Modello 231/2001 – Allegato alla parte speciale D “DELITTI INFORMATICI E DI TRATTAMENTO ILLECITO DI DATI ”

Relazione dettagliata sulla gestione dell’area ICT, dell’area Museale e all’Hotel Cavour et des Officiers.

ASSOCIAZIONE FORTE DI BARD

REDATTO AI SENSI E PER GLI EFFETTI DEL D. LGS. 231/2001

ENTE	FIRMA	DATA
Redatto da: Edist Engineering Srl	_____	_____
Autorizzato da: Amministratore	_____	_____

Edizione n° 1

Sommario

Sommario

Introduzione

Il presente documento descrive in maniera dettagliata le modalità di gestione della struttura informatica dell'Associazione Forte di Bard con riferimento all'area ICT, all'area museale e all'Hotel Cavour et des Officiers.

Metodologia utilizzata per la redazione del documento

Pianificazione e ricognizione di tutti i componenti che richiedono un livello di protezione per vulnerabilità relative al reato di frode informatica, inclusi i sistemi, le reti, le applicazioni e i dati.
La valutazione delle risorse è stata verificata in termini quantitativi e qualitativi per consentire la corretta pianificazione di contromisure o di misure di protezione, oltre che delle risorse da coinvolgere nel progetto.

Gestione del rischio informatico

- Analisi del rischio
    - Suddivisa in due fasi:
        1. Classificazione delle informazioni
        2. Identificazione delle minacce e delle vulnerabilità
        3. Identificazione del livello di rischio associabile a ciascuna classe di informazioni
- Controllo del rischio
    - Identificazione delle modalità di gestione dei rischi associati alla perdita di un obiettivo di sicurezza

Analisi del Rischio informatico

Analisi del livello di rischio dell'associazione Forte di Bard riguardo la parte di infrastruttura in gestione all'area ICT, all'area museale e all'Hotel Cavour et des Officiers.

Introduzione

Rischio: è la probabilità che un agente di pericolo sfrutti una vulnerabilità, definita come un punto debole nel sistema informatico dell'azienda che può avere un'origine tecnologica piuttosto che legata a persone o processi.

Minaccia: azione accidentale o deliberata che può portare alla violazione di un obiettivo di sicurezza

- Accidentale: terremoto, allagamento, incendio, cancellazione accidentale dei dati
- Deliberata: Virus informatico, attacco hacker

Vulnerabilità: è una debolezza intrinseca del sistema informatico, tale che, qualora esista una minaccia che la sfrutti, si arriverebbe alla violazione di almeno un obiettivo di sicurezza

- Non dipende da fattori esterni
- Non comporta automaticamente la violazione di obiettivi di sicurezza

Impatto: conseguenze che l'attuarsi di una minaccia determina

- Diretta relazione con gli obiettivi di sicurezza

Livelli di rischio informatico

Di seguito la scala di valori determinata secondo i seguenti criteri.

Probabilità con cui si può verificare un evento:

Livello 1 - l'evento è estremamente improbabile; non sono noti episodi già verificatisi; l'evento potrebbe verificarsi a causa di una concomitanza di eventi singolarmente improbabili

Livello 2 - l'evento è improbabile; sono noti solo casi rari di episodi già verificatisi; l'evento può verificarsi a seguito di circostanze particolarmente sfavorevoli.

Livello 3 - l'evento è probabile; sono noti alcuni episodi già verificatisi; l'evento può verificarsi direttamente per la mancanza o il difetto di pochi elementi.

Livello 4 - l'evento è altamente probabile; si sono già verificati eventi sia nell'Ente che in realtà simili; l'evento si verifica direttamente per la mancanza o il difetto di un solo elemento.

