzazione secondo l'articolo 16 capoverso 1 della legge del 28 settembre 2012[28] sulle epidemie (art. 74*b* cpv. 1 lett. g LSIn);

- le imprese che dispongono di un'omologazione secondo la legge del 15 dicembre 2000[29] sugli agenti terapeutici per la fabbricazione, l'immissione in commercio e l'importazione di medicamenti (art. 74*b* cpv. 1 lett. h LSIn);

- i fornitori di servizi postali registrati presso la Commissione delle poste secondo l'articolo 4 capoverso 1 della legge del 17 dicembre 2010[30] sulle poste (art. 74*b* cpv. 1 lett. l LSIn); e

[26] Raccomandazione della Commissione del 6 maggio 2003 relativa alla definizione delle microimprese, piccole e medie imprese (2003/361/CE).
[27] RS **832.10**
[28] RS **818.101**
[29] RS **812.21**
[30] RS **783.0**

– le imprese che riforniscono la popolazione di beni indispensabili di uso quotidiano e il cui dissesto totale o parziale comporterebbe considerevoli difficoltà di approvvigionamento (art. 74*b* cpv. 1 lett. p LSIn).

In questa sede occorre sottolineare che l'eccezione indicata nel capoverso 2 non si applica ad autorità federali, cantonali e comunali (art. 74*b* cpv. 1 lett. b LSIn) e a scuole universitarie (art. 74*b* cpv. 1 lett. a LSIn).

Art. 17 Obbligo di documentazione delle richieste di informazioni sull'assoggettamento all'obbligo di segnalazione

Questa disposizione si basa sull'articolo 74*a* capoverso 2 LSIn.

Dato che conformemente all'elenco di cui all'articolo 74*b* capoverso 1 LSIn l'obbligo di segnalazione comprende un gran numero di settori ed esistono numerose autorità e organizzazioni che conformemente all'articolo 74*c* LSIn e all'articolo 16 dell'ordinanza in oggetto sono esentate dall'obbligo di segnalazione, è lecito attendersi che nonostante queste regolamentazioni dettagliate determinate autorità e organizzazioni non avranno ben chiaro se sono assoggettate o meno all'obbligo di segnalazione. Di conseguenza le autorità e le organizzazioni interessate possono rivolgersi all'UFCS e chiedere di essere informate in merito all'esistenza di un obbligo di segnalazione secondo l'articolo 74*b* LSIn o di essere esentate dall'obbligo di segnalazione secondo l'articolo 74*c* LSIn.

Per fare in modo che l'UFCS possa trattare queste richieste di informazioni, il presente articolo 17 prevede che le autorità e le organizzazioni debbano mettere a disposizione dell'UFCS tutti i documenti necessari affinché l'Ufficio possa fornire informazioni in merito all'assoggettamento all'obbligo di segnalazione previsto dalla legge. Questo requisito assicura che l'UFCS possa effettivamente far fronte ai propri compiti nel settore della cibersicurezza. Dato che l'informazione fornita dall'UFCS rappresenta per così dire un'istantanea che si basa sulle circostanze in essere al momento della sua formulazione, spetta all'autorità o all'organizzazione interessata far fronte senza indugio all'obbligo di segnalazione a suo carico nel caso vi siano cambiamenti sostanziali dei fatti o delle circostanze rilevanti o indirizzare una richiesta di informazioni all'UFCS in caso di incertezze.

Art. 18 Ciberattacchi da segnalare

Questa disposizione si basa sull'articolo 74*d* LSIn.

In generale

I ciberattacchi da segnalare sono specificati nell'articolo 74*d* lettera a–d LSIn. In linea di principio i ciberattacchi sono assoggettati all'obbligo di segnalazione se sono particolarmente rilevanti per l'UFCS ai fini della preallerta e della valutazione della situazione di minaccia. I criteri per determinare gli attacchi assoggettati all'obbligo di se-

gnalazione sono stati selezionati in modo tale da essere il più possibile direttamente individuabili per le autorità e le organizzazioni. Con il presente articolo vengono ulteriormente precisati a livello di ordinanza.

