Sicurezza dei sistemi e-commerce

Valerio Morfino[1] and Claudio Fornaro[2]

[1] Futuridea Innovazione Utile e Sostenibile, Via Piano Cappelle, Benevento, Italia
valerio.morfino@ctcgroup.it
[2] Università Telematica Internazionale Uninettuno,Corso Vittorio Emanuele II, 39, Roma, Italia
c.fornaro@uninettunouniversity.net

Abstract. L'utilizzo delle applicazioni di commercio elettronico, sia quelle rivolte agli utenti finali (B2C) che quelle rivolte ad utenti professionali (B2B) stanno crescendo in modo importante a livello globale. Contemporaneamente, si assiste alla crescita dei rischi di sicurezza legati all'utilizzo di Internet. Nell'articolo vengono analizzati i principali aspetti relativi alla sicurezza dei siti e-commerce da un punto di vistra infrastrutturale, funzionale e di integrazione con altri software, quali gli ERP.

Keywords: e-commerce, B2B, B2C, Sicurezza Informatica, Cybercrime, ERP.

1 Introduzione

Il mercato e-commerce sta crescendo velocemente ed in modo significativo. Nel 2016 il solo mercato italiano B2C (Business to Consumer), ossia la vendita al dettaglio su Internet, ha registrato un fatturato che sfiora i 20 Mld di euro [1]. A livello globale si stima che nel 2020 il mercato B2C varrà 3600 Mld di dollari e 6.700 Mld il mercato B2B (Business to Business), ossia la vendita online tra aziende [2]. La crescita di questo mercato avviene in un luogo virtuale frequentato da un pubblico molto variegato, buona parte del quale non è umano e nemmeno ben intenzionato: solo il 44% del traffico web viene generato da esseri umani, mentre ben il 55% viene generato da sistemi automatici ("bot"), da strumenti con finalità di hacking e di spam [3]. Negli ultimi anni si segnala un significativo aumento dei reati relativi ai sistemi informatici online. Viste in una "prospettiva criminale" le frodi online sono più semplici, spesso più redditizie e soprattutto meno rischiose, considerati i limiti oggettivi che caratterizzano l'attività investigativa e giudiziaria e la cooperazione internazionale in materia di reati commessi in Rete [4]. Le tendenze globali mettono in evidenza il carattere organizzato e transnazionale dei criminali, sempre più spesso legati al terrorismo [5]. I grandi operatori di eCommerce e di mCommerce (mobile Commerce) sono i soggetti più colpiti [6]. Questi fenomeni possono rendere rischioso l'utilizzo del commercio elettronico e minare la fiducia di acquirenti e venditori verso uno strumento capace di formidabili possibilità di business. Nell'articolo verranno evidenziati i principali elementi che hanno un ruolo significativo nell'ambito della sicurezza dei siti di e-commerce in termini di integrità, disponibilità e riservatezza.

2 Infrastruttura Hardware e Software

Un sito e-commerce è un negozio virtuale che deve essere sempre aperto in quanto navigato ad ogni ora del giorno ed in ogni giorno dell'anno [1, 7]. Inoltre i bot dei motori di ricerca, in testa Google, ne scandagliano continuamente i contenuti. La non raggiungibilità comporta un impatto negativo sul posizionamento del sito [8], normalmente ottenuto con investimenti, spesso importanti, in attività di Web Marketing.

Per fare sì che il sito sia sempre "aperto" è fondamentale avere una infrastruttura di base che possa garantire adeguati livelli di sicurezza e di disponibilità. Per questo è sempre più comune che i siti di e-commerce non risiedano su un server presso l'azienda venditrice, ma su una infrastruttura presso un Internet Service Provider, sempre più spesso in modalità Cloud. Un provider, grazie ad un'adeguata struttura di data center è in grado di garantire diverse caratteristiche fondamentali per la sicurezza, quali, a mero titolo esemplificativo, la sicurezza fisica dei server (accesso fisico, protezione da incendi, ecc.), la continuità elettrica, la ridondanza della connessione verso Internet, nodi di backup, firewall e diversi altri. Vengono, inoltre, comunemente garantiti servizi sistemistici quali monitoraggio, presidio 24 ore, backup e sempre più speso disaster recovery. Inoltre, a richiesta, sono spesso disponibili sistemi o servizi in grado di aumentare la sicurezza delle comunicazioni (es. VPN), la resistenza agli attacchi e diversi altri.

