HOUSERS
SMART INVESTMENT

Contenuto

POLITICA DI CONTINUITÀ AZIENDALE

1. Introduzione

Lo scopo del piano di continuità dei servizi IT è di definire precisamente come HOUSERS recupererà o continuerà il funzionamento di servizi IT, applicazioni, sistemi o componenti al livello concordato nei requisiti aziendali.

Questo piano si applica a tutte le attività critiche nell'ambito del sistema di gestione della continuità dei servizi IT.

2. Gli utenti di questo documento sono tutti i membri del personale, sia interni che esterni, che hanno un ruolo nella continuità del servizio IT.

3. Responsabilità per l'attuazione della politica di continuità operativa

Le squadre di lavoro, le loro attività e i loro membri sono conformati secondo la seguente tabella:

Compagnie	Funzioni	Membri
Compagnia Direttore	Dirigere le attività durante la contingenza e il recupero. - Analisi della situazione. - Attivazione o meno del piano di recupero. - Follow-up del processo di recupero. • - Valutazione dei danni.	CTO (leader) Responsabile dei sistemi
Equipe di recupero	Ripristinare tutti i principali servizi IT che sono:	CTO (capo)

	- Servizio database MariaDB - Servizio API - Servizio web anteriore - Servizio web Admin - Servizio web dei blog - Microservizio di gestione della comunicazione - Microservizio di gestione dei documenti - Microservizio di pagamento - Microservizio notifiche - Housers office file server	Responsabile dei sistemi (vice) Assistenti di sviluppo del Software
Strumenti di prova	Eseguiranno i test di verifica operativa dei principali servizi informatici. Ogni profilo dovrebbe avere il suo piano di test di verifica che dovrebbe essere dato al team di recupero.	Responsabile della qualità del software (CTO) Assistenti allo sviluppo del software

Identificazione dei problemi

La valutazione del rischio valuta il livello della minaccia (cioè l'incidente dirompente) e la misura in cui HOUSERS è vulnerabile a tale minaccia. La valutazione del rischio è attuata attraverso la tabella di valutazione del rischio e del trattamento. Il processo di valutazione del rischio è coordinato dal CTO e la valutazione del rischio per i singoli servizi è eseguita dai responsabili dei servizi.

3.1. Livelli di categorizzazione degli incidenti:

Conseguenze irrilevanti	1	La durata dell'incidente dirompente non influisce significativamente sulle finanze dell'organizzazione, sugli obblighi legali o contrattuali o sulla reputazione.
Conseguenza accettabile	2	La durata dell'incidente dirompente causa un danno alle finanze dell'organizzazione, agli obblighi legali o contrattuali o alla reputazione, ma questo danno è ancora accettabile considerando la sua grandezza e le circostanze specifiche.
Conseguenza importante	3	La durata dell'incidente dirompente causa un danno alle finanze, agli obblighi legali o contrattuali o alla reputazione dell'organizzazione e questo danno non è accettabile a causa della sua grandezza e delle circostanze specifiche.
Conseguenza catastrofica	4	La durata dell'incidente dirompente causa un danno importante alle finanze dell'organizzazione, agli obblighi legali o contrattuali o alla reputazione che le farà perdere la maggior parte del suo capitale e/o dovrà chiudere permanentemente le sue operazioni.

1. Tipi di segnalazioni

2. Alertas derivadas de Monitorizaciones de servicios

3. 2. Avvisi derivati dal monitoraggio del servizio

4. a. Caduta o rallentamento del livello di risposta del server a causa di un attacco Denial of Service.

5. b. Nessuna risposta dal server a causa di un calo della connettività isp.

6. c. Guasto della connettività API con LemnonWay

7. d. Crollo del sistema DB

8. Avvisi derivati dal monitoraggio attivo della sicurezza
    a. Notifiche del centro di allarme rápido

9. Avvisi da controlli periodici della sicurezza
    a. Avvisi derivati dall'errore nelle funzionalità della piattaforma.

b. associati alle operazioni degli investitori
associato al suo pannello di amministrazione

3.2. **Procedura di segnalazione dei problema**

- Sistema di monitoraggio attivo
- - Attraverso il sistema Teramonitor attivato con il deployment dell'infrastruttura in AWS, tutti gli eventi relativi al funzionamento dell'infrastruttura così come la sua manutenzione e il backup sono monitorati in tempo reale.