Capoverso 1: Compromissione del funzionamento di un'infrastruttura critica (art. 74d lett. a LSIn)

Il funzionamento di un'infrastruttura critica può essere compromesso da un ciberattacco se i sistemi informatici, le reti o i sistemi di controllo che sono essenziali per il funzionamento dell'infrastruttura sono compromessi in misura tale da comportare interruzioni del sistema per collaboratori e terzi (art. 18 cpv. 1 lett. a) o l'organizzazione o l'autorità interessata può mantenere le proprie attività soltanto con l'aiuto di piani d'emergenza (art. 18 cpv. 1 lett. b). Si è in presenza di un'interruzione del sistema se collaboratori o terzi non possono più eseguire fasi di lavoro importanti per la loro attività, perché gli strumenti informatici necessari allo scopo non sono più disponibili. Sono considerate piani d'emergenza tutte le misure di carattere tecnico o organizzativo che devono essere adottate se gli strumenti informatici di solito utilizzati improvvisamente e inaspettatamente non sono più disponibili.

Capoverso 2: Manipolazione o fuga di informazioni (art. 74d lett. b LSIn)

Si presuppone la presenza di un ciberattacco soggetto all'obbligo di segnalazione in seguito a manipolazione o a una fuga di informazioni in particolare se gli aggressori sono in grado di accedere in modo non autorizzato a dati sensibili delle organizzazioni e delle autorità interessate, di criptarle, di sottrarle, di cancellarle, di divulgarle o di renderle accessibili a persone non autorizzate. Tramite un ciberattacco i dati possono essere manipolati da persone non autorizzate in maniera tale da mettere queste ultime in condizione di immettere informazioni rilevanti per le attività aziendali conformemente all'articolo 18 capoverso 2 lettera a dell'ordinanza in oggetto, che in seguito alla loro modifica o divulgazione comportano errori in processi aziendali, decisioni errate o addirittura rischi per la sicurezza. Conformemente all'articolo 18 capoverso 2 lettera b dell'ordinanza in oggetto però è possibile anche che in seguito a una manipolazione o a una fuga di informazioni sia stata violata la sicurezza dei dati personali secondo l'articolo 5 lettera h in combinato disposto con l'articolo 24 LPD.

Capoverso 3: Ciberattacco non identificato per un periodo prolungato (art. 74d lett. c LSIn)

Sono assoggettati all'obbligo di segnalazione anche i ciberattacchi non identificati per un periodo prolungato e per i quali esistono indizi che siano stati eseguiti per preparare ulteriori attacchi. L'articolo 18 capoverso 3 dell'ordinanza in oggetto stabilisce che si è in presenza di un periodo prolungato ai sensi dell'articolo 74*d* lettera c LSIn se, dopo che è stato identificato, si constata che il ciberattacco è stato compiuto già più di 90 giorni prima (ad es. mediante l'analisi di dati di log). Ciberattacchi di questo tipo rappresentano una seria minaccia per le infrastrutture critiche. Spesso vengono definiti anche «Advanced Persistent Threats» (APTs). Di norma sono altamente sofisticati, mirati e difficili da individuare. Per questa ragione sono particolarmente rilevanti per poter avvisare gli altri gestori di infrastrutture critiche. Quando si verifica

questo tipo di attacchi non è possibile escludere attività di spionaggio (ad es. spionaggio industriale o a danno delle autorità). Spesso gli attacchi sono molto complessi e vengono eseguiti da aggressori esperti che impiegano tecniche e strumenti avanzati per nascondersi nel sistema e dissimulare le loro attività. Di norma sono diretti contro organizzazioni, autorità o settori selezionati. È ipotizzabile anche che gli aggressori procedano in modo graduale per ampliare i diritti di accesso e sfruttare ulteriori vulnerabilità. Se vi sono indizi che un ciberattacco sia stato eseguito per preparare ulteriori attacchi è probabile che gli aggressori abbiano già accesso a sistemi o a dati critici e che possano utilizzarli per attacchi futuri.

Capoverso 4: Ciberattacco connesso ai reati di estorsione, minaccia o coazione (art. 74d lett. d LSIn)

Questo capoverso stabilisce che, in presenza di circostanze concomitanti rilevanti sotto il profilo penale, un ciberattacco debba essere segnalato in ogni caso se questi reati sono rivolti contro l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione, contro attuali o ex responsabili nonché contro attuali o ex collaboratori oppure contro persone che lavorano per l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione. Minacciando o eseguendo attacchi, numerosi cibercriminali tentano di ricattare gestori di infrastrutture critiche, i loro clienti o singoli collaboratori (ad es. mediante il criptaggio per mezzo di ransomware, minacciando attacchi rivolti contro la disponibilità mediante attacchi Distributed-Denial-of-Service [attacchi DDoS] oppure minacciando di pubblicare informazioni sensibili come dati personali o segreti aziendali). I ciberattacchi con circostanze concomitanti rilevanti sotto il profilo penale devono essere segnalati se l'estorsione, la minaccia o la coazione presenta un nesso con l'organizzazione o l'autorità assoggettata all'obbligo di segnalazione e può avere conseguenze negative sulla loro attività commerciale o amministrativa. In tale contesto si tratta di conseguenze gravi, comprese perdite finanziarie, danni alla reputazione o conseguenze legali. Segnalare tali attacchi è importante affinché l'UFCS possa valutare quanto sia importante la minaccia dovuta a cibercriminali a cui sono esposte le infrastrutture critiche.