Da un punto di vista software, un sito di e-commerce viene generalmente realizzato a partire da un prodotto, nel caso di software commerciali, i produttori offrono sempre una "Software Assurance" che comprende aggiornamenti di sicurezza periodici che, in base al contratto, possono essere installati dal Fornitore o dall'IT dell'azienda cliente.

Anche grazie all'assenza di costi di licenza d'uso, molto diffuso è l'utilizzo di software open source. Benché si possa ritenere che, essendo software molto diffusi e valutati da un'ampia "comunità", vi sia un ottimo controllo della qualità, va considerato che non vi è alcuna software assurance. Va inoltre prestata particolare atenzione per gli "add-on" che permettono di estendere le funzionalità dei principali software open-source, normalmente disponibili in marketplace specifici. Non sempre gli add-on di terze parti hanno la stessa qualità del prodotto base e non sempre ci si ricorda di prestare attenzione agli aggiornamenti di sicurezza per essi rilasciati. In generale l'uso di add-on non certificati e in generale non strettamente necessari aumenta la superficie di attacco, in particolare se non sottoposti a opportuni controlli.

3 Vettori di attacco al software e-commerce

Un software di e-commerce può essere attaccato sul canale di comunicazione o su delle sezioni specifiche. I principali attacchi sul canale di comunicazione, quali Intercettazione di dati, Hijacking (dirottamento della sessione), Man In The Middle (MITM - dove una terza parte si frappone tra utente e sito e impersona l'uno per l'altro), ed altri, possono essere evitati cifrando il canale grazie a protocolli sicuri quali SSL/TLS, che corrispondono all'utilizzo del protocollo applicativo HTTPS al posto di HTTP.

In un sito, la sezione di autenticazione è tra le più soggette ad attacco. Nel caso di siti B2C essa avviene comunemente utilizzando Userid e Password o tramite "Social

Login". Il caso di maggiore vulnerabilità è quello relativo all'uso di autenticazione tramite Userid/Password, soggetto ad attacchi tipo Brute Force o di Dizionario. Per questi attacchi, lato applicativo, possono essere adottate una o più contromisure quali Captcha (Completely Automated Public Turing test to tell Computers and Humans Apart); limitazione del numero di tentativi di login; tecniche basate sull'uso di Token. Specialmente per i siti B2C, è importante valutare l'impatto sull'usabilità di queste tecniche: la perdita di utenti/clienti per via di pagine di difficile utilizzo significa perdita di risorse economiche investite in pubblicità. Considerazioni analoghe sono valide per la sezione relativa alla Richiesta di Registrazione al sito.

Altra sezione importante è quella relativa al pagamento. In generale, le modalità di pagamento possono essere offline (ad es. bonifico Bancario o RID) e online. Le modalità di pagamento online prevedono una transazione diretta ed in tempo reale con una banca o con un sistema di e-wallet, quale PayPal. E' possibile adottare due strategie di integrazione verso il Gateway di pagamento, entrambe sicure se correttamente implementate. La prima consiste nell'inglobare il meccanismo di pagamento direttamente nel sito e-commerce, mascherando al cliente l'interazione con il sistema esterno. Il numero della carta di credito, benché non memorizzato nel sito (che ha solo un token), comunque vi transita ed è quindi fondamentale che il sito sia navigato con il protocollo HTTPS. La seconda possibilità è di reindirizzare il cliente alla pagina della banca, che è sempre protetta da una connessione SSL/TLS, per completare il pagamento. La scelta della modalità da usare va considerate anche in termini di comunicazione. Infatti per un sito e-commerce relativo ad un marchio importante, il cliente tenderà a fidarsi e sarà lieto di non dover essere reindirizzato ad un sito esterno per effettuare il pagamento. Per un sito relativo ad un marchio non (ancora) di grande notorietà o in startup, il cliente potrebbe fidarsi maggiormente ad effettuare il pagamento sul "sito della banca".

4 Connessione con sistemi esterni

I sistemi e-commerce hanno necessità di colloquiare con diversi sitemi esterni, quali ERP, CRM, Marketplace (come Amazon e Ebay) e diversi altri. A titolo esemplificativo esamineremo il caso particolarmente rilevante dell'ERP aziendale.

