CONVENZIONE INTERBANCARIA
PER I PROBLEMI DELL'AUTOMAZIONE
(CIPA)

GRUPPO DI LAVORO

IL RISCHIO INFORMATICO

NOVEMBRE 2004

In relazione alle indicazioni contenute nel Piano delle attività della CIPA, il gruppo di lavoro incaricato di analizzare la tematica del rischio informatico rassegna il proprio rapporto.

La Segreteria della Convenzione desidera ringraziare i componenti del gruppo di lavoro di seguito indicati per la collaborazione prestata e il contributo fornito nello svolgimento delle attività del gruppo:

Giuseppina	MOLTENI	Banca d'Italia (Coordinatore) *
Sabina	DI GIULIOMARIA	Banca d'Italia
Enrico	EBERSPACHER	ABI
Anthony Cecil	WRIGHT	Banca Nazionale del Lavoro
Gian Paolo	VELLA	S. Paolo-IMI
Gianpaolo	BORGHI	Credito Emiliano
Stefania	PATAVIA	Banca 121
Antonio	CARICATO	Banca Eurosistemi
Mario	SESTITO	ICCREA
Pier Luigi	BARADELLO	SIA
Alessandra	CARAZZINA	SSB
Arturo	SALVATICI	SECETI – ACTALIS

IL SEGRETARIO
(A. M. Contessa)

* Cessata dal servizio a novembre 2003

INDICE

Sintesi

Il documento del gruppo di lavoro CIPA "Il rischio informatico" si compone di otto capitoli. Dopo una descrizione degli obiettivi della funzione aziendale preposta alla sicurezza informatica e il richiamo di alcuni principi generali di riferimento per le politiche aziendali in tema di sicurezza, sono indicati i principali standard internazionali esistenti in materia. Lo studio analizza poi il processo di gestione del rischio informatico, gli aspetti organizzativi della sicurezza informatica, i profili di sicurezza nella gestione delle risorse umane, informative e tecnologiche e quelli connessi con lo sviluppo delle applicazioni e la gestione dei sistemi e delle reti. Gli ultimi capitoli sono dedicati agli aspetti di sicurezza nell'utilizzo di Internet, della posta elettronica e degli strumenti di mobile computing, all'analisi di particolari modalità di attacco ai sistemi, alla gestione degli incidenti di sicurezza e ad alcune considerazioni sui costi della sicurezza informatica. Negli allegati sono contenute classificazioni, indicazioni pratiche e riferimenti normativi, che possono risultare utili ai fini della concreta impostazione di una policy di sicurezza.

Il **primo capitolo** si apre con alcune considerazioni sull'evoluzione dell'approccio delle aziende alle problematiche della sicurezza informatica, sempre più orientata alla promozione della continuità e della qualità dei servizi resi all'utenza che alla mera protezione dei sistemi informativi aziendali. L'attivazione del circolo virtuoso "più sicurezza - più qualità dell'offerta - maggiore fiducia della clientela" assume importanza strategica nell'attività bancaria che sul trattamento delle informazioni e sulla costruzione di un rapporto di fiducia con i clienti fonda la propria operatività; la massiccia introduzione di tecnologie nell'interazione banca-cliente, poi, fa sì che la garanzia di un adeguato livello di sicurezza informatica diventi una componente essenziale dell'offerta. L'interesse delle banche per il tema della sicurezza informatica si accentua inoltre in vista dell'entrata in vigore del nuovo accordo di Basilea sul capitale ("Basilea II") che introduce nel calcolo dei requisiti patrimoniali minimi l'esposizione al rischio operativo, di cui il rischio informatico è una componente di rilievo. Sono infine richiamati alcuni principi fondamentali enunciati dalla Banca Centrale Europea che costituiscono per le banche un'importante base di partenza per l'impostazione di un'efficace politica di sicurezza, nonché i processi chiave che, alla luce di detti principi, caratterizzano la funzione di gestione della sicurezza informatica.

Nel **secondo capitolo** sono indicati gli standard internazionali che possono essere presi a riferimento nell'attività di definizione delle *policy* di sicurezza e nell'analisi e gestione del rischio informatico.

Nel **terzo capitolo** vengono poi descritte le varie fasi in cui si articola il processo di gestione del rischio informatico, attraverso il quale un'azienda individua le vulnerabilità del proprio sistema informatico, identifica le minacce e la loro probabilità di accadimento, stima i possibili danni e definisce le necessarie contromisure.

Nel **quarto capitolo** sono trattati gli aspetti organizzativi della sicurezza informatica. La precisa individuazione delle attività critiche e dei ruoli aziendali coinvolti nella gestione della sicurezza è fondamentale ai fini della prevenzione di comportamenti scorretti o criminosi, ma anche ai fini del ripristino della normale operatività, a seguito del verificarsi di un evento dannoso, nel minor tempo e al minor costo possibili.

L'adozione di efficaci misure organizzative può consentire, a fronte della rapida evoluzione tecnologica, di sopperire ai possibili ritardi nell'adozione di contromisure tecniche adeguate agli attacchi perpetrati. È necessario innanzitutto che siano chiaramente definite *policy* di sicurezza

coerenti con gli indirizzi dei vertici aziendali, al rispetto delle quali occorre sensibilizzare tutti gli utenti, sia interni sia esterni, dei sistemi informatici. Altre fondamentali attività da svolgere sono quelle di progettazione, implementazione e gestione delle singole misure di sicurezza e quelle di verifica e controllo dell'osservanza delle misure adottate. Le varie funzioni inerenti alla sicurezza vanno poi univocamente assegnate alla responsabilità dei diversi ruoli coinvolti nella gestione del sistema informatico aziendale.

Nel **quinto capitolo** ci si sofferma sugli interventi che vanno posti in essere nella gestione delle risorse umane, informative e tecnologiche, per realizzare un'efficace politica di sicurezza informatica. La considerazione che qualsiasi presidio tecnico-organizzativo di sicurezza può essere messo in crisi da comportamenti dannosi, più o meno intenzionali, del personale, induce a porre particolare attenzione all'effettuazione di specifici interventi per migliorare la "affidabilità" della compagine dei dipendenti. Il rapporto fa pertanto una ricognizione delle principali attività - dalla formazione alla definizione delle mansioni, dalla previsione di ridondanze nei ruoli specialistici alla predisposizione di un adeguato sistema sanzionatorio - che consentono di conseguire questo obiettivo.

Una corretta gestione del rischio richiede che siano adottate politiche di controllo (logico e fisico) dell'accesso alle risorse informative e tecnologiche coerenti con l'importanza dei beni da proteggere. A tal fine risulta indispensabile l'inventario e la classificazione delle risorse stesse. Il rapporto descrive quindi i modelli e gli strumenti maggiormente utilizzati per regolamentare l'accesso ai dati e alle applicazioni.

In connessione con gli aspetti di sicurezza relativi alla gestione delle risorse, viene trattato il tema della continuità operativa, facendo riferimento alla necessità, recentemente evidenziata anche dalla normativa di vigilanza bancaria, di dotarsi di un *business continuity plan*, al fine di assicurare la prosecuzione dei processi di business vitali al verificarsi di eventi che determinano l'interruzione dell'operatività ordinaria.

Nel **sesto capitolo** sono trattati gli aspetti di sicurezza informatica da tenere in considerazione nelle attività di sviluppo, manutenzione e gestione dei sistemi e delle reti. In particolare, vengono richiamate le vulnerabilità che si possono determinare a seguito di errori o omissioni nelle attività di sviluppo, di manutenzione e di gestione, suscettibili di generare minacce alla riservatezza, all'integrità e alla disponibilità del patrimonio informativo aziendale. Il rapporto contiene un'accurata ricognizione delle contromisure da adottare nella fase di acquisizione e/o sviluppo dei programmi, nonché delle attività di monitoraggio e di controllo degli accessi, finalizzate alla sicurezza, da prevedere nella gestione dei sistemi operativi e delle reti.

Il **settimo capitolo** è dedicato all'analisi dei rischi - e delle relative contromisure – derivanti dall'utilizzo di tecnologie innovative quali quelle relative al mondo Internet, alla posta elettronica, al *mobile computing*.

Tra i principali rischi connessi con l'accesso al web figurano quelli derivanti dall'eventuale installazione di codici dannosi sui posti di lavoro, che potrebbero poi propagarsi tramite la rete aziendale. È possibile fronteggiare questa minaccia con l'adozione di diverse contromisure, che il rapporto elenca, avendo presente tuttavia che le modalità ottimali per rendere sicuro l'accesso alla rete Internet variano in relazione alle caratteristiche del sistema informativo e del business delle singole aziende. Sono inoltre presi in considerazione gli specifici rischi correlati allo sviluppo delle applicazioni *web-based*.

La mancata adozione di adeguate misure di sicurezza nella posta elettronica può determinare, oltre che rischi di natura tecnologica, conseguenze di tipo legale e di immagine, ad esempio nel caso di diffusione di virus o di divulgazione di comunicazioni riservate. È necessario pertanto adottare idonee contromisure tecnologiche e prevedere una specifica *policy* aziendale che disciplini il corretto utilizzo dello strumento da parte degli utenti.

Di diversa natura sono poi i rischi connessi con l'utilizzo da parte dei dipendenti della "navigazione" su Internet e della posta elettronica non strettamente correlato all'attività aziendale, che può generare costi e inefficienze anche significativi. In tal caso, nella predisposizione delle opportune contromisure, tecnologiche e organizzative, va tenuta presente l'esigenza di operare un corretto bilanciamento tra gli interessi aziendali e i diritti dei lavoratori, in specie per quanto attiene alla tutela della privacy.

La sempre più ampia diffusione dei dispositivi di *mobile computing* quali strumenti di lavoro e di accesso alle risorse informatiche aziendali pone all'attenzione della sicurezza informatica gli specifici rischi connessi con il loro utilizzo, richiedendo l'adozione di particolari misure per la protezione dei dati memorizzati e per la disciplina delle modalità di collegamento con la rete aziendale. Vengono quindi indicate alcune delle tecniche di protezione che le aziende che utilizzano tali dispositivi possono adottare per minimizzare il rischio di danni al proprio sistema informativo.

Sono infine illustrate talune delle più insidiose modalità di attacco informatico che si vanno diffondendo di pari passo con l'evoluzione delle tecnologie innovative*: social engineering*, *malicious code*, *spoofing*, *denial of service*, ecc.; per ognuna di tali tipologie di attacco vengono indicate le possibili contromisure.

La conoscenza aggiornata delle modalità di attacco – e delle maggiori vulnerabilità delle risorse tecnologiche, organizzative e umane - è oggi indispensabile per affrontare il problema della prevenzione del rischio informatico in modo globale. In particolare, oltre alla predisposizione di un efficiente apparato di prevenzione, deve essere previsto un adeguato strumentario per la reazione agli incidenti di sicurezza. Viene quindi descritta la metodologia da seguire per l'approntamento di un piano di azione, opportunamente formalizzato e periodicamente verificato e aggiornato, che consenta di intervenire tempestivamente ed efficacemente al verificarsi di un incidente di sicurezza; viene, tra l'altro, sottolineata l'importanza della costituzione di un adeguato *team* di intervento, composto di elementi in possesso di conoscenze specialistiche e capaci di operare efficacemente anche in situazioni di emergenza.

Nell'**ottavo capitolo** vengono infine svolte alcune considerazioni sui costi della sicurezza e viene proposta una struttura di piano dei conti suddivisa in due macro-sezioni: una relativa ai costi direttamente imputabili alla struttura che gestisce la sicurezza, l'altra relativa ai costi sostenuti da altri comparti del settore ICT ma comunque inerenti alla protezione del sistema informativo aziendale. La scomposizione dei costi in tali categorie costituisce la base per l'attivazione di forme di controllo di gestione della sicurezza informatica, quali il monitoraggio dell'andamento della spesa per la sicurezza nelle sue diverse componenti, il controllo degli scostamenti rispetto al budget, la rappresentazione ai vertici aziendali dei costi complessivamente sostenuti rispetto al livello di esposizione dell'azienda al rischio informatico.

1 Il rischio informatico. Principi generali.

Con la rapida evoluzione delle tecnologie dell'informazione e della comunicazione, i sistemi informatici hanno assunto importanza centrale nell'assetto organizzativo e funzionale delle imprese e delle istituzioni. La diffusione delle tecnologie fondate sul paradigma Internet, poi, ha favorito il ridisegno dei confini organizzativi dell'impresa, sempre più aperta e connessa con altri soggetti e sistemi informatici.

In questo contesto, l'adozione di efficaci politiche di sicurezza informatica ha rilevanza cruciale, in quanto da essa possono dipendere le stesse sorti dell'impresa/istituzione.

Si tratta di un compito non facile, in ragione soprattutto dei continui cambiamenti delle tecnologie e dell'elevato impegno operativo, organizzativo e finanziario richiesto a tutti i livelli della struttura aziendale.

Ciò è vero soprattutto per le banche, per le quali l'offerta di servizi sicuri e affidabili ha da sempre costituito un fattore di vantaggio competitivo. Oggi, con la diffusione dei canali distributivi ad elevato contenuto tecnologico, eventuali disservizi conseguenti a una non adeguata politica di sicurezza possono ancor più tradursi in danni alla reputazione e all'immagine dell'azienda.

In questa consapevolezza, il gruppo di lavoro CIPA sul rischio informatico si è posto, con il presente rapporto, l'obiettivo di contribuire alla sensibilizzazione sulle problematiche della sicurezza informatica attraverso una panoramica delle minacce, vecchie e nuove, collegate all'evoluzione tecnologica e delle possibili contromisure, favorendo indicazioni di carattere operativo e organizzativo per una corretta implementazione delle *policy* di sicurezza da parte delle banche. Sul piano del metodo di lavoro, il gruppo si è basato sulla concreta esperienza delle banche rappresentate, corroborata dall'analisi delle norme e degli standard comportamentali più diffusi a livello internazionale.

La Rilevazione dello stato dell'automazione del sistema creditizio riferita al 2002 – condotta dalla CIPA in collaborazione con l'ABI – mette in evidenza che per le banche la componente di spesa per la sicurezza all'interno del budget informatico rappresenta mediamente il 3,1% del totale; l'analisi del rischio informatico costituisce ormai un dato di fatto presso la gran parte delle banche (96,6%), sebbene essa sia prevalentemente effettuata in maniera non strutturata, senza fare riferimento a metodologie formalizzate; ampiamente diffusi sono l'EDP auditing (89,3%) e l'analisi di vulnerabilità (87,2%), per lo più effettuata tramite società di servizi esterne alle banche.

Quanto agli aspetti qualitativi, le osservazioni condotte mostrano che è in atto, anche nel sistema bancario italiano, un mutamento di concezione della sicurezza, che diventa sempre più attiva e, tramite servizi avanzati di monitoraggio, tende a "prevenire" per evitare che "attacchi" di varia natura possano arrecare danni all'immagine dell'azienda e comprometterne il business. Nella sua accezione più ampia, pertanto, la sicurezza si presenta oggi caratterizzata da una triplice dimensione:

– una sicurezza che promuove la protezione dei sistemi e delle informazioni dai potenziali attacchi. Questa sicurezza deve essere attuata secondo due direttrici: quella organizzativa e quella tecnologica. Con riferimento alla prima, va ricordato che l'elemento umano rappresenta da sempre l'anello più debole della catena della sicurezza; la creazione di una "cultura aziendale"

attenta agli aspetti di sicurezza è presupposto necessario per la protezione del patrimonio informativo aziendale e va perseguita anche mediante un'adeguata sensibilizzazione di tutto il personale. Con riferimento alla direttrice tecnologica, la sicurezza come difesa viene perseguita attraverso gli strumenti atti a prevenire e a reagire a fronte delle diverse tipologie di attaccanti (dipendenti, collaboratori esterni, *hacker*, terroristi, ecc.) e di attacchi (*malicious code*, *spamming*, *sniffing*, *spoofing*, *cracking*, *defacement*, ecc.);

- una sicurezza che mira a garantire – in ogni situazione – la massima continuità di servizio. Tale obiettivo rientra in una visione allargata della sicurezza informatica che tiene in considerazione non solo gli strumenti di *disaster recovery* ma anche tutti gli altri presidi tecnici e organizzativi che confluiscono nel *business continuity plan*[1];

- una sicurezza che promuove la qualità del servizio, venendo incontro alla domanda di "fiducia" dell'utente. È il caso, ad esempio, dei servizi bancari e finanziari offerti via rete, il cui successo dipende anche dal livello di sicurezza offerto nello svolgimento dell'operazione.

Va infine evidenziato come la gestione della sicurezza informatica, e in particolare l'analisi dei rischi informatici cui le banche sono esposte, assumerà nuovo rilievo con l'entrata in vigore del nuovo accordo di Basilea sul capitale ("Basilea II"): nel calcolo dei requisiti patrimoniali minimi delle banche, infatti, si terrà conto dell'esposizione al rischio operativo, ovvero del rischio di perdite derivanti, in particolare, da anomalie dei processi interni, da carenze nel grado di conoscenza e professionalità delle risorse umane, da sistemi informatici interni inadeguati, da sistemi di sicurezza insufficienti.

1.1 Definizioni e principi di riferimento

Secondo una definizione ormai consolidata, per sistema aziendale di sicurezza informatica si intende l'insieme delle misure tecniche e organizzative volte ad assicurare la protezione dell'integrità, della disponibilità, della confidenzialità dell'informazione automatizzata e delle risorse usate per acquisire, memorizzare, elaborare e comunicare tale informazione.

Gli obiettivi fondamentali della sicurezza informatica sono quindi:

Riservatezza garanzia che un determinato dato sia preservato da accessi impropri e sia utilizzato esclusivamente dai soggetti autorizzati. Le informazioni riservate devono essere protette sia nella fase di trasmissione sia nella fase di memorizzazione/conservazione, in modo tale che l'informazione sia accessibile esclusivamente a coloro i quali sono autorizzati a conoscerla.

[1] Dalla citata indagine CIPA emerge che un piano di *disaster recovery* formalizzato è presente nel 68% delle banche segnalanti ed è in via di formalizzazione nel 18%. Il livello di sensibilità nei confronti della continuità di servizio è evidenziato dalla quota di banche che dispone già di un *business continuity plan* (43%), che contempla anche le attività organizzative volte ad assicurare la corretta prosecuzione del business aziendale.

Integrità	garanzia che ogni dato aziendale sia realmente quello originariamente immesso nel sistema informatico e sia stato modificato esclusivamente in modo legittimo. Si deve garantire che le informazioni vengano trattate in modo tale che non possano essere manomesse o modificate da soggetti non autorizzati.
Disponibilità	garanzia di reperibilità di dati aziendali in funzione delle esigenze di continuità dei processi e nel rispetto delle norme che ne impongono la conservazione storica.

La gestione e il miglioramento della sicurezza informatica fanno parte di un processo continuo che deve tenere conto di molteplici fattori di resistenza, interni ed esterni all'azienda, e che deve ricercare costantemente il miglior compromesso tra sicurezza e fruibilità del sistema.

Nella concreta definizione di una politica di sicurezza può quindi essere utile tenere in considerazione alcuni principi generali la cui applicazione può favorire il conseguimento del giusto punto di equilibrio tra le esigenze in gioco. Un buon riferimento è costituito dalle linee guida per la sicurezza dei sistemi informativi elaborate dall'OCSE e dalla BCE[2], che inquadrano la gestione della sicurezza nell'ambito delle altre variabili dell'organizzazione aziendale. Si fornisce di seguito una sintesi dei principi richiamati dalla BCE.

Le misure di sicurezza devono essere conformi ai requisiti di business aziendali, nonché alle normative vigenti.

Lo scopo della sicurezza informatica è quello di proteggere le risorse informatiche aziendali attraverso la selezione e l'applicazione di appropriate misure precauzionali, che non devono essere percepite come vincoli e costrizioni alla missione dell'organizzazione, ma come elementi che contribuiscono al raggiungimento degli obiettivi aziendali fissati dal management.

La sicurezza riguarda tutti e la consapevolezza individuale gioca un ruolo fondamentale nel conseguimento degli obiettivi di sicurezza prefissati.

Al fine di assicurare che i compiti correlati con la sicurezza siano ben assegnati e correttamente svolti, è necessario che ogni persona coinvolta comprenda il proprio ruolo e le proprie responsabilità: l'alta direzione deve cioè assegnare in modo formale le responsabilità relative alla sicurezza a strutture e persone ben individuate all'interno dell'organizzazione. Inoltre la formazione e la sensibilizzazione del personale devono essere curate in modo particolare con l'obiettivo di ottenere la piena consapevolezza della sicurezza da parte di tutti.

[2] OCSE, *Guidelines for the Security of Information Systems;* BCE, Information Technology Committee, *ESCB Information Systems Security Policy*.

Le misure di sicurezza devono essere efficaci e comprensibili e bilanciate rispetto ai relativi costi.

Al fine di conseguire un'efficace riduzione dei rischi identificati secondo scelte che rispondano anche a principi di economicità, i costi decisi devono essere proporzionati ai rischi valutati. È comunque importante tener presente che i benefici ottenibili con l'adozione delle misure di sicurezza non sono sempre facilmente percepibili in quanto generano risultati non immediatamente quantificabili. Inoltre le misure di sicurezza individuate dovrebbero essere semplici da comprendere al fine di favorirne l'applicazione.

La sicurezza richiede una combinazione di misure tecniche e organizzative.

Il conseguimento di un livello di sicurezza adeguato ai requisiti aziendali è quasi sempre vincolato all'adozione di misure organizzative come sostegno e completamento di quelle tecniche, soprattutto nell'attuale epoca caratterizzata da una evoluzione tecnologica rapidissima.

È necessario che la sicurezza sia pianificata e integrata nelle attività di sviluppo dalle fasi iniziali.

L'applicazione di tale principio assicura che i fattori di rischio vengano adeguatamente considerati nei tempi dovuti e previene il rischio che determinate misure di sicurezza debbano essere applicate in momenti successivi e con costi più sostenuti.

Le autorizzazioni devono essere basate sul principio del "need-to-know" correlato al business aziendale.

È opportuno assicurare che l'accesso alle risorse del sistema informativo sia limitato agli utenti che ne hanno ottenuto autorizzazione sulla base delle specifiche esigenze connesse con i compiti loro assegnati; inoltre le attività compiute devono essere regolarmente registrate.

La sicurezza deve essere continuamente monitorata.

Al fine di garantire che le misure di sicurezza adottate si mantengano adeguate ed efficaci, è necessario condurre con regolarità una valutazione periodica della loro conformità alle *policy* aziendali e alle normative esterne, nonché provvedere, ove necessario, a un aggiornamento delle *policy* stesse.

1.2 I processi "chiave" della sicurezza informatica

Nelle linee guida della BCE sopracitate sono messi in evidenza i cinque processi fondamentali che caratterizzano la gestione della sicurezza informatica, di seguito sinteticamente descritti:

- la gestione del rischio informatico, processo basilare, che consiste nell'identificazione, nel controllo, nell'eliminazione o nella minimizzazione dei rischi riguardanti il conseguimento, secondo criteri di economicità, degli obiettivi aziendali di business. Tale processo include una

gestione pianificata e controllata delle risorse al fine di assicurare il contenimento dei rischi entro limiti accettabili;

- il controllo dell'attività di *change management*, ovvero il controllo di qualunque modifica apportata ai sistemi e alle infrastrutture; tale controllo deve essere stringente, al fine di ridurre al minimo i problemi e garantire che la sicurezza non venga compromessa;

- il controllo delle fasi di test e accettazione in produzione dei sistemi; le procedure di controllo devono essere particolarmente accurate al fine di garantire che vengano realizzate, e funzionino correttamente, tutte le funzionalità previste, incluse quelle concernenti le misure di sicurezza. Deve quindi essere formalizzata ed eseguita una procedura formale di accettazione in produzione. È responsabilità dell'utente proprietario assicurare che la procedura applicativa soddisfi tutti i criteri dell'accettazione in ambiente di produzione, ivi inclusa l'accettazione dei rischi residui, e che i livelli di responsabilità del sistema siano ben documentati e consegnati alla struttura di gestione competente;

- la gestione degli incidenti di sicurezza; devono essere formalizzate procedure di controllo che prevedano la registrazione di ogni incidente e il reporting all'utente proprietario del sistema nell'ambito del quale si è verificato l'evento. L'esperienza ricavata da ogni accadimento dovrebbe essere acquisita nel processo di gestione del rischio come elemento utile ai fini di un eventuale aggiornamento del processo stesso;

- la definizione di piani riguardanti misure a garanzia della *business continuity*; tali piani, da sottoporre a costante aggiornamento, devono includere misure di sicurezza addizionali rispetto a quelle ritenute sufficienti con riferimento ai rischi informatici, in modo da consentire all'azienda di fronteggiare eventuali accadimenti disastrosi; in tale ambito dovrebbe essere assicurata la disponibilità di ambienti di recovery e l'attivazione di procedure di ripristino dell'operatività corrente. Tali misure devono essere sottoposte a test periodici utilizzando scenari simulati.

* * *

Il rapporto CIPA, tenendo presenti questi principi e prescrizioni di carattere generale, intende fornire una panoramica il più possibile esaustiva dei vari aspetti che maggiormente rilevano nella gestione operativa del rischio informatico.