Art. 19 Contenuto della segnalazione

Questa disposizione si basa sull'articolo 74*e* capoverso 2 LSIn.

In generale

In sede di redazione di questa disposizione d'esecuzione si è fatto riferimento in ampia misura alla terminologia e ai contenuti del modulo della FINMA concernente l'«obbligo di notificare i cyber-attacchi» introdotto il 1° settembre 2020.[31] Dato che l'UFCS, a differenza della FINMA, non ha una funzione di vigilanza, determinate informazioni non sono state riprese, in quanto non sono fondamentali ai fini dell'obbligo di segnala-

[31] Cfr. Comunicazione FINMA sulla vigilanza 05/2020 del 7 maggio 2020, che si basa sull'art. 29 cpv. 2 della legge federale concernente l'Autorità federale di vigilanza sui mercati finanziari (legge sulla vigilanza dei mercati finanziari, LFINMA; RS 956.1) ed è stata precisata dalla FINMA nella circolare 2023/1 (Circolare FINMA 2023/1 nm. 68).

zione all'UFCS. Ad esempio nella segnalazione all'UFCS non occorre fornire informazioni relative alle funzioni critiche o alle misure di comunicazione, poiché queste informazioni non fornirebbero nessun valore aggiunto per valutare il ciberattacco o per avvisare eventuali altre parti interessate. Inoltre per l'analisi di ciberattacchi sono state riprese anche indicazioni importanti dal modulo per eventi legati alla sicurezza informatica dell'ufficio federale tedesco per la sicurezza nelle tecnologie dell'informazione (BSI).[32] Il modulo di segnalazione per violazioni della sicurezza dei dati[33] che vengono segnalate all'IFPDT è stato utilizzato come riferimento per l'obbligo di segnalazione in caso di ciberattacchi.

L'articolo 74*e* capoverso 2 LSIn riporta il contenuto della segnalazione, ossia le informazioni essenziali che sono necessarie per adempiere all'obbligo di segnalazione. L'entità e i contenuti concreti delle informazioni da segnalare vengono specificati nella presente disposizione d'esecuzione e integrati dall'UFCS in un modulo sul suo sistema di comunicazione. Tale modulo contiene inoltre informazioni dettagliate su come vadano intese le informazioni da comunicare.

In questa sede si precisa ancora una volta che per adempiere all'obbligo di segnalazione nei confronti dell'UFCS non occorre fornire indicazioni che riguardano e violano eventuali segreti professionali o d'affari o che rendono penalmente perseguibile chi effettua la segnalazione (cfr. art. 74*e* cpv. 4 LSIn).

Capoverso 1: Informazioni sul tipo di ciberattacco e sulla sua esecuzione

La segnalazione di cui al *capoverso 1* comprende le seguenti informazioni sul tipo di ciberattacco e sulla sua esecuzione:

- *data e ora in cui è stato rilevato l'attacco (lett. a):* nella segnalazione occorre indicare il momento in cui il ciberattacco è stato scoperto specificando la data e l'ora;

- *data e ora in cui è stato compiuto l'attacco (lett. b):* nella segnalazione occorre indicare anche la data e l'ora in cui l'attacco è stato compiuto. Se non è noto, è possibile indicare anche il momento presunto in cui si è verificato il ciberattacco;

- *tipo di attacco (lett. c):* per quanto riguarda il tipo di ciberattacco e la sua esecuzione, nel modulo di segnalazione è possibile scegliere tra le tipologie di attacco più importanti (ad es. DDoS, accesso non autorizzato, malware, abuso / utilizzo non appropriato di infrastrutture tecnologiche ecc.). In aggiunta il modulo di segnalazione offre la possibilità di descrivere il ciberattacco all'interno di un campo di testo libero;

- *metodo di attacco (lett. d):* tra i metodi più frequenti, chiamati vettori di attacco nel linguaggio specialistico, rientrano ad esempio attacchi di phishing, lo sfruttamento di vulnerabilità, attacchi volti a sovraccaricare server, furti d'identità

[32] Cfr. il Modulo di segnalazione per eventi rilevanti per la sicurezza informatica sul portale di segnalazione e di informazione dell'ufficio federale tedesco per la sicurezza nelle tecnologie dell'informazione (disponibile in tedesco).

