Modello di clausola contrattuale della CA concernente i ciber-rischi

La Conferenza degli acquisti della Confederazione (CA) ha elaborato per i servizi d'acquisto dell'Amministrazione federale una clausola sulla protezione dei sistemi informatici e di telecomunicazione contro eventuali attacchi e sul relativo obbligo di comunicare siffatti incidenti, da inserire nei modelli di contratto di appalto. Si tratta di una disposizione contrattuale a sé stante, articolata in vari numeri che può essere ripresa in un contratto di appalto. Le spiegazioni a complemento della clausola sono intese ad agevolarne la comprensione e a concretizzarne l'applicazione, tuttavia non sono parte integrante del contratto. Il modello di clausola è adatto innanzitutto per gli acquisti che comportano un alto potenziale di rischio per quanto riguarda i ciberattacchi, ai sensi delle disposizioni seguenti. Esso deve essere applicato in funzione delle esigenze e ha contenuto dispositivo, in quanto per ciascun contratto occorre concordare la formulazione che meglio si adegua ai rischi insiti nella situazione concreta.

Il presente documento contiene altresì delle spiegazioni sul contenuto e sull'applicazione del modello di clausola.

Numero X Protezione dei sistemi informatici e di telecomunicazione contro eventuali attacchi, obbligo di comunicazione

1. N.N (nome del partner dell'Amministrazione federale indicato nel contratto)[1] si impegna, ai fini dell'esecuzione del contratto e durante l'esecuzione dello stesso, a proteggere nel proprio ambito di responsabilità i sistemi informatici e di telecomunicazione (in particolare i sistemi infrastrutturali, le reti, i dispositivi e le applicazioni, come pure i dati[2] e le informazioni[3]) – di seguito denominati «sistemi» – contro eventuali attacchi, adottando misure economicamente ragionevoli e possibili dal punto di vista tecnico e organizzativo secondo lo stato attuale della tecnica.

2. Sono considerati «attacchi» (termine equivalente a «ciberattacchi») in special modo l'accesso indebito, le perturbazioni, la manipolazione oppure l'utilizzo abusivo dei sistemi dall'interno o dall'esterno. Lo stesso vale in particolare per il furto, l'elaborazione illecita oppure la distruzione di informazioni o dati nonché ogni altra intrusione illecita nei sistemi (cfr. segnatamente gli art. 143, 143bis,144bis, 147,179^{novies}, 272–274 del Codice Penale [CP][4]).

3. Ai fini della corretta esecuzione del contratto N.N si impegna in particolare a proteggere, conformemente alle disposizioni del presente numero X, i dati e le informazioni messi a sua disposizione o a disposizione di terzi incaricati[5] (ad es. subappaltatori e fornitori) oppure prodotti da essa o da terzi incaricati. Questo vale soprattutto se si tratta di dati rilevanti per la sicurezza o di dati personali. In tale contesto, occorre osservare i requisiti e le prescrizioni della legge federale del 19 giugno 1992[6] sulla protezione dei dati (LPD), dell'ordinanza del

---

1 Adeguare la terminologia al relativo modello di contratto (ad es. mandatario, appaltatore).
2 Ad esempio i dati personali relativi a collaboratori, indirizzi email, codici di accesso ecc.
3 Ad esempio la descrizione di processi, fasi lavorative, piani, regole di accesso, infrastrutture ecc.
4 RS **311.0**
5 Sono considerate tutte le parti della catena di fornitura e di produzione, compresi i titolari di diritti e i fabbricanti.
6 RS **235.1**

Ufficio federale delle costruzioni e della logistica UFCL
Fellerstrasse 21, 3003 Berna
Tel. +41 41 58 462 38 50, fax +41 58 465 50 09
bkb@bbl.admin.ch
www.bbl.admin.ch/bkb

27 maggio 2020[7] sui ciber-rischi (OCiber) e dell'ordinanza del 4 luglio 2007[8] sulla protezione delle informazioni (OPrI).

4. N.N comunica spontaneamente al beneficiario della prestazione[9] e/o al servizio designato nel contratto qualsiasi evento che potrebbe pregiudicare l'osservanza dei propri obblighi, subito dopo il verificarsi dell'evento o dopo averne preso atto, ma al più tardi entro X ore. Comunica in particolare i tentativi di attacco o gli attacchi riusciti come pure altre compromissioni tecniche sospettate o avvenute di sistemi, dati e/o informazioni, nonché gli eventuali danni arrecati. Informa altresì sulle misure previste oppure adottate per rimediare a tali danni. Per evitare danni o ulteriori attacchi, N.N accorda al beneficiario della prestazione o a terzi da esso incaricati, alla prima richiesta e senza indugio, il pieno accesso ad analisi, rapporti d'indagine e altre constatazioni (documenti, dati, dati d'accesso, oggetti ecc.) che consentono di analizzare l'evento. N. N si accerta che le attività predefinite con il beneficiario della prestazione siano registrate (logging) e valutate, al fine di individuare e evitare gli attacchi. Le falle di sicurezza scoperte devono essere chiuse al più presto.

