Sicurezza e siti web: cosa significa, e perchè non devi sottovalutarla su internet?

È fatta! Un altro gran bel sito è pronto per il rilascio, e dietro all'eleganza di un interfaccia utente intuitiva e semplice, di un layout grafico efficace e lavorato al minimo dettaglio si nascondono migliaia di linee HTML, blocchi di codice Javascript con funzionalità innovative a base di AJAX, jQuery, magari mixati con un po' di REST - e ancora, dal lato server, altre centinaia o migliaia di linee PHP, e tabelle SQL.

Tra te, il tuo sito ed il giusto compenso che renderà fattibili le agognate vacanze estive, il cliente e l'approvazione del sito. Il cliente che magari non è così a digiuno di IT in generale come cerca di dare a vedere, o forse lo è ma sa a chi appoggiarsi per le decisioni nel settore ... la dimostrazione del sito prosegue senza perder colpi, fino alla domanda fatidica, una variazione qualunque sul tema di:

"Ma è sicuro il sito?"

Puoi dare una risposta che lasci tranquillo te sulla spiaggia, e tranquillo il tuo cliente alle prese con il suo nuovo investimento?

In questo articolo cercherò di aiutare a dare non solo risposte motivate, ma anche a fare in modo che queste risposte siano sincere e soddisfino i requisiti di sicurezza dei siti web. L'argomento sicurezza, in realtà, è estremamente più ampio, e copre in maniera uniforme tutto ciò che coinvolge i nostri dati sia in termini di danni mal intenzionati che quelli causati da guasti software o hardware o anche eventi catastrofici, ma qui ci concentreremo soprattutto sulla sicurezza nelle Rich Internet Application e nei siti web dinamici (per comodità indicherò tutto semplicemente come 'siti web' - molti siti odierni hanno complessità anche superiori alle RIA classiche) e su come rendere più solidi i siti web basati su Javascript, jQuery, JSON, Apache, PHP e SQL. Quindi, su come fare non solo per andarci, in vacanza, ma anche per godersele senza rischiare di ricevere sotto il sole il classico:

"Ma ci sono foto sconce in home page!"

Concetti di base

Per prima cosa, sgombriamo il campo dalla domanda numero 1. **È possibile avere un sito sicuro al 100%?**

La risposta è la prima legge della sicurezza: **no, non è possibile**. Posso avere un sito sicuro al 100% *ora*, ma *dopo* non lo sarà, vuoi perché qualche genio in qualche parte del mondo scoprirà un nuovo modo per infrangere la security del server web, o perché un trojan nella struttura del cliente aprirà un passaggio da cui qualche pirata preleverà, tra gli altri files, anche le password del

backoffice del sito che qualche impiegato distratto avrà memorizzato in un file di testo sul desktop. O anche, molto banalmente, letta sul postit attaccato vicino alla tastiera sempre dal medesimo impiegato. Distratto, o anche malintenzionato: mai escludere nulla e nessuno.

Il primo concetto è lampante: la sicurezza del tuo sito è una catena molto, molto lunga, che comprende solo in parte la tua opera, ma anche strutture e personale:

- il lato utente, ovvero quello che il navigatore carica: HTML, CSS, Javascript, all'interno del browser che utilizza (Firefox, IE, Chrome, etc) e del sistema operativo (Windows, OS/X, etc);
- la rete internet, con tutti i punti di raccolta, i gateway, ovvero dove le nostre richieste HTTP viaggiano;
- la web farm, dove il nostro sito risiede fisicamente, tutti i files PHP, tutti i database;
- il lato del cliente: se l'applicazione ha un backoffice che permette al nostro cliente di gestire i database, o scrivere i testi, o scaricare immagini ... anche questo diventa un anello della nostra catena.

Ovunque esista una macchina ad accesso in rete, hai un possibile punto d'attacco tecnologico, basato su sicurezza di rete che lascia a desiderare, bugs software nuovi o vecchi e mai corretti (un caso molto comune al giorno d'oggi, dove i tagli di budget colpiscono senza pietà anche le fondamenta stesse di qualunque reparto IT), possibili intrusioni hardware.

Ovunque esista personale, non importa se dirigenti, impiegati o personale di servizio, hai un possibile punto d'attacco sociale, basato sul phishing, o su banalissima ingegneria dei rapporti umani che permette di carpire password a volte molto riservate ... semplicemente chiedendole al telefono. O sbirciando dietro la foto sulla scrivania, o sotto al mouse, o scritte in corpo 24 sull'etichetta del monitor LCD, o banalmente intuibili ...

L'integrità della catena è compromessa quando anche uno solo degli anelli viene compromesso. E da qui si ricava la seconda legge della sicurezza:

la sicurezza di tutta la catena è pari alla sicurezza dell'anello più debole.

