Modello di organizzazione, gestione e controllo ex D.Lgs. 231/01.

PARTE SPECIALE ñDò: I DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI.

La presente Parte Speciale, dedicata alla prevenzione dei delitti informatici e di trattamento illecito di dati e alla disciplina dei comportamenti ed attività che potrebbero astrattamente configurarli, è strutturata nelle seguenti parti:

1) illustrazione delle fattispecie di reato ascrivibili alla famiglia dei delitti informatici e di trattamento illecito di dati contro la Pubblica Amministrazione, astrattamente configurabili nella realtà dellôAssociazione Forte di Bard;

2) identificazione dei processi ed attività aziendali dellôAssociazione Forte di Bard a rischio di potenziale commissione dei suddetti reati e derivanti dalle attività di risk assessment condotte e delineazione dei principi di comportamento e regole di condotta applicabili nella realizzazione delle attività a rischio, ad integrazione del sistema etico.

Costituiscono parte integrante della presente Parte Speciale, anche i seguenti documenti qui allegati:

i) Regolamento per l'utilizzo dei sistemi informatici dellôAssociazione Forte di Bard

ii) Documento descrittivo dellôorganizzazione e gestione della rete informatica dellôAssociazione Forte di Bard.

La presente Parte Speciale verrà ulteriormente dettagliata attraverso la redazione di un documento volto a meglio precisare le modalità di gestione della struttura informatica dellôAssociazione Forte di Bard con riferimento allôarea museale, allôHotel Cavour et des Officiers e allôarea ITC e ad eventualmente implementare le misure volte a minimizzare il rischio di commissione dei reati informatici.

I) LE FATTISPECIE DI REATO:

Tra i reati informatici, si riportano di seguito quelli astrattamente configurabili nellôambito delle attività svolte dallôAssociazione Forte di Bard:

***Delitti informatici e trattamento illecito di dati (art. 24 bis del D.lgs. 231/2001)** ï Tali ipotesi di reato rappresentano varie forme di aggressione a ñsistemi informaticiò o ñdati informaticiò e possono essere distinti in due gruppi:

- reati informatici in senso stretto, che sono la quasi totalità;

- reati commessi attraverso lôuso di un sistema informatico, che sono quelli di falsità connesse a documenti informatici (art.491-bis c.p.) e di frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.).

Prendendo le mosse dai reati informatici in senso stretto, di cui al primo punto che precede, gli stessi sono posti a presidio di beni giuridici diversi, quali lôinviolabilità del domicilio, lôinviolabilità dei segreti, lôintegrità di dati o sistemi.

Per quanto riguarda le condotte di accesso abusivo, il più delle volte propedeutiche alla commissione degli altri illeciti, vengono in rilievo i comportamenti dei cosiddetti hacker o cracker, i quali, seppure con finalità parzialmente diverse, forzano sistemi di protezione o alterano parte del codice dôaccesso. In particolare, sebbene le due figure siano equiparate, lôhacker forzerebbe il sistema al solo scopo di mostrarne la vulnerabilità, mentre il cracker sarebbe mosso dal fine di danneggiarne il contenuto.

Lôipotesi di accesso abusivo ricorre:

- sia nei casi in cui abbia ad oggetto un sistema che è interconnesso a una rete (ad es, internet) per cui non si possiede alcun tipo di autorizzazione, nella quale ipotesi lôautore del reato effettua connessioni triangolate su server esteri in modo da complicare la ricostruzione del percorso dôaccesso;

- sia quando lo si effettui ai danni di un sistema rispetto al quale si dispone di credenziali, ma per una funzione differente da quella per cui avviene lôaccesso. Tale condotta appare facilmente integrabile in relazione a una rete aziendale, ove i dipendenti accedano ad unôarea del server aziendale, senza esservi autorizzati. Il caso potrebbe verificarsi ove il dipendente sottraesse le credenziali di un collega onde accedere ad ambiti allo stesso vietati.

Come anticipato, lôaccesso abusivo è punito a prescindere dalla finalità per cui venga posto in essere e dal danneggiamento dello stesso: tuttavia, premesso che nella generalità dei casi i sistemi informatici o telematici sono protetti da misure di sicurezza, appare assai improbabile che lôaccesso prescinda da rimozioni di sicurezze, alterazione di password o altre forzature del sistema, tali da integrare forme di danneggiamento.

Con riguardo alle ipotesi di danneggiamento appena menzionate, deve farsi riferimento alle modifiche che intervengano sulla componente hardware o software, in modo da impedirne, anche parzialmente, il funzionamento.

Il Legislatore punisce altresì il danneggiamento di dati e programmi informatici, che può essere posto in essere tramite la diffusione di virus o, più semplicemente, attraverso i normali comandi del sistema o i programmi di cui dispone.