5. Il beneficiario della prestazione (o un terzo da esso incaricato) può, se necessario e al massimo due volte all'anno, eseguire audit presso N. N. Gli audit sono preceduti da un preavviso di X giorni lavorativi. Ciascuna parte si assume i propri costi dell'audit. Tuttavia, se nell'ambito dell'audit si dovessero constatare lacune gravi ai sensi della presente disposizione, N. N si assume anche i costi per colmare tali lacune e quelli sostenuti dal beneficiario della prestazione a seguito dell'audit. N. N è tenuto a colmare le lacune entro X giorni dalla comunicazione e a notificare al beneficiario della prestazione l'avvenuta esecuzione dei relativi lavori.

6. Se non ha adottato le misure previste nella presente clausola, N. N. deve pagare una pena convenzionale. Per ogni violazione essa ammonta al 10 per cento della retribuzione totale, ma almeno a 3000 franchi. Il pagamento della pena convenzionale non esonera N. N dall'osservanza dei propri obblighi contrattuali. La pena convenzionale è computata in un eventuale risarcimento dei danni.

7. N. N risponde per il danno arrecato al beneficiario della prestazione se non prova che non gli è imputabile alcuna colpa.

In caso di violazione sostanziale della presente clausola o di mancata collaborazione nei casi sopracitati, il beneficiario della prestazione si riserva il diritto di non acquisire altre prestazioni e di porre fine al rapporto contrattuale.

Eventualmente introdurre il numero 8 per disciplinare l'obbligo di stipulare un'assicurazione di responsabilità civile *(vedi le relative spiegazioni più sotto, con la proposta di testo)*

Conferenza degli acquisti della Confederazione (CA)

Edizione: 1.9.2020

Stato: 9.11.2022

Le spiegazioni figurano sulle pagine seguenti.

[7] RS 120.73
[8] RS 510.411
[9] Adeguare la terminologia al relativo modello di contratto (ad es. committente, acquirente).

Spiegazioni relative al modello di clausola

Indicazione sul completamento del modello di clausola

Redigendo il contratto bisogna sostituire le parti evidenziate in giallo con i contenuti desiderati.

In generale

Lo scopo del modello di clausola è la protezione dei dati, delle informazioni e dei sistemi, prima e durante i ciberattacchi.

Il modello va utilizzato quale disposizione generale per le operazioni esposte ai suddetti rischi, ossia nei contratti relativi all'acquisto di tecnologie dell'informazione e della comunicazione la cui conclusione può determinare una situazione particolarmente rischiosa. In linea di principio, si corrono rischi ogni volta che, fornendo una prestazione, una parte contraente utilizza sistemi informatici e di telecomunicazione. Nello specifico si tratta di evitare che un ciberattacco nei confronti di uno dei partner commerciali dell'Amministrazione federale causi danni o perdite di dati, informazioni e sistemi dell'Amministrazione federale ed eventualmente di limitare gli effetti di tali danni o perdite. Lo stesso vale se i sistemi informatici dei partner commerciali sono o potrebbero essere usati per sferrare un ciberattacco contro l'Amministrazione federale. In questi casi bisogna ad esempio proteggere i codici e le password oppure le informazioni come i piani di occupazione, i piani di costruzione o i piani degli impianti tecnici (ulteriori esempi alla nota 3 del modello).

Nella stesura di un contratto con un partner commerciale occorre tenere conto delle esigenze di protezione e di informazione inserendo il presente modello di clausola.

Il modello di clausola deve essere adeguato in base alle necessità e ha contenuto dispositivo. Se la parte contraente elabora dati e/o informazioni che soggiacciono al segreto d'ufficio o ad altre disposizioni sul mantenimento del segreto oppure che sono considerate classificate ai sensi delle vigenti disposizioni sulla protezione delle informazioni della Confederazione, bisogna inoltre verificare se, nel singolo caso, le disposizioni della clausola devono essere definite in modo più dettagliato nel contratto.

Per converso è possibile dare il giusto peso alle situazioni meno rischiose adeguando nel caso specifico singole disposizioni della clausola, ad esempio scegliendo una formulazione meno rigorosa per la pena convenzionale o attenuando le condizioni del diritto di audit.

Non si esclude nemmeno la possibilità di stabilire di comune accordo misure relative alla protezione e alla comunicazione se, dal canto loro, i partner commerciali affidano all'Amministrazione federale segreti d'affari, informazioni o dati degni di protezione. Qualora le presenti disposizioni contrattuali o parti di esse siano stabilite di comune accordo dalle parti, prima della conclusione del contratto occorre però verificare accuratamente gli obblighi assunti dall'unità contraente dell'Amministrazione federale relativi ai diritti di accesso e di audit come pure la regolamentazione concernente la pena convenzionale. Si raccomanda a tal fine di consultare il servizio giuridico competente.