Impatto, quindi gravità delle conseguenze che il verificarsi dell'evento può produrre:

Livello 1 – Lieve: l'evento provoca effetti trascurabili

Livello 2 – Significativo: l'evento provoca effetti che potrebbero generare disservizi informatici ma gestibili in tempi brevi con azioni immediate

Livello 3 – Grave: l'evento provoca effetti che implicano gravi disservizi alla struttura informatica, sia pure senza comportare il verificarsi di un reato

Livello 4 – Gravissimo: l'evento potrebbe provocare il verificarsi di un reato e disservizi molto gravi alla struttura informatica

Molto Alto 16	• Attuare misure immediate di prevenzione e protezione dai rischi, eventualmente intervenire con azione di blocco dei sistemi o dei processi • Identificare misure di miglioramento nel breve periodo ai fini della riduzione del livello di rischio
Alto 9-12	• Attuare misure immediate di prevenzione e protezione dai rischi, non è necessario intervenire con azione di blocco dei sistemi o dei processi • Identificare misure di miglioramento nel breve periodo ai fini della riduzione del livello di rischio
Medio 4-8	• Programmare misure di prevenzione e protezione dai rischi nel breve periodo • Identificare misure di miglioramento e predisporre attività di monitoraggio anche se il rischio è comunque accettato e non produrrebbe danni gravi • E' possibile che non siano necessarie misure di prevenzioni in quanto già implementate anche se la probabilità che un evento succeda sia alta e impattante.
Basso 1-3	• non sono necessarie misure di protezione e prevenzione, quelle in atto si possono ritenere sufficienti

Tali valutazioni vengono inserite nel seguente modello:

		Probabilità (scala da 1 a 5)			
		Improbabile	*Poco probabile*	*Probabile*	*Molto probabile*
		1	*2*	*3*	*4*
Impatto (Scala da 1 a 5)					
4	*Gravissimo*	4 Medio	8 Alto	12 Alto	16 Elevato
3	*Grave*	3 Medio	6 Medio	9 Alto	12 Alto
2	*Significativo*	2 Basso	4 Medio	6 Medio	8 Alto
1	*Lieve*	1 Basso	2 Basso	3 Medio	4 Medio
		1	2	3	4

Analisi dei protocolli penal-preventivi per area ICT, area Museale e per l' Hotel Cavour et des Officiers

- Definizione e pubblicizzazione di specifiche deleghe nelle varie aree aziendali (in particolare, nell'area Informatica), con precisa indicazione di poteri e responsabilità dell'amministratore di sistema e dei suoi collaboratori;
- Proceduralizzazione delle attività informatiche, nonché delle altre attività da considerarsi a rischio-reato, svolte con strumenti informatici;

Sono presenti le procedure informatiche relative alla protezione dei dati (backup e ripristino) e alla gestione dell'infrastruttura in caso di manutenzione o malfunzionamento.

Classificazione delle informazioni AREA ICT

Aree di rischio informatico

I processi a rischio informatico sono i seguenti:

- Gestione del sito internet;
- Gestione della rete intranet dell'Associazione Forte di Bard;
- Gestione dell'hardware e del software aziendale;
- Sviluppo, manutenzione e gestione modifiche dei software applicativi;
- Ogni altra attività svolta con l'utilizzo di strumenti di lavoro informatici e telematici.

Nello specifico è stata eseguita l'analisi degli strumenti informatici di cui l ' area ICT è direttamente responsabile per garantire la sicurezza dei dati e la protezione dai reati informatici:

- Sicurezza perimetrale e protezione del collegamento internet
- Infrastruttura server e storage
- Salvataggio e replica dei dati
- Autenticazione e autorizzazioni di accesso ai dati
- Collegamenti Wi-Fi
- Gestione accessi VPN
- Gestione posta elettronica
- Gestione Antivirus e Antispyware
- Gestione aggiornamenti software e sistemi operativi
- Gestione e manutenzione del sito internet
- Gestione Videosroveglianza

Sicurezza perimetrale e protezione del collegamenti ad internet

L'associazione Forte di Bard dispone di un firewall di rete per garantire la sicurezza della rete e divide i due principali segmenti di rete:

- La rete interna (LAN), collegata ad un sistema centrale di switch di rete che gestisce a sua volta diverse rete virtuali (VLAN), separando di fatto fisicamente i vari settori del Forte di Bard: la rete dei server, la rete dei PC, i musei, etc.
- La rete esterna per il collegamento ad Internet collegata e gestita da due linee dati ADSL, una principale e una di backup.