2 Riferimenti metodologici

A livello internazionale sono stati formalizzati standard di riferimento che possono guidare le aziende nell'impostazione delle *policy* di sicurezza e nell'analisi/gestione del rischio informatico; tra i più diffusi si annoverano i seguenti:

BS7799/ISO17799I. Tali standard sono rivolti ai responsabili della progettazione e della gestione della sicurezza IT in azienda; forniscono raccomandazioni e linee guida che possono essere utilizzate come riferimento nella stesura delle *policy* di sicurezza aziendali.

Gli standard sono frutto di un lavoro congiunto tra il *Department of Trade and Industry* della Gran Bretagna e alcune importanti compagnie e industrie britanniche. Essi derivano dalle regole emanate dal British Standard per la sicurezza dei sistemi IT nel Regno Unito attraverso due documenti:

- "BS7799 Parte Uno" - noto anche come "*Standard code of practice*" - che fornisce una guida di riferimento su come rendere sicuro il sistema informativo. Nel corso del 2000, il "BS7799 Parte Uno" è stato "promosso" a standard ISO diventando ISO 17799 con titolo "*Code of practice for Information Security Management*".

- "BS7799 Parte Due" - noto anche come "*Specification for information security management system*" - che fornisce una guida base per il processo di valutazione di un ISMS *(Information Security Management System).*

La costruzione dell'ISMS è un processo articolato in sei fasi:

1. Definizione di una *policy* della sicurezza (*Information Policy*), al fine di far prendere coscienza all'azienda dei propri *asset* e del loro valore.
2. Individuazione dell'ambito di applicazione (*Scope*) dell'ISMS - intera azienda o un particolare sistema/ambiente - e del grado di sicurezza che si intende raggiungere.
3. Valutazione del rischio (*Risk Assessment*) in caso di perdita delle informazioni che devono essere protette, in relazione al loro valore all'interno dell'azienda. Il *risk assessment* permette di individuare le minacce agli *asset*, le vulnerabilità e l'impatto sull'organizzazione.
4. Gestione del rischio (*Risk Management*) attraverso interventi di tipo tecnologico, organizzativo e logistico, in funzione del grado di sicurezza richiesto e dell'organizzazione del sistema di sicurezza.
5. Definizione di controlli e contromisure (*Choose your safeguards*) per proteggere gli *asset* aziendali.
6. Formalizzazione della dichiarazione di applicabilità (*Statement of Applicability*), cioè della scelta di tutti i controlli di sicurezza adottati al fine di garantire la corretta gestione dei rischi individuati, nonché delle motivazioni che hanno portato all'eventuale esclusione di alcuni controlli previsti dallo standard BS.

Common Criteria ICC (Common Criteria, abbreviazione di *Common Criteria for Information Technology Security Evaluation*). Rappresentano l'armonizzazione di differenti standard di sicurezza, nazionali e internazionali, dei sistemi informatici. I Common Criteria sono organizzati in tre parti:

parte 1 (Introduzione e modello generale): comprende una definizione dei concetti e dei principi della valutazione di sicurezza di un sistema IT e un modello generale di valutazione;

parte 2 (Requisiti funzionali di sicurezza): individua i componenti che il sistema di sicurezza deve possedere;

parte 3 (Requisiti di *assurance* di sicurezza): definisce i criteri di valutazione per i *Protection Profile* e per i *Security Target* e presenta i livelli di valutazione di *assurance* che definiscono la scala di classificazione predefinita dai Common Criteria.

ITSEC (*Information Technology Evaluation Criteria*). Rispondono all'esigenza di creare uno standard di valutazione efficace e internazionalmente accettato relativamente alla sicurezza dei sistemi informatici. Il processo di accreditamento ITSEC prevede tre fasi:

1. **valutazione** del livello di sicurezza del sistema o del prodotto informatico;

2. **certificazione** del livello di sicurezza del sistema o del prodotto informatico;

3. **accreditamento** quale risultato dei processi precedenti. Tale fase si esplica nell'assegnazione di un certificato, nel quale è stabilito il livello di *assurance* del sistema o prodotto.

CObIT (*Control Objectives for Information and related Technologies*). È un metodo di verifica dei sistemi informativi sviluppato per favorire la comprensione dei controlli esistenti da parte della Direzione, dell'auditor e degli utilizzatori. Consente l'individuazione e la classificazione degli *asset* che devono essere controllati attraverso l'identificazione delle attività, dei processi e dei domini.

CRAMM (*Central Computer and Telecommunication Agency Risk Analysis and Management*). È una delle metodologie più note e utilizzate per la gestione del rischio informatico. Il metodo è corredato da uno strumento software per lo svolgimento delle varie attività e per la produzione di report finali che includono suggerimenti per il top management riguardo le contromisure da adottare. CRAMM è concettualmente compatibile con BS7799 e con ITSEC con riferimento ai livelli di *assurance* e alle funzionalità di sicurezza.

OCTAVE (*Operationally Critical Threat, Asset and Vulnerability Evaluation*). È una delle metodologie emergenti specificamente dedicate al rischio informatico. OCTAVE è concettualmente compatibile con BS7799 e con ITSEC con riferimento ai livelli di *assurance* e alle funzionalità di sicurezza.

3 Gestione del rischio informatico

La gestione del rischio informatico si svolge attraverso un articolato processo che mira a identificare le vulnerabilità del sistema informatico, le possibili minacce e la relativa probabilità di accadimento nonché a stimare i potenziali danni.

In particolare, possono essere individuate le seguenti fasi:

1. identificazione e classificazione delle risorse e individuazione delle relative vulnerabilità - ovvero le carenze di protezione relativamente a una determinata minaccia - con riferimento alle seguenti componenti:

- infrastrutture (incluse quelle tecnologiche quali le reti e gli impianti)
- hardware
- software
- documentazione
- dati/informazioni
- risorse umane;

2. individuazione delle minacce, interne ed esterne, cui possono essere esposte le risorse, raggruppabili nelle seguenti tipologie:

- errori e malfunzionamenti
- frodi e furti
- software dannoso
- danneggiamenti fisici
- sovraccarico del sistema
- mancato rispetto della legislazione vigente.

In Allegato 1 è riportata una tabella di dettaglio delle classi di minacce identificate.

3. individuazione dei danni che possono derivare dal concretizzarsi delle minacce, tenendo conto della loro probabilità di accadimento. In funzione della loro natura, si può distinguere tra danni economici e danni di immagine (cfr. Allegato 2 per una descrizione di dettaglio). In relazione al collegamento causale con l'evento dannoso, poi, si distingue tra danni diretti (es. distruzione, perdita o danneggiamento dei dati e/o del software, ferimento delle persone) e danni indiretti, conseguenti al blocco totale o parziale di un processo aziendale (es. perdita della produzione, risarcimenti a terzi, penali); in taluni casi, gli effetti prodotti dall'evento dannoso possono permanere anche dopo il ripristino dello *status quo ante* (è il caso, ad esempio, dei danni all'immagine aziendale).

4. identificazione delle possibili contromisure; le contromisure sono le funzioni di sicurezza che devono essere adottate per contrastare le minacce e gli attacchi portati alle risorse informatiche e possono essere distinte in relazione all'obiettivo perseguito, che può essere di :

- prevenzione: impedire che l’attacco venga perpetrato;
- rilevazione: rilevare, a fronte di un attacco, l’evento e/o le sue conseguenze dannose;
- ripristino: minimizzare i danni attraverso il ripristino, quanto più immediato possibile, dei sistemi.

Negli Allegati 3 e 4 sono illustrate schematicamente alcune delle possibili contromisure, rispettivamente di natura tecnologica/organizzativa e di natura comportamentale, che l’azienda può adottare; approfondimenti specifici sul tema delle contromisure sono contenuti nei successivi capitoli, in relazione alle varie tipologie di rischio informatico di volta in volta esaminate.

5. effettuazione di un'analisi costi/benefici degli investimenti per l’adozione delle contromisure;
6. definizione di un piano di azioni preventive e correttive da porre in essere e da rivedere periodicamente in relazione ai rischi che si intendono contrastare;
7. documentazione e accettazione del rischio residuo.

4 Gli aspetti organizzativi della sicurezza informatica

Nel definire un "sistema" di sicurezza informatica particolare attenzione deve essere riservata agli aspetti organizzativi, in quanto la disponibilità di una struttura accuratamente disegnata, in cui ruoli, funzioni e mansioni siano ben assegnati, riconosciuti e svolti, offre a un'azienda lo strumento fondamentale per contrastare la sempre più rapida evoluzione tecnologica delle minacce dirette al sistema informativo.

In particolare, la strategia di intervento sulle variabili organizzative deve mirare a: impedire o ridurre ragionevolmente il verificarsi di comportamenti scorretti, fraudolenti o criminali (prevenzione); ricreare, nel minor tempo e al minor costo possibili, le condizioni di normale svolgimento delle attività aziendali, allorquando una minaccia abbia già superato le misure preventive di sicurezza fisica, logica e organizzativa (ripristino).

A tal fine, oltre ai già citati obiettivi di integrità, riservatezza e disponibilità dei dati, assumono particolare rilievo quelli di controllabilità delle risorse e di verificabilità del loro utilizzo (ovvero la possibilità di ricostruire, ove necessario, qualsiasi tipo di evento verificatosi). Una strategia globale richiede quindi un'articolata serie di interventi procedurali e organizzativi:

- definizione del quadro normativo riferito a tutte le strutture aziendali, con una chiara attribuzione di compiti e responsabilità e indicazione dei corretti comportamenti individuali;
- costituzione di un polo di competenza in azienda che sia in grado di fornire il necessario supporto consulenziale e specialistico per affrontare le problematiche del trattamento dei dati personali e della tutela legale del software;
- puntuale pianificazione delle attività di sicurezza informatica;
- progettazione, realizzazione/test e gestione di un sistema di protezione preventivo;
- definizione di un sistema di emergenza, ovvero predisposizione di tutte le procedure tecnico/organizzative per poter affrontare stati di emergenza e garantire la *business continuity* attraverso meccanismi di superamento di situazioni anomale;
- applicazione di misure specifiche per garantire la controllabilità e la verificabilità dei processi, anche sotto il profilo della riconducibilità in capo a singoli soggetti delle azioni compiute[3].

4.1 I principi organizzativi della sicurezza

Alla luce delle più diffuse *best practices* in materia di gestione della sicurezza, per realizzare un'efficace soluzione organizzativa devono essere rispettati i seguenti principi:

---

[3] Ad esempio possono essere attuate misure quali:

- la riconciliazione dei flussi elaborativi;
- la registrazione di tracce di audit di sistema e/o applicative;
- la registrazione di dati attinenti a eventi particolarmente significativi dell'iter elaborativo;
- la predisposizione di strumenti per consentire il controllo, da parte dei responsabili, delle attività particolarmente critiche.

- precisa imputazione delle azioni svolte sui dati e sulle risorse (cfr. oltre);
- stretta correlazione tra accesso alle informazioni riservate ed effettive esigenze lavorative (*need to know*);
- adozione del principio di "autorizzazione minima" (o "espressa"): tutto di norma è vietato tranne ciò che è espressamente autorizzato;
- ridondanza delle risorse che devono avere alta disponibilità;
- contrapposizione degli interessi ovvero separazione dei ruoli di:
  - gestione di un processo e di controllo dello stesso;
  - progettazione ed esercizio;
  - acquisto di beni e risorse e relativa contabilizzazione;
- specializzazione o segregazione delle risorse con criticità alta sotto i profili della riservatezza, integrità o disponibilità;
- controllo “duale” (*four eyes*) ovvero controllo da parte di almeno due soggetti sullo svolgimento di azioni relative a risorse che richiedono elevati livelli di sicurezza.

4.2 Le funzioni della sicurezza informatica

L’organizzazione della sicurezza di un sistema informativo richiede lo svolgimento di una serie di attività a diversi livelli, che si possono ricondurre a tre specifiche funzioni:

- definizione delle *policy* in tema di sicurezza informatica;
- progettazione, realizzazione e gestione delle misure di sicurezza in attuazione delle *policy* di cui al punto precedente;
- verifica e controllo della corretta attuazione e dell’efficienza delle misure di sicurezza adottate (audit di sicurezza).

Funzione di definizione delle policy in tema di sicurezza informatica

È la funzione che all’interno dell’azienda definisce le *policy* di sicurezza, coerentemente con gli indirizzi espressi dai vertici aziendali e le normative vigenti, sia interne sia esterne, e ponendo attenzione, ai fini del contenimento dei costi, alla individuazione di misure coerenti con il “valore” del patrimonio informativo da proteggere.

Le principali attività che rientrano in tale funzione sono:

- definire i requisiti di sicurezza per la protezione del complesso di archivi, procedure e sistemi informatici, sulla base delle linee di indirizzo stabilite dai vertici aziendali;
- condurre l’analisi dei rischi informatici;
- partecipare alla definizione dell’architettura di sicurezza che soddisfi i requisiti di cui sopra;

- pianificare i test di sicurezza e analizzarne le risultanze;
- monitorare le vulnerabilità dei sistemi;
- aggiornare periodicamente le *policy* per adeguarle alle nuove minacce;
- emanare procedure interne inerenti alla sicurezza (regolamentazione degli accessi fisici e logici agli archivi e ai sistemi informativi, norme operative di utilizzo e gestione dei sistemi, gestione delle password, ecc.);
- simulare attacchi estemporanei e imprevedibili ai sistemi informativi (tali, comunque, da non creare danni ai sistemi stessi);
- garantire adeguato supporto alla formazione del personale in tema di sicurezza.

Funzione di progettazione, implementazione e gestione delle misure di sicurezza

È la funzione che progetta, realizza e gestisce le misure di sicurezza, mantenendole adeguate ai requisiti indicati dalla funzione di cui al punto precedente.

Le principali attività ricomprese in tale funzione sono:

- progettare il sistema di sicurezza;
- implementare il sistema di sicurezza progettato;
- manutenere il sistema di sicurezza per assicurarne costantemente l'efficienza e la disponibilità;
- eseguire i test di sicurezza pianificati;
- gestire gli "allarmi", analizzarli e fornire adeguato supporto per l'eliminazione delle cause;
- gestire il sistema di sicurezza, eventualmente in modo decentrato presso le strutture periferiche.

Funzione di verifica e controllo della corretta attuazione e dell'efficienza delle misure di sicurezza adottate (Audit di sicurezza)

È la funzione che controlla l'adozione delle misure di sicurezza, verificandone l'efficacia e la coerenza con le *policy* di sicurezza.

Le principali attività che connotano tale funzione sono:

- controllare la coerenza delle misure di sicurezza adottate con gli standard nazionali e/o internazionali e le normative vigenti in materia;
- eseguire audit periodici sull'applicazione delle misure di sicurezza realizzate;
- partecipare all'analisi in occasione di incidenti informatici.

Per le sue specifiche attività, è una funzione che richiede autonomia operativa e un elevato livello di conoscenze tecniche e giuridiche.

4.3 I ruoli aziendali della sicurezza informatica

La gestione della sicurezza informatica, come accennato, è un processo continuo che riguarda l'intera struttura organizzativa aziendale, presupponendo l'assegnazione di precise responsabilità a tutti i ruoli che, in vario modo, sono coinvolti nella gestione del patrimonio informatico aziendale, come previsto anche dai principali standard internazionali. Nell'attribuzione dei compiti e delle responsabilità particolare attenzione va posta ad evitare la sovrapposizione di ruoli e all'applicazione del principio del contraddittorio.

Il gruppo di lavoro, sulla base di una ricognizione degli schemi organizzativi più ricorrenti, ha individuato i ruoli "chiave" coinvolti nella gestione della sicurezza.

4.3.1 Responsabile della sicurezza

È il ruolo preposto alla definizione delle *policy* di sicurezza.

4.3.2 Utenti dell'applicazione informatica

- Utente proprietario

Per ogni applicazione informatica è la struttura responsabile delle informazioni trattate e dei relativi utilizzi, individuata sin dal momento in cui si decide di avviare lo sviluppo di una nuova applicazione. L'utente proprietario provvede alla classificazione delle informazioni delle quali è responsabile, nonché all'individuazione del relativo livello di protezione sulla base dei criteri di carattere generale stabiliti dal quadro normativo; autorizza, eventualmente avvalendosi di apposite strutture operative, l'accesso ai dati e alle applicazioni per le quali esercita il ruolo di utente proprietario e ne controlla il corretto utilizzo; per le risorse, le applicazioni e i dati di propria competenza, collabora con le strutture competenti nell'azione propositiva per quanto attiene alla valutazione dei rischi e all'utilizzo dei meccanismi di protezione.

- Utente gestore

È la struttura che cura l'applicazione dal punto di vista della funzionalità, dell'aggiornamento e della qualità dei dati sui quali ha competenza. Di norma l'utente gestore coincide con l'utente proprietario.

- Utente finale

È colui al quale è assegnata la facoltà di accedere a determinate risorse informatiche. In genere tale facoltà viene attribuita a livello individuale. L'utente finale è tenuto a mantenere livelli di presidio coerenti con quelli individuati dall'utente proprietario dei dati originari e a garantire la correttezza dei dati eventualmente immessi.

4.3.3 Responsabile della fornitura di risorse informatiche

È il ruolo preposto all'acquisizione e/o allo sviluppo/manutenzione delle risorse informatiche aziendali (hardware, software di base e applicativo, reti di telecomunicazione), nel rispetto delle metodologie e degli standard di sicurezza e di sviluppo adottati dall'azienda.

4.3.4 Gestore dei sistemi elaborativi

È il responsabile, per ogni sistema elaborativo, della disponibilità e dell'integrità degli apparati e degli interventi che si rendano necessari nel caso di malfunzionamento, nonché dell'integrità dei dati di sistema relativi alla gestione.

4.3.5 Amministratore delle misure di sicurezza informatica

È la struttura che amministra la sicurezza dei sistemi elaborativi in dotazione, curando gli adempimenti connessi con la gestione delle misure di protezione installate su detti sistemi.

4.3.6 Auditor

È la struttura aziendale che effettua controlli e verifiche sulle misure adottate a tutela della sicurezza informatica. Definisce le opzioni e gli standard di auditing. È il primo destinatario delle segnalazioni di eventi anomali sotto il profilo dell'integrità, riservatezza e disponibilità delle risorse informatiche.

Va garantita la completa indipendenza strutturale e operativa della funzione di auditing dalle funzioni di definizione, implementazione e gestione delle *policy* di sicurezza. Una corretta collocazione della funzione di auditing nell'ambito dell'organigramma è quella in staff, alle dirette dipendenze dei vertici aziendali.

È importante anche che venga assicurata una stretta collaborazione con il settore legale per il continuo aggiornamento su disposizioni di legge, regolamenti e normative applicabili a ciascun sistema informatico.

4.3.7 Gestore degli impianti

È la struttura aziendale che gestisce gli impianti tecnologici che consentono il regolare funzionamento dei sistemi elaborativi e l'efficienza degli apparati di sicurezza fisica.

4.4 Il contenuto delle *policy* di sicurezza informatica

Il sistema di sicurezza informatica deve essere sostenuto da *policy* che regolamentino gli aspetti organizzativi della sicurezza tenendo conto del contesto normativo e operativo esterno e interno.

Fanno parte del contesto esterno:

- le disposizioni normative di rango primario (nazionali e sovranazionali) nonché i regolamenti emanati da autorità competenti per particolari settori o processi produttivi;
- i requisiti fissati da organismi esterni (standard, *best practices*) liberamente adottati per migliorare i propri sistemi di gestione, anche al fine di acquisire un'eventuale certificazione;
- i requisiti imposti da eventuali vincoli contrattuali.

Fanno parte invece del contesto interno:

- le disposizioni cogenti come lo statuto, le deleghe o i poteri conferiti dal consiglio di amministrazione;
- le procedure, le istruzioni e le prassi operative vigenti all'interno dell'azienda.

In una *policy* di sicurezza devono essere sempre esattamente individuati:

1. l'emittente, ovvero l'unità organizzativa o la funzione che si occupa di gestire la specifica problematica trattata nella *policy*, fornire interpretazioni e gestire le eventuali deroghe;
2. l'ambito di applicazione;
3. i destinatari, siano essi specifiche figure professionali o aree aziendali;
4. il tipo di diffusione, ovvero se la *policy* deve avere diffusione generalizzata o circoscritta a particolari ambiti;
5. la data di entrata in vigore (deve essere evitata l'emanazione di *policy* retroattive);
6. la data di scadenza: è comunque opportuno pianificare un'attività di revisione periodica della *policy* – anche prima della data di scadenza - soprattutto in occasione di significative modifiche organizzative e/o tecnologiche;
7. i riferimenti a leggi o ad altre norme correlate;
8. le norme che vengono sostituite: è bene provvedere alla riemissione integrale di una *policy* anche in caso di modifiche parziali (che vanno comunque evidenziate);
9. le eventuali sanzioni applicabili ai sensi dei contratti di lavoro per l'inosservanza delle prescrizioni emanate.

Quanto al contenuto, le *policy* in materia di sicurezza devono regolamentare lo svolgimento di attività/processi aziendali quali:

- l'analisi e la gestione del rischio informatico (es. misure preventive e regole operative per contrastare i virus informatici, norme sull'utilizzo dei programmi antivirus; norme di utilizzo di Internet, posta elettronica e *mobile computing*);
- l'amministrazione delle misure di sicurezza logica relativamente alle applicazioni, ai sistemi e alle reti (es. regolamentazione degli accessi di terzi; modalità di assegnazione/revoca, gestione e utilizzo di userid e password; definizione e documentazione, monitoraggio e gestione della rete);
- la gestione e il controllo della sicurezza fisica degli ambienti e delle risorse che vi operano (es. misure per la protezione degli apparati dai furti);
- la gestione e il controllo del ciclo di vita del software applicativo e di sistema (es. regole per l'installazione, l'aggiornamento e l'utilizzo del software);
- la gestione e il controllo delle attività operative (es. regole per l'installazione, la manutenzione, la disinstallazione e la dismissione degli apparati informatici; per l'utilizzo, la conservazione, il trasporto e la distruzione dei supporti; per l'accesso, la conservazione, il trasporto e la distruzione di documenti e dati);
- la gestione degli incidenti di sicurezza;

- la continuità operativa.

Specifiche *policy* devono poi stabilire le norme fondamentali che il personale nonché i collaboratori esterni devono seguire nell'utilizzo delle risorse informatiche aziendali:

- utilizzare le informazioni, le applicazioni e le apparecchiature esclusivamente per motivi di ufficio;
- rispettare le procedure e gli standard previsti, segnalando senza ritardo alle funzioni competenti eventuali utilizzi e/o funzionamenti anomali delle risorse informatiche;
- impiegare sulle apparecchiature dell'azienda solo prodotti ufficialmente acquisiti dall'azienda stessa;
- astenersi dall'effettuare copie non specificamente autorizzate di dati e di software;
- astenersi dall'utilizzare gli strumenti informatici a disposizione al di fuori delle prescritte autorizzazioni;
- osservare ogni altra norma specifica riguardante gli accessi ai sistemi e la protezione del patrimonio di dati e applicazioni dell'azienda.

4.5 Verifiche di conformità dei processi alle *policy* di sicurezza

La conformità dei processi aziendali alle *policy* di sicurezza deve essere sottoposta a periodiche verifiche, con particolare riferimento all'efficacia delle contromisure installate (test di vulnerabilità).

A livello organizzativo assumono particolare rilevanza i controlli finalizzati ad assicurare nel tempo la permanenza dei livelli di sicurezza a fronte di:

- cambiamenti derivanti da innovazioni nel sistema informatico conseguenti a: realizzazione di nuove procedure o funzionalità; aggiornamento del software; revisione dell'hardware; creazione di nuove classi di utenza; evoluzione della rete e interconnessione con altre infrastrutture;
- aggiornamenti dei sistemi operativi e dei software applicativi, anche a seguito dell'installazione di *patch* di sicurezza;
- incidenti di sicurezza, per i quali, in un'ottica di prevenzione, è opportuno analizzare le cause contingenti e gli eventuali dati storici.

A livello operativo, la conformità dei processi alle *policy* di sicurezza è valutata attraverso i test di vulnerabilità, che devono essere eseguiti da risorse specialistiche.

Una particolare tecnica per l'esecuzione dei test di vulnerabilità è quella che prevede il ricorso a forme di *Ethical Hacking*, consistenti nella ricerca delle vulnerabilità di un sistema attraverso l'adozione delle stesse tecniche di violazione dei sistemi utilizzate dagli *hacker*, al fine di verificare sul campo il livello di sicurezza dei sistemi e la loro capacità di difendersi. Ciò consente di progettare le azioni necessarie per proteggere adeguatamente i sistemi stessi.

È bene comunque che il ricorso a tale pratica venga gestito con la massima prudenza, avendo cura di definire puntualmente la portata e i limiti dell'intervento, prevedendo clausole contrattuali di

salvaguardia e, ovviamente, selezionando con estrema cura e attenzione gli esperti ai quali commissionare l'incarico.

5 Aspetti di sicurezza relativi alle risorse

5.1 Le risorse umane

Per realizzare un'efficace politica di sicurezza informatica è necessario che le risorse umane coinvolte nei vari processi aziendali siano attentamente formate e sensibilizzate anche sugli aspetti di sicurezza.

Va infatti rimarcato che qualunque presidio di sicurezza tecnico-organizzativo adottato può essere vanificato da comportamenti dannosi posti in essere, in modo intenzionale o meno, dal personale dell'azienda.