Numero 1

«N. N.» sta per l'espressione latina «nomen nominandum» (nome da definire). Al momento della stesura del contratto, va sostituito con il nome corretto del partner contrattuale che deve proteggere dai ciberattacchi i dati o le informazioni ricevuti dall'Amministrazione federale ai fini dell'esecuzione del contratto.

Numero 2

A complemento si veda anche la «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» (pag. 27) al link seguente:

https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/ncs_strategie-2012.html

Numero 3

«X» riprende la numerazione del contratto in cui la clausola s'inserisce. Deve corrispondere al numero indicato nella denominazione (titolo) della stessa clausola.

In determinate circostanze il rispetto delle basi legali svizzere può rivelarsi difficile se una parte contraente è straniera. L'esperienza insegna che questi contratti richiedono trattative supplementari; ciononostante l'unità contraente dell'Amministrazione federale potrà basarsi sulla clausola per condurre tali trattative e appianare eventuali divergenze. Per far valere il diritto svizzero è necessario verificare se la prestazione è fornita in Svizzera o all'estero. In linea di principio si raccomanda di convenire l'applicabilità del diritto svizzero e di stabilire di comune accordo che il foro competente è Berna.

Numero 4

Per «beneficiario della prestazione» s'intende l'unità contraente dell'Amministrazione federale.

Il termine per l'esercizio dell'obbligo di comunicazione (X ore) deve essere fissato di volta in volta nel contratto in cui tale obbligo trova applicazione, in funzione delle necessità e dei rischi concreti. In merito non esiste alcuna regola generalizzabile.

È consigliabile fissare una scadenza breve e adeguata al livello di rischio potenziale; ad esempio, quando gli incidenti e le loro conseguenze possono essere critici, di poche ore.

L'obbligo di comunicazione riguarda in particolare le vulnerabilità critiche e i ciberincidenti che possono compromettere la protezione dei dati o la funzionalità del sistema. Non concerne invece le e-mail di phishing, le spam o i port scan. Un sistema o una banca dati, ma anche una singola serie di dati, sono considerati tecnicamente compromessi[10] se l'integrità delle informazioni memorizzate non può più essere garantita, a prescindere dal fatto che l'attacco o la compromissione siano atti intenzionali. Il contenuto e la forma della comunicazione devono essere definiti dalle parti contraenti, in considerazione dell'esigenza di proteggere i dati e il sistema.

[10] Cfr. definizione di «technische Kompromittierung» su Wikipedia: https://de.wikipedia.org/wiki/Technische_Kompromittierung.

Numero 5

Il termine per il preavviso di un audit (X giorni lavorativi) deve essere fissato di volta in volta nel contratto in cui tale preavviso trova applicazione, in funzione delle necessità e dei rischi concreti. Per esperienza si propone un termine di 20 giorni lavorativi. In merito non esiste però alcuna regola generalizzabile. Se ragionevole, nel caso specifico si possono definire modalità dell'audit diverse.

Al posto di «X» deve essere indicato il numero preciso di giorni. In alternativa si può convenire una data concreta e adeguare di conseguenza la frase.

Numero 6

La regolamentazione concernente la pena convenzionale ricalca la clausola standard delle varie condizioni generali (CG) della Confederazione. L'importo e il calcolo della pena possono essere adeguati nel contratto sempreché nel caso concreto, dopo aver valutato il rischio, i servizi competenti lo ritengano opportuno.

Numero 7

Questa disposizione può essere tralasciata o deve essere adeguata se la responsabilità e la fine del contratto sono regolamentate in altri numeri (cfr. anche i modelli di contratto della CA e le CG della Confederazione) oppure se la situazione di rischio specifica lo permette o lo richiede. Di norma la parte contraente risponde di tutti i danni arrecati a seguito degli attacchi di cui al numero 2 della clausola.

Eventuale numero 8

Determinate imprese di assicurazione offrono la possibilità di assicurare i rischi legati ai ciberattacchi. Nel caso specifico e nei contratti che vertono sulla fornitura di prestazioni mediante sistemi informatici e di telecomunicazione – in particolare in quelli conclusi con grandi imprese (non tanto con le PMI) – può perciò essere opportuno obbligare la parte contraente a stipulare un'assicurazione supplementare in base al danno potenziale.

Proposta di un accordo corrispondente:

«8. N. N. si impegna a stipulare un'assicurazione di responsabilità civile adatta a coprire i rischi legati ai ciberattacchi e il rischio di danni e a comprovare, al momento della conclusione del contratto, di avere una copertura assicurativa sufficiente.