[33] Cfr. il Servizio online per la notifica di violazioni della sicurezza dei dati (art. 24 LPD).

ecc. Nel modulo di segnalazione sono riportati i vettori di attacco più frequenti ed è possibile selezionare più opzioni o specificare metodi o vettori non indicati;

- *indicazioni sull'autore (lett. e):* identificare gli autori di un ciberattacco può essere un compito complesso e impegnativo, dato che spesso cercano di dissimulare le loro tracce e di mantenere l'anonimato. Tuttavia ci sono diverse tipologie di informazioni che possono contribuire a identificare gli autori di un ciberattacco, come ad esempio indirizzi IP, record DNS, URL di pagine sospette, valori hash di malware, firme di virus, anomalie nel traffico di rete o comportamenti sospetti del software. Se sono disponibili informazioni di questo tipo occorre indicarle nella segnalazione.

Capoverso 2: Informazioni che indicano se il ciberattacco era connesso ai reati di estorsione, minaccia o coazione e se è stata sporta una denuncia penale

La divulgazione di tentativi di estorsione o minacce connessi a un ciberattacco può contribuire ad avvisare altre potenziali vittime e ad adottare misure volte a prevenire situazioni simili. Dato che un reato di estorsione, minaccia o coazione connesso a un ciberattacco può avere conseguenze sotto il profilo penale, può accadere che autorità oppure organizzazioni assoggettate all'obbligo di segnalazione sporgano una denuncia penale. Indicare se è stata sporta una denuncia penale aiuta l'UFCS a reagire in maniera adeguata all'accaduto.

Capoverso 3: Informazioni sulle ripercussioni del ciberattacco

Le indicazioni che devono essere fornite secondo il *capoverso 3 lettere a–c* aiutano l'UFCS a effettuare una prima valutazione delle ripercussioni del ciberattacco e a stabilire sotto quale profilo il ciberattacco comporta la compromissione di strumenti informatici e dati.

- *Indicazione delle unità dell'organizzazione o dell'autorità interessate (lett. a):* indicare l'unità interessata dal ciberattacco aiuta l'UFCS in particolare a valutare se sono interessati strumenti informatici o dati appartenenti alle infrastrutture critiche in particolare per quanto riguarda grandi imprese, conglomerati e gruppi con numerosi settori di attività.

- *Grado di compromissione della disponibilità, dell'integrità e della confidenzialità delle proprie informazioni e delle informazioni di terzi (lett. b):* l'autorità e l'organizzazione assoggettata all'obbligo di segnalazione è tenuta a valutare quali obiettivi di protezione (disponibilità, integrità e confidenzialità) sono interessati dal ciberattacco e in quale misura. A seconda di come vengono valutate le ripercussioni del ciberattacco, alla compromissione degli obiettivi di protezione viene assegnata una valutazione «bassa, media, elevata o grave» in funzione della gravità in analogia al modulo di segnalazione della FINMA.[34] Sulla base di questa prima valutazione delle ripercussioni e dell'assegnazione dei gradi di gravità è eventualmente possibile stabilire se per quanto riguarda le ripercussioni si sta delineando una tendenza. Questa informazione è preziosa in

[34] Cfr. al riguardo l'allegato 1 della Comunicazione FINMA sulla vigilanza 05/2020 del 7 maggio 2020, pag. 7.

particolare quando vi sono indizi di un peggioramento. Inoltre questa classificazione è utile anche per prendere una decisione nel caso in cui l'UFCS chieda aiuto per definire il modo di procedere concreto per gestire l'accaduto.

- *Ripercussioni del ciberattacco sul funzionamento delle unità dell'organizzazione e dell'autorità interessate (lett. c):* le indicazioni relative alle ripercussioni del ciberattacco sul funzionamento dell'organizzazione o dell'autorità devono far capire in che modo sono interessati ad esempio l'accesso a sistemi e dati, la disponibilità di servizi per clienti o cittadini, le procedure e i processi interni, la disponibilità di sistemi di approvvigionamento elettrico e idrico, i servizi sanitari o altre infrastrutture critiche. L'organizzazione o l'autorità assoggettata all'obbligo di segnalazione può fornire indicazioni riguardo ai tempi e alla durata delle ripercussioni del ciberattacco e rendere noto per quanto tempo persisteranno presumibilmente le ripercussioni dovute al ciberattacco.