Quindi: la catena è attaccabile in tutti i suoi punti ed in tutti i modi, tecnologici quanto sociali, con vari gradi di resistenza all'attacco. Alcuni sono assolutamente imprevedibili ed inevitabili, o impraticabili, ragione per cui un sito non sarà mai sicuro al 100%! E come sviluppatore web, puoi ben poco contro una buona parte di quei problemi.

Ma questo non significa lasciar perdere del tutto il problema: tutt'altro! Hai tre compiti:

1. creare un sito che non presti il fianco ad attacchi tecnologici - di questo parleremo dopo, e molto approfonditamente;

2. coinvolgere il cliente nel problema, assicurarsi che capisca gli attacchi sociali e sappia gestirli: se la nostra applicazione genera o usa password, non transigere sulla qualità delle password: le password 'uguali per tutti' non sono accettabili (oltre che, per i discorsi di tutela della privacy, illegali)! Che sappia e sia reso responsabile dei rischi che corrono i suoi dati: gli stessi che correrebbe se tutte le automobili come la sua avessero la stessa chiave;
3. preparare le risorse e gli strumenti nel caso dovesse succedere il peggio: copie del sito nelle varie versioni, backup, configurazioni, tool e materiali forensici - anche questo sarà argomento di discussione. E preparare anche le spiegazioni da fornire al cliente, quando necessario.

E se non lo fai? A parte il rischio, quasi certezza, di perdere un cliente magari importante in caso di problemi, potresti essere considerato come parte in causa, potresti non essere in grado di dimostrare di aver fatto del tuo meglio - perchè magari il tuo sito potrebbe essere usato come cavallo di troia per aver accesso a parti ben più critiche e riservate, e questo magari per un banalissimo

mal gestito all'interno di uno nei nostri php.

Come parlarne con il cliente?

È assolutamente necessario mantenere sin da principio un rapporto sincero con il cliente, ma allo stesso tempo essere forti sui propri argomenti. Il concetto che un sito non sia mai sicuro al 100% spaventa - ma la stessa cosa vale per un negozio, un automobile lasciata in un parcheggio, un appartamento, ancora di più se parliamo di banche, automobili di lusso e ville - in diretta proporzione. Nessuno rinuncia a comprare un automobile solo per il rischio che possa essere rubata: semmai, ci si preoccupa di custodire le chiavi, di parcheggiarla in un posto sicuro e di assicurarla!

Così come un antifurto in casa dissuade e scaccia, ma non da sicurezza assoluta, allo stesso modo la sicurezza su web dissuade e scaccia - e a differenza, ahimè, dei soldi nascosti in banca, noi possiamo effettivamente fare backup estremamente sicuri per permetterci, perlomeno, di ripristinare quanto danneggiato in tempi rapidi. Su questo, il cliente deve essere rassicurato.

In molti casi, il cliente capirà e sarà disposto a partecipare alla gestione della sicurezza. In altri lo sarà di meno, e le questioni che solleverà saranno una variazione su questi temi:

- "Non mi è mai successo!"
- "Non ci conosce nessuno - è un url che non si conosce!"
- "Non c'è nulla di valore nel sito!"
- "Non possiamo ricordarci tutte queste password strane!"

Temi che dobbiamo saper affrontare dimostrando di conoscere le risposte:

- non perché non è mai successo, significa che non possa succedere! È proprio sottostimando il pericolo che si causano i danni peggiori;
- i link si diffondono molto in fretta, non importa chi sei: grande o piccolo, sei sempre e comunque interessante per il fatto di avere uno spazio su web utilizzabile per altri scopi. Anzi: se proprio sei piccolo, sei interessante perché sei meno 'potente' dei grandi nomi, che possono permettersi di scatenare armate di avvocati da fare tremare la terra;
- lo spazio web, i dettagli dei clienti, la tua immagine ed il tuo marchio sono elementi di valore - puoi immaginare che effetto farebbe se accanto al tuo nome apparisse materiale, per così dire, ad alta risoluzione e colorito nei contenuti?
- le password sono l'equivalente delle chiavi - la complessità, nonché la frequenza con cui le cambiamo e la cura con cui le custodiamo le mantengono sicure.

Nel prossimo articolo, inizieremo ad esaminare la struttura completa di un sito web attraverso tutte le sue parti, come se fosse una casa e dovessimo valutarne la sicurezza osservando finestre, porte, serrature, muri e le facce di postini e addetti alla lettura del contatore.

Ma prima di allora, parliamo ...

Nei tuoi progetti, come hai affrontato il problema sicurezza di fronte ai clienti? Hai mai dovuto gestire situazioni di emergenza?