3.3. - Il servizio di monitoraggio si trova nel nodo di Parigi di Amazon Web Services, mentre i servizi Pro sono a Francoforte e i servizi di sviluppo sono in Irlanda.

a. 3.4. Avvisi derivati dal monitoraggio del servicio
    b. Caduta o rallentamento del livello di risposta del server a causa di un attacco Denial of Service; rapporti:
        a. Avviso di inattività via e-mail all'account di supporto Housers attraverso un sistema di monitoraggio esterno (Uptimerobot). La comunicazione avviene al momento della caduta, è immediata e automatica.
b. In caso di rallentamento, comunicazione da parte degli utenti della piattaforma o dei dipendenti Housers. La comunicazione avviene quando un utente rileva il calo delle prestazioni.
    a. Nessuna risposta dal server a causa di un errore di connettività dell'isp; rapporti:
    b. Avviso di inattività via e-mail all'account di supporto Housers attraverso un sistema di monitoraggio esterno (Uptimerobot). La comunicazione avviene al momento della caduta, è immediata e automatica.
c. Allarme crash emesso dal dipartimento dei sistemi esterni (fornito dalla società Teralevel) a partire dagli avvisi ricevuti dal sistema di monitoraggio Teramonitor. Questo avviso viene emesso via e-mail o

attraverso il canale di supporto specifico che entrambe le aziende condividono in Microsoft Teams.

a. Guasto di connettività API con LemnonWay; rapporti:

d. Avviso di fallimento della connessione con LemonWay tramite e-mail all'account di supporto Housers inviato dall'API. La comunicazione avviene al momento del taglio, è immediata e automatica.

a. Blocco del sistema BD; rapporti:

b. Aviso de fallo de conexión con la BD mediante correo electrónico a la cuenta de soporte de Housers enviado por la API. La comunicación se produce en el momento del corte, es inmediata y automática.

c. Avviso di fallimento della connessione con il DB via e-mail all'account di supporto Housers inviato dall'API. La notifica avviene al momento del taglio ed è immediata e automatica.

3.4. Allarmi derivati dal monitoraggio attivo della sicurezza

e. Notifiche dal centro di allarme rapido; rapporti:

a. Invio di una notifica via e-mail della vulnerabilità all'e-mail di supporto di Housers. Invio automatico e immediato al rilevamento della caduta.

f. Avvisi derivati da controlli di sicurezza periodici; rapporti:

a. Invio del rapporto derivato dagli audit di sicurezza all'indirizzo e-mail del CTO di Housers.

3.5. Avvisi derivati dall’errore nelle funzionalità della piattaforma

g. associati al funzionamento degli investitori; rapporti:

a. Avviso di fallimento via e-mail all'account di supporto Housers inviato dall'API. La comunicazione avviene al momento del taglio, è immediata e automatica.

b. Notifica diretta attraverso il modulo di supporto del sito web da parte degli utenti Housers o attraverso il sistema di

supporto esterno (Freshdesk) comunicato dai dipendenti Housers. La comunicazione avviene quando un utente rileva il problema.

h. associato al pannello di amministrazione dello stesso; rapporti:

a. Avviso di fallimento via e-mail all'account di supporto Housers inviato dall'API.

b. Notifica diretta attraverso il sistema di supporto esterno (Freshdesk) da parte dei dipendenti Housers. La comunicazione avviene quando un utente rileva il problema.

4. Risposta agli incidenti segnalati

Il CTO è responsabile di assicurare la continuità delle operazioni..

4.1. Tempi di reazione:

Tipo di incidente	**gravità**	**Tempo di reazione**
Conseguenza insignificante	1	24-48 h.
Conseguenza accettabile	2	24-48 h
Conseguenza importante	3	Reazione immediata dopo la comunicazione
Conseguenza catastrofica	4	Reazione immediata dopo la comunicazione

4.2. Sistemi di backup e recupero delle informazioni:

- - Clustering di server in ambiente cloud Amazon Web Services:
  - I servizi di produzione sono distribuiti tra i 3 nodi AWS situati a Francoforte. I servizi di backup e sviluppo sono distribuiti tra i 3 nodi

AWS situati in Irlanda. Infine, i servizi di monitoraggio e controllo sono distribuiti nei 3 nodi AWS situati a Parigi. In questo modo, l'integrità e la stabilità dei servizi è garantita e in caso di caduta di uno dei nodi, il servizio può essere recuperato su qualsiasi altro nodo o addirittura migrato in una delle altre 2 zone.