Talvolta, mutuando la terminologia applicata ai sistemi, si parla di affidabilità della risorsa umana, intendendo la capacità della persona di assicurare riservatezza, disponibilità e integrità, nonché uso legale delle informazioni che tratta.

Ai fini del miglioramento di tale capacità, assumono rilievo le seguenti attività aziendali:

- la selezione accurata del personale (in termini di competenze, conoscenze, capacità e qualità personali);
- la formazione e l'addestramento sui diversi aspetti della sicurezza informatica[4]; a titolo esemplificativo, può essere prevista l'organizzazione di corsi, modulati in relazione ai ruoli e alle competenze dei partecipanti, su argomenti quali: la normativa sulla privacy; le leggi e le normative aziendali in tema di sicurezza; gli standard di riferimento e le metodologie di analisi del rischio; la progettazione delle misure di protezione; i principi di audit;
- la precisa definizione delle attività e delle responsabilità dei diversi ruoli che prevedono interventi sulle risorse informatiche aziendali (*job description*);
- la progettazione attenta dei processi aziendali in modo da ridurre la possibilità che le singole risorse si trovino in posizione critica;
- l'introduzione di ridondanze delle competenze specialistiche nei ruoli critici. Alcuni ruoli specialistici rappresentano punti di criticità nel senso che l'assenza delle persone che li ricoprono potrebbe compromettere lo svolgimento dei processi aziendali;
- la proceduralizzazione e la documentazione delle diverse attività;
- la fissazione nel sistema normativo dell'azienda (regolamenti interni, ordini di servizio, ecc.), dei comportamenti che devono essere tenuti dal personale al fine di non compromettere la

[4] Queste due attività devono essere coordinate: obiettivo della formazione è quello di fornire elementi che consentano di affinare la conoscenza e la sensibilità delle tematiche inerenti alla gestione del rischio informatico. Obiettivo dell'addestramento è quello di allenare a fornire una risposta quanto più immediata possibile alle diverse situazioni in cui il rischio informatico minaccia una risorsa o un'informazione. I risultati dell'attività di addestramento possono essere apprezzati in particolare attraverso la verifica della risposta agli incidenti di sicurezza (ovvero l'applicazione di procedure di reazione) che si articola in: individuazione di vulnerabilità o debolezze della sicurezza; comunicazione tempestiva e corretta di incidenti di sicurezza; reazione di difesa agli incidenti; esperienza tratta dagli incidenti.

sicurezza del sistema informatico aziendale (cfr. par. 4.4); la valutazione del grado di affidabilità delle risorse umane anche successivamente all'assunzione *(risk assessment* riferito alle persone);

- la previsione di un adeguato sistema sanzionatorio; le misure disciplinari che l'azienda definisce devono avere a riferimento anche le vigenti disposizioni di legge in tema di criminalità informatica. La previsione di sanzioni è tanto più necessaria in quanto vi è una scarsa o errata percezione della liceità o illiceità dei comportamenti nel mondo "virtuale".

In generale, la promozione della cultura della sicurezza presso il personale deve essere considerata un fattore fondamentale per la protezione del patrimonio informativo aziendale. La consapevolezza e il coinvolgimento del personale devono essere assicurati attraverso idonei interventi di sensibilizzazione e comunicazione che mirino a valorizzare, nell'ambito della missione aziendale, le attività di sicurezza rendendo tutti partecipi dell'importanza che riveste l'osservanza delle procedure di protezione del sistema informativo.

5.2 Le informazioni e le risorse tecnologiche

La puntuale conoscenza del patrimonio dell'azienda, ossia dell'insieme dei beni (materiali e immateriali) che costituiscono gli *asset* aziendali e che vanno pertanto protetti, rappresenta in generale la premessa indispensabile per la corretta gestione del rischio. Tale assunto vale in particolare per la gestione del rischio informatico, che deve quindi prendere avvio dal "riconoscimento" dei beni coinvolti nei processi informatici.

I beni più rilevanti sul piano del rischio informatico possono essere distinti in almeno due categorie:

- le risorse tecnologiche ([5])
- le informazioni.

Ai fini del "riconoscimento" dei beni sono essenziali le seguenti attività:

- **Inventario**, ovvero il censimento degli *asset* che l'azienda intende proteggere da eventuali furti, smarrimenti o gestioni non autorizzate; esso consiste nell'elencazione completa dei beni, nell'individuazione delle correlazioni tra di essi al fine di anticipare una possibile propagazione del rischio, nell'assegnazione della responsabilità della custodia e conservazione del bene considerato. Questa operazione va effettuata con continuità, e non solo occasionalmente, anche per la rilevanza che riveste per numerosi altri processi di

[5] Queste comprendono:

- sistemi e dispositivi che trattano le informazioni (sistemi informatici o telematici);
- sistemi e dispositivi di supporto ai primi (es. sistemi di controllo accessi alle sale che contengono i sistemi informatici o telematici, sistemi ausiliari per l'energia elettrica, condizionamento);
- supporti che custodiscono le informazioni (es. dischi, nastri, documenti cartacei);
- contenitori di supporti (es. faldoni, armadi, casseforti);
- processi e procedure che elaborano le informazioni (es. procedure informatiche, spedizione e ricezione di fax/e-mail per l'attivazione di servizi) e processi e procedure che, pur non trattando direttamente le informazioni, possono influire sulle medesime (es. *tool* di sviluppo applicativo, manutenzione delle procedure informatiche).

business e di supporto (es. aspetti fiscali, assicurativi, di *asset management*, di sicurezza e incolumità delle persone).

- **Classificazione**, ovvero ordinamento dei beni secondo criteri di priorità di protezione, dettati di norma dal valore dei beni stessi, nonché ordinamento di questi secondo la capacità di ciascuno di assicurare un determinato livello di protezione alle informazioni su cui può influire. Lo scopo della classificazione è quello di stabilire una priorità di intervento in fase di protezione e di graduare le azioni di gestione dei rischi che devono essere condotte in funzione della rilevanza delle informazioni. Il processo di classificazione deve essere reso evidente e documentato per assicurare una migliore protezione all'informazione. I principali parametri rispetto ai quali viene suggerito di classificare le informazioni sono la **riservatezza**, l'**integrità**, la **disponibilità**. Rispetto ai parametri individuati si suggerisce di prevedere tre livelli di classificazione: alto, medio, basso. È importante infine che l'azienda effettui nel tempo aggiornamenti della classificazione.
- **Etichettatura**, ovvero l'apposizione ai beni inventariati di elementi identificativi univoci. L'etichetta deve accompagnare il bene durante tutto il suo ciclo di vita. La carenza di una puntuale etichettatura vanifica ovviamente lo stesso processo di classificazione.

5.3 Il controllo logico dell'accesso alle risorse

Un sistema informatico può essere visto come un sistema caratterizzato da soggetti (utenti, processi) che accedono a oggetti (applicazioni, dati, programmi) mediante operazioni (lettura, aggiornamento, esecuzione). Il controllo degli accessi consiste nel garantire che tutti gli accessi agli "oggetti" del sistema informatico avvengano esclusivamente secondo modalità prestabilite e controllate.

Funzionalmente, il controllo logico dell'accesso alle risorse si realizza attraverso:

- un insieme di regole, specificate in apposite *policy*, che stabiliscono le modalità (lettura, aggiornamento, ecc.) secondo le quali i vari soggetti possono accedere agli oggetti;
- un insieme di procedure di controllo (meccanismi di sicurezza) che verificano se l'accesso è consentito o negato, in base alle suddette regole (validazione della richiesta).

Il controllo logico dell'accesso ai dati può essere svolto a livello di sistema operativo e a livello di applicazione; per l'accesso alle infrastrutture e alle reti può essere svolto a livello di protocollo, origine e destinazione.

Sulla base dei principali standard internazionali (norma BS7799-standard ISO 17799) e delle *best practices* possono essere individuati alcuni modelli di riferimento per il controllo logico degli accessi.

5.3.1 Il controllo logico dell'accesso ai dati

Relativamente al controllo logico dell'accesso ai dati possono essere citati i seguenti modelli:

Amministrazione dei privilegi di accesso. L'amministrazione dei privilegi è l'attività svolta dall'amministratore della sicurezza per concedere, modificare e revocare agli utenti dell'azienda i

diritti di accesso alle risorse sulla base delle indicazioni fornite dall'utente proprietario delle stesse. Essa può essere:

- centralizzata, se svolta da un amministratore per tutti gli utenti dell'azienda;
- decentrata, se svolta da un amministratore per ogni unità operativa;
- gerarchica, se svolta da una gerarchia di amministratori, ciascuno responsabile di una porzione di dati, collegati fra loro da privilegi di amministrazione (gli amministratori di più alto livello possono creare e rimuovere amministratori di livello più basso nella gerarchia, oppure concedere o revocare loro privilegi);
- cooperativa, se per la concessione di un privilegio di accesso è necessaria la cooperazione da parte di più soggetti.

Sistemi di controllo chiusi/aperti: in un sistema di controllo "chiuso" tutti i privilegi che non sono esplicitamente autorizzati sono negati, mentre in un sistema aperto tutti i privilegi che non sono esplicitamente negati sono autorizzati. I sistemi chiusi forniscono un livello più alto di sicurezza e sono adatti per basi dati con requisiti di protezione elevati.

Privilegio minimo (need-to-know) oppure *massimo:* in una logica di privilegio minimo ogni soggetto deve possedere i privilegi sulle risorse nella misura minima necessaria per svolgere le proprie mansioni; in una logica di privilegio massimo, tipica di ambienti in cui la condivisione di risorse deve essere massima (es. ricerca scientifica, collaborazione su progetti), a tutti i soggetti deve essere riconosciuto il massimo privilegio di accesso alle risorse.

5.3.2 Il controllo logico dell'accesso alle applicazioni

Normalmente l'accesso ai dati da parte dei soggetti non avviene in modalità "diretta", salvo specifiche autorizzazioni in deroga, ma per mezzo di applicazioni.

Per l'accesso alle applicazioni vengono comunemente adottate regole di controllo che definiscono per ogni coppia soggetto – oggetto le possibili operazioni che possono essere svolte. Gli approcci più usati per la definizione di tali regole sono:

- DAC (*Discretionary Access Control*);
- RBAC (*Role Based Access Control*).

Con il *Discretionary Access Control* il proprietario di un oggetto determina chi vi può accedere e quali operazioni può svolgere sull'oggetto stesso. Il DAC viene usato in tutti quei sistemi in cui i dati possono essere facilmente ricondotti a un proprietario ed esiste la necessità di condividere o scambiarsi tali dati con altri utenti, senza dover chiedere l'autorizzazione in ogni occasione.

L'approccio più diffuso per l'implementazione di un sistema DAC è quello che usa le ACL (*Access Control List*): ogni lista di controllo specifica, per ogni oggetto di un sistema, tutti i soggetti abilitati all'accesso e le operazioni consentite.

Il *Role Based Access Control* è una tipologia di controllo degli accessi basata sulla definizione del ruolo aziendale dell'utente all'interno dell'organizzazione: l'utente è autorizzato a eseguire le sole operazioni/applicazioni che competono al ruolo ricoperto.

Questa tipologia di sistema di controllo degli accessi è più facilmente utilizzabile in quei contesti che prevedono ruoli operativi ben definiti; in tali contesti, l'adozione della metodologia RBAC è in grado di semplificare notevolmente gli aspetti gestionali.

5.3.3 Il controllo logico dell'accesso ai sistemi distribuiti

Nel caso di accesso di un utente a più sistemi tra loro connessi in rete, direttamente o attraverso l'utilizzo di un'applicazione, occorre attivare specifici presidi:

- devono essere definiti: un profilo che consenta all'utente di essere "accettato" da tutti i sistemi interessati; i punti di origine (accesso dell'utente) e di destinazione (posizionamento dei dati acceduti); i protocolli e i servizi di rete utilizzati;
- la richiesta di accesso di un'applicazione a un sistema deve essere eseguita con i diritti di accesso dell'utente che sta eseguendo l'applicazione;
- sistemi diversi possono avere meccanismi diversi per la classificazione e protezione dei dati: in questo caso deve essere garantito il livello di protezione più elevato.

5.3.4 Gli strumenti per il controllo logico degli accessi

Il controllo logico degli accessi alle risorse si basa sull'utilizzo di meccanismi che consentono l'autenticazione dell'utente (cioè l'attestazione della propria identità), il più diffuso dei quali è il rilascio di userid e password.

Molteplici sono peraltro i problemi legati all'uso delle password che possono inficiare l'efficacia del meccanismo di autenticazione: scelta non ottimale della lunghezza e del contenuto delle password stesse, custodia non adeguata, rischio di intercettazione.

Sono stati quindi individuati dei meccanismi di *autenticazione forte*, che consentono di rendere molto più sicura la fase di autenticazione; essi sono basati sul riconoscimento di un attributo posseduto dall'utente, che può essere:

- una caratteristica fisica, quale l'impronta digitale, la forma della mano, l'iride, la retina o la voce (*autenticazione biometrica*);
- una password generata dinamicamente (*one-time password*) da un apposito dispositivo personalizzato per ciascun utente (*token*);
- un certificato digitale che attesta l'identità dell'utente, solitamente memorizzato su *smart card*.

I certificati digitali sfruttano la tecnica di crittografia asimmetrica basata sull'utilizzo di chiavi pubbliche. Al fine di utilizzare tali meccanismi è necessario fare riferimento a una PKI (*Public Key Infrastructure*), cioè a una infrastruttura che emette dei certificati digitali e che provvede alla loro gestione (pubblicazione in rete, revoca, sospensione)[6]. Il ricorso ai certificati digitali consente la realizzazione di obiettivi estremamente importanti in tema di sicurezza informatica, quali l'autenticità, l'integrità, la confidenzialità e la non ripudiabilità dei messaggi.

---

[6] In tale scenario ogni utente possiede una coppia di chiavi (pubblica e privata) che lo identifica. La chiave pubblica viene inserita in una *directory* pubblicata dalla PKI che ne attesta inequivocabilmente l'appartenenza all'utente stesso. La chiave privata viene invece custodita segretamente dall'utente.

Un meccanismo di sicuro interesse nell'ambito di strumenti per il controllo degli accessi è rappresentato dai sistemi di *Single Sign-On* (SSO). Tali strumenti sono realizzati per facilitare la gestione degli accessi in quei sistemi in cui l'utente si trova di fronte a una moltitudine eterogenea di *workstation*, *server* e applicazioni, e si vede costretto a effettuare la fase di autenticazione (*log-in*) ogni qualvolta deve accedere a uno di essi. In tali situazioni un sistema SSO presenta all'utente una singola istanza iniziale di identificazione; è poi il sistema che, sfruttando un *Security Information Base* interno, fornisce automaticamente le *log-in* di tutte le applicazioni o sistemi. Il sistema di SSO gestisce in proprio e automaticamente le *log-in* (nuova attribuzione, rinnovo o cancellazione) mediante colloquio diretto con i sistemi e le applicazioni. In relazione alla delicatezza della funzione, è raccomandabile l'uso, in abbinamento al SSO, di forme di autenticazione forte.

Alla luce delle più diffuse *best practices* è possibile individuare alcune regole minimali – da riportare nelle *policy* di sicurezza – riguardanti i vari strumenti adottati dall'azienda per il controllo logico degli accessi (cfr. Allegato 5).

Il controllo degli accessi alle risorse informatiche assume infine, nel contesto normativo relativo alla tutela dei dati personali, una valenza che va al di là della sola protezione dei beni aziendali. Si richiamano al riguardo le norme del codice sulla privacy (D. Lgs. n.196/2003) che, nel compendiare e integrare le disposizioni in materia di protezione dei dati personali emanate successivamente alla legge n. 675/1996, ha aggiornato sulla base dell'evoluzione tecnologica e dell'esperienza applicativa più recente vari aspetti attinenti alle misure minime di sicurezza che ogni organizzazione deve applicare nel trattamento di tale tipologia di dati. Le modalità di applicazione delle misure minime sono compendiate in un apposito Disciplinare tecnico (cfr. Allegato 6), contenente, tra l'altro, prescrizioni riguardanti i sistemi di autenticazione basati su userid e password e i sistemi di autorizzazione degli accessi.

5.4 Il controllo fisico dell'accesso alle risorse

Le *policy* di sicurezza informatica devono contenere anche misure relative al controllo fisico degli accessi, indirizzate, in particolare, a coloro che non sono dipendenti dell'azienda ma devono accedere ai locali dell'azienda a diverso titolo (supporto e assistenza hardware e sistemi operativi, sviluppo e manutenzione software, consulenza, servizi ausiliari, clienti, ecc.). Le misure di sicurezza della specie devono tenere conto delle diverse esigenze di accesso, possibilmente applicando la *policy* del "minimo privilegio", dell'affidabilità dei singoli e delle responsabilità, anche contrattuali, delle società di appartenenza, nonché della necessità di riservare comunque alcune attività al personale dell'azienda.

Tra le attività da prevedere si ricordano:

- il censimento puntuale di coloro che devono accedere alle risorse tecnologiche o ai locali, individuando anche eventuali vincoli all'accesso (es. presenza di elementi esterni solo se accompagnati da personale interno);
- la definizione dei diritti minimi per l'accesso sia ai locali sia alle risorse tecnologiche;
- la limitazione dell'utilizzo di strumenti quali *mobile computer* e telefoni cellulari nelle aree classificate come critiche;
- la formalizzazione dei requisiti di sicurezza richiesti al personale esterno, integrando eventualmente gli accordi contrattuali con clausole di *non disclosure*;

- il rilascio di autorizzazioni nominative, eventualmente attraverso la verifica dei presupposti per la nomina a "incaricato del trattamento dei dati personali" ai sensi della legge sulla privacy;
- la verifica che ogni persona abbia preso visione e compreso le *policy* aziendali;
- la diffusione dell'informativa ai singoli sulle misure di protezione e sulle modalità di risposta alle emergenze ai sensi della legge 626/94[7];
- la revisione periodica delle autorizzazioni all'accesso e l'eventuale rimozione delle stesse in caso di dimissioni e/o scadenza dei contratti.

5.5 La continuità operativa

In caso di evento che determini l'interruzione dell'operatività ordinaria, assume particolare importanza la presenza in azienda di un *business continuity plan* che contempli tutte le attività volte ad assicurare la prosecuzione dei processi di business considerati critici. Esso è costituito dall'insieme dei piani di continuità sviluppati per ogni singola funzione interessata e prevede processi organizzativi di ripristino differenziati in funzione della gravità degli eventi presi in considerazione e del grado di importanza/essenzialità dei processi.

Nell'ambito di tale piano specifico rilievo rivestono le misure di *disaster recovery* tese a consentire, nell'ipotesi di evento disastroso, una ripartenza dei sistemi informatici nel più breve tempo possibile, attraverso, ad esempio, la definizione di piani organizzativi di intervento e il sistematico salvataggio dei dati presso la propria sede e presso una sede alternativa, opportunamente individuata, dotata di apparecchiature elaborative in grado di prendere in carico l'attività primaria dell'azienda.

Al tema della continuità operativa è stata dedicata una particolare attenzione, negli ultimi anni, dalla comunità bancaria e finanziaria, nazionale e internazionale, in relazione al sempre più intenso utilizzo della tecnologia dell'informazione e all'emergere di nuovi scenari di rischio.

Nel nostro paese, la Banca d'Italia, d'intesa con altre istituzioni e operatori del mondo bancario e finanziario, ha avviato specifiche iniziative volte a individuare i servizi critici di sistema, i rischi da presidiare e le priorità di intervento a fronte del verificarsi di eventi catastrofici.

In quest'ambito, a seguito di un ciclo di consultazioni con il sistema bancario, è stata emanata una specifica normativa di vigilanza sulla continuità operativa delle banche che disciplina i vari aspetti inerenti alla redazione di un piano di continuità aziendale e alla definizione delle responsabilità per la gestione delle emergenze. Il testo della normativa viene riportato nell'Allegato 7 . Considerata la possibilità dell'insorgere di rischi sistemici a fronte di catastrofi di ampia portata, altri approfondimenti sono in corso relativamente ai processi critici nel sistema dei pagamenti e nei mercati finanziari, a seguito dei quali è prevista l'emanazione di ulteriori norme volte a promuovere l'adozione di efficaci presidi per la continuità di servizio anche da parte dei soggetti operanti in tali comparti.

[7] Legge riguardante la Sicurezza sul Lavoro.

6 Aspetti di sicurezza nello sviluppo e nella manutenzione delle applicazioni e nella gestione dei sistemi e delle reti

Nell'ambito di un sistema informatico "sicuro" vanno tenuti ben presenti i rischi connessi con le attività di implementazione e gestione di applicazioni, sistemi operativi e reti. In quest'ambito possono rinvenirsi delle vulnerabilità in grado di generare minacce alla riservatezza, all'integrità e alla disponibilità delle informazioni aziendali, come ad esempio:

- la presenza di errori involontari commessi in fase di progettazione e/o implementazione che possono consentire a utenti non autorizzati l'esecuzione di operazioni e programmi riservati a altre categorie di utenti;
- la presenza di un codice malizioso inserito volontariamente dai programmatori del sistema o dell'applicazione stessa, al fine di poter svolgere operazioni non autorizzate (rientrano in queste categorie di minacce i virus, i *trojan horse*, le *backdoor*, ecc.)

Nei paragrafi seguenti vengono esaminate, nel dettaglio, le attività da porre in essere al fine di far fronte a tali minacce, tenendo presente che, per poter definire sicuro un sistema o un'applicazione occorre che siano soddisfatti non soltanto i requisiti di riservatezza, integrità e disponibilità, ma anche quelli di:

- autenticità – ovvero che sia possibile accertarsi che l'applicazione/sistema con cui si sta interagendo sia proprio quello atteso;
- tracciabilità - ovvero che rimanga traccia dei dettagli di ogni operazione effettuata in modo da consentirne l'eventuale ricostruzione;
- non ripudiabilità - ovvero che né il mittente né il destinatario di uno scambio informativo possano negare di avere inviato/ricevuto i dati in questione.

6.1 La sicurezza nello sviluppo e nella manutenzione delle applicazioni

Per sviluppo e manutenzione delle applicazioni si intende l'insieme delle attività di realizzazione, installazione e aggiornamento dei prodotti software sviluppati per il fabbisogno aziendale, sia che siano prodotti internamente, sia che vengano acquisiti all'esterno come pacchetti ed eventualmente personalizzati per le proprie esigenze.

Nella catena dello sviluppo e della distribuzione del software (analisi, stesura delle specifiche, sviluppo, test, rilascio), come anche nel processo di manutenzione, si possono facilmente evidenziare talune vulnerabilità, dovute anche al coinvolgimento di risorse sia interne sia esterne.

I test effettuati per l'accettazione dell'applicazione, benché ampi, possono non evidenziare tutti gli errori e non danno certezza assoluta che l'applicazione esegua correttamente tutto e solo quanto dichiarato. Eventuali malfunzionamenti rappresentano pertanto un potenziale rischio per la sicurezza aziendale poiché:

- possono compromettere la disponibilità, la riservatezza e l'integrità di una parte più o meno critica del sistema informativo;

- possono essere rilevati tardivamente; è quindi sempre possibile che errori avvenuti nella realizzazione di un'applicazione si presentino durante l'utilizzo nell'ambiente aziendale, anche parecchio tempo dopo il rilascio in esercizio.

A fronte dei predetti rischi possono essere adottate specifiche contromisure quali:

- utilizzo dei soli software acquisiti o sviluppati lecitamente, secondo procedure verificate dalle strutture aziendali preposte[8];
- gestione costante di un inventario del software e delle relative licenze, al fine di verificare la lecita installazione di ciascun prodotto; a tal fine è utile disporre di uno strumento di *asset management* che correli il software al relativo hardware;
- adozione di un processo interno di "certificazione/validazione" della produzione del software, che garantisca la qualità dei test, l'originalità e l'integrità del codice. Per tale ultimo aspetto potrà essere utilizzato un codice di validazione o una firma elettronica;
- disponibilità di ambienti separati per il test, il collaudo e la produzione, evitando di mettere in produzione qualsiasi software senza prima averne verificato la funzionalità e la compatibilità con il resto del sistema;
- fissazione di norme specifiche per lo sviluppo, la modifica, la copia e la cancellazione dei programmi;
- formalizzazione di procedure autorizzative per l'inserimento/variazione dei programmi nel sistema;
- adozione di procedure di *change management* per tutte le modifiche in modo da poter tenere traccia di tutte le variazioni apportate[9];
- classificazione dei programmi;
- contrattualizzazione con i fornitori del rispetto delle *policy* di sicurezza e verifica della loro osservanza;
- divieto di utilizzo di programmi e/o applicazioni prelevati da Internet o forniti da terze parti e non formalmente autorizzati dall'azienda;
- attivazione di meccanismi di *back-up* e *recovery* che permettano di avere sempre a disposizione il salvataggio di precedenti versioni di programmi e/o dati per eventuali ripristini;
- identificazione del responsabile del passaggio in produzione di ciascun programma;
- protezione adeguata, anche tramite strumenti crittografici, delle basi dati di sicurezza (con l'utilizzo, ad esempio, di chiavi di autenticazione o di crittografia);
- eliminazione periodica di tutto il software obsoleto per evitare utilizzi non consentiti e/o inutili oneri di manutenzione;

---

[8] Nel caso in cui non si disponga del codice sorgente di un software, è opportuno tutelarsi chiedendo contrattualmente che il relativo codice sia "depositato" presso una terza parte fidata, in modo tale che sia eventualmente possibile, nel caso di eventuali controversie, eseguire tutte le verifiche necessarie o salvaguardare la possibilità di mantenimento dell'applicazione, anche a seguito di una eventuale cessazione del servizio da parte del fornitore.