Il firewall prevede la gestione unificata degli attacchi, comunemente abbreviata in UTM (Unified Threat Management) ed è stato configurato per i seguenti servizi:

- antivirus perimentrale
- anti-spyware
- Filtri di accesso ai siti web

- firewall di rete per il filtraggio delle connessioni in uscita
- Sistema IPS per il rilevamento e la prevenzione delle intrusioni
- filtraggio dei contenuti, controllo applicazioni (blocco peer to peer, chat).
- Servizi VPN per il collegamento dall'esterno tramite protocollo IPSEC oppure SSL
- Limitazione del traffico internet e gestione priorità
- Raccolta dei log degli eventi

I contenuti dei servizi sopra citati si aggiornano automaticamente tramite internet dal sito del produttore e periodicamente viene eseguito l'aggiornamento del firmware per garantire il massimo della sicurezza.
Il Firewall del Forte di Bard si presenta come un server virtuale che funziona su un sistema cluster di server per garantirne la continuità operativa ed escluderlo da guasti hardware.

Infrastruttura server e storage

L' associazione Forte di Bard dispone di uno chassis Blade che ospita cinque Server (Blades) fisici su cui vengono fatte funzionare diverse macchine virtuali che servono a garantire le procedure e i servizi informatici. L'ambiente dispone inoltre di due macchine Storage, una utilizzata per l'ambiente di produzione e una utilizzata per l'ambiente di Disaster Recovery in Campus.
Precisamente i 5 server Blade hanno i ruoli così suddivisi:

- N 3 server Blade fisici sono configurati in un cluster tramite il software di virtualizzazione su cui sono distribuiti circa 20 server Virtuali. I tre server fisici sono collegati allo Storage di produzione su cui risiedono tutti i dati aziendali.
- N 1 server Blade fisico collegato allo storage utilizzato per il Disaster recovery in campus. Tutto l'ambiente dei server virtuali e tutti i dati aziendali sono replicati in questo ambiente di backup.
- N 1 server Blade fisico utilizzato per il management hardware e per il backup su dischi di rete e su nastro

Tutti gli elementi hardware sono ridondati per garantire la continuità operativa in caso di guasto di un componente e sono configurati per spedire messaggi di avviso agli amministratori di sistema in caso di guasto o malfunzionamento.
In caso di guasto di uno dei server Blade del cluster di produzione la continuità di servizio viene sempre garantita.

Tutto il sistema si trova in una sala server chiusa a chiave con porta tagliafuoco, con sistema di condizionamento e gruppo di continuità.

Salvataggio e replica dei dati

L 'Associazione Forte di Bard dispone di un sistema di salvataggio dati installato su un server Blade fisico che comunica in rete con un NAS (disco di rete) per il backup su disco esterno ed è inoltre collegato ad una libreria di nastri.
Tramite il software di backup sono state impostate le seguenti politiche di salvataggio e replica dei dati al fine di garantirne il ripristino in caso di perdita o danneggiamento:

- Salvataggio giornaliero dell'intera infrastruttura server virtuale su disco di rete.
- Salvataggio giornaliero dell'intera infrastruttura server virtuale su nastri magnetici.
- Salvataggio giornaliero su disco del server dei dati denominato "Fileserver" con conservazione delle ultime 30 versioni per garantire una rotazione mensile.
- Salvataggio mensile su disco del "Fileserver" con conservazione di 12 versioni per garantire una rotazione annuale
- Salvataggio mensile dell'intera infrastruttura server su nastro con politica di esportazione dei nastri e conservazione in cassaforte ignifuga per 6 mesi.
- Replica dell'intera infrastruttura del cluster di produzione su un sistema server e storage esterno per garantire in breve tempo continuità operativa in caso di guasto completo del cluster di produzione.