Lôart.24-bis individua tra le fattispecie delittuose in esame anche la detenzione o diffusione abusiva di codici di accesso a sistemi informatici o telematici: di conseguenza, devono essere scongiurati in ambito aziendale comportamenti sostanziantisi nellôuso di password troppo semplici o mnemoniche o di abitudini errate nella gestione dei dati.
Per quanto riguarda lôintercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche, si tratta di ipotesi di frequente verificazione in relazione alla rete internet e ai server di posta elettronica (in questa ultima ipotesi, lôinterruzione del servizio può essere provata mediante lôinvio di milioni di messaggi in modo ripetitivo e massivo verso un server).

La condotta assume rilevanza penale anche nei casi in cui si provochi un rallentamento (il cd « impedimento ») e non solo la vera e propria interruzione del servizio.

Lôipotesi potrebbe ricorrere anche in relazione a una rete informatica aziendale, ove lôutente, ad esempio mediante lôinstallazione di un software volto alla trasmissione di dati che esulano dallo scopo del sistema informatico, dovesse cagionare un rallentamento o il vero e proprio blocco della rete informatica.
Con riferimento allôintercettazione di dati, questa può avvenire mediante lôaccesso fisico alla struttura tecnologica, per la necessità di collegamento della sonda alla centrale telefonica o agli altri apparati che gestiscono le comunicazioni della rete, ovvero attraverso lôimpiego di software, chiamati spyware. Tali programmi sono ad esempio in grado di acquisire i dati digitati su una tastiera, consentendo in questo modo di acquisire password o informazioni nel momento in cui le stesse vengono digitate, ovvero di verificare i siti web visitati, le email inviate, le informazioni memorizzate sulle memorie di massa.
Venendo ai delitti che si consumano attraverso lôuso di sistemi informatici, devono essere menzionate le falsità aventi ad oggetto documenti informatici, in considerazione dellôequiparazione operata dallôart.491-bis c.p.
Assume infine rilevanza la frode informatica del soggetto che presta servizi di certificazione di firma elettronica (art. 640-quinquies c.p.), in qualche modo assimilata alla falsificazione di firme olografe. Tale ipotesi delittuosa non assume particolare rilevanza nel presente ambito aziendale, posto che lôAssociazione Forte di Bard non pone in essere attività certificativa del tipo menzionato.

Ai fini di eventuali responsabilità degli Enti ai sensi del D.Lgs.231/2001, i reati informatici in esame si caratterizzano per lôaggressione verso sistemi di terzi: in tale locuzione rientrano tanto i dati di dipendenti che operano allôinterno dellôEnte, quanto quelli di soggetti, anche collettivi, esterni alla Azienda (pubblici o privati).

È tuttavia innegabile come il requisito dellôinteresse o del vantaggio appaia più facilmente integrabile quando lôatto delittuoso si indirizzi verso lôesterno, potendo venire a colpire entità rispetto alle quali potrebbe essere vantaggiosa lôacquisizione di informazioni o lôinterferenza sul funzionamento del sistema.

In ottica prudenziale, lôAssociazione adotta misure volte a tutelare i propri sistemi e dati e detta principi idonei a scongiurare condotte illecite nei confronti di terzi.

II) I PROCESSI SENSIBILI.

I processi identificati come a rischio di commissione dei Reati ai sensi del Decreto ed emersi dallôanalisi di risk assessment svolto sono:

a. Gestione del sito internet e della rete intranet dellôAssociazione Forte di Bard;

b. Gestione dell'hardware e del software aziendale;

c. Sviluppo, manutenzione e gestione modifiche dei software applicativi;

d. Ogni altra attività svolta con l'utilizzo di strumenti di lavoro informatici e telematici.

Nell'ambito della gestione di tali attività, ad esempio, le risorse interne dellôAssociazione potrebbero:

a. accedere abusivamente ai sistemi informatici protetti da misure di sicurezza, eventualmente manipolarne i dati al fine di ottenere un vantaggio in ordine agli adempimenti contabili e di bilancio;

b. con riferimento alla gestione delle emergenze, distruggere o danneggiare sistemi informatici i cui dati possano provare il mancato adempimento di un obbligo in capo allôAssociazione;

c. distruggere o danneggiare il sistema informatico di rilevazione accessi al fine di impedire la consultazione dei dati e la rilevazione di eventuali carenze nella gestione delle emergenze.

III) I PRINCIPI DI COMPORTAMENTO.

Eô fatto espresso **divieto** ï a carico dei Destinatari del presente Modello - di porre in essere comportamenti da integrare le fattispecie di reato sopra considerate .