[9] Si tratta di procedure che consentono la gestione delle nuove versioni dei programmi, la registrazione della data di avvio dei programmi, l'impostazione della data di scadenza della versione precedente, il tracciamento delle variazioni prodotte con le relative date.

- previsione, per l'espletamento di operatività particolarmente critiche, dell'intervento contemporaneo di più persone (*four eyes principle*);
- definizione delle regole di trasferimento a terzi del software o dell'hardware su cui il software è installato (ad esempio in caso di outsourcing);
- redazione e aggiornamento di tutta la documentazione a supporto delle varie fasi del ciclo di vita del software.

Un altro aspetto importante che va attentamente curato riguarda lo sviluppo dei presidi di sicurezza nelle applicazioni.

A livello di studio di fattibilità o di documenti di *start-up* di un progetto, l'utente deve fornire una chiara rappresentazione del livello di sicurezza richiesto in termini di disponibilità, riservatezza e integrità. Tale attività può essere svolta attraverso la compilazione di *check-list* che costituiranno la documentazione da allegare agli studi di fattibilità o agli analoghi documenti che costituiscono lo *start-up* del progetto.

Una volta identificata la tipologia di presidi da applicare al progetto, è necessario precisarne le fasi di sviluppo, che possono articolarsi come segue:

- definizione dei requisiti di sicurezza utente e analisi dei rischi;
- definizione delle specifiche di dettaglio dei requisiti di sicurezza;
- definizione del piano di test di sicurezza e dei criteri di accettazione;
- analisi degli impatti di sicurezza connessi con specifiche esigenze dell'architettura applicativa e/o tecnologica (es. utilizzo di pacchetti software di mercato; necessità di supporto remoto da parte della casa costruttrice; ricorso all'esterno per la gestione del sistema);
- scelta e acquisizione delle soluzioni tecniche di sicurezza, avendo presenti fattori quali: la coerenza con gli standard aziendali; la possibilità di attivare le funzionalità di sicurezza in modo trasparente all'utente; la facilità di utilizzo; l'informativa all'utente circa l'attivazione delle funzionalità di sicurezza; la robustezza delle funzionalità fornite;
- predisposizione delle procedure tecnico–organizzative che descrivano in dettaglio gli adempimenti tecnici e procedurali per l'applicazione dei presidi in linea con gli standard aziendali;
- collaudo e accettazione dei presidi di sicurezza.

6.2 La sicurezza nella gestione dei sistemi operativi

Il sistema operativo costituisce la base su cui poggiano tutte le applicazioni dell'utente. Pertanto, particolare cura deve essere posta nelle fasi di installazione, messa in opera ed evoluzione del sistema, con particolare riferimento agli aggiornamenti resi disponibili dal fornitore, soprattutto se finalizzati a rimuovere problemi di sicurezza.

Tali attività richiedono elevate competenze tecnico-specialistiche per ciascun tipo di ambiente/software e spesso devono essere effettuate operando con privilegi di sicurezza elevati e prevedono di norma il coinvolgimento di risorse interne ed esterne.

Una volta progettati in modo sicuro, i sistemi devono essere gestiti in modo altrettanto sicuro: è opportuno pertanto progettare anche la sicurezza di gestione. Tra le varie attività da prevedere rilevano, in particolare:

- il controllo degli accessi ai sistemi;
- la definizione dei principi da seguire nella fase di configurazione dei sistemi;
- l'applicazione di *policy* di *change management* che rispettino l'architettura di sicurezza progettata;
- la definizione di procedure di gestione dei malfunzionamenti;
- l'applicazione di misure di prevenzione da utilizzare in caso di malfunzionamenti, come i *back-up*;
- l'applicazione di regole di segregazione (delle responsabilità, delle mansioni, degli ambienti operativi, delle funzioni) per tutte le risorse;
- l'uso di particolari software di *utility* e l'applicazione delle *fix* che pongono riparo ai *bug* di sicurezza rilevati;
- il monitoraggio dei sistemi di sicurezza posti a protezione dei sistemi operativi.

6.2.1 Controllo degli accessi ai sistemi

Tutti i sistemi, inclusi quelli di gestione, devono prevedere meccanismi di identificazione e autenticazione. L'accesso alle risorse deve essere sottoposto a sistemi di controllo degli accessi che verifichino i profili del soggetto e delle entità che richiedono l'accesso, registrino ed eventualmente rifiutino quegli accessi che non rientrano nei profili autorizzati e anche quelli che non seguono percorsi prestabiliti.

Tutti i terminali e gli apparati devono essere univocamente identificati, tramite opportune convenzioni di nomenclatura, e non deve essere permesso l'accesso ai servizi e ai sistemi da parte di apparati non riconosciuti. I terminali devono essere anche provvisti di meccanismi di autenticazione del terminale stesso, in modo da garantire la sicurezza di specifiche transazioni od operazioni (che possono, in questo modo, essere eseguite in modo vincolato a una specifica postazione o a uno specifico utente).

6.2.2 I principi per la configurazione dei sistemi

Particolare cura va posta nella fase di configurazione dei sistemi, al fine di contrastare le possibili minacce connesse con l'eventualità di indebiti accessi al software di base e di attacchi esterni. In particolare deve essere attuata una politica di *hardening*: con tale termine, riferito a un prodotto software (es. un sistema operativo), si intende quella attività di configurazione che si basa sul principio che "quello che non c'è non può essere sfruttato per condurre attacchi", il che porta a eliminare dal software le parti/servizi/funzioni non strettamente necessari.

6.2.3 Change management

I processi di *change management* (es. gli aggiornamenti del sistema operativo) devono essere eseguiti nel rispetto di regole predefinite, quali:

- la separazione delle librerie: ove possibile le partizioni riservate al sistema operativo devono contenere solo codice eseguibile;
- per l'accesso alle librerie relative alle componenti di base deve essere applicato il principio del "minimo privilegio";
- il rilascio di componenti di base deve essere:
  - consentito unicamente a personale o a processi espressamente autorizzati dal corretto livello manageriale;
  - autorizzato esclusivamente in presenza della documentazione che attesti il superamento di test di accettazione;
  - effettuato previa predisposizione di un piano di ripristino della situazione precedente in caso di problemi.
- la registrazione di tutti gli aggiornamenti e le variazioni apportate ai sistemi e la protezione di queste registrazioni;
- il costante allineamento della documentazione di supporto al sistema sia per l'operatività corrente sia per utilizzo in caso di emergenze;
- la conservazione delle versioni precedenti;
- l'effettuazione di test di accettazione documentati del sistema prima del passaggio in produzione[10];
- l'attivazione in produzione del sistema a seguito di un'autorizzazione formale.

6.2.4 Gestione dei malfunzionamenti

Tutti i malfunzionamenti relativi ai sistemi devono essere registrati e devono formare una base di conoscenza per la valutazione dei parametri di affidabilità dei sistemi. Dovrebbero essere oggetto di valutazione statistiche relative, ad esempio, al tempo medio tra due successivi guasti - MTBF (*mean time between failures*), al tempo medio di ripristino - RMT (*recovery mean time*), al tempo medio di rimozione della causa che ha generato l'incidente -MTTR (*mean time to repair*).

La gestione dei malfunzionamenti consiste nella rapida presa di conoscenza dell'evento, nell'analisi di primo ed eventualmente secondo livello del problema che è stato generato[11], nella approvazione delle soluzioni proposte (eventualmente coinvolgendo anche i proprietari delle applicazioni), nell'attuazione di queste soluzioni e nella documentazione della soluzione adottata.

---

[10] I criteri di accettazione dovrebbero includere la documentazione dei requisiti di performance e di capacità, dei piani di gestione delle emergenze e delle procedure di ripristino e ripartenza, dell'insieme dei controlli di sicurezza previsti, dei rapporti di esecuzione di *stress test* in condizioni limite (scadenze temporali, fine mese, condizioni di punta di uso del sistema, ecc.), delle istruzioni e del *training* del personale addetto all'uso o alle operazioni sul sistema. Test di regressione dovrebbero essere previsti almeno per i servizi a criticità media o alta.

[11] Primo livello di analisi: ricerca della soluzione o di soluzioni analoghe già predisposte in occasione di episodi o eventi simili già accaduti. Secondo livello di analisi: costruzione, a partire dall'esame delle cause e di eventi simili, di una soluzione del tutto nuova o di complessità elevata e non fornita in modo standard a chi effettua l'analisi di primo livello.

6.2.5 Back-up

Le *policy* di *back-up* devono essere definite a livello aziendale in funzione della criticità dei dati elaborati dai sistemi e devono prevedere:

- un livello minimo di *back-up*[12];
- le modalità di conservazione dei *back-up*;
- le regole e i profili di accesso ai *back-up*;
- il tempo di *retention* per le informazioni essenziali e le regole relative al *back-up* di informazioni che devono essere conservate indefinitamente (è essenziale in questi casi assicurare la "bontà" del *back-up* anche a fini legali);
- le modalità di distruzione dei *back-up* obsoleti.

Particolare attenzione deve essere posta, infine, alla verifica e alla documentazione delle procedure di ripristino: devono essere in particolare stabiliti e testati i tempi di ripristino che hanno impatto sui livelli di servizio.

6.2.6 Regole di segregazione

Si tratta di regole che disciplinano la separazione delle applicazioni e dei sistemi con l'obiettivo di ridurre la concentrazione di criticità e consentire l'adeguata applicazione dei presidi di sicurezza su un numero limitato di elementi proteggendoli da interazioni e effetti determinati, anche involontariamente, da altri sistemi e applicazioni. Tale misura permette anche di mettere in pratica il principio del "minimo privilegio".

6.2.7 Software di utility e applicazione di fix

L'uso dei software di *utility* e l'applicazione di *fix* ai sistemi sono funzioni critiche che occorre monitorare strettamente perché tramite esse è possibile compromettere l'integrità e la disponibilità (nonché la riservatezza) del sistema e delle applicazioni. Occorre pertanto: controllare che tali funzioni siano effettuate nel rispetto dei privilegi di accesso, verificarne la funzionalità, inibirne l'utilizzo durante i processi critici, registrarne l'utilizzo (log).

6.2.8 Monitoraggio

I processi di monitoraggio dei sistemi di seguito indicati hanno lo scopo di verificare i livelli di efficacia ed efficienza prefissati ed eventualmente anche contrattualizzati:

- *capacity planning*: devono essere previste e pianificate, a livello aziendale, le necessità future in termini di capacità operativa al fine di evitare pericolosi "colli di bottiglia" nei processi di implementazione o di *upgrading* dei sistemi;
- monitoraggio dell'uso dei sistemi e di particolari eventi; deve essere prevista una registrazione per le seguenti aree:

[12] È necessario definire: modalità di *back-up* standard, numero di cicli o serie di *back-up* conservati, standard di nomenclatura, distanza minima del luogo di conservazione che deve separare i *back-up* dal sistema a cui si riferiscono, modalità di verifica della bontà del *back-up*.

- accessi autorizzati effettuati e tentativi di accesso non autorizzato;
- operazioni con privilegi particolari (fra cui le modifiche alle *policy* di audit e di *accounting*, la gestione di utenze/gruppi/ecc.);
- *shut down/restart* dei sistemi;
- allarmi o incidenti del sistema.

L'analisi degli eventi prevede l'esame di grandi masse di dati utilizzando sistemi automatici (es. *Intrusion Detection System*, analizzatori di log) coerentemente con le *policy* stabilite.

6.3 La sicurezza nella gestione delle reti

La sicurezza nella gestione delle reti e dei servizi resi attraverso le reti stesse si avvale di una articolata serie di presidi: fondamentale è innanzitutto l'adozione di misure di controllo degli accessi e di monitoraggio analoghe a quelle previste per i sistemi operativi; rilevano poi misure specifiche, quali ad esempio:

- autenticazione delle connessioni esterne e autenticazione dei nodi: poiché l'accesso dall'esterno rappresenta una fonte potenziale di rischio per l'organizzazione, è estremamente importante che il processo di presentazione sia oggetto di autenticazione. Anche in questo caso il livello di autenticazione deve essere proporzionale al livello di rischio. Occorre valutare in particolare il livello di sicurezza offerto da soluzioni che prevedono l'uso di tecniche di autenticazione forte, quali *token hardware*, protocolli "a sfida", procedure di *call-back*, ecc. L'autenticazione dei nodi può essere complementare all'autenticazione di gruppi di utenti remoti connessi a sistemi sicuri;
- protezione delle porte di diagnostica remota: le porte di diagnostica remota e quelle utilizzate per la gestione degli apparati devono essere disabilitate o controllate da dispositivi fisici e procedure di abilitazione esplicite e formalizzate che impediscano di intervenire sul sistema senza controllo;
- regole sulle limitazioni di utilizzo delle connessioni di rete: è importante che siano attivati meccanismi e procedure che limitino la possibilità per un utente di connettersi alle risorse di rete in modo non controllato. È consigliabile in questo senso l'utilizzo di tavole e regole che filtrino il traffico in base a *policy* generali di controllo accessi, esigenze di business e requisiti delle applicazioni. Devono in particolare essere regolate le seguenti funzioni: la posta elettronica, i meccanismi di *file transfer*, gli accessi interattivi;
- politiche di *routing*: per la gestione sicura delle reti è necessario prevedere la definizione di precise regole di instradamento, sia per ottimizzare il bilanciamento dei carichi, sia per garantire la separazione dei flussi critici e quindi la possibilità che apparati divengano *single point of failure*;
- politiche di gestione degli *sniffer*, ovvero delle apparecchiature che possono essere collocate sulla rete per rilevare ai fini della sicurezza il tipo di traffico in transito; la definizione di tali *policy* è critica, considerato che tramite *sniffer* possono essere anche condotti attacchi alla sicurezza informatica (cfr. oltre);
- percorsi obbligati: la flessibilità e la condivisione di un gran numero di risorse, richiesta implicitamente dai requisiti di interconnessione, rappresenta una debolezza in termini di

controllo e facilita anche la possibilità per i malintenzionati di produrre danni all'organizzazione che si avvale sempre più dei servizi di rete. La misura principale per ridurre questi rischi è quella di forzare il percorso tra l'utente di rete e le risorse accedute limitando le opzioni di instradamento[13].

[13] Ad esempio attraverso: l'assegnazione di numeri telefonici o linee dedicate, la connessione automatica di specifiche porte a specifiche applicazioni o *gateway* di sicurezza (*firewall, router*), la limitazione dei menu e dei sottomenu per ciascun utente, la prevenzione dell'utilizzo del *roaming* illimitato; l'assegnazione di specifici sistemi di *security gateway* per gli utenti di reti esterne, il controllo attivo del traffico attraverso i *secure gateway*; la restrizione di accesso alla rete separando domini logici e creando ad esempio VPN per gruppi o servizi omogenei.

7 Aspetti di sicurezza connessi con l'utilizzo di nuove tecnologie

Poiché l'utilizzo delle nuove tecnologie informatiche può esporre l'azienda a molteplici rischi, non sempre adeguatamente percepiti e valutati (es. patrimoniali, legali, di immagine, di sicurezza), è necessario fornire al personale idonee indicazioni e istruzioni sull'utilizzo delle stesse, al fine di evitare comportamenti, anche inconsapevoli, non corretti.

Nei paragrafi che seguono il tema della sicurezza informatica è trattato in relazione al mondo Internet (inteso non solo come accesso al *World Wide Web* ma anche come tecnologia al servizio dello sviluppo applicativo), alla gestione della posta elettronica e all'utilizzo di dispositivi di *mobile computing*; sono infine descritte le nuove tipologie di attacco – e le relative contromisure – che vanno diffondendosi in relazione all'utilizzo di tali tecnologie.

7.1 Utilizzo di Internet in ambito aziendale

7.1.1 Accesso al World Wide Web

I principali rischi connessi con l'accesso ai siti web sono quelli derivanti dalla possibilità che l'utente, anche in modo inconsapevole, installi sul proprio posto di lavoro (e veicoli nella rete aziendale alla quale esso è connesso) del codice potenzialmente "dannoso" (virus e *trojan horse*), progettato, ad esempio, per alterare o catturare dati, spedire documenti all'esterno, generare un traffico elevatissimo in rete, aprire "varchi" sul computer per consentire il controllo remoto del sistema da parte di soggetti malintenzionati. Tramite i varchi anzidetti eventuali *hacker* possono presentarsi nelle LAN come un utente interno, una volta superate le difese perimetrali; tale possibilità non deve essere trascurata quando si progettano le contromisure.

Vanno altresì tenuti in considerazione i costi e le inefficienze connessi con il tempo impiegato dai dipendenti nella consultazione di pagine web non strettamente correlate all'attività aziendale.

Pur avendo presente che la scelta delle modalità per garantire l'accesso sicuro alla rete Internet in ambito aziendale deve essere effettuata dalle singole aziende secondo approcci funzionali agli specifici obiettivi perseguiti, si forniscono di seguito alcune indicazioni di massima sulle possibili contromisure da attivare in relazione ai predetti rischi:

- tempestivo aggiornamento dei software di base e delle configurazioni dei prodotti tramite *patch* o *service pack* fornite dal produttore[14];
- accesso a Internet tramite stazioni di lavoro dedicate, isolate dalla rete aziendale, oppure realizzando un disaccoppiamento logico tra le stazioni di lavoro e la navigazione mediante l'utilizzo di strumenti di emulazione di terminale;
- separazione degli ambienti e delle reti utilizzando la separazione fisica o logica per creare "domini di sicurezza" a protezione degli *asset* ritenuti più importanti;

[14] Il software di base presenta delle vulnerabilità non indifferenti che, una volta individuate e corrette, richiedono la distribuzione tempestiva delle *patch* su tutti i *server* e i posti di lavoro.

- utilizzo di software che impediscono l'accesso a determinati siti contenuti in una *black list* o che rispondano a determinati requisiti, fissati dall'azienda, e valutati di volta in volta da un sistema esperto che ne analizza il contenuto[15]; in alternativa, può essere consentito l'accesso soltanto a determinati siti contenuti in una *white list*; dette liste possono essere gestite direttamente dall'azienda oppure dal fornitore;
- accesso al mondo esterno via *proxy server*, ai quali spetta anche la verifica dell'abilitazione all'accesso dei dipendenti;
- utilizzo di *firewall* sulla rete aziendale e di *personal firewall* anche sui computer portatili;
- utilizzo di un prodotto antivirus su tutti i computer (*server* e *client*), sistematicamente e tempestivamente aggiornato;
- importazione controllata dei file mediante scansione dei flussi, privando i file stessi di ogni contenuto attivo (eseguibili, macro, ecc.);
- ricorso a sistemi di *intrusion detection*;
- uso di tecniche VPN per accessi "in remoto";
- duplicazione delle risorse critiche;
- predisposizione di appositi piani di *contingency* per poter contrastare le diverse eventuali tipologie di attacco, prevedendo anche azioni drastiche quali la disconnessione di taluni sistemi o addirittura l'interruzione dei servizi di rete;
- adeguamento costante delle infrastrutture tecnologiche a fronte dei nuovi rischi e delle nuove vulnerabilità;
- creazione di una struttura di intervento da contattare in caso di sospetto attacco informatico;
- definizione di una *policy* per l'utilizzo di Internet, inserita nelle *policy* di sicurezza e portata a conoscenza di tutto il personale.

Particolare attenzione va posta inoltre alla scelta dell'ISP (*Internet Service Provider*) e alla relativa contrattualizzazione dei livelli di servizio, ivi inclusi i presidi di sicurezza ritenuti più adeguati al livello di protezione che l'azienda intende conseguire.

Problemi analoghi a quelli appena descritti si possono porre nell'utilizzo delle **intranet aziendali**: infatti, in relazione alla caratteristica di accesso a diffusione capillare, tali infrastrutture sono spesso utilizzate dai virus per la diffusione di codice malevolo all'interno dell'azienda.

7.1.2 La sicurezza delle applicazioni web-based

Nello sviluppo di applicazioni basate su tecnologia web, va rivolta particolare attenzione ai rischi che l'utilizzo di detta tecnologia può presentare e vanno tenute in considerazione le principali contromisure a oggi note.

Se da una parte l'impiego del *browser* consente di realizzare applicazioni più snelle, dall'altra va considerato che in quest'area lo sviluppo applicativo presenta alcuni peculiari aspetti critici, connessi da una parte con scelte orientate alle funzionalità più che alla sicurezza e, dall'altra,

[15] I siti a contenuto pornografico, ludico o comunque correlati ad attività non lecite, costituiscono spesso veicoli per l'introduzione di virus informatici o di codice malevolo.

con la necessità di prevedere collaudi specifici, coerenti con le vulnerabilità proprie del mondo web, e sistematici test di vulnerabilità e di intrusione sui *server* e sui *client.*

La pericolosità delle applicazioni *web-based* deriva dalla diffusione di tecnologie di *scripting* (Active X, ASP, ecc.) che spesso sono in grado di superare la sicurezza del sistema e/o suscettibili di veicolare codice malevolo. In particolare possono presentarsi le seguenti minacce dirette a *web application server*: accessi non controllati ai servizi di rete, vulnerabilità di sicurezza del sistema operativo e del sofware applicativo, sfruttamento della configurazione aperta del sistema operativo e del software web, disponibilità di software non necessario, disponibilità di funzionalità pericolose, errori di scrittura del codice, interazione con i *client*, attacchi diretti ai controlli formali (dati di input, URL, informazioni utili, ecc.), esecuzione remota di software.

Le principali contromisure relative alle minacce citate sono basate sull'adozione di log e strumenti di controllo, su un'attenzione massima in fase di disegno dell'applicazione, sulla definizione di un'architettura applicativa che preveda un *client* il più possibile *light* - cioè scarico da funzionalità applicative -, sull'utilizzo di un'appropriata metodologia di sviluppo del codice sicuro[16].

Risulta infine indispensabile per le applicazioni che nascono o che vengono "tradotte" in tecnologia web effettuare, prima della consegna in ambiente di produzione, un *application vulnerability assessment*, basato sull'analisi del codice applicativo e volto essenzialmente a individuare eventuali errori di programmazione e/o vulnerabilità dell'architettura, avvalendosi di appositi strumenti di test.

7.2 Posta elettronica

La rapida diffusione della posta elettronica nelle aziende, favorita dalle sue caratteristiche di semplicità d'uso e di standardizzazione, non sempre è stata accompagnata da una piena consapevolezza dei rischi insiti nel suo utilizzo, quali ad esempio:

- attacchi tramite virus/*trojan horse*, che possono diffondersi a tutti i sistemi elaborativi aziendali;
- intercettazione e modifica dei messaggi durante la trasmissione (attacco definito "*the man in the middle*");
- indisponibilità del servizio per la mancanza di connessione o al *server* di posta o alla rete;
- identificazione non certa del mittente;
- non certezza della consegna al destinatario;
- accesso non autorizzato al contenuto delle caselle di posta.

Alla mancata adozione di misure di sicurezza nella posta elettronica è altresì associata l'esposizione a rischi di tipo legale; tra questi rilevano, ad esempio, quelli connessi con l'inosservanza delle prescrizioni normative di cui al D. Lgs. n. 196/2003 (Codice in materia di protezione dei dati personali) ovvero quelli derivanti da un'eventuale integrazione della fattispecie di reato di cui all'art. 615 quinquies del codice penale, che punisce la diffusione di programmi che

[16] Non dovrebbe essere fornita nessuna informazione utile a un attacco, come, ad esempio, che la passwor*d* inserita risulta errata.

provochino il danneggiamento, l'interruzione o l'alterazione del funzionamento di un sistema informatico o telematico.

Non bisogna poi dimenticare particolari fenomeni che possono presentare profili di illegalità come, ad esempio, il cosiddetto *spamming*, volontario o involontario.

Un'ulteriore delicata problematica è quella relativa all'utilizzo della posta elettronica da parte dei dipendenti per finalità non correlate all'attività aziendale (analoga questione si pone per la consultazione dei siti Internet); si tratta di una pratica che può esporre l'azienda a rischi di natura economica, per i costi sostenuti e per la possibile perdita di produttività del personale, oltre che a rischi legali e di immagine. Nell'adozione delle necessarie contromisure (v. oltre), l'azienda dovrà peraltro tenere conto dell'esigenza di operare un corretto bilanciamento tra gli interessi aziendali e i diritti dei lavoratori, in materia ad esempio di tutela della riservatezza[17].

A fronte delle diverse tipologie di rischio sopra descritte l'azienda può quindi adottare varie contromisure, tecnologiche e organizzative, quali ad esempio:

- utilizzare più antivirus in sequenza - di produttori diversi - per analizzare i flussi di posta;
- applicare filtri sugli allegati mediante *black-list* o *white-list*;
- configurare in sicurezza i *client* di posta elettronica;
- non consentire l'invio di posta da parte di utenti non autenticati sulla rete aziendale;
- bloccare comunque le e-mail rilevate infette, disattivando la funzione di bonifica, in modo da evitare di esportare informazioni, anche inconsapevolmente.