Per il ripristino dei dati è possibile eseguire le seguenti attività

- Ripristino dell'intero server virtuale senza doverlo reinstallare
- Ripristino dei singoli file di qualsiasi sistema sottoposto a backup
- Ripristino della posta elettronica degli utenti
- Ripristino dei dati dall' ambiente di Disaster Recovery locale
- Avvio di tutti i sistemi virtuali nell'ambiente di Disaster Recovery locale

Sono escluse dal salvataggio dei dati le registrazioni video della videosorveglianza che per legge non possono essere conservate oltre le 48 ore.

Autenticazione e riservatezza dei dati

Autenticazione

Il Forte di Bard utilizza il sistema di autenticazione Microsoft Active Directory per l'accesso degli utenti ai personal computer Windows e Macintosh.
Le regole di autenticazione come la scadenza delle password e la complessità sono gestite centralmente.
Ogni 3 mesi viene inviata all'utente la richiesta di sostituzione della password
La gestione delle password degli utenti è dettagliata nel paragrafo 2 del documento allegato "Regolamento per l'utilizzo dei sistemi informatici"

Riservatezza dei dati aziendali
I dati aziendali risiedono nel server virtuale denominato "Fileserver". Ogni utente può accedere soltanto ai dati a cui è autorizzato e alla sua cartella personale.
Sul file server vengono svolte regolari attività di controllo, amministrazione e backup da parte del servizio ICT.

Tramite il documento allegato "Regolamento per l'utilizzo dei sistemi informatici", l'utente è stato istruito è informato riguardo l'utilizzo degli strumenti informatici che hanno accesso ai dati e che ne permettono la divulgazione.
Agli utenti in sintesi è stato consegnato un regolamento con precise istruzioni per:

- Utilizzo della rete e dei dati presenti sul server "Fileserver"
- Utilizzo del personal computer
- Utilizzo della posta elettronica
- Utilizzo e conservazione dei supporti rimovibili
- Utilizzo navigazione internet
- Utilizzo dei telefoni, Fax e fotocopiatrici

Collegamenti WI-FI

L'associazione Forte di Bard dispone di un servizio WI-FI per i clienti.
Per il cliente che volesse usufruire del servizio WI-FI è necessaria la registrazione tramite un portale interno che obbliga a fornire nome, cognome, numero di telefono cellulare. Il sistema invierà al numero di telefono inserito un nome utente e una password e permetterà l'accesso ad internet in modalità sicura e filtrata. I dati inseriti dagli utenti inoltre sono tracciati dal software e rimangono memorizzati e salvati.

Collegamenti VPN

Per l'accesso alla rete aziendale dall'esterno tramite internet si dispone di un accesso VPN configurato sul firewall.
Le persone o le aziende esterne possono accedere da remoto tramite connessione SSL oppure IPSEC con credenziali di accesso personalizzate e soltanto alle risorse aziendali per cui è stato autorizzato l'accesso.

Gestione posta elettronica

Il sistema di posta elettronica del Forte di Bard è composto da due elementi principali:

- Un servizio di hosting esterno su cui sono presenti le caselle postali degli utenti
- Un server di posta all'interno dell'infrastruttura per la gestione della posta interna

Nello specifico il servizio di posta esterna, in gestione ad una società esterna, è la destinazione primaria della posta elettronica del Forte di Bard, il quale adotta un sistema di identificazione delle email indesiderate (Antispam). Nello specifico la procedura di identificazione si basa su:

- Aggiornamento automatico del comportamento di individuazione in base alla verifica delle risultanze di alcune "black-lists"
- Un processo "euristico" di accumulazione della conoscenza che tiene traccia di tutte le comunicazione indesiderate ricevute, per poterle scartare automaticamente qualora si ripresentassero

Il sistema di posta elettronica interno, invece, si occupa di scaricare la posta elettronica presente sul server esterno in Hosting, per poi distribuirla alle caselle postali interne, alle quali gli utenti hanno accesso tramite il proprio personal computer.

