Dipartimento della Gioventù – POAT Per la Gioventù - CUP J71I09000020007

Supporto allo sviluppo della sicurezza e legalità informatica nell'ambito delle iniziative rivolte ai giovani

Michele Crudele - 2011-10-11

B.2.a) Linee guida sulla gestione dei portali secondo standard di sicurezza - Guida operativa

Premessa

La gestione dei portali si distingue in due attività principali, quella sistemistica e quella redazionale. Nel primo caso, il responsabile è un informatico che ha in carico il *web server* e l'eventuale CMS (*Content Management System*) sul quale è costruito il portale. Nel secondo, è più comune che la responsabilità sia affidata a un esperto di comunicazione, che non ha abitualmente conoscenze approfondite di informatica gestionale.

Il problema della sicurezza di un portale *web* va affrontato sia a livello sistemistico che contenutistico, soprattutto se sono attive funzioni avanzate di collaborazione, tipiche del *web 2.0*.

Questa breve guida pratica è rivolta a entrambi i responsabili, con indicazioni specifiche per ciascuno, in modo che sia garantita la sicurezza degli utenti nell'impiego delle risorse messe a loro disposizione.

Non è un trattato sulla sicurezza informatica e presuppone, per quanto riguarda il gestore di sistema, la conoscenza dei principi fondamentali e delle attività necessarie per la gestione sicura di un *web server*.

Non sono indicate fonti di ulteriori approfondimenti o archivi di programmi specializzati, perché facilmente reperibili in rete e soggetti a forte variabilità e aggiornamento.

In molti casi la gestione sistemistica dei portali è affidata a imprese specializzate. Questa guida può servire a coloro che devono preparare il bando di gara per l'affidamento della gestione, in modo da garantire che siano rispettati gli standard minimi di sicurezza.

È esclusa la situazione, particolarmente pericolosa, della gestione amatoriale di un portale su un computer gestito direttamente dall'incaricato, non collocato in un *data center*.

Introduzione

L'obiettivo comune di ogni portale destinato ai giovani è di raggiungere il massimo numero di destinatari fornendo loro i servizi previsti. Nel caso più semplice si tratta di informazioni o di documentazione oppure di riferimenti a risorse in rete. In altri casi, si cerca un dialogo con gli utenti, attraverso sistemi di pubblicazione e collaborazione che devono tutelare l'identità personale e garantire sicurezza informatica.

In tutte le situazioni non si può sottovalutare l'importanza di seguire alcune buone pratiche per la continuità del servizio e la prevenzione degli attacchi che spesso sono attivati automaticamente da programmi di scansione continua della rete, comandati da criminali in cerca di vittime. Non è una protezione sufficiente l'avere un portale poco conosciuto o poco importante: la maggior parte degli attacchi prescindono dalla portata mediatica e cercano normalmente di invadere computer per propagare i propri contenuti dannosi (*malware*) che hanno finalità abitualmente economica con furto di credenziali, diffusione di *spam*, vendita camuffata di materiale proibito.

La gestione sistemistica dei portali

Un portale *web* è un insieme di contenuti digitali accessibile via Internet. Può essere impostato su una varietà di *web server* di cui i più diffusi nel mondo sono Apache e Microsoft IIS che coprono l'80% circa delle situazioni. Il rimanente 20% utilizza altri *web server* più complessi o specializzati in particolari ambiti.

Un sito *web* può quindi essere semplicemente una collezione di pagine scritte in HTML statico, che non comportano particolari configurazioni, oppure avere caratteristiche dinamiche (PHP, .net, Java) che permettono l'accesso a basi di dati e danno agli utenti possibilità di pubblicare o realizzare contenuti elaborati e ricchi di effetti.

È sempre più diffusa la configurazione di un *web server* su un CMS (*Content Management System*) all'interno del quale sono gestite le autorizzazioni di pubblicazione, a volte estese anche all'utente finale.

Nei paragrafi seguenti sono indicate, in forma di glossario alfabetico, alcune buone pratiche, non esaustive, per tutelare l'integrità dei contenuti dei portali e dei dati degli utenti. Esistono programmi gratuiti, disponibili in rete, per gestire alcune delle caratteristiche elencate. Non è difficile recuperarli attraverso semplici ricerche su Internet, avendo cura di prelevarli da siti affidabili, come sono quelli delle riviste di informatica o dai siti ufficiali degli sviluppatori di ogni programma.