È poi necessario emanare *policy* dirette agli utenti interni che prevedano:

- istruzioni per l'utilizzo della posta elettronica aziendale, che deve essere limitato alle sole finalità aziendali;
- indicazioni sulle modalità per l'eventuale consultazione del sistema di posta elettronica aziendale dall'esterno dell'azienda;
- limitazioni dell'uso e della tipologia degli allegati ai messaggi di posta, in particolare per quanto riguarda la ricezione /spedizione di file di tipo eseguibile;
- regole per l'iscrizione a *mailing list* degli utenti interni;
- regole per l'invio di risposte automatiche;
- modalità per una corretta gestione delle e-mail, attraverso prescrizioni quali ad esempio:
  - cancellare la posta ricevuta da mittenti sconosciuti;
  - cancellare le e-mail ricevute con oggetti /messaggi seducenti;

[17] Non esiste allo stato in Italia una normativa specifica che regoli l'uso della posta elettronica e la navigazione su Internet da parte dei dipendenti e i connessi poteri di controllo del datore di lavoro. Alcune pronunce giurisprudenziali subordinano la liceità dei suddetti controlli al rispetto del criterio di proporzionalità, valutato in funzione dell'obiettivo perseguito, ammettendo ad esempio l'accesso al contenuto della posta elettronica o l'utilizzo dei log inerenti alla navigazione Internet se necessario per la repressione di fatti illeciti. In altri paesi europei la materia è regolata da codici di condotta o linee guida emanate, previa consultazione con le organizzazioni rappresentative dei datori di lavoro e dei lavoratori, dalle autorità preposte alla protezione della privacy (così in Germania, Regno Unito e Francia).

- eliminare la posta con allegati aventi doppia estensione.

7.3 Mobile computing

Molteplici sono i dispositivi utilizzati per il *mobile computing*: personal computer portatili (*desktop, laptop*, ecc.), palmari (*workpads*, *personal digital assistant*, *palm pilots*, ecc.) e telefoni cellulari con funzioni multimediali.

Per l'utilizzo di dispositivi mobili, da parte di personale interno o esterno, è opportuno adottare una logica di sicurezza delle basi dati con requisiti di protezione elevati, dove sono negati tutti i privilegi non esplicitamente autorizzati.

Assume quindi particolare importanza, soprattutto con riguardo alla salvaguardia della rete interna, la redazione di appropriate *policy* che regolamentino le procedure e le modalità di accesso, il riconoscimento dell'utente e il tipo di utilizzo consentito di dati e informazioni.

Inoltre, nonostante si tratti di apparecchiature di norma mantenute sotto il controllo diretto dell'assegnatario, per la salvaguardia dei dati in esse contenuti è raccomandabile l'utilizzo, ove possibile, di strumenti di controllo degli accessi che garantiscano alti livelli di sicurezza, nonché specifiche modalità di protezione dei dati, al fine di evitare che l'eventuale furto di un *mobile computer* infici la sicurezza aziendale.

Per la connessione dall'esterno alla rete aziendale è opportuno adottare:

- sistemi di autenticazione forte dell'utente (es. *token* o *smart card*) e di autorizzazione all'accesso sulle risorse, di tipo RADIUS (Remote Dial-in User Service, protocollo sviluppato per i servizi di autenticazione e di gestione degli *account* su *server* di accesso alla rete), Terminal Access Controller Control System (protocollo di autenticazione, autorizzazione e gestione degli *account* largamente utilizzato per le connessioni telefoniche dirette), KERBEROS (protocollo di autenticazione a chiave segreta), ecc.;
- tecniche di restrizione dell'accesso quali RPN (Remote Private Network), VPN (Virtual Private Network), CUG (Closed User Group), *call-back*, ecc.;
- sistemi di protezione e di anti-intrusione (quali *firewall*, *proxy*, traslazione degli indirizzi privati, ecc.);
- sistemi di autenticazione dei nodi;
- sistemi di *logging* per la verifica degli accessi, degli eventi e delle violazioni;
- crittografia dei dati critici archiviati e trasmessi.

Anche nel caso in cui i dispositivi si connettano alla rete aziendale dall'interno, devono essere adottati, oltre ai consueti sistemi di autenticazione dell'utente, *logging* e crittografia dei dati critici, anche tecniche di restrizione dell'accesso quali VLAN (Virtual Local Area Network), identificazione dei MAC Address (Medium Access Control Address), ecc.

Si sottolinea comunque che tale tipologia di connessione deve essere attuata con estrema prudenza, soprattutto nel caso in cui gli apparati non siano configurati preventivamente dall'azienda che ne mantiene il controllo (es. personal computer di personale esterno).

Per le particolari caratteristiche di tali dispositivi, dotati di modem interno o aventi la possibilità di comunicazione con apparecchi di telefonia mobile, risulta facilitata la possibilità di connessione a sistemi e reti esterne all'azienda, incluso Internet.

Nel caso in cui tali apparecchiature siano utilizzate per la connessione a Internet, e quindi soggette al rischio di infezioni virali e di acquisizione inconsapevoli di *malicious code*, è opportuno che siano dotate di *personal firewall* opportunamente configurati e che siano in grado di effettuare l'aggiornamento automatico delle impronte dell'antivirus a ogni connessione a Internet. È inoltre buona norma prevedere che, prima di ogni accesso a Internet effettuato al di fuori di una infrastruttura di protezione aziendale, la stazione di lavoro venga disconnessa dalla rete interna.

Un fattore di rischio nell'utilizzo di dispositivi mobili risiede anche nell'architettura di tipo *client/server* delle relative applicazioni[18]: al riguardo è raccomandato l'utilizzo di protocolli di comunicazione sicuri (es. protocollo SSL3, VPN, ecc.) tra le componenti applicative *client* e *server*.

7.4 Nuove modalità di attacco informatico e relative contromisure

Di seguito si illustrano alcune delle nuove tipologie di attacco - finalizzate a ledere le attività e gli interessi economici dell'azienda - che vanno diffondendosi in connessione con lo sviluppo dell'offerta di nuovi servizi informatici e con l'utilizzo di tecnologie innovative.

7.4.1 Social engineering

Tra le forme di attacco sta assumendo sempre maggiore rilevanza nel contesto informatico la c.d. *social engineering*, che consiste in una particolare tecnica psicologica che sfrutta l'inesperienza e, nella maggior parte dei casi, la buona fede degli utenti per carpire informazioni utili a portare successivi attacchi tecnologici ai sistemi.

Al di là dell'accezione apparentemente positiva della denominazione, il *social engineering* è una delle tecniche di attacco potenzialmente più dannose per la vittima.

Questo attacco ha di solito lo scopo di acquisire informazioni al fine di compiere azioni non consentite dai sistemi di controllo (quali avere accesso a locali o a dati riservati di pertinenza dell'azienda della vittima).

L'attacco è di solito condotto mediante un'impersonificazione, ovvero una sostituzione di identità o, nelle forme più sofisticate, con una pseudo-impersonificazione. In sostanza il soggetto che attacca si presenta, ad esempio mediante contatto telefonico, alla vittima prescelta - che ha accesso a informazioni utili all'attaccante o che svolge attività di controllo – e adotta, con finalità diverse, i seguenti comportamenti o atteggiamenti:

- assertivi: l'attaccante si finge un'altra persona in possesso dell'autorità necessaria a poter derogare alle regole[19] (impersonificazione) e porta il suo attacco usando come elemento di

[18] Ad esempio quando vengono effettuate transazioni di tipo finanziario (richiesta di bonifico, vendita o acquisto di valori, richiesta di informazioni personali, ecc.) o più semplicemente quando si ricevono o spediscono messaggi di posta elettronica (l'utilizzo del palmare con l'ausilio di un GPRS).

[19] Ad esempio si qualifica come una persona che ha una posizione notevolmente più elevata dell'interlocutore in un'altra azienda che ha rapporti con l'azienda cui appartiene la vittima.

coercizione la minaccia implicita di danni che potrebbero derivare alla vittima o alla società se non viene soddisfatta la propria richiesta;

- empatici e spesso allusivi: l'attaccante induce la vittima ad attribuirgli un'identità o un'autorità che in realtà non è quella corretta (pseudo-impersonificazione);
- esplicitamente complici: l'attaccante induce la vittima a violare le regole di controllo nella convinzione che sia bene farlo (manipolazione);
- candidamente corruttivi: l'attaccante propone scambi tra quanto a lui interessa e benefici per la vittima.

Le prime tre modalità hanno in comune il fatto che l'attaccante costruisce situazioni nelle quali la vittima percepisce come lecita o conforme alle regole aziendali l'azione che è indotto a eseguire. Pertanto, questa tipologia di attacco ha buone probabilità di avere successo, considerata anche la frequente presenza di ulteriori circostanze favorevoli all'attaccante:

- scarsa conoscenza da parte della vittima delle responsabilità e dei ruoli aziendali, delle regole e delle prassi operative soprattutto in condizioni non ordinarie o di emergenza;
- scarsa preparazione della vittima in tema di gestione della comunicazione (in modo particolare delle fasi conflittuali e delle interviste);
- sottovalutazione da parte della vittima delle conseguenze delle violazioni.

Contromisure

La possibile difesa da questa tipologia di attacco consiste nell'adozione di sistemi di formalizzazione delle richieste secondo gli standard aziendali e di controllo dell'autenticità dell'interlocutore.

Considerato, inoltre, che gran parte dei danni è spesso causata dalla superficialità e da comportamenti non accorti all'interno dell'azienda, al fine di contenere i rischi di questo tipo di attacco può essere utile effettuare alcuni interventi, quali:

- stabilire norme volte a prevenire l'indebita pubblicizzazione, comunicazione o diffusione di dati e informazioni inerenti all'azienda, sia sul posto di lavoro, sia al di fuori dello stesso, anche in contesti non lavorativi[20];
- prevedere l'obbligo di segnalare qualsiasi contatto dall'esterno di natura sospetta;
- attuare un piano di formazione nei confronti di tutti i dipendenti e dei collaboratori esterni in merito a questo tipo di attacco, alle sue possibili conseguenze e alle relative contromisure;
- svolgere una specifica attività di formazione nei confronti della struttura di *help-desk/customer–care*.

7.4.2 Tecniche varie per l'acquisizione di informazioni

Sono molteplici le tecniche utilizzate dall'attaccante per acquisire informazioni utili. Le più diffuse sono le seguenti:

[20] Predisporre regole da adottare per il comportamento da tenere in viaggio di lavoro, in riunioni con esterni, in conferenze e convegni, nella vita privata circa il lavoro svolto.

sniffing

Consiste in una operazione di intercettazione passiva delle comunicazioni per la cattura di dati; l'attaccante può riuscire a intercettare informazioni e dati di varia natura (password, messaggi di posta elettronica, ecc.). Normalmente questa attività di intercettazione illecita viene effettuata con l'ausilio di strumenti informatici denominati *sniffer* – talora posizionati illecitamente su un sistema di proprietà di un utente inconsapevole – che catturano le informazioni in transito nel punto in cui sono stati installati: si tratta in sostanza di hardware o software - legali e reperibili normalmente in commercio - analizzatori, in grado di intercettare, selezionare per protocollo, tradurre, visualizzare e memorizzare tutti i tipi di pacchetti in transito sulla rete.

Contromisure

Riconoscere la presenza di tali tipologie di strumenti non è sempre facile. Un rilevamento specifico può essere effettuato mediante:

- il controllo locale dello stato dell'interfaccia di rete dei singoli sistemi o la verifica della presenza di schede di rete configurate in modalità promiscua;
- l'utilizzo di software specializzati;
- l'analisi delle segnalazioni delle eventuali "sonde" utilizzate.

Per impedire un attacco della specie, si hanno a disposizione diverse possibilità:

- realizzazione di una topologia di rete sicura adottando tecniche di segmentazione;
- applicazione di funzioni crittografiche per rendere i dati intelligibili al solo legittimo destinatario;
- adozione di sistemi di autenticazione forte;
- preclusione della possibilità di configurare le interfacce di rete in modalità promiscua.

connection hijacking

È un metodo di attacco che riguarda principalmente le transazioni o, comunque, i flussi di dati che transitano da un computer all'altro. Con tale violazione l'intrusore, dopo averne analizzato il flusso, si inserisce materialmente nella transazione alterandone il contenuto e riuscendo a operare con le credenziali di chi legittimamente ha iniziato la sessione.

Contromisure

Si basano generalmente sull'adozione di tecniche crittografiche, utilizzate sia per gestire la cifratura delle informazioni in transito, sia per l'autenticazione dei poli terminali della transazione.

network scanning

È il tentativo di rilevare indirizzi IP o porte TCP al fine di individuare quali servizi o sistemi siano presenti e attivi, per poter successivamente procedere a un tentativo di intrusione.

Contromisure

Adottare *firewall* di rete, *personal firewall* sulle stazioni di lavoro e strumenti di *intrusion detection* che consentano l'attivazione delle forme di reazione più appropriate.

spoofing

Lo *spoofing* non rappresenta un attacco nel senso stretto del termine, ma piuttosto una tecnica complementare a vari tipi di attacco. Consiste nel falsificare l'origine della connessione in modo tale da far credere di essere un soggetto/sistema diverso da quello reale.

Le principali tipologie di *spoofing* sono:

- **User account spoofing**: consiste nell'utilizzo della userid e della password di un altro utente senza averne il diritto. Può essere attuato sfruttando comportamenti non corretti degli utenti o utilizzando strumenti quali *sniffing* e *password crackers*.
- **DNS spoofing**: è il sostituirsi a un *server* DNS[21] lecito nei confronti di un *client* che ha effettuato una richiesta a un *Name Server*.
- **IP Address spoofing**: è l'attacco più diffuso. Si basa sul fatto che la maggior parte dei *routers* all'interno di una rete utilizzano solo l'indirizzo IP di destinazione e non quello di origine. Questo fa sì che un attaccante possa inviare dei pacchetti a un sistema bersaglio utilizzando *source* IP fittizi in maniera che le risposte siano inviate al falso IP indicato dall'attaccante.

Contromisure

La principale contromisura è costituita dall'utilizzo di tecniche crittografiche finalizzate all'autenticazione forte dei soggetti/sistemi coinvolti.

L'IP Address *spoofing* può essere limitato inserendo dei filtri sull'indirizzo IP sorgente a livello di *routers* e *firewall*.

7.4.3 Sfruttamento di servizi non autenticati

L'acquisizione indebita di informazioni o l'attacco di tipo *spoofing* possono essere più agevolmente condotti nei confronti di servizi di rete che non utilizzano tecniche di autenticazione, quali ad esempio:

- **TFTP** (*Trivial Files Transfer Protocol*): è un protocollo che si basa solo sulla gestione degli accessi a livello del *file-system* e può essere sfruttato per acquisire *file* sensibili del sistema;
- **SMTP** (*Simple Mail Transfer Protocol*): si tratta di un diffuso protocollo che non effettua i controlli sulla vera identità degli utenti; pertanto i servizi che si basano su di esso sono soggetti più di altri ad attacchi di tipo *spoofing*;
- **DNS** (*Domain Name Server*): è il sistema che, nel caso sia oggetto di attacco di tipo *spoofing*, può fornire agli utenti richiedenti indirizzi errati.

Contromisure

[21] *Domain Name Server*, ovvero *server* che traduce un nome di dominio nel relativo indirizzo IP.

La migliore contromisura consiste nel disabilitare i servizi che non vengono utilizzati o limitarne l'accesso a soggetti identificati e autenticati. Per quanto riguarda in particolare l'SMTP è raccomandabile l'utilizzo di funzioni crittografiche oltre a quelle di autenticazione.

7.4.4 Malicious code

Questo termine, che ha come sinonimi "*malware"* e "*MMC (Malicious Mobile Code*)", si riferisce a quella famiglia di software che ha come obiettivo il danneggiamento, totale o parziale, o l'alterazione del funzionamento di un sistema informatico/telematico.

Alcune forme di codice malevolo, quali virus, *worm, trojan horse, mass mailing* e *mixed mmc,* sono in grado di autoinstallarsi, di autoriprodursi, di diffondersi, di determinare alterazioni del corretto funzionamento del sistema e anche di esportare i dati o di prendere il controllo del sistema stesso, spesso sfruttando vulnerabilità presenti nei software di sistema e/o applicativi.

Contromisure

Si richiamano di seguito le principali cautele da adottare per contrastare eventuali infezioni da *malicious code*:

- utilizzare solo software "certificato";
- assegnare al software solo i privilegi minimi necessari;
- innalzare e mantenere elevato il livello di sicurezza delle stazioni di lavoro;
- aggiornare tempestivamente i software anti-virus;
- applicare tempestivamente al software le correzioni (*patch*) rilasciate dai produttori;
- utilizzare specifici software antivirus in grado di rilevare i *malicious code* analizzando i flussi informativi in transito o sui sistemi;
- sensibilizzare tutto il personale con riferimento ai rischi inerenti all'introduzione di software estraneo sulle postazioni di lavoro.

7.4.5 Denial of Service (DoS)

È una tipologia di attacco che ha come obiettivo la riduzione o l'annullamento della capacità di utilizzo di una risorsa e agisce attraverso la produzione di un sovraccarico dell'impegno della risorsa stessa; tale attacco si può realizzare, ad esempio, attraverso l'invio di un flusso massiccio di dati verso uno o più sistemi con l'obiettivo finale di mandarli in *crash* o di rendere talmente lenti i tempi di risposta da bloccare di fatto qualsiasi operazione. Gli attacchi diretti a un determinato sistema possono essere attivati localmente oppure tramite rete da sistemi esterni. Inoltre, si possono distinguere due tipologie di DoS[22]:

- **esaurimento di banda:** la tecnica consiste nel sovraccaricare la rete bersaglio in modo da consumarne tutta l'ampiezza di banda;
- **esaurimento delle risorse elaborative:** consiste nel colpire direttamente un sistema, attraverso un consumo straordinario delle risorse della macchina (cicli CPU, memoria).

[22] Per completezza si richiamano gli attacchi di tipo *distributed denial of service* (DDOS) e gli atti dimostrativi telematici (*netstrike*) condotti su larga scala da una platea di attori eterogenea e distribuita.

Va rilevato come sono oggi disponibili software particolarmente aggressivi in grado di automatizzare i processi di attacco, con la conseguenza che anche un dilettante può portare un attacco DoS anche senza capirne il funzionamento o rendersi conto di cosa stia esattamente facendo.

Contromisure

Oltre alle contromisure già indicate, si possono indicare le seguenti:

- adozione di sistemi di monitoraggio sull'utilizzo delle risorse per rilevare prontamente gli scostamenti da valori medi;
- adozione di sistemi di *intrusion detection*;
- utilizzo di *proxy* e *firewall* a protezione delle connessioni con l'esterno.

7.4.6 Defacement

Il *defacement* di un sito web è un tipo di attacco che consiste nella modifica della *home page* mediante la sostituzione delle immagini e/o dei testi originali. Attraverso questa tecnica si possono perseguire due diversi obiettivi: danneggiare l'immagine di un determinato sito web; trarre in inganno il navigatore facendogli trovare su un sito web informazioni diverse da quelle ricercate.

Contromisure

La prevenzione di tale forma di intrusione può essere realizzata adottando le contromisure già previste per il *Denial of Service*.

7.4.7 Gestione degli incidenti di sicurezza

Oltre all'attivazione delle specifiche contromisure preventive appena descritte, l'azienda deve dotarsi di un adeguato apparato di reazione, pronto a intervenire secondo schemi predefiniti che contemplino in modo dettagliato la tipologia dei possibili incidenti, le conseguenti azioni da intraprendere e le funzioni aziendali che devono essere coinvolte.

È necessario innanzi tutto costituire un *Incident Response Team* (IRT), composto da elementi puntualmente individuati in grado di intervenire all'occorrenza, ben addestrati e agevolmente reperibili anche al di fuori dell'orario di lavoro. Tali elementi devono possedere, tra le proprie caratteristiche personali, anche la capacità di operare con efficacia in condizioni difficili, in un clima di stretta collaborazione con gli altri soggetti coinvolti. Particolare attenzione deve essere riservata all'individuazione della figura del coordinatore dell'IRT, che assume la responsabilità della conduzione del lavoro e che è tenuto a curare anche il *reporting* finale dell'incidente.

La gestione degli incidenti di sicurezza va comunque attuata secondo un piano di azione che deve essere preventivamente formalizzato, adeguatamente testato e manutenuto. Tale piano deve prevedere almeno le seguenti fasi:

- rilevazione dell'incidente, utilizzando idonei strumenti, tecnici e organizzativi; è importante che in questa fase siano considerati incidenti anche quegli avvenimenti che potrebbero poi non rivelarsi tali; è infatti preferibile gestire un falso allarme che ignorare un reale incidente;
- attivazione della figura individuata come responsabile dell'IRT;

- accertamento della natura e dell'entità dell'incidente e coinvolgimento dei diversi comparti aziendali interessati e degli opportuni livelli decisionali e, laddove sussistano gli estremi di un possibile reato, segnalazione alle Autorità competenti, in particolare al Servizio di Polizia Postale e delle Comunicazioni[23] (si fa rinvio all'Allegato 8 per un'elencazione delle principali disposizioni di legge inerenti ai crimini informatici);
- documentazione dei dettagli dell'evento, attivazione delle misure di contrasto e ripristino delle condizioni di funzionamento normale ovvero degradato, prospettando in quest'ultimo caso tempi e modi per il completo ripristino;
- dichiarazione della fine dell'emergenza e redazione del rapporto finale.

Al termine del processo, è opportuno verificare l'eventuale necessità di effettuare interventi organizzativi e tecnologici in modo da ridurre la possibilità che l'incidente si ripeta.

[23] Il Servizio di Polizia Postale e delle Comunicazioni costituisce l'organo centrale del Ministero dell'Interno per la sicurezza e la regolarità dei servizi delle telecomunicazioni. Il Servizio opera a livello periferico attraverso i Compartimenti di Polizia Postale e le Sezioni provinciali, avvalendosi di risorse distribuite sul territorio, sia investigative sia tecniche. Al Servizio sono affidate le seguenti competenze:

- prevenzione e repressione dei reati postali;
- studio, analisi e contrasto dei crimini informatici ovvero dei reati commessi attraverso l'uso di mezzi di comunicazione ad alta tecnologia quali, ad esempio, le violazioni del diritto d'autore, le frodi e pedofilia on-line;
- formazione specialistica del personale;
- instaurazione di relazioni internazionali finalizzate allo studio dei fenomeni criminali e alla collaborazione investigativa.

8 Considerazioni sui costi della sicurezza

La sicurezza dei sistemi informativi è un tema che travalica le competenze esclusive del settore ICT, sia perché le *policy* di sicurezza tendono oggi a porre l'enfasi anche sulla sensibilizzazione delle risorse umane oltre che sugli aspetti puramente tecnologici, sia per il crescente coinvolgimento delle *business unit*, ossia delle strutture proprietarie dei dati.

Da ciò discende la necessità di compendiare in un unico schema le informazioni relative agli investimenti e alle spese in materia di sicurezza effettuati nell'azienda in modo da poter avere una rappresentazione completa a livello aziendale del costo totale della sicurezza informatica e poterne verificare l'andamento nel corso del tempo e rispetto ai mutamenti del contesto, sia interno sia esterno.

In altre parole, il budget della sicurezza dei sistemi informativi deve poter raccogliere tutte le voci a essa riconducibili, ovvero sia i costi direttamente imputabili alla struttura specialistica della sicurezza informatica, sia quelli di competenza di altre strutture aziendali.

I costi direttamente imputabili alla struttura specialistica (cfr. schema riportato in Allegato 9) possono essere, a loro volta, riferiti alla componente progettuale, cioè relativa allo studio e all'adeguamento delle architetture di sicurezza, e a quella gestionale e operativa. Tra i costi direttamente imputabili alla sicurezza informatica vanno contabilizzati gli investimenti e le spese relative al personale, ai posti di lavoro, ai locali utilizzati, agli apparati e ai software utilizzati, alle consulenze e ai servizi di assistenza specialistica, ecc.

Ovviamente, ove le strutture o le risorse specialistiche utilizzate siano in comune con le altre funzioni ICT, va riportata la quota parte di tali costi direttamente imputabile alla sicurezza. In questo caso può essere valutata l'opportunità di suddividere i costi in: direttamente sostenuti dalla struttura di sicurezza; ribaltati dagli altri settori ICT.

Ogni voce indicata (hardware, software di base, ecc.) va suddivisa in acquisizioni iniziali, canoni di manutenzione, noleggi e licenze.

I costi non direttamente imputabili alla struttura di sicurezza (cfr. Allegato 10) sono quelli sostenuti da altri comparti del settore ICT e da altre *business unit* dell'azienda in relazione alla materia della sicurezza informatica. Altri costi di cui è opportuno tenere conto in questa sezione sono quelli connessi con la sicurezza fisica e con la stipula delle polizze assicurative, nelle componenti strettamente attinenti alle competenze del settore ICT. Anche in questa sezione le voci di costo vanno suddivise per acquisizioni iniziali, canoni di manutenzione, noleggi, licenze, ecc.

La suddivisione delle informazioni di costo nelle categorie suggerite consente al management aziendale di:

- monitorare l'andamento dei costi suddivisi per le componenti di struttura, architetturali e gestionali, per *business unit* e per strutture divisionali;

[24] Per gli investimenti è consigliabile un periodo di ammortamento di tre anni, data la rapida obsolescenza tecnologica degli apparati hardware e software di quest'area.