Capoverso 4: Informazioni sull'autorità o sull'organizzazione assoggettata all'obbligo di segnalazione

Se l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione non è già registrata per partecipare allo scambio di informazioni e nel momento in cui viene effettuata la segnalazione non è possibile effettuare la registrazione (ad es. in seguito al mancato funzionamento degli strumenti informatici) o se l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione non intende effettuarla, conformemente al *capoverso 4* la segnalazione del ciberattacco deve contenere in aggiunta le seguenti informazioni relative all'autorità o all'organizzazione assoggettata all'obbligo di segnalazione:

- *ragione sociale, nome o designazione nonché indirizzo dell'autorità o dell'organizzazione assoggettata all'obbligo di segnalazione (lett. a)*: per l'identificazione ordinaria delle autorità e delle organizzazioni assoggettate all'obbligo di segnalazione queste devono indicare la loro ragione sociale, il loro nome o la loro designazione nonché il loro indirizzo con le seguenti informazioni: via, numero civico, numero postale d'avviamento e nome del luogo;

- *dati di contatto della persona che effettua la segnalazione (lett. b):* la segnalazione deve contenere almeno il nome e il cognome della persona che effettua la segnalazione. Inoltre occorre indicare il numero di telefono e l'indirizzo e-mail della persona che effettua la segnalazione, dato che si tratta della persona di contatto per l'UFCS. Le organizzazioni o le autorità possono indicare diverse persone di contatto.

Art. 20 Trasmissione della segnalazione

Questa disposizione si basa sull'articolo 74*f* LSIn.

Conformemente all'articolo 20 l'UFCS conferma immediatamente alle autorità e alle organizzazioni assoggettate all'obbligo di segnalazione di aver ricevuto la loro segnalazione, se questa non viene effettuata utilizzando il sistema di comunicazione

dell'UFCS. Se ad esempio la segnalazione viene effettuata via e-mail, l'UFCS informa eventuali persone di contatto registrate delle autorità e delle organizzazioni assoggettate all'obbligo di segnalazione conformemente all'articolo 13 capoverso 2 lettera b dell'ordinanza in oggetto. Con tale riscontro si intende fare in modo che l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione abbia la possibilità di comunicare all'UFCS se si è in presenza di una falsa segnalazione (ad es. una «segnalazione per scherzo» fatta da terzi).

Art. 21 Termine per registrare la segnalazione

Questa disposizione si basa sull'articolo 74*e* capoverso 1 e 3 LSIn.

In generale

Le autorità e le organizzazioni assoggettate all'obbligo di segnalazione sono tenute a segnalare immediatamente i ciberattacchi non appena ne vengono a conoscenza, in quanto vige il principio secondo cui la velocità prevale rispetto alla completezza. Questo è dovuto al fatto che l'UFCS ha assoluto bisogno che ciberattacchi assoggettati all'obbligo di segnalazione vengano segnalati immediatamente per poter far fronte al suo mandato legale di preallerta.

Capoverso 1: Completamento o modifica della segnalazione

Dato che in particolare per la preallerta e la prevenzione è determinante che le autorità e le organizzazioni assoggettate all'obbligo di segnalazione segnalino ciberattacchi immediatamente dopo che sono stati scoperti, l'articolo 74*e* capoverso 1 LSIn stabilisce un termine di 24 ore per procedere alla segnalazione. Il termine decorre a partire dal momento in cui il ciberattacco è stato scoperto. Entro tale termine occorre comunicare tutte le informazioni note in tale momento. Molto spesso quando si verificano ciberattacchi l'effettiva gravità dell'attacco e i contorni precisi dell'accaduto rimangono poco chiari per diverso tempo. Se le indicazioni richieste dall'UFCS conformemente all'articolo 19 dell'ordinanza in oggetto sono incomplete nel momento in cui viene effettuata la segnalazione, gli interessati possono completare la segnalazione con le indicazioni mancanti sulla base di nuovi elementi o conoscenze sufficienti oppure confermare che queste informazioni non sono disponibili. Questa segnalazione successiva deve essere trasmessa all'UFCS entro un termine di 14 giorni dal momento in cui è stata effettuata la segnalazione del ciberattacco. Entrambi i termini non sono prorogabili, in quanto si tratta di termini stabiliti dalla legge (cfr. art. 22 cpv. 1 PA).

