MODELLO DI ORGANIZZAZIONE, GESTIONE E CONTROLLO EX D. LGS. 8 GIUGNO 2001 N. 231

PARTE SPECIALE B

REATI INFORMATICI

(ART. 24 BIS)

APPROVATO DAL CONSIGLIO DI AMMINISTRAZIONE IL 6/12/2023

FINCANTIERI INFRASTRUCTURE OPERE MARITTIME S.P.A.

SEDE LEGALE IN TRIESTE, VIA GENOVA 1

ISCRIZIONE AL REGISTRO DELLE IMPRESE DI TRIESTE N. 01336990328

LE FATTISPECIE DI REATO

La presente Parte Speciale si riferisce ai reati informatici, richiamati dall'art. 24 bis del D. Lgs. 231/2001, ed in particolare riporta le singole fattispecie di reato considerate rilevanti per la responsabilità amministrativa di Fincantieri Infrastructure Opere Marittime S.p.A.. Individua inoltre le cosiddette attività "sensibili" (quelle dove è teoricamente possibile la commissione del reato e che sono state individuate nell'ambito dell'attività di *risk assessment*) specificando i principi comportamentali ed i presidi di controllo operativi per l'organizzazione, lo svolgimento e la gestione delle operazioni svolte nell'ambito delle sopracitate attività "sensibili".

In considerazione dell'analisi dei rischi effettuata, sono risultati potenzialmente realizzabili nel contesto aziendale di Fincantieri Infrastructure Opere Marittime S.p.A. i seguenti reati:

DOCUMENTI INFORMATICI (ART. 491 BIS C.P.)

L'articolo in oggetto stabilisce che tutti i delitti relativi alla falsità in atti, tra i quali rientrano sia le falsità ideologiche che le falsità materiali, sia in atti pubblici che in atti privati, sono punibili anche nel caso in cui la condotta riguardi non un documento cartaceo, bensì un documento informatico.

I documenti informatici, pertanto, sono equiparati a tutti gli effetti ai documenti tradizionali.

Per documento informatico deve intendersi la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti (art. 1, co. 1, lett. p), D. Lgs. 82/2005).

ACCESSO ABUSIVO AD UN SISTEMA INFORMATICO O TELEMATICO (ART. 615 TER C.P.)

Tale reato si realizza quando un soggetto abusivamente si introduce in un sistema informatico o telematico protetto da misure di sicurezza ovvero vi si mantiene contro la volontà espressa o tacita di chi ha diritto ad escluderlo.

L'accesso è abusivo poiché effettuato contro la volontà del titolare del sistema, la quale può essere implicitamente manifestata tramite la predisposizione di protezioni che inibiscano a terzi l'accesso al sistema stesso.

Risponde del delitto di accesso abusivo a sistema informatico anche il soggetto che, pur essendo entrato legittimamente in un sistema, vi si sia trattenuto contro la volontà del titolare del sistema oppure il soggetto che abbia utilizzato il sistema per il perseguimento di finalità differenti da quelle per le quali era stato autorizzato.

DANNEGGIAMENTO DI INFORMAZIONI, DATI E PROGRAMMI INFORMATICI (ART. 635 BIS C.P.)

Tale fattispecie reato si realizza quando un soggetto "distrugge, deteriora, cancella, altera o sopprime informazioni, dati o programmi informatici altrui". Il reato, ad esempio, si integra nel caso in cui il soggetto proceda alla cancellazione di dati dalla memoria del computer senza essere stato preventivamente autorizzato da parte del titolare del terminale.

DANNEGGIAMENTO DI SISTEMI INFORMATICI O TELEMATICI (ART. 635-QUATER)

Salvo che il fatto costituisca più grave reato, chiunque, mediante le condotte di cui all'articolo 635-bis, ovvero attraverso l'introduzione o la trasmissione di dati, informazioni o programmi, distrugge, danneggia, rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ne ostacola gravemente il funzionamento è punito con la reclusione da uno a cinque anni.
Se ricorre la circostanza di cui al numero 1) del secondo comma dell'articolo 635 ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è aumentata.

IDENTIFICAZIONE DELLE ATTIVITA' A RISCHIO REATO

Le attività che la Società ha individuato come sensibili, nell'ambito dei delitti informatici, sono indicate in dettaglio nella Matrice delle Attività a Rischio-Reato conservata a cura della Segreteria di Direzione, unitamente a potenziali esemplificazioni di modalità e finalità di realizzazione della condotta illecita.

Tali attività sono di seguito riepilogate:

- Falsificazione di documenti informatici relativi ad esempio a rendicontazione in formato elettronico di attività e/o a attestazioni elettroniche di qualifiche o requisiti della Società.
- Accesso ai sistemi informatici aziendali o di terze parti, che contengono:
  - brevetti, disegni, attività di R&S;
  - dati di marketing;
  - informazioni riservate di enti pubblici;
  - informazioni bancarie;
  - parametri per l'attivazione di servizi;
  - dati di fatturazione o di credito;
  - dati relativi a pagamenti.
- Gestione di strumenti e dispositivi e programmi, da parte di soggetti aziendali e amministratori di sistema, mediante i quali possono:
  - essere intercettate informazioni rilevanti di terze parti o impedite comunicazioni anche alla Pubblica Amministrazione;
  - danneggiare un sistema informatico o telematico, nell'ambito delle strutture di un concorrente.