Aggiornamenti
È indispensabile attivare la segnalazione quotidiana degli aggiornamenti del sistema operativo e dell'eventuale CMS. L'installazione automatica può essere conveniente in alcuni casi, ma spesso provoca disservizi determinati da incompatibilità di programmi antichi. È più prudente supervisionare l'installazione degli aggiornamenti e monitorarne gli effetti.

Banda
Configurare un controllo di banda può prevenirne la saturazione da parte di un solo utente che attiva connessioni multiple dallo stesso IP al fine di accelerare lo scaricamento di contenuti o di perpetrare un attacco *denial of service*. Gli attacchi DDOS (*distributed denial of service*) sono più difficili da arginare ma nei *firewall* più attrezzati ci sono strumenti per mitigarne gli effetti negativi.

Business continuity
È un concetto più ampio dell'indispensabile *backup* quotidiano di tutti i contenuti, affiancato da un sistema di facile *restore*. È un'impostazione globale del sistema per evitare interruzioni del servizio. Dipende dall'importanza del portale quanto investire in *business continuity* attraverso virtualizzazione, *mirroring*, *load balancing*, *content delivery network* e altre tecniche di *high availability*.

Collegamenti
Controllare periodicamente i *link* nel portale alla ricerca di collegamenti sospetti o non pertinenti. Un effetto positivo del controllo è rimuovere i *link* non più validi, migliorando quindi la qualità generale dei contenuti del portale.

Database
Separare le basi di dati dal *web server*, collocandole su *server* diversi. Concedere l'accesso in sola lettura alle applicazioni che non devono modificare i dati. Mantenere un *log* delle transazioni degli utenti in scrittura, anche quando a livello di DBMS la credenziale di autorizzazione alla scrittura è unica per tutti.

Poiché i CMS devono poter effettuare operazioni di lettura e scrittura su uno o più *database*, conviene creare credenziali *ad hoc* con i permessi necessari, evitando di usare quelle del *db system administrator*.

Firewall
È assolutamente necessario installare il *server* dietro un *firewall* opportunamente configurato per far passare esclusivamente le richieste necessarie, con i protocolli e le porte TCP definiti. Non è però più sufficiente limitarsi al filtraggio delle connessioni: è importante dotarsi di sistemi di *Intrusion Prevention* (IPS) e *stateful inspection*.

Password
Implementare una politica di gestione *password* robusta e sicura. Evitare di memorizzare le *password* in chiaro o semplicemente codificate: usare *hash*, possibilmente con algoritmi del livello di sicurezza di SSHA.

Imporre *password* non banali, obbligando a usare almeno 8 caratteri tra lettere, numeri e altri segni.

Non inviare *password* via posta elettronica agli utenti per conferma o per variazione, ma spedire un *link* a una pagina *https* dove poter reimpostare la propria *password* in caso di dimenticanza o di scadenza: in questo modo nessuno, tranne l'utente, è in grado di conoscerla.

Permessi
Concedere agli utenti solamente i permessi minimali per svolgere le funzioni a loro affidate.

Disabilitare gli utenti predefiniti del *web server* e del CMS, creandone *ad hoc* con i permessi desiderati. Sfruttare il *Role Based Access Control* (RBAC) tipico dei più diffusi CMS.

Le credenziali di amministratore devono essere nominali e non condivise tra più persone: in questo modo si può risalire all'autore di operazioni che hanno conseguenze importanti. In questo ambito ci sono anche disposizioni precettive del Garante della Privacy per quanto riguarda gli amministratori di sistema.

Nell'installare un CMS verificare il modo in cui gli utenti esterni accedono alle cartelle del *web server* per evitare che possano essere sfogliate, rivelandone tutto il contenuto.

Privacy
Se sono previste registrazioni di dati personali degli utenti, consigliare al gestore dei contenuti di limitare la richiesta a quelli effettivamente necessari. Prestare particolare attenzione quando sono presenti dati sensibili o si tratta di minorenni: è consigliato crittografare questi dati e renderli disponibili solamente all'utente stesso oppure per uso aggregato.