- fornire al vertice aziendale una rappresentazione del costo complessivo della sicurezza (*Total Cost of Ownership*) a fronte dell'andamento dell'indice di esposizione dell'azienda ai rischi informatici;

- relazionare sugli scostamenti rispetto al budget;

- relazionare sul costo dei progetti avviati e terminati;

- proporre il nuovo budget di funzionamento della struttura.

Allegato 1 Classificazione delle minacce

Errori e malfunzionamenti	Descrizione
Errori in fase di progettazione iniziale/evolutiva	Si tratta di errori od omissioni nell'impostazione dell'architettura tecnologica o applicativa, che provocano disservizi e impattano sulla riservatezza, sulla integrità o sulla disponibilità dei dati.
Errori in fase di *back-up*	Si tratta di malfunzionamento delle procedure di *back-up* che può determinare una perdita di integrità durante la trasmissione o la memorizzazione dei dati.
Errori in fase di aggiornamento e manutenzione del software	A causa di errori nell'installazione o per incompatibilità con altro software, si può determinare una perdita/diminuzione della disponibilità di servizio e/o della integrità dei dati.
Errori in fase di aggiornamento e di manutenzione dell'hardware	Vi sono dei rischi sia per quanto riguarda un eventuale malfunzionamento dei singoli dispositivi, sia per quanto riguarda la loro compatibilità reciproca, con conseguente perdita di disponibilità del servizio e/o di integrità dei dati.
Errori in fase di aggiornamento e di manutenzione della rete	Durante l'aggiornamento o manutenzione della rete si possono verificare delle interruzioni nella erogazione del servizio o perdita di informazioni.
Malfunzionamento software (sia di sistema sia applicativo)	Il malfunzionamento del software, che può essere determinato da errori dell'operatore o da cause tecnologiche, può comportare disservizi (ritardi nell'erogazione del servizio) ed errori. Inoltre, può esporre il sistema alla perdita di disponibilità e/o di integrità dei dati elaborati. Non esiste recovery.
Malfunzionamento hardware	Generato da un errore dell'operatore ovvero da cause tecnologiche, può determinare disservizi (ritardi nell'erogazione del servizio) ed errori. Inoltre, può esporre il sistema alla perdita di integrità e/o disponibilità dei dati elaborati.
Malfunzionamento della rete	Problemi con la rete di comunicazione possono comportare la perdita di disponibilità del servizio.
Sovrascrittura della memoria di massa	La memorizzazione di dati su supporti interni o esterni al sistema comporta il rischio di cancellazione di dati ancora operativamente validi.
Sovraccarico elaborativo del sistema	L'avvio di processi elaborativi autoiterativi o mal dimensionati può provocare la saturazione delle capacità elaborative e della memoria, causando l'indisponibilità del sistema.
Sovraccarico delle linee di trasmissione	L'avvio di processi elaborativi autoiterativi o mal dimensionati può provocare la saturazione della banda disponibile delle linee di trasmissione causandone l'indisponibilità. Occorre pertanto prevedere, in tali casi, la raggiungibilità dei sistemi da punti alternativi.

Frodi e furti	Descrizione
Furto di hardware	Può comportare il rischio di indisponibilità del sistema e/o di perdita della riservatezza dei dati.
Acquisizione illecita o esportazione illegale di software	Un'acquisizione illecita (furto e/o copia) o un'esportazione illegale di software possono comportare una perdita patrimoniale e di immagine aziendale con eventuali ricadute legali ex D.Lgs. 518/92 (copia di software di licenze acquistate).
Acquisizione di dati da supporti cartacei	Conoscenza/appropriazione di informazioni critiche concernenti i sistemi informatici disponibili su supporti cartacei non opportunamente conservati o riutilizzati per altri scopi con conseguente perdita di riservatezza e disponibilità.
Acquisizione dati su supporti magnetici	Conoscenza/appropriazione di informazioni critiche disponibili su supporti magnetici non opportunamente conservati oppure riutilizzati senza essere stati adeguatamente cancellati.
Manipolazione di software e dati	Alterazione di programmi e di informazioni per scopi illeciti.
Uso improprio di privilegi	Utilizzo illecito e illegittimo di risorse informatiche.

Software dannoso	Descrizione
Introduzione di software dannoso	L'introduzione volontaria/involontaria di software dannoso (es. virus, "bombe logiche", *trojan horse*) per mezzo di file presenti su *floppy disk*, CDROM o in rete, può - oltre a compromettere l'integrità, la riservatezza e la disponibilità dei dati - impedire il funzionamento del sistema e quindi l'erogazione del servizio.

Danneggiamenti fisici	Descrizione
Indisponibilità dei sistemi in seguito a eventi ineluttabili (naturali e non)	Il sistema può essere esposto a fenomeni, naturali e non, ineluttabili; è necessario, pertanto, prevedere soluzioni di emergenza per scongiurare il protrarsi dei disservizi e la perdita di dati.
Inagibilità dei locali	Derivante da cause naturali o umane, essa comporta il pericolo di interruzione del servizio.
Danneggiamento delle reti	Le linee di trasmissione, spesso non assistite da adeguate protezioni fisiche, possono essere involontariamente danneggiate nel corso di lavori, con conseguente interruzione del traffico.
Danneggiamento hardware (dispositivi, schede)	Il danneggiamento dell'hardware può comportare la perdita di disponibilità del sistema e dell'integrità dei dati.
Interruzione servizi elettrici, condizionamento d'aria	Possono causare l'interruzione del servizio e il danneggiamento delle risorse.

Altre minacce esterne	Descrizione
Accesso non autorizzato al sistema	L'accesso (locale/remoto) non autorizzato al sistema espone lo stesso a numerosi pericoli, quali l'acquisizione indebita di informazioni, l'alterazione tramite introduzione di nuovi dati, la modifica/cancellazione/spostamento dei dati esistenti.
Modifica non autorizzata dei privilegi	La modifica dei privilegi da parte di persone non autorizzate comporta gli stessi rischi dell'accesso non autorizzato, con l'aggravante dell'esercizio indebito del potere di modifica.
Mascheramento dell'identità dell'utente	Il mascheramento dell'identità dell'utente è una forma particolare di accesso non autorizzato che comporta i medesimi rischi di quest'ultimo.
Alterazione instradamento di rete	Si tratta dell'alterazione dei percorsi dei dati sulla rete, allo scopo di inficiare il funzionamento del sistema, sottrarre dati e/o informazioni.
Intercettazione del traffico di rete	Attraverso apposito software è possibile visualizzare il traffico di rete al fine di intercettare e/o modificare i dati trasmessi.
Sovraccarico del sistema elaborativo/trasmissivo	Saturazione delle capacità elaborative o della banda disponibile a seguito di attacchi tramite appositi software.

Altre minacce interne	Descrizione
Manipolazione di software	Si esplica nella manipolazione del software applicativo con l'obiettivo di sabotarne il corretto funzionamento con conseguente perdita di integrità dei dati.
Abuso di privilegi	La minaccia consiste nell'esercizio improprio dei privilegi, goduti in virtù del ruolo aziendale, al fine di attuare azioni illecite sul sistema e/o sui dati.
Utilizzo illecito del sistema (hardware/software/rete)	Si intende l'utilizzo non autorizzato del sistema al fine di sfruttarne illecitamente le potenzialità elaborative, con conseguente degrado delle prestazioni.
Trattamento illecito di dati personali (cfr. Codice in materia di protezione dei dati personali – D. Lgs. n. 196/2003)	La violazione della legislazione vigente in materia di privacy può comportare sanzioni amministrative e penali a carico dei responsabili aziendali.
Sovraccarico del sistema elaborativo/trasmissivo.	Saturazione delle capacità elaborative o della banda disponibile a seguito di attacchi tramite appositi software.

Allegato 2 Classificazione dei danni

Danni economici	Descrizione
Sanzioni conseguenti a un trattamento non corretto dei dati personali	Si fa riferimento alle sanzioni civili previste dal D. Lgs. 196/2003. Questo evento, le cui conseguenze possono anche essere di tipo penale, può determinare inoltre un danno di immagine.
Riduzione di fatturato/flusso di cassa	È uno dei possibili danni derivanti dalla compromissione dell'operatività aziendale conseguente all'alterazione, alla perdita o all'intercettazione dei dati; in quest'ambito, rilevano anche i possibili danni connessi con i ritardi nell'elaborazione dei flussi finanziari.
Riduzione dell'efficienza operativa	L'alterazione o la perdita di dati può compromettere la qualità dei processi di gestione e di controllo dai quali dipende l'efficiente funzionamento dell'azienda.
Costi di ripristino	Sono le spese che l'azienda deve sostenere per ripristinare la situazione antecedente all'evento dannoso.
Risarcimento danni a terzi	Il verificarsi di un evento dannoso (es. alterazioni delle informazioni o delle transazioni economiche dirette alle terze parti) può determinare responsabilità contrattuali o extra-contrattuali dell'azienda nei confronti di terzi.
Pagamento multe/penali	Il verificarsi di un evento dannoso può determinare violazioni contrattuali con conseguente soggezione al pagamento di multe e penali.

Danni di immagine	Descrizione
Perdita di competitività	Il verificarsi di eventi dannosi può determinare un degrado dei servizi offerti alla clientela con conseguenti riflessi negativi sulla capacità dell'azienda di mantenere o migliorare le posizioni di mercato acquisite.
Danni all'immagine verso l'esterno	Il verificarsi di eventi dannosi può incidere sull'immagine e sulla credibilità dell'azienda nei confronti di clienti, partner e fornitori, comportando, in prospettiva, possibili perdite economiche.

Danni di immagine	Descrizione
Danni all'immagine verso l’interno	Eventuali perdite o alterazione dei dati aziendali possono comportare tensioni interne con riflessi negativi sulla produttività del personale e possibile aumento delle controversie legali.

Allegato 3 Contromisure tecnologiche e organizzative

Contromisure tecnologiche	Descrizione
Identificazione e autenticazione	Il sistema di protezione deve identificare e autenticare univocamente gli utenti che intendono ottenere l'accesso a un sistema elaborativo o trasmissivo. L'identificazione e l'autenticazione devono essere effettuate prima di ulteriori interazioni operative tra il sistema e l'utente; le relative informazioni devono essere memorizzate e accedute solo dagli utenti autorizzati. Sono comprese tra queste funzioni quelle di mutua autenticazione tra utente e sistema.
Controllo accesso logico	Questa funzione, che ha lo scopo di controllare l'uso delle risorse da parte dei processi e degli utenti, si esplica attraverso la verifica e la gestione dei diritti d'accesso.
Tracciamento	Il sistema deve prevedere il tracciamento delle operazioni che possono influenzare la sicurezza dei dati critici.
Revisione	Si tratta delle attività di analisi degli eventi registrati volte a rilevare e a segnalare eventi anomali che, discostandosi da standard, soglie e prassi stabilite, possono essere indicativi di eventuali minacce.
Strumenti per il riutilizzo di supporti di memoria in condizioni di sicurezza	Si tratta di strumenti per la cancellazione o l'inizializzazione di supporti riutilizzabili (dischi, nastri, memorie, ecc.) al fine di permetterne il riutilizzo senza problemi di sicurezza.
Ridondanza delle risorse elaborative	Si tratta dei processi e meccanismi che garantiscono la ridondanza delle risorse al fine di un loro ripristino in tempi brevi in caso di indisponibilità dei supporti (es. *mirroring* dei dischi, salvataggi periodici).
Protezione del trasferimento dati	Si tratta degli strumenti adottati per assicurare riservatezza, integrità e disponibilità ai canali trasmissivi e alle componenti di *networking*.

Contromisure organizzative	Descrizione
Formazione e comunicazione	Si tratta degli interventi formativi e/o di comunicazione inerenti alla sicurezza volti a sensibilizzare tutti gli utenti e/o particolari figure professionali.

Contromisure organizzative	Descrizione
Elaborazione delle *policy*	Devono essere previste la redazione, la diffusione e la conservazione dei documenti normativi, tecnici e di indirizzo necessari per un corretto utilizzo del sistema informatico da parte degli utenti e per una efficiente amministrazione della sicurezza da parte delle funzioni aziendali a ciò preposte.
Strumenti di gestione delle risorse	Si tratta delle procedure organizzative volte ad assicurare il corretto utilizzo dei beni aziendali.

Allegato 4 Contromisure di natura comportamentale

Presupposto fondamentale per l'attuazione di un efficace sistema di contromisure è la presa di coscienza, da parte di tutti i soggetti coinvolti nell'amministrazione della sicurezza del sistema informatico, delle vulnerabilità del sistema stesso e della necessità di adottare una serie di comportamenti atti a prevenire eventi dannosi o a intervenire tempestivamente al loro verificarsi.

1) <u>Comportamenti da adottare a fini di prevenzione:</u>

- stabilire un piano di sicurezza e farlo rispettare;
- conservare i log di sistema su supporti non alterabili;
- testare periodicamente la sicurezza della rete;
- ridurre al minimo il numero di modem nella rete;
- non tenere collegata alla rete una macchina non utilizzata;
- disattivare i servizi e i software non necessari;
- operare regolarmente controlli sullo stato di attività delle porte locali[25];
- cancellare tempestivamente gli *account* di coloro che lasciano l'azienda;
- fare regolarmente il *back-up* dei dati critici, sensibili e personali;
- utilizzare sempre utenze con i privilegi minimi necessari per il lavoro corrente;
- utilizzare e far utilizzare password complesse[26];
- usare sempre antivirus, ossia:
  - installare un antivirus su ogni macchina e permetterne l'attivazione prima di ogni altra operazione;
  - controllare almeno quotidianamente l'eventuale rilascio di impronte virali aggiornate;
  - operare tempestivamente l'aggiornamento del motore dell'antivirus e/o delle impronte virali;
  - operare con regolarità lo *scan* di tutti i file presenti sull'*hard disk* (non solo programmi ed eseguibili);
- non aprire mai allegati di posta provenienti da fonte sconosciuta[27];

---

[25] Questi controlli (effettuabili mediante l'utilizzo di Portscanner o Active Connection Checker) sono finalizzati alla individuazione delle porte di ascolto sul sistema locale. Un successivo controllo con gli elenchi delle porte utilizzate dai *trojan horse* risulta spesso il modo migliore per sondare l'eventuale presenza di *backdoor* attive sulla *workstation***.**

[26] Nella scelta della password, preferire parole con caratteri inconsueti, evitando nomi, termini di senso compiuto e, soprattutto, evitare l'utilizzo della medesima password per più *account*. Evitare assolutamente l'utilizzo di password di lunghezza inferiore ai sei caratteri, prediligendo lunghezze uguali o superiori a otto caratteri. Utilizzare, ove consentito, lettere maiuscole e minuscole, numeri e segni di interpunzione.

[27] È sempre buona norma leggere quanto riportato nei campi "Da – From" e "Oggetto – Subject" e fare massima attenzione al contenuto e all'estensione dell'eventuale allegato. Evitare di aprire allegati con estensione eseguibile o creati con *word processor* a meno che non se ne conosca l'esatta provenienza. In concreto, questo significa che

- fare il tempestivo *download* delle *security patch* dal sito ufficiale dei *vendor*, atteso che la mancata o ritardata applicazione delle *patch* di sicurezza è unanimemente considerata uno dei maggiori fattori di vulnerabilità dei sistemi. Ad esempio, apposite *security patch* vanno installate, qualora disponibili, sui *browser* al fine di prevenire i danni conseguenti all'accesso da parte di un *hacker* ai *cookies*; questi sono file di testo di piccola dimensione che vengono scritti sul disco rigido della postazione di lavoro in fase di consultazione di siti web e forniscono al *server* informazioni riguardo l'attività di consultazione effettuata.

2) <u>Comportamenti da adottare per rilevare tempestivamente l'insorgenza di un problema</u>:

- verificare da *consolle* chi è connesso al sistema;
- verificare periodicamente parti del sistema ritenute critiche;
- verificare periodicamente il contenuto dei log dell'attività sui *server*;
- verificare l'utilizzo di *account* in orari o da sistemi inconsueti;
- analizzare l'eventuale comportamento anomalo di alcuni processi;
- analizzare eventuali rallentamenti non previsti del sistema;
- approfondire eventuali improvvise modifiche dello spazio disponibile sui supporti di massa;
- tenere presente che l'azienda potrebbe non essere l'obiettivo dell'attacco, ma il "ponte" per attaccare terzi.

3) <u>Comportamenti da adottare al verificarsi di incidenti di sicurezza</u>

- reagire all'evento dannoso con la massima tempestività al fine di contenere i danni;
- attivare le procedure previste al fine di preservare le prove dell'attacco o dell'incidente, utili per la successiva attività di indagine;
- non tentare contatti o "duelli" con l'aggressore;
- attivare il comparto aziendale titolato a presentare denuncia/querela;
- attivare i punti di contatto prestabiliti per le emergenze (ad esempio riferendo l'accaduto alla sede provinciale della Polizia Postale e delle Comunicazioni);
- evitare l'utilizzo dei servizi di rete per comunicazioni inerenti all'incidente, ove non si abbia certezza che gli stessi non siano compromessi;
- preservare dati/prove:
  - non effettuare l'arresto del sistema prima di aver raccolto i dati relativi all'attacco;
  - preservare i dati raccolti su supporti non modificabili;
  - eventualmente fare ulteriori verifiche su copie delle memorie di massa;
  - documentare e giustificare eventuali modifiche apportate ai dati;

---

occorre diffidare dei files aventi, a puro titolo esemplificativo, estensione COM, EXE, VBS, SCR, DLL, INI, VXD, SYS, JS, JSE, DOC, DOT, XL, XLS, XLA, XLC, XLM, XLW, PIF, MTM e quelli con doppia estensione. È consigliabile, comunque, essere sempre cauti dal momento che anche un allegato trasmesso da persona conosciuta non è escluso che risulti infetto all'insaputa dello stesso mittente.

- durante un attacco, se possibile, attivare processi di monitoraggio dell'attività in LAN;

- raccogliere dati/prove:
  - dai file di log del *web server* o del *firewall* registrati anche precedentemente all'incidente;
  - dai file di log del sistema compromesso e dai relativi *user log*, anche conservati su supporti di *back-up*;
  - controllare i messaggi e-mail ricevuti prima dell'attacco;
  - verificare la possibilità di recuperare dati o file cancellati dall'aggressore prima di reinstallare il sistema;
- interagire con la Polizia Postale e delle Comunicazioni fornendo:
  - una topologia della rete;
  - i log relativi all'incidente;
  - una relazione dettagliata, anche tecnica, sull'accaduto;
  - assistenza al personale incaricato delle indagini;
  - le generalità del personale di eventuali fornitori esterni di servizi in grado di prestare assistenza (in caso, ad esempio, di servizi di *hosting*, *housing*, ecc.);
- stimare i danni in termini di :
  - tempo impiegato dal personale per ripristinare il sistema;
  - riduzione della produttività degli utenti durante l'indisponibilità dei sistemi;
  - aggiornamento e/o necessità di acquisto di nuovi software e hardware;
  - costi per assistenze e consulenze.

Allegato 5 Contenuti di *policy* in materia di controllo logico degli accessi

Identificazione e Autenticazione

La fase di identificazione e autenticazione degli utenti è particolarmente critica per la salvaguardia dei sistemi e pertanto assume particolare rilevanza la fissazione nella *policy* delle regole di gestione degli elementi identificativi (userid e password) e delle procedure di logon.

Gli identificativi utente (userid) che garantiscono che le attività svolte possano essere ricondotte a specifiche persone:

- non devono fornire indicazioni sui livelli di privilegio e sul profilo dell'utente a cui sono assegnati;
- devono essere strettamente personali; utenze di gruppo possono essere previste limitatamente a casi specifici previa autorizzazione dell'adeguato livello di management;
- possono essere vincolati a operare su specifici terminali.

Le password devono:

- essere generate, secondo regole di qualità[28], in modo tale che siano difficili da scoprire da parte di personale non autorizzato;
- avere una lunghezza elevata affinché la ricostruzione delle stesse non risulti troppo facile; al riguardo, si può prendere a riferimento quanto stabilito dalla normativa in materia di protezione dei dati personali, secondo la quale le password utilizzate nei sistemi che trattano dati della specie devono avere una lunghezza minima di 8 caratteri (cfr. allegato 6);
- essere distribuite agli utenti secondo modalità tali da salvaguardarne la riservatezza;
- essere memorizzate in modo tale da garantire che nessuno, neanche l'Amministratore di Sistema, possa venirne a conoscenza;
- essere aggiornate autonomamente dall'utente, secondo modalità che garantiscano il mantenimento della loro riservatezza;
- essere modificate obbligatoriamente dall'utente al primo accesso;
- avere un periodo massimo di validità alla scadenza del quale l'aggiornamento da parte dell'utente è obbligatorio; in ogni eventualità di aggiornamento, il sistema non deve accettare una password precedentemente utilizzata dallo stesso utente.

Le procedure di logon devono:

- non fornire informazioni sulle applicazioni e sui sistemi dei quali controllano l'accesso, finché il processo di autorizzazione non venga completato;

[28] La password dovrebbe essere non facilmente identificabile, cioè non associata a parole o a nomi riconducibili in qualche modo al titolare dell'*account*, quali, ad esempio: il nome dei familiari o date rilevanti. Non deve inoltre coincidere con lo userid, né essere un termine esistente sul dizionario.

- non fornire informazioni di supporto alle azioni che devono essere compiute dall'utente per completare il logon, al fine di evitare che utenti non autorizzati traggano beneficio da questi suggerimenti;
- non informare l'utente su eventuali errori che potrebbero interrompere il processo autorizzativo;
- limitare il numero di tentativi di logon permessi per fallimento del processo:
  - registrando tutti tali tentativi (ora, utente);
  - forzando un tempo di ritardo per la riattivazione della procedura;
  - interrompendo le connessioni al raggiungimento del limite di tentativi previsto;
- fornire evidenza, al momento della connessione, circa:
  - l'ultima connessione valida (data, utente, ora);
  - i tentativi di connessione falliti dall'ultima connessione valida;
- impedire la connessione con il medesimo *account* da terminali diversi nello stesso momento.

Gestione degli accessi

Devono essere presenti meccanismi di gestione degli accessi alle risorse che consentano di:

- individuare a quali risorse un determinato utente può accedere;
- determinare quali attività l'utente può compiere su quelle specifiche risorse;
- revisionare periodicamente i poteri di accesso degli utenti a cura dei responsabili delle risorse;
- limitare alle persone che ne hanno effettiva necessità l'utilizzo di funzioni privilegiate;
- registrare e controllare l'utilizzo delle funzioni privilegiate; in particolare devono essere opportunamente registrati tutti gli interventi effettuati in situazioni di emergenza;
- aggiornare tempestivamente i privilegi non più necessari sulla base di puntuali comunicazioni;
- definire chiaramente i requisiti aziendali per l'accesso al sistema da parte di terzi.

Accounting* e *audit

Per *accounting* si intende l'insieme dei meccanismi attraverso i quali è effettuata la raccolta di informazioni utili per l'analisi a posteriori degli eventi[29], con particolare riferimento agli incidenti di sicurezza.

L'accesso ai dati rilevati deve essere protetto e il suo utilizzo deve essere limitato a ben precise utenze.

Le misure da intraprendere per poter disporre di un sistema di tracciabilità sono:

[29] Ai fini della precisa registrazione dell'istante in cui l'evento è accaduto, è necessario che tutti gli orologi dei sistemi connessi siano sincronizzati.

- adottare sistemi di identificazione/autenticazione che garantiscano l’identità dell’utente e l’impossibilità di praticare tecniche di impersonificazione;
- adottare adeguate *policy* di classificazione delle risorse e di controllo degli accessi;
- generare, per ogni evento particolarmente rilevante sotto il profilo della sicurezza, una registrazione (log) su un opportuno *database*, che deve essere messo al riparo da possibili danneggiamenti o manomissioni. Il *database* conterrà, quindi, una storia (*audit trail*) di tutti gli eventi rilevanti avvenuti nel sistema;
- prevedere un dimensionamento e una modalità di trattamento di tali file che garantisca la conservazione delle informazioni per un periodo commisurato alle esigenze aziendali e alle disposizioni di legge vigenti;
- adottare un controllo della configurazione di sistema in grado di evidenziare prontamente ogni difformità rispetto alla configurazione "certificata".

Le tracce della registrazione dei file di log devono essere sottoposte ad audit per verificare che gli utenti effettuino solo processi esplicitamente autorizzati.

Gli *account* degli amministratori di sistema, che godono di utenze privilegiate, devono essere sottoposti a controlli più stringenti.

Allegato 6 Disciplinare tecnico in materia di misure minime di sicurezza

(Allegato B al Decreto legislativo n. 196 del 30 giugno 2003)

(Artt. da 33 a 36 del codice)

Trattamenti con strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile ove designato e dell'incaricato, in caso di trattamento con strumenti elettronici:

Sistema di autenticazione informatica

1. Il trattamento di dati personali con strumenti elettronici è consentito agli incaricati dotati di credenziali di autenticazione che consentano il superamento di una procedura di autenticazione relativa a uno specifico trattamento o a un insieme di trattamenti.

