OsservatoriO AttacchInformatici

# Business Continuity a rischio? Le possibili cause

Si sono moltiplicati negli ultimi tempi notizie su blocchi informatici anche critici. Ecco cosa c'è dietro.

*M.R.A. Bozzetti, OAI founder*

Considerando il solo mese di febbraio 2011 appena trascorso, sui quotidiani e non solo sulle riviste tecniche sono apparsi, quasi ogni giorno, informazioni e articoli su malfunzionamenti e/o blocchi di importanti sistemi informativi, in Italia e all'estero. Nell'ultima settimana di febbraio 2011 sono occorsi ben quattro incidenti informatici ad altrettante Borse. Andando a ritroso dalla fine di febbraio, il 28/2 blocco del sistema per gli operatori della Borsa di Sydney, con conseguente blocco del listino e delle transazioni. Sull'evento Il Sole 24 Ore l'1/3/2011 titola un articolo Borse, il virus colpisce Sydney. Il termine virus è in questo caso improprio, ma di effetto e il giornalista usa il concetto come metafora per simili eventi occorsi nella stessa settimana in altre Borse. Infatti il 24/2, il CAC 40, il paniere principale della Borsa di Parigi, si ferma per più di un'ora per problemi tecnici al sistema informatico, con conseguente blocco del paniere nelle altre Borse, in particolare nei listini telematici di Amsterdam, Bruxelles e Lisbona. Il giorno prima, mercoledì 23, blocco del sistema informativo di Londra, anche se solo di poche ore. Martedì 22 febbraio, blocco di quasi sei ore al sistema in formativo della Borsa di Milano.

Blocchi limitati, ma a dir poco imbarazzanti dato che i sistemi finanziari, e in particolare quelli delle Borse, operando a livello mondiale 24 ore su 24, dovrebbero essere i più protetti e i più affidabili. Quali le cause per blocchi su piattaforme informatiche diverse e gestite da organizzazioni diverse? Le indagini sono in corso, ma si considera con maggior probabilità l'occorrenza di errori di sistema piuttosto che un attacco intenzionale. Sempre nell'ultima settimana di febbraio un incidente in casa Google: migliaia di caselle della posta elettronica Gmail svuotate a causa di un errore (bug) del programma software. In 24 ore il problema è stato risolto, ma è stato più complesso ripristinare tutti i contenuti nelle caselle postali. Il 6 febbraio è stato attaccato il portale del Governo italiano (www.governo.it) da parte di un gruppo di hacker chiamato Anonymous Italy (venuto alla ribalta per iniziative pro Wikileaks). L'attacco, preannunciato via Twitter e siti alternativi, è stato attuato tramite saturazione di risorse (DDoS, Distributed Denial of Service) provocando rallentamenti al sito ma non il suo collasso. Il 13 febbraio di nuovo attacco al sito del governo e al sito della Camera, che è rimasto inaccessibile per qualche ora, sempre da parte dello stesso gruppo e via DDoS. Nello stesso giorno si è avuto anche un oscuramento di circa mezz'ora del portale Mediaset. I problemi occorsi ai siti delle Borse e gli attacchi ai siti italiani hanno cause diverse, ma hanno portato allo stesso effetto: un'interruzione più o meno lunga del servizio erogato.

## Il codice non sicuro

Errori nei programmi e relative vulnerabilità (si veda sul tema L'errore nella programmazione genera vulnerabilità, pubblicato su *Office Automation* di luglio-agosto 2010 e scaricabile dal sito dell'autore, www.malaboadvisoring.it) sono fisiologici data la natura artigianale del software. Non considerando la volontà dello sviluppatore di inserire vulnerabilità nel codice o di lasciare porte nascoste e segrete dalle quali accedere anche da remoto, un programma software è il risultato dell'attività di una o più persone, la cui correttezza e qualità dipen-

dono dalla bravura ed esperienza, oltre che da quella degli analisti che hanno definito le specifiche funzionali del codice (e che possono non avere considerato casi molto particolari, che prima o poi capitano mandando in crisi il software).
Con la programmazione a oggetti e con i moderni linguaggi e ambienti di sviluppo certi errori non si verificano, e creare un programma consiste prevalentemente in un'attività di assemblaggio di moduli preesistenti, più che scrittura di codice. Ma anche i moduli possono contenere errori e/o vulnerabilità e il collaudo tecnico e funzionale del programma, fatto in maniera estensiva, richiede tempi e competenze non trascurabili, ossia costi non sempre sostenibili; in più il collaudo può essere fatto in maniera parziale, superficiale e/o non evidenziare errori che invece sono presenti. Nonostante best practice e linee guida, il software che si mette in produzione può avere vulnerabilità che possono portare al suo mal o non funzionamento.

