IL NOSTRO TEAM :

NOME	RUOLO
FRANCESCO PIO SCOPECE	SOCIO FONDATORE
FRANCESCO MINEO	SOCIO FONDATORE
OLIVIERO CAMARATA	SOCIO FONDATORE
LUCA IANNONE	SOCIO FONDATORE
MARCO DE FALCO	SOCIO FONDATORE
FRANCESCO VITALE	SOCIO FONDATORE

CHI SIAMO?

La PHANTOM s.r.l. è un'azienda leader nel settore della sicurezza informatica con sede legale a Dublino, Irlanda. Ci impegniamo a proteggere le aziende e le organizzazioni da minacce informatiche attraverso servizi di penetration test di alta qualità.

Siamo composti da un team esperto di professionisti certificati in sicurezza informatica. La nostra missione è garantire la sicurezza e la protezione dei dati dei nostri clienti attraverso l'applicazione di pratiche e metodologie avanzate.

Il nostro approccio si basa sull'utilizzo delle ultime tecnologie e metodologie per identificare e mitigare le vulnerabilità dei sistemi informatici. Siamo impegnati a mantenere la massima trasparenza e integrità durante tutte le fasi del processo di penetration testing.

I NOSTRI SERVIZI

Project Phase	*Task*
PENETRATION TEST	**Offriamo servizi di penetration test completi per identificare e correggere vulnerabilità nei sistemi informatici dei nostri clienti. I nostri test sono condotti da esperti certificati e includono una valutazione dettagliata delle infrastrutture IT, delle applicazioni web e dei dispositivi IoT.**
VALUTAZIONE DELLA SICUREZZA	***Forniamo valutazioni approfondite della sicurezza per identificare potenziali rischi e debolezze nei sistemi informatici esistenti dei clienti. Le nostre analisi aiutano le aziende a rafforzare le loro difese e a migliorare la loro postura di sicurezza complessiva.***
CONSULENZA E FORMAZIONE	***Oltre ai servizi di test, offriamo consulenza personalizzata e formazione per aiutare le organizzazioni a comprendere meglio le minacce informatiche e a implementare le migliori pratiche di sicurezza.***

PATRIMONIO IMMOBILIARE

ASSSET AZIENDALE	*VALORE ESPRESSO IN "€"*
EDIFICIO 1	350.000,00€
EDIFICIO 2	150.000,00€
DATA CENTER	100.000,00
Total	**600.000,00€**

Business Continuity Plan

Il Business Continuity Plan (BCP) è stato sviluppato per garantire la continuità operativa e il ripristino delle attività critiche dell'azienda Phantom S.r.l. in caso di emergenza o disastro. Lo scopo del piano è proteggere le risorse aziendali, mantenere l'accesso ai dati sensibili e minimizzare l'impatto sulle operazioni aziendali.

Analisi del Contesto Aziendale:

- Phantom S.r.l. è un'azienda con sede legale a Dublino che si occupa di penetration testing.
- Il capitale sociale dell'azienda è di 600.000 euro.
- L'azienda è composta da 6 soci fondatori.

Identificazione delle Risorse Critiche:

Le risorse critiche di Phantom S.r.l. includono:

- Infrastrutture IT, compresi server, reti e dispositivi di archiviazione.
- Applicazioni e software utilizzati per le attività di penetration testing.
- Dati sensibili dei clienti e dell'azienda.
- Personale chiave coinvolto nelle operazioni aziendali e nei servizi di consulenza.

Analisi del Rischio e Valutazione dell'Impatto:

L'azienda valuta i potenziali rischi e le minacce che potrebbero influenzare le operazioni aziendali, nonché l'impatto finanziario e operativo di un'interruzione. Si considerano eventi come malfunzionamenti dei sistemi, attacchi informatici, catastrofi naturali e errori umani.

Strategie di Continuità Operativa:

- Phantom S.r.l. implementa strategie di backup e ripristino per garantire la disponibilità dei dati critici e il ripristino delle operazioni aziendali in caso di emergenza.
- Vengono sviluppate procedure di lavoro remoto per consentire al personale di continuare a svolgere le attività critiche anche in situazioni di emergenza.

Pianificazione del Ripristino delle Operazioni:

- Phantom S.r.l. pianifica il ripristino delle operazioni utilizzando procedure dettagliate per recuperare l'accesso ai dati e alle applicazioni essenziali entro tempi predeterminati.
- Vengono identificati siti di ripristino alternativi per garantire la continuità operativa in caso di interruzione delle attività presso la sede principale.

Test e Esercitazioni:

- Sono pianificati test periodici e esercitazioni per verificare l'efficacia delle procedure di ripristino e dei piani di continuità operativa.
- Il personale chiave partecipa a esercitazioni di simulazione per garantire che siano preparati ad affrontare emergenze reali.

