Perché WikiLeaks insegna alla tua azienda

9 dicembre, 2010
tags: Assange, business continuity, DDOS, digital economy, digital payment, online economy, pagamenti online, WikiLeaks
di Walter Vannini

Assegna un voto

Il caso Wikileaks ha almeno due cose da insegnare alle aziende, e non hanno nulla a che vedere con le polemiche.

Il primo passo per capire qualcosa è sempre quello di **distinguere ciò che è successo da come ci fa sentire**; è quello che nel counseling viene chiamato **feedback fenomenologico**. In questo modo possiamo rileggere gli avvenimenti degli ultimi giorni in maniera non-pregiudiziale e, naturalmente, non emotiva: allora cosa è successo negli ultimi giorni?

> Un'organizzazione nel corso della propria attività ha irritato nemici potenti che hanno espresso a gran voce propositi vendicativi.

Figure 4: A DDoS Attack

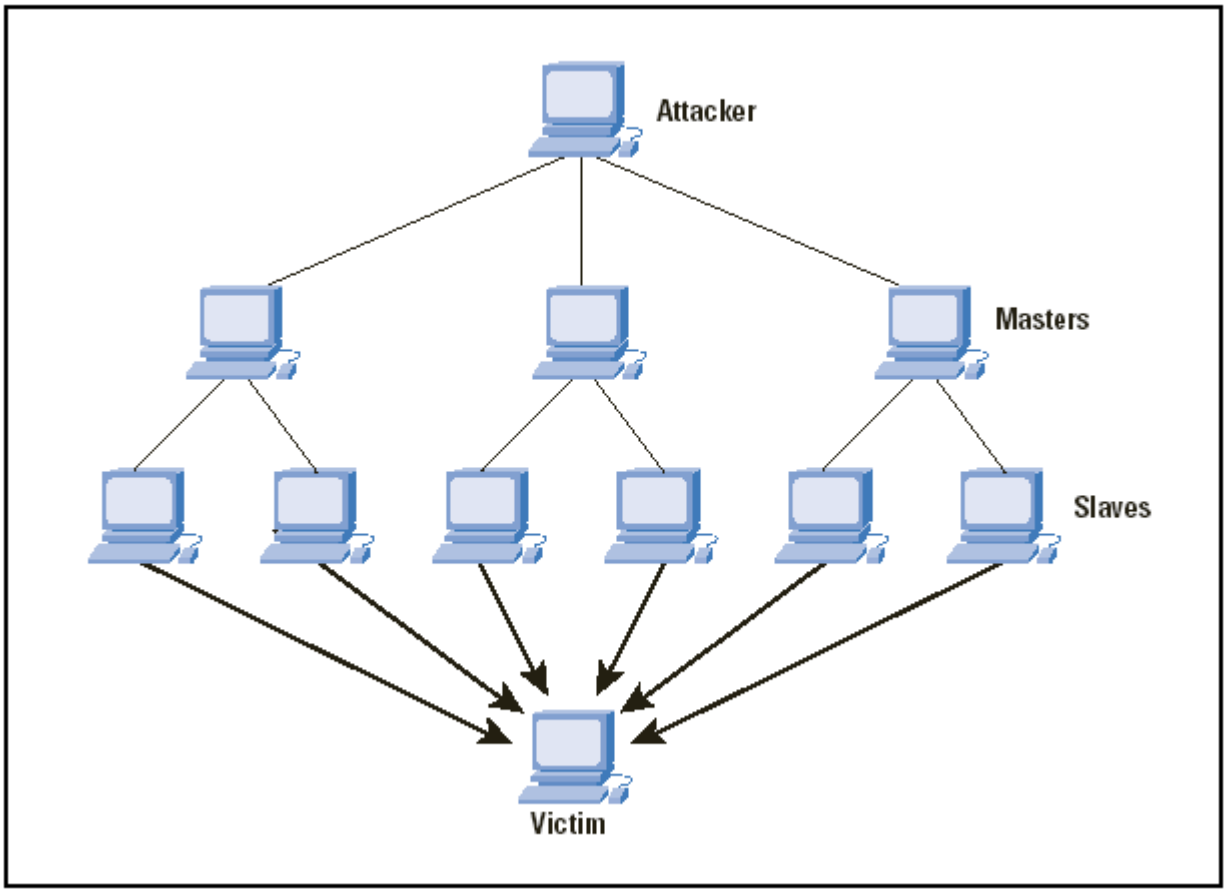

Diagramma di un Distributed Denial of Service (fonte: Cisco)

Non credo che la frase precedente possa essere migliorata senza inserire giudizi di valore che in questo contesto non ci interessano, quindi proseguiamo.