Il sistema di posta interna inoltre è sottoposto a backup e viene quindi garantito il salvataggio e il ripristino delle email per tutti gli utenti.

Gestione antivirus e antispyware

Tutti i personal computer del Forte di Bard con sistema operativo Microsoft Windows dispongono di un antivirus che si aggiorna periodicamente in automatico tramite il sito internet del produttore. Inoltre il firewall prevede un antivirus e un antispyware periferico abilitato con le politiche di navigazione internet.

Gestione aggiornamenti software e sistemi operativi

L' area ICT dell'associazione forte di Bard pianifica abitualmente le attività di aggiornamento del software e dei sistemi operativi dei server, inoltre vengono sempre aggiornati i firmware dei sistemi hardware e del firewall. Le attività vengono svolte dagli amministratori di sistema o dalle società esterne che hanno competenze specifiche sui sistemi da aggiornare.
I personal computer con sistema operativi Microsoft vengono automaticamente aggiornati da un servizio centralizzato, mentre i sistemi Apple Macintosh vengono periodicamente aggiornati dall'amministratore di sistema.

Per quanto riguarda gli aggiornamenti di sicurezza del sito internet vengono svolte abitualmente attività di manutenzione dalla società esterna che gestisce il sito.

Videosorveglianza

E' presente un sistema di videosorveglianza le cui immagini video vengono salvate all'interno di un server virtuale nel Blade e che vengono successivamente cancellate a rotazione ogni 48 ore. La rete della videosorveglianza è separata da tutte le altri tramite una VLAN.

Controllo del rischio e contromisure

Il **R**ischio è il prodotto tra la **G**ravità delle conseguenze di un evento (impatto) e la **P**robabilità che esso accada:

$$R=GxP$$

Minaccia deliberata:

$$P=f(V,M)$$

- Dove
  - V = vulnerabilità
  - M = motivazioni dell'attaccante o livello della minaccia

Minaccia accidentale:

$$P=f(V,p)$$

- Dove
  - V = vulnerabilità
  - p = probabilità intrinseca di accadimento della minaccia

In base all'analisi effettuata possiamo considerare che il livello di rischio dell'infrastruttura informatica in gestione all'area ICT è BASSO
Di seguito, si illustrano le considerazioni che supportano l'opinione di un livello di rischio complessivamente BASSO.
Resta comunque inteso che la valutazione dei rischi espressa nel presente documento è basata sul presupposto che le procedure e i controlli descritti vengano effettivamente applicati.

L'Ente è adeguatamente strutturato in termini di:

- Infrastruttura hardware e Software
- Sistema di sicurezza perimetrale
- Sistema di accesso dall'esterno e autenticazione
- Sistema di conservazione e salvataggio dei dati
- Sistemi di protezione da Virus, Spyware e Spam

Classificazione delle informazioni Area Museale

Aree di rischio informatico

I processi a rischio informatico sono i seguenti:

- Gestione della rete intranet dell'Area Museale;
- Gestione dell'hardware e del software aziendale;
- Servizio alla clientela

Gestione area museale

Nello specifico è stata eseguita l'analisi degli strumenti informatici di cui l ' area Museale è direttamente responsabile per garantire la sicurezza dei dati e la protezione dai reati informatici:

- Gestione apparati Hardware e Software
- Autenticazione ai sistemi
- Salvataggio contenuti Audio/Video
- Servizi interattivi per la clientela

Di seguito si descrive la gestione dell'area museale:

- Le funzionalità dei museo sono controllate quotidianamente dai tecnici manutentori
- Il sistema di rete è configurato e gestito dagli apparati di networking certificati e permette una suddivisione dell'infrastruttura dei musei in tante sottoreti virtuali per garantire il massimo della sicurezza. Solo alcune di queste sottoreti hanno accesso ad internet.
- I Pc abilitati alla navigazione ad internet per l'aggiornamento degli applicativi sono su VLAN (sottorete virtuali) abilitate all'uscita verso internet con riconoscimento del "Mac-address" (indirizzo fisico univoco), sono muniti di antivirus e sono mantenuti con sistema operativo sempre aggiornati.
- Nessun dispositivo, che in qualche modo possa collegarsi in rete, può navigare liberamente su internet, ma la navigazione è automaticamente bloccata e all'interno dei musei tutte gli accessi di rete fisici non utilizzati sono disabilitati.
- Le password degli apparati di rete rispettano le regole di complessità, inoltre tutte le utenze interne possono accedere ai sistemi per il controllo con credenziali dedicate e non per l'amministratone del sistema, la quale e demandata ad un solo utente designato.

- L’ area museale è munita di sistema di backup dei contenuti Audio/Video che in caso di disservizio del funzionamento ne permette il ripristino.
- Le regie sono all’interno di aree protette e chiuse a chiave
- E’ presente un’installazione nel Museo Alpi dei ragazzi che permette al cliente di decidere di scattarsi in autonomia una fotografia e salvarla su un supporto USB personale, come specificato nel DPS ex Dlgs 196/03.

In base all’analisi effettuata possiamo considerare che il livello di rischio dell’infrastruttura informatica in gestione all’area Museale è BASSO.
Di seguito, si illustrano le considerazioni che supportano l’opinione di un livello di rischio complessivamente BASSO.
Resta comunque inteso che la valutazione dei rischi espressa nel presente documento è basata sul presupposto che le procedure e i controlli descritti vengano effettivamente applicati.

L'Ente è adeguatamente strutturato in termini di:

- Infrastruttura hardware e Software
- Sistema di sicurezza perimetrale
- Sistema di accesso
- Sistema di conservazione e salvataggio dei dati
- Sistemi di protezione da Virus

Classificazione delle informazioni Hotel Cavour et des Officiers

Aree di rischio informatico

I processi a rischio informatico sono i seguenti:

- Gestione della rete intranet e Internet dell'hotel;
- Gestione dell'hardware e del software aziendale;

Gestione area Hotel

Di seguito si descrive la gestione dell'area Hotel Cavour et des Officiers:

- L'hotel dispone di un personal computer protetto con antivirus da cui è possibile collegarsi al servizio internet per la registrazione dei clienti come richiesto a norma di legge.
- Sul Pc non vengo salvati dati sensibili
- E' presente un firewall configurato per i seguenti servizi:
    - anti-spyware
    - antivirus periferico
    - Filtri di accesso ai siti web
    - firewall di rete per il filtraggio delle connessioni in uscita
    - Sistema IPS per il rilevamento e la prevenzione delle intrusioni
    - filtraggio dei contenuti, controllo applicazioni (blocco peer to peer).

- Per il cliente che volessero usufruire del servizio WI-FI viene fornito alla reception un ticket con le credenziali di accesso per navigare in modalità sicura e filtrata. Le credenziali hanno valenza temporale limitata.

In base all'analisi effettuata possiamo considerare che il livello di rischio dell'infrastruttura informatica in gestione all'area Hotel Cavour è BASSO.
Di seguito, si illustrano le considerazioni che supportano l'opinione di un livello di rischio complessivamente BASSO.
Resta comunque inteso che la valutazione dei rischi espressa nel presente documento è basata sul presupposto che le procedure e i controlli descritti vengano effettivamente applicati.

Classificazione delle informazioni Hotel Cavour et des Officiers

L'Ente è adeguatamente strutturato in termini di:

- Infrastruttura hardware e Software
- Sistema di sicurezza perimetrale
- Sistema di accesso
- Sistema di conservazione e salvataggio dei dati
- Sistemi di protezione da Virus