In particolare, è fatto divieto di porre in essere i seguenti comportamenti:

- introdursi senza autorizzazione in un sistema informatico o telematico interno o esterno allôAssociazione Forte di Bard protetto da misure di sicurezza ovvero mantenervisi contro la volontà altrui;
- procurare, riprodurre, diffondere, comunicare o consegnare abusivamente codici, parole chiave o altri mezzi idonei allôaccesso ad un sistema informatico o telematico, protetto da misure di sicurezza o comunque fornire indicazioni o istruzioni idonee al predetto scopo, al fine di procurare a sé o ad altri un profitto o arrecare ad altri un danno;
- diffondere, comunicare o consegnare un programma informatico anche da altri redatto, avente per scopo o per effetto il danneggiamento di un sistema informatico o telematico, dei dati o dei programmi in esso contenuti o ad esso pertinenti, ovvero lôinterruzione, totale o parziale, o lôalterazione del suo funzionamento;
- falsificare o utilizzare documenti informatici falsi o commettere una delle condotte previste dal Capo Terzo del Libro secondo del codice penale su documenti informatici;
- intercettare fraudolentemente ogni tipo di comunicazione proveniente dallôesterno o dallôinterno dellôAssociazione Forte di Bard, relativa ad un sistema informatico o telematico o intercorrente tra più sistemi, ovvero impedirla, interromperla, o infine rivelarne, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto;
- installare, fuori dai casi previsti dalla legge, apparecchiature atte ad intercettare, impedire o interrompere comunicazioni relative ad un sistema informatico o telematico ovvero intercorrenti tra più sistemi;
- distruggere, deteriorare, cancellare, alterare o sopprimere informazioni, dati o programmi informatici altrui; ovvero commettere fatti diretti a commettere tali condotte su informazioni, dati o programmi informatici utilizzati dallo Stato o da altro ente pubblico o ad essi pertinenti, o comunque di pubblica utilità; ovvero ancora distruggendo, deteriorando, cancellando, alterando o sopprimendo informazioni, dati o programmi informatici altrui, ovvero attraverso lôintroduzione o la trasmissione di dati, informazioni o programmi, distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici altrui o ostacolarne gravemente il funzionamento; queste ultime condotte sono anche vietate allorché siano dirette a distruggere, danneggiare, rendere, in tutto o in parte, inservibili sistemi informatici o telematici di pubblica utilità o ad ostacolarne gravemente il funzionamento.

I divieti sopramenzionati devono considerarsi operanti anche nelle ipotesi di svolgimento di attività da parte dei dipendenti, attraverso lôutilizzo di postazioni o di strumenti informatici collocati al di fuori delle sedi sociali, altresì nei casi in cui le attività vietate possano risolversi in un apparente vantaggio per lôAssociazione Forte di Bard.

IV) PROCEDURE SPECIFICHE.

Al fine di scongiurare la commissione dei reati sopra richiamati, lôAssociazione Forte di Bard adotta le seguenti misure precauzionali.

Strumenti e tecnologie

Le misure che seguono:

- assicurano unôadeguata protezione dei sistemi informativi aziendali;
- garantiscono la tracciabilità degli accessi e lôindividuazione, nel caso di episodi violativi delle prescrizioni date, di eventuali responsabilità.

In questa ottica:

- lôaccesso ai sistemi viene realizzato tramite postazioni di lavoro (PC) aziendali, fornite dallôAssociazione Forte di Bard;
- lôAssociazione, per il tramite del proprio Amministratore di Sistema, ha predisposto un inventario recante lôindividuazione dei singoli dispositivi elettronici consegnati a ciascun dipendente;
- sono richieste allôutilizzatore le credenziali nominative (username e password) per mezzo delle quali il sistema è in grado di riconoscerne e validarne lôidentità;
- le password hanno un periodo di validità temporale di sei mesi ed un livello di accesso ai sistemi che può essere limitato o ampliato in funzione della mansione assegnata alla risorsa;
- sui sistemi informatici vengono periodicamente effettuati aggiornamenti di software, volti a migliorare i livelli di sicurezza, con lo scopo di aumentare le contromisure a protezione dei sistemi aziendali;
- trova piena applicazione il Documento Programmatico della Sicurezza, che, seppure ad altre finalità, contiene misure a presidio della integrità e sicurezza dei dati;
- lôAssociazione Forte di Bard garantisce la sicurezza degli impianti rispetto ad accessi abusivi di terzi, sia fisici che informatici, assicurando un continuo monitoraggio sugli edifici e sulla rete;

Gestione dei sistemi informatici

Al fine di scongiurare la commissione di abusi connessi allôutilizzo dei sistemi informatici, è necessario che lôAssociazione Forte di Bard detti una serie di norme di condotta, che individuino tra i dati che devono essere salvaguardati, anche quelli aventi natura informatica (sistemi informativi, sistemi informatici, trasmissione di dati, nastri, dischetti), che necessitano una tutela nel senso della riservatezza, dellôintegrità, della disponibilità dellôinformazione e della tracciabilità delle operazioni effettuate.

LôAssociazione Forte di Bard deve diramare quanto prima specifiche norme per lôutilizzo della postazione di lavoro e dei sistemi informatici aziendali, specificando le cautele che devono essere assunte e le modalità con cui connettersi alla rete internet.