PRINCIPI GENERALI DI COMPORTAMENTO

Coerentemente con i principi deontologici aziendali di cui alla Parte Generale del Modello Organizzativo ex D. Lgs.231/2001 e al Codice di Comportamento, tutti i Destinatari del Modello che, a qualunque titolo, siano stati designati o incaricati alla gestione e manutenzione dei *server*, delle banche dati, delle applicazioni, dei *client* e delle reti di telecomunicazione, nonché a tutti coloro che abbiano avuto assegnate *password* e chiavi di accesso al sistema informativo aziendale, sono tenuti ad osservare i seguenti principi di comportamento e controllo:

- il personale deve astenersi da qualsiasi condotta che possa compromettere la riservatezza e l'integrità delle informazioni e dei dati aziendali e dei terzi ed in particolare si premura di non lasciare incustoditi i propri sistemi informatici e bloccarli, qualora si allontani dalla postazione di lavoro, con i propri codici di accesso ovvero di spegnere il computer e tutte le periferiche al termine del turno di lavoro;
- il personale si astiene da qualsiasi condotta diretta a superare o aggirare le protezioni del sistema informatico aziendale o altrui;
- il personale si impegna a sottoscrivere lo specifico documento relativo al corretto utilizzo delle risorse informatiche aziendali;
- il personale conserva i codici identificativi assegnati, astenendosi dal comunicarli a terzi che, in tal modo, potrebbero accedere abusivamente a dati aziendali riservati;
- il personale non può installare programmi senza aver preventivamente informato la funzione aziendale preposta alla gestione della sicurezza informatica;
- il personale non può utilizzare connessioni alternative rispetto a quelle fornite dalla Società nell'espletamento dell'attività lavorativa resa in suo favore.

PROCEDURE DI CONTROLLO

Ad integrazione delle regole comportamentali di carattere generale sopraindicate, si riportano di seguito ulteriori presidi di controllo operativi a prevenzione della commissione dei reati informatici, con particolare riferimento al processo strumentale alla commissione dei reati quale la gestione della dell'infrastruttura tecnologica.

Gestione dell'infrastruttura tecnologica:

- il personale accede al sistema informativo aziendale unicamente attraverso il profilo identificativo assegnato, attraverso user ID e password strutturate sulle base di un adeguato livello di complessità;
- sono predisposti idonei controlli/monitoraggi sulla rete informatica aziendale al fine di individuare comportamenti anomali o attività eccezionali dei server al di fuori degli orari di operatività sociale e predisposizione di adeguate difese/protezioni fisiche dei server stessi al fine di prevenire l'ingresso e l'uscita di materiale o di personale non autorizzati;
- è previsto un regolamento interno che regoli l'utilizzo della strumentazione tecnologica (e.g. laptop, telefoni) concessa in dotazione al personale della Società;
- è garantita la protezione dei sistemi informatici aziendali, al fine di prevenire l'illecita installazione di dispositivi hardware in grado di intercettare, impedire, interrompere o danneggiare le comunicazioni e/o i dati relativi ad un sistema informatico o telematico di terzi;
- sono definiti controlli di individuazione, prevenzione e ripristino al fine di proteggere da software dannosi (virus), nonché di procedure per la sensibilizzazione degli utenti sul tema;
- sono definiti formalmente i requisiti di autenticazione ai sistemi per l'accesso ai dati e per l'assegnazione dell'accesso remoto agli stessi da parte di soggetti terzi quali consulenti e fornitori;
- sono definiti i criteri e le modalità per l'assegnazione, la modifica e la cancellazione dei profili utente;
- la funzione aziendale preposta alla gestione della sicurezza informatica deve definire i criteri e le modalità per la gestione del processo di dismissione delle utenze cessate;
- sono definiti e regolamentati gli accessi fisici alle sale server aziendali;
- gli amministratori di sistema sono muniti di proprie credenziali di autenticazione e gli accessi sugli applicativi aziendali sono adeguatamente tracciati su log, nel rispetto delle disposizioni del Garante;
- le applicazioni tengono traccia delle modifiche, compiute dagli utenti, ai dati ed ai sistemi;
- il server e i laptop aziendali sono aggiornati periodicamente sulla base delle specifiche necessità; il server e i laptop aziendali sono inoltre protetti da programmi antivirus, aggiornati in modo automatico, contro il rischio di intrusione;
- la rete di trasmissione dati aziendale è protetta da adeguati strumenti di limitazione degli accessi (*firewall* e *proxy*);
- i dispositivi telematici di instradamento sono collocati in aree dedicate e protetti al fine di renderli accessibili al solo personale autorizzato;
- sono previste regole per rilevare e indirizzare tempestivamente le vulnerabilità tecniche dei sistemi;

- sono definite regole per la navigazione in Internet che includono tra le altre l'utilizzo della rete al solo fine lavorativo, il divieto di scarico di software nelle strutture informative aziendali;
- sono definite regole di utilizzo della posta elettronica, che si riassumono nel divieto d'uso della casella di posta personale per finalità estranee alle esigenze di servizio;
- sono previste soluzioni di *content filtering* a difesa dell'integrità del sistema informatico da potenziali attacchi veicolati in modalità vietata (*malware* tipo *botnet*) e presenza nella postazione lavoro di software antivirus aggiornato.

La gestione dei servizi erogati dalla Capogruppo alla Società è regolata sulla base di appositi contratti di service. La Società provvede a nominare un referente interno per l'attività esternalizzata.

Con specifico riferimento alle attività gestite mediante contratto di service infragruppo, le parti si impegnano nei confronti l'una dell'altra dall'astenersi, nell'espletamento delle attività oggetto del rapporto contrattuale, da comportamenti e condotte che, singolarmente o congiuntamente ad altre, possono integrare una qualsivoglia fattispecie di reato contemplata dal Decreto.