2. Le credenziali di autenticazione consistono in un codice per l'identificazione dell'incaricato associato a una parola chiave riservata conosciuta solamente dal medesimo oppure in un dispositivo di autenticazione in possesso e uso esclusivo dell'incaricato, eventualmente associato a un codice identificativo o a una parola chiave, oppure in una caratteristica biometrica dell'incaricato, eventualmente associata a un codice identificativo o a una parola chiave.

3. Ad ogni incaricato sono assegnate o associate individualmente una o più credenziali per l'autenticazione.

4. Con le istruzioni impartite agli incaricati è prescritto di adottare le necessarie cautele per assicurare la segretezza della componente riservata della credenziale e la diligente custodia dei dispositivi in possesso ed uso esclusivo dell'incaricato.

5. La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito; essa non contiene riferimenti agevolmente riconducibili all'incaricato ed è modificata da quest'ultimo al primo utilizzo e, successivamente, almeno ogni sei mesi. In caso di trattamento di dati sensibili e di dati giudiziari la parola chiave è modificata almeno ogni tre mesi.

6. Il codice per l'identificazione, laddove utilizzato, non può essere assegnato ad altri incaricati, neppure in tempi diversi.

7. Le credenziali di autenticazione non utilizzate da almeno sei mesi sono disattivate, salvo quelle preventivamente autorizzate per soli scopi di gestione tecnica.

8. Le credenziali sono disattivate anche in caso di perdita della qualità che consente all'incaricato l'accesso ai dati personali.

9. Sono impartite istruzioni agli incaricati per non lasciare incustodito e accessibile lo strumento elettronico durante una sessione di trattamento.

10. Quando l'accesso ai dati e agli strumenti elettronici è consentito esclusivamente mediante uso della componente riservata della credenziale per l'autenticazione, sono impartite idonee e preventive disposizioni scritte volte a individuare chiaramente le modalità con le quali il titolare può assicurare la disponibilità di dati o strumenti elettronici in caso di prolungata assenza o

impedimento dell'incaricato che renda indispensabile e indifferibile intervenire per esclusive necessità di operatività e di sicurezza del sistema. In tal caso la custodia delle copie delle credenziali è organizzata garantendo la relativa segretezza e individuando preventivamente per iscritto i soggetti incaricati della loro custodia, i quali devono informare tempestivamente l'incaricato dell'intervento effettuato.

11. Le disposizioni sul sistema di autenticazione di cui ai precedenti punti e quelle sul sistema di autorizzazione non si applicano ai trattamenti dei dati personali destinati alla diffusione.

Sistema di autorizzazione

12. Quando per gli incaricati sono individuati profili di autorizzazione di ambito diverso è utilizzato un sistema di autorizzazione.

13. I profili di autorizzazione, per ciascun incaricato o per classi omogenee di incaricati, sono individuati e configurati anteriormente all'inizio del trattamento, in modo da limitare l'accesso ai soli dati necessari per effettuare le operazioni di trattamento.

14. Periodicamente, e comunque almeno annualmente, è verificata la sussistenza delle condizioni per la conservazione dei profili di autorizzazione.

Altre misure di sicurezza

15. Nell'ambito dell'aggiornamento periodico con cadenza almeno annuale dell'individuazione dell'ambito del trattamento consentito ai singoli incaricati e addetti alla gestione o alla manutenzione degli strumenti elettronici, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

16. I dati personali sono protetti contro il rischio di intrusione e dell'azione di programmi di cui all'art. 615-quinquies del codice penale, mediante l'attivazione di idonei strumenti elettronici da aggiornare con cadenza almeno semestrale.

17. Gli aggiornamenti periodici dei programmi per elaboratore volti a prevenire la vulnerabilità di strumenti elettronici e a correggerne difetti sono effettuati almeno annualmente. In caso di trattamento di dati sensibili o giudiziari l'aggiornamento è almeno semestrale.

18. Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.

Documento programmatico sulla sicurezza

19. Entro il 31 marzo di ogni anno, il titolare di un trattamento di dati sensibili o di dati giudiziari redige anche attraverso il responsabile, se designato, un documento programmatico sulla sicurezza contenente idonee informazioni riguardo:

19.1. l'elenco dei trattamenti di dati personali;

19.2. la distribuzione dei compiti e delle responsabilità nell'ambito delle strutture preposte al trattamento dei dati;

19.3. l'analisi dei rischi che incombono sui dati;

19.4. le misure da adottare per garantire l'integrità e la disponibilità dei dati, nonché la protezione delle aree e dei locali, rilevanti ai fini della loro custodia e accessibilità;

19.5. la descrizione dei criteri e delle modalità per il ripristino della disponibilità dei dati in seguito a distruzione o danneggiamento di cui al successivo punto 23;

19.6. la previsione di interventi formativi degli incaricati del trattamento, per renderli edotti dei rischi che incombono sui dati, delle misure disponibili per prevenire eventi dannosi, dei profili della disciplina sulla protezione dei dati personali più rilevanti in rapporto alle relative attività, delle responsabilità che ne derivano e delle modalità per aggiornarsi sulle misure minime adottate dal titolare. La formazione è programmata già al momento dell'ingresso in servizio, nonché in occasione di cambiamenti di mansioni, o di introduzione di nuovi significativi strumenti, rilevanti rispetto al trattamento di dati personali;

19.7. la descrizione dei criteri da adottare per garantire l'adozione delle misure minime di sicurezza in caso di trattamenti di dati personali affidati, in conformità al codice, all'esterno della struttura del titolare;

19.8. per i dati personali idonei a rivelare lo stato di salute e la vita sessuale di cui al punto 24, l'individuazione dei criteri da adottare per la cifratura o per la separazione di tali dati dagli altri dati personali dell'interessato.

Ulteriori misure in caso di trattamento di dati sensibili o giudiziari

20. I dati sensibili o giudiziari sono protetti contro l'accesso abusivo, di cui all'art. 615-ter del codice penale, mediante l'utilizzo di idonei strumenti elettronici.

21. Sono impartite istruzioni organizzative e tecniche per la custodia e l'uso dei supporti rimovibili su cui sono memorizzati i dati al fine di evitare accessi non autorizzati e trattamenti non consentiti.

22. I supporti rimovibili contenenti dati sensibili o giudiziari se non utilizzati sono distrutti o resi inutilizzabili, ovvero possono essere riutilizzati da altri incaricati, non autorizzati al trattamento degli stessi dati, se le informazioni precedentemente in essi contenute non sono intelligibili e tecnicamente in alcun modo ricostruibili.

23. Sono adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.

24. Gli organismi sanitari e gli esercenti le professioni sanitarie effettuano il trattamento dei dati idonei a rivelare lo stato di salute e la vita sessuale contenuti in elenchi, registri o banche di dati con le modalità di cui all'articolo 22, comma 6, del codice, anche al fine di consentire il trattamento disgiunto dei medesimi dati dagli altri dati personali che permettono di identificare direttamente gli interessati. I dati relativi all'identità genetica sono trattati esclusivamente all'interno di locali protetti accessibili ai soli incaricati dei trattamenti ed ai soggetti specificatamente autorizzati ad accedervi; il trasporto dei dati all'esterno dei locali riservati al loro trattamento deve avvenire in contenitori muniti di serratura o dispositivi equipollenti; il trasferimento dei dati in formato elettronico è cifrato.

Misure di tutela e garanzia

25. Il titolare che adotta misure minime di sicurezza avvalendosi di soggetti esterni alla propria struttura, per provvedere alla esecuzione riceve dall'installatore una descrizione scritta dell'intervento effettuato che ne attesta la conformità alle disposizioni del presente disciplinare tecnico.

26. Il titolare riferisce, nella relazione accompagnatoria del bilancio d'esercizio, se dovuta, dell'avvenuta redazione o aggiornamento del documento programmatico sulla sicurezza.

Trattamenti senza l’ausilio di strumenti elettronici

Modalità tecniche da adottare a cura del titolare, del responsabile, ove designato, e dell’incaricato, in caso di trattamento con strumenti diversi da quelli elettronici:

27. Agli incaricati sono impartite istruzioni scritte finalizzate al controllo ed alla custodia, per l’intero ciclo necessario allo svolgimento delle operazioni di trattamento, degli atti e dei documenti contenenti dati personali. Nell’ambito dell’aggiornamento periodico con cadenza almeno annuale dell’individuazione dell’ambito del trattamento consentito ai singoli incaricati, la lista degli incaricati può essere redatta anche per classi omogenee di incarico e dei relativi profili di autorizzazione.

28. Quando gli atti e i documenti contenenti dati personali sensibili o giudiziari sono affidati agli incaricati del trattamento per lo svolgimento dei relativi compiti, i medesimi atti e documenti sono controllati e custoditi dagli incaricati fino alla restituzione in maniera che ad essi non accedano persone prive di autorizzazione, e sono restituiti al termine delle operazioni affidate.

29. L’accesso agli archivi contenenti dati sensibili o giudiziari è controllato. Le persone ammesse, a qualunque titolo, dopo l’orario di chiusura, sono identificate e registrate. Quando gli archivi non sono dotati di strumenti elettronici per il controllo degli accessi o di incaricati della vigilanza, le persone che vi accedono sono preventivamente autorizzate.

Allegato 7 Normativa emanata dalla Banca d'Italia sulla continuità operativa in casi di emergenza (luglio 2004)

GESTIONE DELLA CONTINUITÀ OPERATIVA

1. Premessa

La crescente complessità dell'attività bancaria, l'intenso utilizzo della tecnologia dell'informazione e i nuovi scenari di rischio hanno messo in evidenza l'esigenza che le banche aggiornino la valutazione dei rischi operativi, adeguino le strategie in tema di sicurezza e rafforzino i presidi di emergenza in modo da garantire adeguati livelli di continuità operativa.

L'approccio tradizionale dei piani di emergenza non considera ipotesi di crisi estesa e blocchi prolungati delle infrastrutture essenziali; le soluzioni più comuni sono basate su misure tecnico - organizzative finalizzate alla salvaguardia degli archivi elettronici e al funzionamento dei sistemi informativi.

Tali misure possono risultare insufficienti ad assicurare la continuità operativa dell'azienda in caso di eventi disastrosi.

Nel nuovo contesto risulta essenziale adottare un approccio esteso che, partendo dalla identificazione dei processi aziendali critici, definisca per ciascuno di essi presidi organizzativi e misure di emergenza commisurati ai livelli di rischio.

Per prevenire l'insorgere di rischi sistemici occorre inoltre elevare e uniformare la qualità delle soluzioni di emergenza dei maggiori operatori, in particolare nei comparti dei servizi di pagamento e dell'accesso ai mercati finanziari, anche attraverso iniziative di cooperazione tra intermediari e gestori delle infrastrutture.

La Banca d'Italia ha definito linee guida per la gestione della continuità operativa rivolte a tutte le banche; per quanto riguarda la prevenzione del rischio sistemico si fa riserva di chiedere ad alcuni intermediari l'attivazione di misure di emergenza più rigorose.

2. Definizioni

La gestione della continuità operativa comprende tutte le iniziative volte a ridurre a un livello ritenuto accettabile i danni conseguenti a incidenti e catastrofi che colpiscono direttamente o indirettamente un'azienda.

Il piano di continuità operativa, nel seguito denominato anche piano di emergenza, è il documento che formalizza i principi, fissa gli obiettivi e descrive le procedure per la gestione della continuità operativa dei processi aziendali critici.

Il piano di *disaster recovery* stabilisce le misure tecniche e organizzative per fronteggiare eventi che provochino la indisponibilità dei centri di elaborazione dati. Il piano, finalizzato a consentire il funzionamento delle procedure informatiche rilevanti in siti alternativi a quelli di produzione, costituisce parte integrante del piano di continuità operativa.

3. Ambito del piano di continuità operativa

Le banche definiscono un piano di continuità operativa per la gestione di situazioni critiche conseguenti sia a incidenti di portata settoriale sia a catastrofi estese che colpiscono l'azienda o le sue controparti rilevanti (altre società del gruppo, principali fornitori, clientela primaria, specifici mercati finanziari, istituzioni di regolamento e compensazione).

Per i gruppi bancari, i piani di continuità possono essere definiti e gestiti in modo accentrato per l'intero gruppo o decentrato per singola società; in ogni caso la capogruppo assicura che tutte le controllate siano dotate di piani di continuità operativa e verifica la coerenza degli stessi con gli obiettivi strategici del gruppo in tema di contenimento dei rischi.

Laddove alcuni processi critici siano svolti da soggetti specializzati appartenenti al gruppo (ad es. allocazione della funzione informatica o del *back-office* presso una società strumentale), i relativi presidi di emergenza costituiscono parte integrante dei piani di continuità delle banche.

Il piano si inquadra nella complessiva politica aziendale sulla sicurezza e tiene conto delle vulnerabilità esistenti e delle misure preventive poste in essere per garantire il raggiungimento degli obiettivi aziendali.

Il piano prende in considerazione almeno i seguenti scenari di crisi:

- distruzione o inaccessibilità di strutture nelle quali sono allocate unità operative o apparecchiature critiche;
- indisponibilità di personale essenziale per il funzionamento dell'azienda;
- interruzione del funzionamento delle infrastrutture (tra cui energia elettrica, reti di telecomunicazione, reti interbancarie, mercati finanziari);
- alterazione dei dati o indisponibilità dei sistemi a seguito di attacchi perpetrati dall'esterno attraverso reti telematiche;
- danneggiamenti gravi provocati da dipendenti.

3.1 Correlazione ai rischi

L'analisi di impatto, preliminare alla stesura del piano di emergenza e periodicamente aggiornata, individua il livello di rischio relativo ai singoli processi aziendali e pone in evidenza le conseguenze della interruzione del servizio. I rischi residui, non gestiti dal piano, sono documentati ed esplicitamente accettati dalla banca. L'allocazione delle risorse e le priorità di intervento sono correlate al livello di rischio.

L'analisi di impatto tiene conto dei parametri caratteristici della struttura organizzativa e dell'operatività aziendale, tra cui:

- le specificità - in termini di probabilità di catastrofe - connesse con la localizzazione dei siti rilevanti (ad es. sismicità dell'area, dissesto idrogeologico del territorio, vicinanza ad insediamenti industriali pericolosi, prossimità ad aeroporti o a istituzioni con alto valore simbolico);

- i profili di concentrazione geografica (ad es. presenza di una pluralità di operatori nei centri storici di grandi città);

- la complessità dell'attività tipica o prevalente e il grado di automazione raggiunto;

- le dimensioni aziendali e l'articolazione territoriale dell'attività;

- il livello di esternalizzazione di funzioni rilevanti (ad es. outsourcing del sistema informativo o del *back-office*);

- l'assetto organizzativo in termini di accentramento o decentramento di processi critici;

- i vincoli derivanti da interdipendenze, anche tra e con fornitori, clienti, altri intermediari.

L'analisi di impatto prende in considerazione, oltre ai rischi operativi, anche gli altri rischi (ad es. di mercato e di liquidità).

4. Definizione del piano e gestione dell'emergenza

4.1 Ruolo dei vertici aziendali

I vertici aziendali promuovono lo sviluppo, l'aggiornamento e le verifiche del piano di continuità operativa, garantendo che il tema della continuità operativa sia adeguatamente considerato a tutti i livelli di responsabilità.

Il consiglio di amministrazione stabilisce gli obiettivi e le strategie di continuità del servizio; assicura risorse umane, tecnologiche e finanziarie adeguate per il conseguimento degli obiettivi fissati; approva il piano; viene informato, con frequenza almeno annuale, sulla adeguatezza dello stesso.

L'alta direzione nomina il responsabile del piano di emergenza; promuove il controllo periodico del piano e l'aggiornamento dello stesso a fronte di rilevanti innovazioni organizzative, tecnologiche e infrastrutturali nonché nel caso di lacune o carenze riscontrate ovvero di nuovi rischi sopravvenuti; approva il piano annuale delle verifiche delle misure di continuità ed esamina i risultati delle prove.

L'attività svolta e le decisioni assunte sono adeguatamente documentate.

4.2 I processi critici

Gli intermediari identificano in modo circostanziato i processi che, per la rilevanza dei danni conseguenti alla loro indisponibilità, necessitano di elevati livelli di continuità operativa da conseguire mediante misure di prevenzione e con soluzioni di emergenza da attivare in caso di incidente.

A tal fine vengono considerati con particolare attenzione i processi che attengono alla gestione dei rapporti con la clientela e alla registrazione dei fatti contabili.

Per ciascun processo critico sono individuati il responsabile, le procedure informatiche di supporto, il personale addetto, le strutture logistiche interessate, le infrastrutture tecnologiche e di comunicazione utilizzate.

Il responsabile del processo individua il tempo massimo accettabile di interruzione del servizio e collabora attivamente alla realizzazione delle misure di continuità in accordo con gli indirizzi strategici e con le regole stabilite nel piano.

4.3 La responsabilità del piano

La responsabilità dello sviluppo, della manutenzione e delle verifiche del piano di emergenza è affidata dall'alta direzione a un esponente aziendale con posizione gerarchico - funzionale adeguata.

Il piano attribuisce l'autorità di dichiarare lo stato di emergenza e stabilisce la catena di comando incaricata di gestire l'azienda in circostanze eccezionali. Sono esplicitamente individuati i membri della struttura preposta alla gestione della crisi (ad es. comitato di crisi), il responsabile della stessa struttura, le modalità interne di comunicazione e le responsabilità attribuite alle funzioni aziendali interessate.

Le unità operative coinvolte nei processi critici individuano i responsabili di settore del piano di emergenza. Essi coordinano, per gli aspetti di competenza, i lavori per la definizione del piano, per l'attuazione delle misure previste nello stesso e per la conduzione delle verifiche.

Prima della attivazione di nuovi sistemi o processi operativi, i responsabili di settore definiscono le opportune modifiche del piano.

4.4 Il contenuto del piano

Il piano di continuità documenta le modalità per la dichiarazione dello stato di emergenza, l'organizzazione e le procedure da seguire in situazione di crisi, l'iter per la ripresa della normale operatività.

Il piano stabilisce il tempo massimo accettabile di ripartenza di sistemi e processi critici.

Il piano individua i siti alternativi, prevede spazi e infrastrutture logistiche e di comunicazione adeguate per il personale coinvolto nell'emergenza, stabilisce le regole di conservazione delle copie dei documenti importanti (ad es. contratti) in luoghi remoti rispetto ai documenti originali.

Con riferimento ai sistemi informativi centrali e periferici, il piano fornisce indicazioni su modalità e frequenza di generazione delle copie degli archivi di produzione e sulle procedure per il ripristino presso i sistemi secondari.

La frequenza dei *back-up* è correlata al volume di operatività dell'intermediario; gli archivi di produzione sono duplicati almeno giornalmente. Sono assunte cautele per il tempestivo trasporto e la conservazione delle copie elettroniche in siti ad elevata sicurezza fisica posti in luoghi remoti rispetto ai sistemi di produzione.

Nel caso di sistemi secondari *off-line*, in cui non siano presenti archivi di dati ovvero questi non siano allineati in tempo reale ai dati di produzione, sono definite modalità e tempi di allineamento alla situazione corrente al momento dell'interruzione.

Il piano definisce le modalità di comunicazione con la clientela, le controparti rilevanti e i media.

Gli intermediari che ricorrono a terzi per i servizi di continuità operativa definiscono con i fornitori livelli di servizio adeguati al conseguimento degli obiettivi aziendali. Nel caso in cui il fornitore abbia impegnato le stesse risorse per fornire analoghi servizi ad altre aziende, in particolare se situate nella stessa zona, sono stabilite cautele contrattuali per evitare il rischio che, in caso di esigenze concomitanti di altre organizzazioni, le prestazioni degenerino o il servizio si renda di fatto indisponibile.

Il contratto stipulato con il fornitore consente all'intermediario di utilizzare il sito secondario per periodi prolungati, fino al pieno ripristino del sito primario.

4.5 Le verifiche

Le verifiche delle misure di emergenza sono correlate ai rischi; di conseguenza sono ipotizzabili differenti frequenze e livelli di dettaglio delle prove. In alcuni casi può essere sufficiente la simulazione parziale dell'evento catastrofico; per i processi più critici le verifiche prevedono il coinvolgimento degli utenti finali, degli *outsourcer* e, qualora possibile, delle controparti rilevanti.

Con frequenza almeno annuale viene svolta una verifica complessiva, il più possibile realistica, del ripristino della operatività in condizioni di emergenza, effettuando il controllo della funzionalità e delle prestazioni dei sistemi secondari e riscontrando la capacità dell'organizzazione di attuare nei tempi previsti le misure definite nel piano.

In particolare, le verifiche annuali dei sistemi informativi devono prevedere l'attivazione dei collegamenti di rete presso il sito secondario, l'operatività on-line di almeno una succursale e l'esecuzione delle procedure batch.

I risultati delle verifiche sono documentati per iscritto, portati all'attenzione dell'alta direzione e inviati, per le parti di competenza, alle unità operative coinvolte e alla funzione di auditing. A fronte di carenze riscontrate nelle prove sono tempestivamente avviate le opportune azioni correttive.

4.6 Le risorse umane

Il piano individua il personale essenziale per assicurare la continuità dei processi critici e fornisce allo stesso indicazioni sulle località da raggiungere e sulle attività da porre in essere in caso di emergenza.

Le procedure di emergenza sono chiare e dettagliate, in modo da poter essere eseguite anche da risorse non esperte.

Il personale coinvolto nel piano è addestrato sulle misure di emergenza, dispone della lista di contatto e della documentazione necessaria per operare in situazione di crisi, ha dimestichezza con i siti secondari e con le apparecchiature in essi contenute, partecipa alle sessioni di verifica delle misure di emergenza.

Va valutata l'opportunità di frazionare l'attività connessa con i processi critici in più siti ovvero di organizzare il lavoro del personale su turni.

4.7 Esternalizzazione di attività critiche

L'attribuzione a soggetti terzi di processi critici (ad es. outsourcing dei sistemi informativi o del *back-office*) non esonera l'intermediario dalla responsabilità relativa al mantenimento della continuità operativa.

I contratti di outsourcing definiscono i livelli di servizio assicurati in caso di emergenza e individuano soluzioni di continuità compatibili con le esigenze aziendali e coerenti con le prescrizioni della Vigilanza.

Sono stabilite le modalità di partecipazione, diretta o per il tramite di comitati utente, alle verifiche dei piani di emergenza dei fornitori.

La banca acquisisce i piani di emergenza degli *outsourcer* ovvero dispone di informazioni adeguate, al fine di valutare la qualità delle misure previste e di integrarle con le soluzioni di continuità realizzate all'interno.

4.8 Infrastrutture e controparti rilevanti

Il piano di continuità considera l'eventualità che le principali infrastrutture tecnologiche e finanziarie e le controparti rilevanti siano colpiti da un evento calamitoso e stabilisce le misure per gestire i problemi conseguenti; la capacità di comunicare con i siti secondari di tali soggetti è verificata periodicamente.

Per i servizi essenziali all'operatività della banca, va valutata la possibilità di ricorrere a fornitori alternativi.

4.9 Controlli interni

L'approccio alla continuità operativa e il piano di emergenza sono regolarmente controllati dalla funzione di revisione interna (*internal auditing*). Gli *auditor* prendono visione dei programmi di verifica, assistono alle prove e ne controllano i risultati, propongono modifiche al piano sulla base delle mancanze riscontrate.

Va considerata l'opportunità di sottoporre il piano di emergenza alla revisione da parte di competenti terze parti indipendenti.

La funzione di revisione interna è coinvolta nel controllo dei piani di emergenza degli *outsourcer* e dei fornitori critici; essa puo' decidere di fare affidamento sulle strutture di questi ultimi se ritenute professionali, indipendenti e trasparenti quanto ai risultati dei controlli. L'auditing esamina i contratti per accertare che il livello di tutela sia adeguato agli obiettivi e agli standard aziendali.

4.10 Comunicazioni alla Banca d'Italia

In caso di incidente grave che comprometta il normale funzionamento della banca, l'intermediario informa tempestivamente la Banca d'Italia e fornisce valutazioni circa l'impatto dell'evento sulla operatività delle strutture centrali e periferiche e sui rapporti con la clientela e le controparti.

5. Requisiti particolari

L’operatività del sistema finanziario nel suo complesso si basa sul corretto funzionamento delle infrastrutture tecnologiche e finanziarie e sulla capacità dei maggiori operatori di erogare i servizi essenziali nei comparti dei sistemi di pagamento e dell’accesso ai mercati finanziari.

A tali soggetti la Banca d’Italia può chiedere il rispetto di requisiti di continuità operativa più stringenti rispetto a quelli previsti per la generalità degli intermediari, in particolare con riferimento ai tempi massimi di ripristino dei processi a rilevanza sistemica, alla localizzazione dei siti secondari, alle risorse previste per gestire le situazioni di emergenza.

La Banca d'Italia individua nominativamente i soggetti ai quali si applicano i requisiti particolari, concorda con loro gli adeguamenti dei piani di continuità operativa, verifica le soluzioni adottate. Nel caso di soggetti appartenenti a gruppi bancari, vengono identificate le società del gruppo alle quali si applicano i requisiti particolari; la capogruppo coordina le iniziative necessarie per il raggiungimento degli obiettivi concordati con la Vigilanza.

Allegato 8 Crimini informatici

Di seguito vengono riportati i principali articoli della legge 23 dicembre 1993, n. 547 che ha modificato e integrato le norme del codice penale e del codice di procedura penale in tema di criminalità informatica.