Gestione degli Incidenti e Comunicazioni:

- Sono definiti ruoli e responsabilità per la gestione degli incidenti, con un piano di comunicazione interno ed esterno per informare il personale, i clienti e le altre parti interessate durante un'interruzione.
- Phantom S.r.l. istituisce una linea diretta di contatto per la segnalazione degli incidenti e il coordinamento delle attività di risposta.

Revisione e Aggiornamento Continuo:

- Il BCP è soggetto a revisione periodica per garantire che sia allineato alle esigenze aziendali e alle evoluzioni del panorama della sicurezza informatica.
- Sono pianificate revisioni regolari con coinvolgimento del personale chiave per identificare e apportare modifiche o miglioramenti necessari al piano.

Conformità Normativa:

- Il BCP è conforme ai requisiti normativi e alle linee guida del settore, garantendo la protezione dei dati sensibili e la continuità operativa dell'azienda.

Questo Business Continuity Plan è essenziale per garantire la sicurezza, la resilienza e la continuità operativa dell'azienda Phantom S.r.l. in caso di emergenza o disastro.

DISASTER RECOVERY PLAN

Introduzione e Scopo:

Il Disaster Recovery Plan (DRP) è stato sviluppato per garantire la continuità operativa e il ripristino delle operazioni critiche dell'azienda Phantom S.r.l. in caso di emergenza o disastro. Il piano mira a

minimizzare l'impatto sulle operazioni aziendali e proteggere l'accesso ai dati sensibili durante situazioni di crisi.

Identificazione delle Risorse Critiche:

Phantom S.r.l. identifica le seguenti risorse critiche:

- Infrastrutture IT, compresi server, reti e dispositivi di archiviazione.
- Applicazioni e software utilizzati per svolgere le attività di penetration testing.
- Dati sensibili dei clienti e dell'azienda.
- Personale chiave coinvolto nelle operazioni di business.

Analisi del Rischio e Valutazione dell'Impatto:

L'azienda valuta i potenziali rischi e le minacce che potrebbero influenzare le operazioni aziendali, nonché l'impatto finanziario e operativo di un'interruzione. Si considerano eventi come malfunzionamenti dei sistemi, attacchi informatici, catastrofi naturali e errori umani.

Procedure di Backup e Ripristino:

- Phantom S.r.l. effettua backup regolari dei dati critici e dei sistemi utilizzando soluzioni di backup sicure e affidabili.
- Sono stati sviluppati piani di ripristino dettagliati per recuperare rapidamente l'accesso ai dati e alle applicazioni essenziali in caso di emergenza.

Pianificazione della Continuità Operativa:

- Sono state definite procedure e protocolli per mantenere le operazioni aziendali durante un'interruzione, incluso l'utilizzo di siti di ripristino e l'assunzione di risorse temporanee.
- Phantom S.r.l. ha identificato un sito di ripristino alternativo per continuare le operazioni in caso di interruzione delle attività presso la sede legale a Dublino.

Test e Esercitazioni:

- Sono pianificati test periodici e esercitazioni per verificare l'efficacia delle procedure di ripristino e dei piani di continuità operativa.
- Il personale chiave partecipa a esercitazioni di simulazione per garantire che siano preparati ad affrontare emergenze reali.

Gestione degli Incidenti e Comunicazioni:

- Sono definiti ruoli e responsabilità per la gestione degli incidenti, con un piano di comunicazione interno ed esterno per informare il personale, i clienti e le altre parti interessate durante un'interruzione.
- È stata istituita una linea diretta di contatto per la segnalazione degli incidenti e il coordinamento delle attività di risposta.

Revisione e Aggiornamento Continuo:

- Il DRP è soggetto a revisione periodica per garantire che sia allineato alle esigenze aziendali e alle evoluzioni del panorama della sicurezza informatica.
- Sono pianificate revisioni regolari con coinvolgimento del personale chiave per identificare e apportare modifiche o miglioramenti necessari al piano.

Conformità Normativa:

- Il DRP è conforme ai requisiti normativi e alle linee guida del settore, garantendo la protezione dei dati sensibili e la continuità operativa dell'azienda.

Collaborazione con Fornitori e Partner:

- Phantom S.r.l. collabora con fornitori e partner commerciali per garantire che siano inclusi nei piani di disaster recovery e per stabilire protocolli di comunicazione e collaborazione durante un'interruzione.

Questo Disaster Recovery Plan è essenziale per garantire la sicurezza, la resilienza e la continuità operativa dell'azienda Phantom S.r.l. in caso di emergenza o disastro.

Prepared by: Francesco Mineo, Francesco Pio Scopece, Francesco Vitale, Marco De Falco, Luca Iannone, Oliviero Camarota