## Dagli attacchi involontari a quelli volontari

Gli attacchi intenzionali ai sistemi informatici, se hanno successo, causano il blocco o il mal funzionamento dello stesso e di conseguenza provocano la non continuità operativa sua e dei processi aziendali che supporta. Attacchi tipo saturazione delle risorse (DoS/DDoS) come quelli effettuati sui siti istituzionali di cui sopra, sono specifici proprio per saturare i server che ospitano i siti target, e si basano sull'invio da parte di uno o più sistemi attaccanti di un altissimo numero di richieste contemporanee tali da saturare parzialmente o completamente il sito.
Non vengono manipolati programmi e informazioni, ma si cerca di rendere non più accessibile il sito inondandolo di richieste. In un prossimo articolo verranno approfondite logiche e strumenti per questo tipo di attacco. Attacchi intenzionali o errori e vulnerabilità nei programmi software possono portare a un blocco più o meno lungo della business continuity (1) del sistema informatico e di conseguenza al blocco dell'operatività del business stesso e ai conseguenti danni. La sicurezza assoluta ed eterna non esiste e non può esistere, e prima o puoi qualsiasi sistema informatico è sotto scacco, o per attacchi intenzionali o per suoi malfunzionamenti.

## Se la prevenzione fallisce si passa al ripristino

Oltre alle misure di protezione e prevenzione occorre quindi predisporre opportune misure di ripristino. Se si considerano i casi illustrati all'inizio e i tempi relativamente veloci riscontrati per la riattivazione dei servizi, significa che le misure di ripristino erano state predisposte e attuate: sicuramente blocchi di più di mezza giornata per ambienti così critici come quelli finanziari, o addirittura come quello di una Borsa, non sono tempi brevi, ma in sistemi così complessi e sviluppati ad hoc l'evento di un blocco a causa di un probabile errore del codice non può che essere risolto con l'individuazione e la correzione dell'errore, attività che possono richiedere tempi non brevi.
I casi considerati confermano una volta di più come un sistema informatico possa non funzionare o funzionare male, con dirette conseguenze sui processi e sul business supportato: e questo vale per sistemi e aziende di ogni dimensione e complessità, anche per aziende piccole o micro, per esercizi commerciali e per studi di professionisti, dall'avvocato al medico, dal notaio all'ingegnere.
Il vertice aziendale deve essere consapevole di questi rischi e deve tenerne conto: non solo attivare misure di sicurezza preventive e di protezione, tra le quali tempestivi aggiornamenti dei software con le patch e le nuove versioni rilasciate che correggono gli errori e le vulnerabilità, ma anche misure di ripristino: back-up sistematici e piani di Disaster Recovery. Le recenti disponibilità di soluzioni XaaS (2) e di cloud computing, oltre che di connessioni a banda larga (o medio-larga), a prezzi contenuti facilitano enormemente la possibilità di attivare repliche di ambienti quasi in tempo reale.

*(1) Il termine business continuity, in italiano traducibile in continuità operativa per il business, non fa riferimento solo ai sistemi informativi; la definizione data dal Gruppo di Lavoro omonimo del ClubTI di Milano specifica che è "un processo continuo che protegge il patrimonio aziendale sia in termini di infrastrutture tecniche a supporto del business, sia in termini di asset tangibili e non, al fine di garantire la continuità delle attività operative critiche e per assicurare i flussi degli introiti".*

*(2) XaaS è l'acronimo usato per includere i vari tipi di servizi erogati "as a service" su richiesta e pagati tipicamente a consumo: IaaS, Infrastructure as a Service, PaaS, Platform as a Service, SaaS, Software as a Service ecc. Per approfondimenti si rimanda al libro dell'autore "SOA – Libro Bianco dell'evoluzione della Enterprise Architecture" edito da Soiel e acquisibile on line (http://www.soiel.it/manuali/pop_19.htm)*