- **Violenza sulle cose (art. 1 - aggiunge il seguente comma dopo il 2° comma dell'art. 392 c.p.).** Si ha, altresì, violenza sulle cose allorché un programma informatico viene alterato, modificato o cancellato in tutto o in parte ovvero viene impedito o turbato il funzionamento di un sistema informatico o telematico.

- **Attentato a impianti di pubblica utilità (art. 2 - nuova formulazione dell'art. 420 c.p.).** Chiunque commette un fatto diretto a danneggiare o distruggere impianti di pubblica utilità è punito, salvo che il fatto costituisca più grave reato, con la reclusione da uno a quattro anni.

  La pena di cui al primo comma si applica anche a chi commette un fatto diretto a danneggiare o distruggere sistemi informatici o di pubblica utilità, ovvero dati, informazioni o programmi in essi contenuti o ad essi pertinenti.

  Se dal fatto deriva la distruzione o il danneggiamento dell'impianto o del sistema, dei dati, delle informazioni o dei programmi, ovvero l'interruzione anche parziale del funzionamento dell'impianto o del sistema, la pena è della reclusione da tre a otto anni.

- **Documenti informatici (Art. 3 - inserimento dell'art. 491-bis c.p.)** Se alcuna delle falsità previste dal presente capo riguarda un documento informatico pubblico o privato, si applicano le disposizioni del capo stesso concernenti rispettivamente gli atti pubblici e le scritture private. A tal fine per documento informatico si intende qualunque supporto informatico contenente dati o informazioni aventi efficacia probatoria o programmi specificamente destinati ad elaborarli.

- **Accesso abusivo a un sistema informatico o telematico (art. 4 - inserimento dell'art. 615-ter c.p.).** Chiunque 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 il diritto di escluderlo, è punito con la reclusione fino a tre anni.

  La pena è della reclusione da uno a cinque anni:

  1) se il fatto è commesso da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, o da chi esercita anche abusivamente la professione di investigatore privato, o con abuso della qualità di operatore del sistema;

  2) se il colpevole per commettere il fatto usa violenza sulle cose o alle persone, ovvero se è palesemente armato;

  3) se dal fatto deriva la distruzione o il danneggiamento del sistema o l'interruzione totale o parziale del suo funzionamento, ovvero la distruzione o il danneggiamento dei dati, delle informazioni o dei programmi in esso contenuti.

  Qualora i fatti di cui ai commi primo e secondo riguardino sistemi informatici di interesse militare o relativi all'ordine pubblico o alla sicurezza pubblica o alla sanità o alla protezione

civile o comunque di interesse pubblico, la pena è, rispettivamente, della reclusione da uno a cinque anni e da tre a otto anni.

Nel caso previsto dal primo comma il delitto è punibile a querela della persona offesa; negli altri casi si procede d'ufficio.

- **Detenzione e diffusione abusiva di codici di accesso a sistemi informatici o telematici (art. 4 - inserimento dell'art. 615-quater c.p.).** Chiunque, al fine di procurare a sé o ad altri un profitto, o di arrecare ad altri un danno, abusivamente si procura, riproduce, diffonde, comunica o consegna codici, parole chiave o altri mezzi idonei all'accesso ad un sistema informatico o telematico, protetto da misure di sicurezza, o comunque fornisce istruzioni idonee al predetto scopo, è punito con la reclusione sino ad un anno e con la multa sino a lire dieci milioni.

La pena è della reclusione da uno a due anni e della multa da lire dieci milioni a venti milioni se ricorre taluna delle circostanze di cui ai numeri 1) e 2) del quarto comma dell'articolo 617-quater.

- **Diffusione di programmi diretti a danneggiare o interrompere un sistema informatico (art. 4 - inserimento dell'art. 615-quinquies c.p.).** Chiunque diffonde, comunica o consegna un programma informatico da lui stesso o 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 a esso pertinenti, ovvero l'interruzione, totale o parziale, o l'alterazione del suo funzionamento, è punito con la reclusione sino a due anni e con la multa sino a lire venti milioni.

Da notare che il DPR 318 del 28 Luglio 1999 prevede: "Art. 4 - Codici identificativi e protezione degli elaboratori…..

c) gli elaboratori devono essere protetti contro il rischio di intrusione a opera di programmi di cui all'articolo 615 quinquies del codice penale, mediante idonei programmi, la cui efficacia e aggiornamento sono verificati con cadenza almeno semestrale."

- **Corrispondenza (art. 5 - sostituisce il quarto comma dell'art. 616 c.p.).** Agli effetti delle disposizioni di questa sezione per "corrispondenza" si intende quella epistolare, telegrafica, telefonica, informatica o telematica ovvero effettuata con ogni altra forma di comunicazione a distanza.

- **Intercettazione, impedimento o interruzione illecita di comunicazioni informatiche o telematiche (art. 6 - inserimento dell'art. 617-quater c.p.).** Chiunque fraudolentemente intercetta comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, ovvero le impedisce o le interrompe, è punito con la reclusione da sei mesi a quattro anni. Salvo che il fatto costituisca più grave reato, la stessa pena si applica a chiunque rivela, mediante qualsiasi mezzo di informazione al pubblico, in tutto o in parte, il contenuto delle comunicazioni di cui al primo comma. I delitti di cui ai commi primo e secondo sono punibili a querela della persona offesa. Tuttavia si procede d'ufficio e la pena è della reclusione da uno a cinque anni se il fatto è commesso:

  - in danno di un sistema informatico o telematico utilizzato dallo Stato o da altro ente pubblico o da impresa esercente servizi pubblici o di pubblica necessità;

  - da un pubblico ufficiale o da un incaricato di un pubblico servizio, con abuso dei poteri o con violazione dei doveri inerenti alla funzione o al servizio, ovvero con abuso della qualità di operatore del sistema;

- da chi esercita anche abusivamente la professione di investigatore privato.

- **Installazione di apparecchiature atte a intercettare, impedire o interrompere comunicazioni informatiche o telematiche (art. 6 - inserimento dell'art. 617-quinquies c.p.).** Chiunque, fuori dai casi consentiti dalla legge, installa apparecchiature atte a intercettare, impedire o interrompere comunicazioni relative a un sistema informatico o telematico ovvero intercorrenti tra più sistemi, è punito con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

- **Falsificazione, alterazione o soppressione del contenuto di comunicazioni informatiche o telematiche (art. 6 - inserimento dell'art. 617-sexies c.p.).** Chiunque, al fine di procurare a sé o ad altri un vantaggio o di arrecare ad altri un danno, forma falsamente ovvero altera o sopprime, in tutto o in parte, il contenuto, anche occasionalmente intercettato, di taluna delle comunicazioni relative a un sistema informatico o telematico o intercorrenti tra più sistemi, è punito, qualora ne faccia uso o lasci che altri ne facciano uso, con la reclusione da uno a quattro anni. La pena è della reclusione da uno a cinque anni nei casi previsti dal quarto comma dell'articolo 617-quater.

- **Rivelazione del contenuto di documenti segreti (art. 7 – inserimento del comma 2, art. 621 c.p.)** Agli effetti della disposizione di cui al primo comma (“*Chiunque, essendo venuto abusivamente a cognizione del contenuto, che debba rimanere segreto, di altrui atti o documenti, pubblici o privati, non costituenti corrispondenza, lo rivela, senza giusta causa, ovvero lo impiega a proprio o altrui profitto, è punito, se dal fatto deriva nocumento, con la reclusione fino a tre anni o con la multa da lire duecentomila a due milioni”)* è considerato documento anche qualunque supporto informatico contenente dati, informazioni o programmi.

- **Danneggiamento di sistemi informatici e telematici (art. 9 - inserimento dell'art. 635 bis c.p.)** Chiunque distrugge, deteriora o rende, in tutto o in parte, inservibili sistemi informatici o telematici altrui, ovvero programmi, informazioni o dati altrui, é punito, salvo che il fatto costituisca più grave reato, con la reclusione da sei mesi a tre anni.
  Se ricorre una o più delle circostanze di cui al secondo comma dell'articolo 635, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema, la pena è della reclusione da uno a quattro anni.

- **Frode informatica (art. 10 – inserimento dell'art. 640-ter c.p.).** Chiunque, alterando in qualsiasi modo il funzionamento di un sistema informatico o telematico o intervenendo senza diritto con qualsiasi modalità su dati, informazioni o programmi contenuti in un sistema informatico o telematico o a esso pertinenti procura a sé o ad altri un ingiusto profitto con altrui danno, è punito con la reclusione da sei mesi a tre anni e con la multa da lire centomila a due milioni. La pena è della reclusione da uno a cinque anni e della multa da lire seicentomila a tre milioni se ricorre una delle circostanze previste dal numero 1) del secondo comma dell'articolo 640, ovvero se il fatto è commesso con abuso della qualità di operatore del sistema. Il delitto è punibile a querela della persona offesa, salvo che ricorra taluna delle circostanze di cui al secondo comma o un'altra circostanza aggravante.

- **Intercettazioni di comunicazioni informatiche o telematiche (art. 11 - inserimento dell'art. 266 c.p.).** Nei procedimenti relativi ai reati indicati nell'articolo 266, nonché a quelli commessi mediante l'impiego di tecnologie informatiche o telematiche, è consentita l'intercettazione del flusso di comunicazioni relativo a sistemi informatici o telematici ovvero intercorrente tra due sistemi.

Allegato 9 Costi direttamente imputabili alla struttura della sicurezza informatica

1. Architetture di Sicurezza Logica
    - 1.1. Personale
        - 1.1.1. Stipendi
        - 1.1.2. Missioni, trasferte, indennità, ecc.
        - 1.1.3. Corsi di formazione e documentazione
        - 1.1.4. Consulenza e assistenza informatica
        - 1.1.5. Consulenza professionale [30]
    - 1.2. Hardware[31]
    - 1.3. Software di base[32]
    - 1.4. Software applicativo[33]
        - 1.4.1. Software applicativo per il controllo delle vulnerabilità
        - 1.4.2. Software applicativo per l'audit dei sistemi
        - 1.4.3. Software applicativo per la gestione del rischio informatico
    - 1.5. Telecomunicazioni[34]
    - 1.6. Logistica (fitti figurativi, materiale di ufficio, ecc.)
2. Gestione della Sicurezza Logica
    - 2.1. Personale
        - 2.1.1. Stipendi
        - 2.1.2. Missioni, trasferte, indennità, ecc.

[30] Si intende il costo di assistenza e consulenza specialistica in ambito di sicurezza dei sistemi informatici.

[31] Si ricorda che in queste due sezioni sono inclusi i costi sostenuti per il funzionamento della struttura (posti di lavoro, *lan* di test). Inoltre, si aggiungono i costi sostenuti per il monitoraggio degli accessi.

[32] Fondamentalmente dovrebbe trattarsi del solo software di base dei posti di lavoro e dei *server* utilizzati per l'attività del comparto (W/NT; UNIX; DB; ecc.).

[33] Si intende *packages* per: analisi delle vulnerabilità; monitoraggio; *risk analysis*.

[34] Include gli apparati usati per l'ambiente di test.

2.1.3. Corsi di formazione e documentazione

2.1.4. Consulenza e assistenza informatica

2.1.5. Consulenza professionale

2.2. Hardware[35]

2.3. Software di base

2.3.1. Software per la gestione degli accessi via Internet[36]

2.3.2. Software per la protezione degli *asset* [37]

2.3.3. Altro software di base

2.4. Software applicativo

2.4.1. Software per la gestione dell'*help desk*

2.4.2. Altro software applicativo

2.5. Telecomunicazioni

2.6. Logistica (fitti figurativi, materiale di ufficio, ecc.)

[35] Come detto per la prima sezione, si devono considerare i costi per il funzionamento della struttura. Si suggerisce di aggiungere quelli legati ai sistemi di *help desk* e di allarme.

[36] Trattasi di software, ad esempio, per evitare l'accesso a siti con contenuto non strettamente legato all'attività lavorativa.

[37] Ad esempio: software per il controllo delle configurazioni dei *server*, per individuare eventuali alterazioni.

Allegato 10 Altri costi di sicurezza informatica

1. Sistemi Hardware[38]
    1.1. Apparati di controllo accessi (sicurezza logica)[39]
    1.2. Apparati di controllo accessi (sicurezza fisica)[40]
    1.3. Sistemi di continuità per l'ICT (sicurezza logica)
    1.4. Sistemi di continuità per l'ICT (sicurezza fisica)
    1.5. Sistemi di continuità: altri[41]
    1.6. Sistemi di protezione della riservatezza
2. Sistemi software di base[42]
    2.1. Software di base per il controllo degli accessi
    2.2. Software di base per la gestione della continuità di servizio
    2.3. Software di base per la protezione della riservatezza
3. Sistemi software applicativi[43]
    3.1. Software per il controllo degli accessi
    3.2. Software per la gestione della continuità di servizio
    3.3. Software per la protezione della riservatezza
    3.4. Altri software applicativi
4. Telecomunicazioni
    4.1. Sistemi per la continuità del servizio dell'ICT

---

[38] Include gli eventuali apparati di telecomunicazione (*routers*, *bridge*, *switch*, ecc.) strettamente legati al sistema contabilizzato e che, quindi, essendo accessori al sistema scelto, non sono prevalenti per importo di spesa.

[39] Include i dispositivi *firewall*, apparati dedicati al *content filtering*, ecc., ma anche i dispositivi per il riconoscimento quali i *token*, *smart card*, ecc. Sono quindi inclusi i sistemi di autorizzazione, autenticazione *e strong authentication*, ecc.

[40] Ad esempio: lettori di badge per l'accesso alle infrastrutture informatiche.

[41] Si vogliono indicare quelli di altre *business unit* (es. sala cambi).

[42] Ad esempio, il RACF, per il controllo degli accessi ai sistemi OS/390, è da considerarsi software di base, come il sistema operativo.

[43] Trattasi di *package* che, avvalendosi del software di base (es. gestione degli accessi), permettono di realizzare un livello superiore di protezione.

4.2. Sistemi per la continuità del servizio: altri

5. Risorse Umane[44]

5.1. Formazione e informazione sulla sicurezza

5.2. Consulenze specialistiche di sicurezza[45]

5.3. Assicurazioni

5.4. Polizze assicurative di competenza dell'ICT

5.5. Polizze *Computer Crime*

[44] Includere i costi di sensibilizzazione del personale, formazione, ecc.

[45] Costi sostenuti da altre *business unit* dell'azienda

Glossario

ACRONIMO/ TERMINE	DEFINIZIONE
Accessi (lista degli)	Griglia in cui per ogni persona, programma o processo sono definiti i livelli di privilegio sulle varie componenti del sistema.
Accesso non autorizzato	Accesso indebito a un sistema ottenuto per mezzo di un attacco o grazie ad attività di *Social Engineering*.
Accountability	Capacità di un sistema di tenere traccia delle attività svolte da persone, programmi o processi che hanno effettuato accessi e/o variazioni al sistema stesso.
Accounting	Attività di misura delle risorse consumate da un utente durante l'accesso al sistema in termini di impegno temporale delle stesse e della quantità dei dati inviati o ricevuti dall'utente. L'*accounting* viene attuato registrando le statistiche legate alla sessione e tali informazioni sono utilizzate per compiere attività di verifica, fatturazione, analisi dei trend e dimensionamento strutturale.
Affidabilità	Capacità di un sistema, di una applicazione o di un processo di fornire i risultati attesi, nel rispetto delle specifiche progettuali, in determinate condizioni e per un periodo di tempo prefissato. Riferita ai dati rappresenta il grado di assenza di errori.
Anomalia	Evento: – che non rispetta i requisiti di efficacia e efficienza predefiniti; – che non era stato previsto nella fase di progettazione del governo di un processo; – per il quale non sono stati predefiniti tutti o alcuni dei requisiti di efficacia e efficienza.
Antivirus	Componente software in grado di prevenire e/o verificare l'eventuale presenza di un virus informatico, di identificarlo ed eliminarlo e, se possibile, di ripristinare lo stato delle cose prima dell'infezione.
Audit (auditing)	Revisione o verifica delle procedure contabili, organizzative, informatiche e di controllo interno esistenti in azienda, avente lo scopo di verificare la conformità con criteri prestabiliti o evidenziare eventuali criticità.
Autorizzazione	Facoltà concessa a un utente per l'accesso e l'utilizzo di determinate risorse.

Backdoor	Modalità di accesso a un sistema non documentata. È da considerarsi a tutti gli effetti una falla di sicurezza che viene tipicamente installata dagli stessi progettisti o manutentori del sistema per facilitare un eventuale accesso di emergenza. Nel caso di un sistema compromesso, una *backdoor* potrebbe essere installata dall'attaccante per garantirsi la possibilità di accedere nuovamente al sistema.
Back-up	Costituzione di una disponibilità aggiuntiva di risorse (infrastrutture, dispositivi hardware, personale, ecc.) e duplicazione delle informazioni (copie di *back-up*) al fine di assicurare la disponibilità del servizio.
Bomba logica	Codice introdotto furtivamente all'interno di una applicazione o di un sistema operativo che viene eseguito qualora si verifichino determinate condizioni (ad esempio "a tempo"). Le operazioni attuate da tale codice possono essere distruttive e in ogni caso in grado di compromettere la sicurezza del sistema.
Cavallo di Troia (trojan horse)	Programma che, sotto le false spoglie di software "lecito", si introduce o viene introdotto in un sistema "vittima" svolgendo funzioni dannose.
Compromissione	Violazione di una *policy* di sicurezza di un sistema che può comportare divulgazione, modifica, perdita o distruzione di risorse.
Content Filtering	Tecnica basata sull'utilizzo di prodotti che permettono di filtrare indirizzi che possono rilevarsi improduttivi per l'attività aziendale. Attraverso *database* raggruppati per categorie e costantemente aggiornati, permettono di discriminare la visibilità, o meno, di siti Internet. Agiscono anche come protezione della posta elettronica e consentono di definire e applicare i criteri di protezione della stessa.
Crash di Sistema	Indica il blocco brusco e imprevisto di un sistema.
Crittografia	Metodo di protezione delle informazioni che effettua su di esse una trasformazione reversibile – basata su algoritmi matematici - il cui scopo è quello di rendere tali informazioni non comprensibili a coloro i quali non siano in possesso degli strumenti di decifratura.
Disastro	Evento imprevisto (volontario o meno) con conseguenze gravi per il sistema informativo dell'organizzazione. La gravità dell'imprevisto comporta l'indisponibilità delle principali funzioni del sistema informativo o di alcune sue componenti per un periodo di tempo durante il quale potrebbe essere necessario utilizzare il sistema informativo di *recovery*.
DNS	DNS è l'acronimo di "Domain Name Server". Nelle connessioni di rete (Internet, Intranet) serve per convertire i nomi "intelligibili" in indirizzi numerici IP ADDRESS (es. "www.cipa.it" è convertito in 193.203.230.241).

Emergenza (Piano di)	Implementazione di procedure di emergenza chiaramente documentate e accessibili da parte delle persone autorizzate, comprendenti l'addestramento del personale alla esecuzione di procedure specifiche da attuare in caso di emergenza. Tali procedure devono essere regolarmente aggiornate e sottoposte a test.
Firewall	Letteralmente "Muro taglia fuoco": dispositivo hardware/software atto alla separazione e alla protezione delle risorse appartenenti a due o più segmenti di rete. Il *firewall* permette il passaggio dei soli flussi dati esplicitamente autorizzati; l'autorizzazione può avvenire su basi diverse: indirizzo IP del mittente o del destinatario, servizio, periodo del giorno, risorsa di accesso, ecc.
Hacker	Un esperto informatico che usa la propria conoscenza per entrare fraudolentemente all'interno di reti o sistemi elaborativi altrui.
Intrusione	Accesso logico o fisico non autorizzato a un sistema informatico.
Intrusion Detection System (IDS)	Sistema atto a individuare tentativi di accesso non autorizzato alla rete (*network intrusion detection system*) o ai sistemi.
Livelli di sicurezza	Classificazioni gerarchiche di categorie rappresentanti il livello di criticità delle informazioni. Le specifiche relative a tali classificazioni variano in base alle esigenze di ogni organizzazione.
Looping di sistema	Il *looping* è una tecnica che permette di eseguire una o più linee di codice in maniera ricorsiva e ripetitiva. Riferito a un sistema, identifica il blocco dello stesso per l'esecuzione ripetitiva delle stesse istruzioni.
Outsourcing	Affidamento a società esterne della gestione di funzioni/servizi. Può riguardare i sistemi informatici (gestione sistemi elaborativi e reti, *help desk*, fornitura apparati), le infrastrutture (manutenzione impianti, sorveglianza), la formazione, ecc.
Password	Letteralmente: Parola d'ordine. Stringa di caratteri che deve essere conosciuta solamente dal soggetto assegnatario per consentire, in associazione con il relativo codice identificativo, la sua autenticazione.
Password Cracking	Si tratta di programmi che cercano le password di un *account* esistente consentendo a un *hacker* di accedere illecitamente a un sistema, creare nuovi *account*, ecc. Esistono oggi programmi *password cracking* che consentono di violare la sicurezza anche di file Word o Excel.
Penetrazione (Test di)	Si tratta di processi atti a verificare le difese delle reti effettuando tentativi di accesso al sistema usando le stesse tecniche che verrebbero usate da un *hacker*. Mediante tali test è possibile ottenere una valutazione del livello di protezione dei sistemi nei confronti delle minacce o vulnerabilità note.
Privilegi	Insieme di diritti di accesso concessi a un utente e riconosciuti da parte del sistema di controllo degli accessi.

Privilegio minimo (principio del)	Separazione dei livelli di accesso basata sulla funzione che l'utente deve svolgere per accedere alle sole risorse necessarie. L'implementazione di questo principio implica la suddivisione degli utenti in gruppi differenziati per livelli di privilegi.
Procedure di "call-back"	Procedure di accesso remoto a sistemi di gestione di linee di *dial-up*, che prevedono la richiamata da parte del sistema, su numeri predefiniti, dell'utente che desidera effettuare la connessione, in modo da garantire la sicurezza della connessione stessa.
Protocolli "a sfida"	Protocollo per l'accesso remoto basato sull'autenticazione dell'utente da parte del sistema mediante il test della risposta fornita dall'utente a un quesito crittografico (sfida).
Proxy server	Strumento volto alla riduzione del traffico in Internet e a velocizzare la navigazione da parte degli utenti. Ai fini della sicurezza viene utilizzato per il controllo e il filtraggio dei flussi di informazione tra i segmenti di rete discrezionalmente selezionati, operanti a livello applicativo. Il *proxy server* è costituito da componenti software e/o hardware. Rende possibile l'autenticazione e il controllo degli accessi.
Piano di sicurezza	Insieme delle misure di protezione fisiche, logiche e organizzative finalizzate al raggiungimento degli obiettivi congruenti con le politiche di sicurezza da implementare all'interno di una organizzazione.
Prodotti di sicurezza	Prodotti software o hardware realizzati al fine di implementare, da un punto di vista pratico, i presidi tecnologici coerenti con le politiche di sicurezza stabilite.
Sicurezza logica	Componente particolarmente importante della sicurezza del sistema informativo che riguarda principalmente la protezione dell'informazione, dei dati, delle applicazioni e di tutti i sistemi e processi in relazione a tali informazioni. La sicurezza logica si può quindi definire come l'insieme di misure di sicurezza di carattere tecnologico, di natura procedurale e organizzativa, aventi lo scopo di rendere possibile la realizzazione del livello di sicurezza desiderato.
Single point of failure	Elemento di un sistema informatico, di una rete di telecomunicazione, di un impianto tecnologico che, non disponendo di ridondanza, in caso di guasto comporta l'indisponibilità dell'intero sistema di cui fa parte.
Sistema informatico	Parte del sistema informativo dell'azienda gestita con strumenti informatici (hardware, software, reti, ecc.).
Sistema informativo	Insieme delle risorse umane e tecnologiche per il trattamento delle informazioni.

Spamming	Lo *spam* è una tecnica utilizzata dagli sviluppatori di siti web per cercare di ottenere posizioni più alte nel risultato dei motori di ricerca. L'e-mail Spamming consiste nell'invio di messaggi di posta elettronica non sollecitata (*mail spam*) e costituisce una violazione delle regole di comportamento su web nonché dei principi di uso corretto delle risorse di rete.
Spyware	Software introdotto deliberatamente in un sistema informatico, spesso associato in maniera nascosta a un'applicazione, con l'obiettivo di raccogliere informazioni, anche sensibili, sull'utente e sulle sue attività per poi inviarle, all'insaputa dell'utente stesso, verso centri di raccolta stabiliti dall'autore del software.
Strong Authentication	Letteralmente "autenticazione forte". È una tecnica che incrementa significativamente il livello di sicurezza dei normali sistemi a *password*. L'autenticazione si basa sulla combinazione di almeno due elementi fra i seguenti: – userid/password ; – una caratteristica propria/fisica della persona (impronta digitale, retina, ecc.); – un oggetto (*token*, *smart card*, ecc.).
Token	Letteralmente "gettone". Il possesso del *token* consente all'utente di accedere al sistema/applicazione abilitati a riconoscere quel "gettone".
VPN	Acronimo di *Virtual Private Network* . Il principio di una VPN consiste nel creare una rete privata sicura all'interno di una rete pubblica. Le VPN garantiscono la confidenzialità dei dati (crittografia) e indirettamente il controllo degli accessi (autenticazione degli utilizzatori).