Programmazione
Evitare di dare al gestore dei contenuti e agli utenti la possibilità di inserire codice di programmazione nelle pagine, al di fuori di alcuni modelli preordinati come *script* per video o moduli di richiesta.

Servizi
Disabilitare sul *web server* tutti i servizi non effettivamente utilizzati, come possono essere *ftp*, *nntp*, *telnet*, *finger*, condivisione dei file e altri.

Statistiche
Controllare le statistiche di accesso, non solo ai fini informativi del traffico, ma anche per analizzare comportamenti sospetti.

Transazioni sicure
Usare *https* in tutti i casi in cui è prudente evitare qualsiasi pericolo di intercettazione, come nella fase di creazione di un'utenza o di autenticazione (immissione di utente e *password*). Acquistare un certificato SSL per dare garanzia di qualità e sicurezza all'utente, e aggiornarlo prima della sua scadenza.

La gestione di un CMS

Nella maggior parte dei casi l'incaricato della redazione di un portale agisce tramite un sistema di manipolazione di contenuti, chiamato CMS (*Content Management System*). Ne esistono molti sul mercato e sono molto diffusi alcuni gratuiti.

Il gestore dei contenuti ha in questo caso una serie di autorizzazioni concesse dall'amministratore del sistema, che possono variare dalla semplice modifica di pagine esistenti o creazione di nuove secondo modelli predefiniti, alla possibilità di inserire nuovi moduli per fornire servizi avanzati.

Normalmente è esclusa la possibilità di inserire codice di programmazione che, anche senza intenzione maligna, potrebbe contenere errori utilizzabili da coloro che cercano falle di sicurezza per impadronirsi di portali a scopo criminale.

Le poche buone pratiche di seguito indicate, elencate in base all'importanza, non sono esaustive ma permettono di limitare i rischi di sicurezza di un portale.

Rapporto con il gestore o amministratore di sistema
Il compito della sicurezza del portale è soprattutto in mano al gestore o amministratore di sistema. Concordare perciò con lui una procedura di comunicazione rapida per segnalare anomalie, errori e rischi potenziali. Dialogare per trovare soluzioni che concilino la sicurezza con la funzionalità.

Dati degli utenti
Non richiedere agli utenti dati non strettamente necessari. Non utilizzare i dati personali degli utenti senza la loro esplicita autorizzazione. Assicurarsi che le procedure di iscrizione, autenticazione, cambio *password*, siano gestite in modalità protetta (*https*).

Studiare con attenzione le conseguenze legali della eventuale richiesta di dati a minorenni.

Forum e pubblicazioni degli utenti
Assicurarsi che gli utenti non possano pubblicare codice di programmazione (*javascript* o simili) perché potrebbe essere pericoloso per gli altri. Valutare con attenzione se lasciare agli utenti la possibilità di pubblicare *link* a siti esterni, perché potrebbero essere utilizzati per *spam* commerciale o per finalità inopportune o criminali.

Collegamenti esterni
Limitare i *link* a pagine esterne al portale, curando di verificarne periodicamente la validità. Non è infrequente che un dominio passi in mano di un altro proprietario che ne gestisce i contenuti in modo diverso e non adeguato agli obiettivi del portale di riferimento: per esempio, un *link* che oggi contiene documentazione scolastica potrebbe domani contenere pornografia.

Indicizzazione nei motori di ricerca
Curare i *meta tag* utilizzati dai motori di ricerca, in modo che il portale risponda a parole chiave opportune e non sia indicizzato o catalogato automaticamente, partendo da particolari parole, in portali dedicati ad attività indecenti o illegali.

Un effetto positivo di questa attenzione sarà la visibilità del portale e l'aumento di traffico utile ai fini dell'obiettivo del portale stesso.

Fare formazione sulla legalità informatica
Valutare l'opportunità di inserire nel portale brevi spiegazioni per gli utenti su questioni di legalità informatica (tutela del diritto d'autore, rischi della navigazione, attenzione a truffe, ecc.). È obbligatorio inserire le informazioni sulla *privacy* soprattutto se si ospita pubblicità che raccoglie dati sulla navigazione dell'utente.

Michele Crudele - 2011-10-11