- Sistema di banche dati
  - L'infrastruttura ha 2 ambienti: un ambiente di produzione distribuito a Francoforte e un ambiente di sviluppo distribuito in Irlanda.
  - Ognuno di questi ambienti ha 2 cluster di database: un cluster MariaDB con 3 nodi e un cluster MongoDB con altri 3 nodi..

- Backup del database:
  - Sincronizzazione in tempo reale tra i nodi del cluster di database. Questo sistema impedisce la caduta in uno qualsiasi dei 3 nodi in cui è implementato e permette di lavorare anche con 1 solo dei 3 nodi.
  - Una copia completa del database viene fatta ogni giorno. Una volta che la copia è fatta, viene montata sul server di database di sviluppo, situato nel nodo Amazon Ireland e viene controllata l'integrità del contenuto. Inoltre, il backup viene anche inviato al sistema di archiviazione Amazon S3 (Nodo di Francoforte) e al NAS situato negli uffici di Housers Madrid, garantendo così la continuità del business in caso di qualsiasi contingenza..
  - Il sistema ha una storia di copie giornaliere ininterrotta da quando l'infrastruttura è stata distribuita su AWS.

4.3. Informazioni bancarie e documentazione per l'utente

- - I file transazionali della piattaforma (documentazione del cliente e del progetto) sono immagazzinati nel servizio S3 di Amazon, che ha tutta la protezione contro la perdita di dati e i sistemi di sicurezza informatica che un gigante come Amazon può fornire. Questi file si trovano nel nodo di Francoforte di S3, che a sua volta è composto da 3 nodi, in modo che la caduta

in uno di essi non influenzi la persistenza o il normale funzionamento del sistema.

- - Oltre ai sistemi di backup sopra descritti, tutte le informazioni sui portafogli e sugli investitori sono replicate nel sistema di Lemonway, che ha anche i propri sistemi di continuità operativa e di garanzia di backup..

4.4. Backup del codice sorgente

- - Il backup del codice sorgente della piattaforma è in due strati: in un servizio Git locale di ogni sviluppatore e in un servizio Git esterno..

4.5. Procedura del processo di risposta:

- Identificazione dell'evento che ha scatenato l'incidente
- Analisi della portata dell'incidente:
  - Identificazione dei servizi interessati.
  - Identificazione degli utenti interessati: utenti anonimi, investitori, amministratori della piattaforma, …
  - Affettazione dei dati: tabelle di dati, dati storici, log, …
  - Impatto temporale: identificazione dei problemi derivati dall'incidente prima del suo rilevamento.
  - Identificazione di possibili vulnerabilità del sistema.
- Analisi della soluzione proposta:
  - Analisi del checkpoint da cui viene sollevata la soluzione:
  - Creazione di un nuevo ramo per un hotfix e backup dei dati.
  - Analisi del codice sviluppato per risolvere il problema.
  - Analisi della relazione di questo codice con il resto dei servizi del sistema.
  - Analisi dei dati risultanti.
  - Análisis di sicurezza del sistema dopo l'applicazione della soluzione.
- Valutazione della risposta:
  - Proposta di azioni da realizzare per evitare il ripetersi dell'incidenza.

- Proposta di refactoring del servizio interessato, se necessario.
- Analisi del tempo e delle risorse dedicate alla risoluzione.
- Valutazione dell'impatto sui diversi dipartimenti: Assistenza clienti, marketing, stato reale, finanziario, legale, istituzionale.
- Valutazione dell'impatto sulla relazione azienda-cliente.
- Valutazione dell'impatto sull'affidabilità dell'azienda.
- Sviluppo di un rapporto d'impatto completo.

5. Follow-up e archiviazione

Abbiamo implementato un sistema di dichiarazione e monitoraggio degli incidenti attraverso Freshdesk. Questo sistema permette la dichiarazione, il monitoraggio e l'archiviazione di tutti gli incidenti dichiarati per una successiva revisione.

Dopo la risoluzione dell'incidente, si analizzano le cause che lo hanno originato e le possibili misure preventive da adottare, così come i possibili aggiornamenti che possono essere derivati da queste conclusioni per essere integrati nel processo di risposta.

6. Frequenza degli aggiornamenti

Il sistema di monitoraggio attivo attraverso Teramonitor permette di rilevare le minacce in tempo reale e applicare le misure necessarie per evitare i rischi e correggere le vulnerabilità.