Capoverso 2: Richiesta dell'UFCS

Se l'autorità o l'organizzazione assoggettata all'obbligo di segnalazione non comunica le informazioni richieste concernenti il ciberattacco entro il termine previsto di 14 giorni, l'UFCS è tenuto a emanare una richiesta indirizzata all'autorità o all'organizzazione assoggettata all'obbligo di segnalazione. Con questa richiesta l'UFCS invita

l’autorità o l’organizzazione assoggettata all’obbligo di segnalazione di completare immediatamente la segnalazione o di confermare che tali informazioni non sono disponibili.

Sezione 6: Disposizioni finali

Art. 23 Entrata in vigore

L’ordinanza entrerà in vigore contemporaneamente alla LSIn sottoposta a revisione in data 1° gennaio 2025.

3 Modifica di altri atti normativi

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

Art. 15*a* cpv. 2 lett. f OOrg-DDPS

Dato che l'articolo 7 di questa ordinanza descrive in modo più dettagliato i compiti del Computer Emergency Response Team (CERT) dell'UFCS, l'articolo 15*a* capoverso 2 lettera f OOrg-DDPS viene accorciato al fine di evitare doppioni.

Art. 15*a* cpv. 2 lett. h OOrg-DDPS

Il nuovo articolo 15*a* capoverso 2 lettera h OOrg-DDPS stabilisce che l'UFCS rappresenta la Svizzera in organi internazionali per l'analisi tecnica di ciberminacce e per la gestione di ciberincidenti. Questa precisazione è importante perché ciberincidenti e ciberminacce sono fenomeni internazionali. Gli aggressori utilizzano le stesse tecnologie e gli stessi metodi in numerosi Paesi contemporaneamente. Per questa ragione il dialogo a livello nazionale e internazionale tra servizi specializzati è indispensabile per la protezione da ciberincidenti e ciberminacce. A questo proposito l'UFCS partecipa attivamente a uno scambio di informazioni con organi svizzeri e internazionali che hanno compiti simili a quelli dell'UFCS. Questo scambio di informazioni serve a condividere informazioni e dati rilevanti concernenti minacce attuali e a coordinare misure comuni per gestire ciberincidenti e ciberminacce. Nei confronti degli Stati UE, con il suo CERT l'UFCS ha quindi il rango di un «Computer Security Incident Response Team (CSIRT)» nazionale, come prescritto dalla direttiva NIS-2 dell'UE per tutti gli Stati membri dell'UE.[35] Inoltre l'UFCS rappresenta la Svizzera all'interno di organi specializzati internazionali che si occupano dell'analisi tecnica di ciberincidenti e ciberminacce nonché della gestione di incidenti sotto il profilo tecnico. Ciò significa che l'UFCS partecipa a forum e gruppi di lavoro internazionali per mettere a disposizione le sue conoscenze tecniche e la sua esperienza nel settore della cibersicurezza e trarre beneficio dagli insegnamenti tratti dagli altri Paesi. Con lo scambio di informazioni e la partecipazione a organi specializzati internazionali l'UFCS contribuisce a fare in modo che la Svizzera sia sempre aggiornata per quanto riguarda gli sviluppi nel settore della cibersicurezza e possa beneficiare delle buone pratiche di altri Paesi. Ciò migliora la capacità dell'UFCS di reagire in maniera adeguata a ciberincidenti e ciberminacce e di contribuire alla sicurezza globale. Tutti questi compiti richiedono uno scambio di informazioni con organi svizzeri, stranieri e internazionali, le cui basi legali sono contenute nell'articolo 73*d* capoverso 1 e negli articoli 76, 76*a* e 77 LSIn.

[35] Direttiva (UE) 2022/2555 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO del 14 dicembre 2022 relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS-2)).

2. Ordinanza del 31 agosto 2022 sulla protezione dei dati

Art 41 cpv 1 OPDa

Dato che il 29 settembre 2023 il Parlamento ha approvato una modifica della LSIn che comporta l'introduzione dell'obbligo di segnalare ciberattacchi a infrastrutture critiche dal 1° gennaio 2025, in base alle modifiche decise occorre abrogare l'articolo 41 capoverso 1 dell'ordinanza del 31 agosto 2022 sulla protezione dei dati.