Una riflessione sulla continuità operativa negli sportelli al pubblico

Author : Francesco Ermini

Date : 23 luglio 2018

Alcuni sistemi informatici prevedono la figura dell'operatore. Ad esempio gli impiegati che troviamo dietro agli sportelli delle amministrazioni pubbliche. Il loro compito è quello di mediare la richiesta dell'utente verso il sistema informatico.

Ogni tanto però qualcosa nel sistema non va; che si tratti di un attacco informatico o di un aggiornamento andato male, quando il sistema non funziona è il caos.

Gli impiegati chiamano l'azienda che mantiene l'infrastruttura informatica per segnalare il guasto o chiedere spiegazioni sulle procedure di ripristino del sistema.

Nel frattempo le persone in attesa si accumulano. Se il guasto non si risolve in poco tempo l'operatore chiude lo sportello, attacca con lo scotch un cartello con scritto "guasto" ed invita le persone a tornare un'altra volta. Queste situazioni non sono poi così rare nel nostro paese. A me personalmente è successo più volte e in queste situazioni ho rimpianto l'uso della carta.

L'intento dell'articolo è quello di considerare la continuità di servizio allo sportello dell'operatore. In particolare verrà discusso un approccio naive che potrebbe servire come "tampone" durante l'emergenza.

Il contesto

Gli addetti ai lavori tendono a considerare la continuità di servizio in termini tecnici: ridondanza, disaster recovery, etc., ma come funziona la continuità di servizio allo sportello dell'operatore?

L'intento dell'operatore è quello di accontentare le persone in attesa, ovvero non farle tornare un'altra volta.

Ci sono operatori che, durante il malfunzionamento del server centrale, segnano i dati dell'utente su carta e penna. Un volta che il sistema torna funzionante l'operatore procede ad

esaudire la richiesta dell'utente. Non sempre è possibile, ma in alcuni casi sì.

(Astraendo il concetto) si tratta di un supporto, esterno al sistema, su cui scrivere temporaneamente dati e/o richieste da parte degli utenti in attesa che il sistema funzioni correttamente.

Dal punto di vista tecnico il disservizio rimane lo stesso. Ma dal punto di vista percettivo il disservizio dell'utilizzatore migliorerebbe notevolmente.

Tuttavia la gestione dei dati così fatta comporta numerosi problemi ed inefficienze.

In primis è un problema di organizzazione. Il fatto che si debbano accumulare tanti fogli i cui dati sono inseriti a giorni di distanza dalla richiesta aggiunge caos al caos ed aumenta la probabilità di errori (dati non corretti, perdita di documenti).

Inoltre è uno spreco di tempo. L'operatore deve scrivere i dati due volte; la prima su carta e la seconda in via digitale. Per finire l'utente in questa situazioni non è tutelato, non ha ricevute che dimostrino la presa in carico dell'operazione.

Quello che ci domandiamo è: possiamo creare una soluzione altrettanto semplice e resiliente che sia migliore rispetto all'uso di carta e penna?

Soluzione Naive

Riassumiamo i requisiti:

- Il sistema deve poter essere usato con facilità dall'operatore.
- Il sistema deve essere eseguito lato client, perché interviene in caso di malfunzionamento lato server
- I dati devono essere inseriti nativamente in formato machine readable in modo da automatizzare le procedure di acquisizione sul server.
- Il sistema implementato deve essere di semplice da implementare.
- Il sistema deve garantire AAA (Accountability authentication authorization)

In particolare, in riferimento allo scenario valutato all'inizio si avrebbe che:

- In caso di malfunzionamento del server centrale, l'operatore apre un file, nello specifico una pagina html, che ha precedentemente scaricato dal sito di chi gestisce il sistema informatico.
- L'operatore scrive su questa pagina i dati che la persona allo sportello comunica.
- L'operatore invia in modo sicuro i dati raccolti al centro informatico.
- Quando il sistema torna a funzionare il gestore del sistema (non l'operatore, neanche l'utente) si occuperà di inserire i dati ricevuti automatizzando la procedura di acquisizione.

In particolare la soluzione proposta ha due vantaggi:

E’ facile e veloce da implementare. Sono sufficienti un paio d’ore di lavoro con un solo uomo per creare una pagina html che legga i dati essenziali da registrare e li traduca in formato machine readable. Questo permette, in situazioni non prevedibili, di realizzare velocemente soluzioni tampone. Se invece si tratta di situazioni prevedibili allora questa soluzione ha il vantaggio di avere un costo molto ridotto per essere implementata.

E’ user-friendly per l’utilizzatore e conveniente per il gestore. L’azione “invio” trasforma i dati inseriti nei campi html in formato machine-readable (xml, json…) e li invia ad una email temporanea (gmail, yahoo…) che è stata creata appositamente per l’emergenza. Dall’altra parte il gestore che riceve i dati in formato machine readable potrà automatizzare il processo di inserimento dei dati. Infatti dopo che il sistema è stato ripristinato sarà sufficiente adoperare degli script che leggano i dati dai file ricevuti e li inseriscano nel sistema.

Per garantire un minimo di sicurezza in questo sistema si potrebbe usare una password OTP (one time password) per cifrare il file allegato. Questo sistema di gestione della OTP potrebbe essere fatto in vari modi. Il modo semplice, anche se comporta alcuni rischi, è quello di concordare le password OTP prima dell’emergenza.

In questo caso l’operatore dovrà custodire un foglio con dei codici. Questo foglio sarà distribuito da chi gestisce il sistema informatico. Il gestore dovrà conservare le copie degli OPT e le email a cui sono associati. Per far questo il gestore potrebbe creare dal proprio database un file in formato machine readable in cui ad ogni email di un operatore si associa un certo numero di OTP randomiche. Ogni OTP è accoppiata con un semplice flag per impedire il riuso di quel codice. Il grosso file sarà conservato in un posto sicuro, offline e inaccessibile a terzi. In caso di emergenza l’operatore consumerà gli OTP a sua disposizione, uno per ogni richiesta.

In seguito quando il gestore dovrà leggere i dati degli allegati email utilizzerà uno script che estrarrà l’OTP per decriptare quel file.

Cosa altro manca al sistema?

Una volta premuto invio non c’è conferma che l’operazione sia correttamente avvenuta. In questo caso si potrebbe prevedere una email di ritorno all’operatore ed una di notifica allo studente. Le email così accumulate potrebbero servire al gestore che ha creato disservizi per scusarsi del disagio con gli utenti coinvolti e per accertarsi che i dati siano stati correttamente inseriti in seguito.

Alla fine cosa abbiamo ottenuto?

Abbiamo offerto un servizio all’operatore che è affidabile come la carta ma molto più efficiente. Abbiamo aiutato tutte quelle persone che in quella settimana hanno dovuto rispondere al telefono e sorbirsi le lamentele per il disservizio. Ma in particolare abbiamo creato una procedura da seguire in caso di disservizio del server centrale per garantire continuità di servizio al cittadino.

Anche se le pratiche che si possono svolgere con queste sistema sono limitate, sviluppare un

sistema come quello descritto dall’articolo è veramente un gioco da ragazzi.

A cura di: **Francesco Ermini**