Lo scambio dati tra sistemi e-commerce ed ERP può avvenire in modalità asincrona o sincrona. La prima viene generalmente utilizzata per dati che vanno aggiornati periodicamente, la seconda per dati che vanno aggiornati o verificati in tempo reale.

La modalità sincrona è una scelta normalmente desiderata dal venditore perché, anche da un punto di vista emotivo, comunica la sensazione di un allineamento dei sistemi in tempo reale (o meglio quasi tempo reale essendovi comunque un ritardo). In molti casi questa scelta è necessaria, ma in altri potrebbe non esserlo. Un semplice esempio, che potremmo chiamare del "cassiere imbarazzato" rende bene l'idea. Immaginiamo di avere la disponibilità di un prodotto P, in quantità 1, condivisa tra un e-commerce ed un negozio fisico. Siano le giacenze di e-commerce e negozio allineate in tempo reale. Un acquirente A presso il negozioprende il prodotto dallo scaffale. Intanto un acquirente e-commerce, benché i due sistemi siano allineati in tempo reale, non ha notizia di

questo fatto e riesce a mettere il prodotto P nel suo carrello virtuale, completando l'acquisto e pagando. Il cliente del negozio, intanto, va alla cassa per pagare. A questo il cassiere imbarazzato si trova innanzi ad un dilemma: a chi vendere l'unico prodotto P?

Il semplice fatto di avere un allineamento delle giacenze sincrono e (quasi) in tempo reale non offre di per sé le garanzie di allineamento richieste dal business. Di contro, un collegamento sincrono crea una dipendenza forte tra i due sistemi che può avere degli impatti sulla disponibilità del sito. Infatti, se per qualsiasi motivo i sistemi non fossero in grado di comunicare, la disponibilità del sito (o quantomeno parte di esso) sarebbe fortemente minata. Inoltre, lato ERP è necessario un servizio per rispondere alle richieste del sito. Questo può aumentare la superficie di attacco verso l'interno dell'Azienda che, specialmente nel caso delle PMI, è spesso priva delle più elmentari misure di sicurezza e sempre più frequentemente oggetto di attacchi ransomware quali Cryptolocker [9].Quindi, in generale, sono da evitare funzionalità che aumentino la superficie di attacco senza dare benefici al business.

5 Conclusioni

In questo articolo sono stati messi in evidenza gli elementi principali relativi agli aspetti di sicurezza dei siti di commercio elettronico, alcune pratiche comunemente utilizzate per mitigarne alcuni rischi ed alcuni punti di attenzione nell'adottare queste pratiche.

In conclusione occorre sottolineare quanto sia importante non solo porre attenzione a tutti gli aspetti di sicurezza, ma anche comunicarli all'Azienda che deve investire per proteggere il proprio business e la propria reputazione online. Questo potrà certamente aumentare la fiducia di clienti e negozianti ed essere un fattore abilitante per uno sviluppo sempre più sostenuto dell'e-commerce.

References

1. Rangone A., Liscia R., Perego A., Mangiaracina R., L'ECOMMERCE IN ITALIA CRESCE DEL 18% E SFIORA I 20 MLD DI € NEL 2016, Politecnico di Milano, 2016
2. Future of B2B Online Retailing, The Global B2B E-commerce Market Will Reach $6.7 Trillion by 2020, Frost & Sullivan Research, 2014
3. List of Internet, E-commerce & Hosting statistics for 2016, Internet Stats & Facts for 2016 https://hostingfacts.com/internet-facts-stats-2016/, last accessed 2017/04/03
4. Rapporto statistico sulle frodi con le carte di pagamento No. 5/2015, Ministero dell'Economia e delle Finanze, 2015
5. A. Acharya, Targeting Terrorist Financing: International Cooperation and New Regimes, Routledge, 2009
6. True Cost of Fraud Study. Post-Recession Revenue Growth Hampered by Fraud As All Merchants Face Higher Costs, LexisNexis, 2014.
7. E-commerce Consumer Behaviour Report 2011, Consorzio Netcomm, Contactlab, 2011
8. Google Webmaster Central Blog, https://webmasters.googleblog.com/2011/05/do-404s-hurt-my-site.html, last accessed 2017/04/04
9. Rapporto sulla Sicurezza ICT in Italia 2015, Clusit, 2015 http://www.clusit.it/download/Rapporto_Clusit%202015.pdf, last accessed 2017/04/04