Allora, nel corso di una breve settimana:

1. il 28/11/2010 il sito di Wikileaks (wikileaks.org) è oggetto di un attacco DDOS (Distributed Denial of Service)

2. il 30/11/2010 il sito subisce un secondo attacco DDOS
3. l'1/12/2010 il provider Amazon interrompe il contratto di hosting
4. il 3/12/2010 il gestore del DNS di Wikileaks EveryDNS interrompe il servizio
5. il 3/12/2010 il sistema di pagamento online PayPal blocca donazioni e pagamenti a WikiLeaks
6. il 6/12/2010 anche Mastercard blocca donazioni e pagamenti a WikiLeaks
7. il 6/12/2010 la svizzera PostFinance blocca un conto usato per la raccolta di fondi intestato al fondatore di WikiLeaks
8. il 7/12/2010 anche Visa blocca donazioni e pagamenti a WikiLeaks…

…e questo è solo quello che è successo fino al momento in cui scrivo. La timeline completa è sul Guardian.

Dopo tutto ciò, e al momento in cui scrivo, WikiLeaks è pienamente operativo su WikiLeaks.ch e su svariate decine di mirror in contemporanea.

A questo la conclusione: a mia conoscenza, **nessuna azienda saprebbe mantenere l'operatività** a fronte di una simile serie di eventi avversi, e questo dovrebbe farci ragionare.

Lezione 1: la Business Continuity fa la differenza

Qui non stiamo parlando di disastri naturali, ma di **eventi ordinari e ripetibili**. Le aziende italiane tradizionalmente **sottovalutano i rischi** operativi, e ancor di più quelli legati alla infrastruttura informatica, nonostante oggi **senza computer ogni azienda smette di operare**.

WikiLeaks è un esempio eccezionale di Business Continuity: qualsiasi cosa succeda, *business as usual*. Nel caso specifico, WikiLeaks non solo ha **cambiato continente in 24 ore**, ma ha **replicato e ridondato** la propria infrastruttura rendendola **robusta** contro gli attacchi informatici e (almeno nel breve periodo) finanziari (grazie al fatto che il lavoro viene svolto su base volontaria).

E la tua azienda? Quante cose fuori dalla norma bastano perché tutto si fermi? Ecco una piccola lista di possibilità

1. la varicella blocca a letto tutti i tuoi informatici per una settimana
2. c'è un contenzioso amministrativo ed Enel sospende temporaneamente la fornitura
3. la Polizia Postale mette i sigilli ai tuoi server (ad es. per un caso di scarico di file piratati, o problemi di licenze)
4. due dischi dei tuoi server si rompono
5. il tuo provider Internet subisce un incendio
6. hai un problema di brevetti con le autorità cinesi; i tuoi uffici di Shanghai finiscono sotto sequestro.

Se tutte queste cose succedessero nel giro di tre giorni, che ne sarebbe della tua azienda?

Siccome ogni decisione aziendale deve vagliare costi e vantaggi, a che livello di problemi sei disposto a **chiudere bottega** fino a nuovo ordine?

Lezione 2: il Cloud è (ancora) un'infrastruttura fragile

La seconda lezione di WikiLeaks è forse anche più importante: il **Cloud Computing e l'infrastruttura dell'economia digitale sono fragili.**

Aziendalmente parlando, **Amazon, EveryDNS, PayPal, MasterCard e VISA hanno rescisso unilateralmente un contratto**, senza nessuna ordinanza legale. Lo hanno fatto perché, a loro giudizio, i termini del contratto non sono stati rispettati da WikiLeaks.

Può un'azienda correre lo stesso rischio? Io credo di no. Le aziende dipendono dall'informatica in

modo assoluto, ormai, e questo dovrebbe essere tenuto in conto anche nella redazione dei contratti di fornitura. Quando si tratta di **infrastruttura informatica** o finanziaria, il servizio **non può essere interrompibile a discrezione** della controparte, fatti salvi i casi conclamati di insolvenza.

Il Cloud Computing e la remotizzazione dei servizi rappresentano fonti di **risparmio** e di maggiore **efficienza? Sì,** e anche **potenziali rischi per la perdita di controllo** su processi vitali.

Un'azienda non può accettare che chi fornisce quei processi vitali possa interromperli a propria discrezione.

Quello che è successo in questi giorni a WikiLeaks succederà di nuovo, con molta meno enfasi mediatica, ad altre aziende. Magari per qualche appalto , magari per un contenzioso su brevetti o diritti, magari per "suggerire" un subappaltatore. Che un'azienda riceva pressioni è inevitabile. Ma **l'autonomia** e la **competitività** di un'azienda si basano anche sulla possibilità di **subire pressioni senza crollare** immediatamente.

Il nostro Paese sconta una arretratezza informatica enorme, ma questa non è una scusa. Se la tua azienda trascura il ruolo vitale dell'informatica e di Internet (e quindi non si impegna per renderne robusti processi e forniture) **stai costruendo sull'acqua**.