
Report S1-L3 Digital Risk Management

Identificazione del rischio

a cura di:

Lisa Bonato

Maria Flavia Minotti

Alex Fiorillo



B F M CYBER

Sommario

Traccia	3
Su cosa stiamo lavorando?.....	3
Treath Modelling.....	3
Cosa potrebbe andare storto?	4
Vulnerabilità.....	4
Minacce	4
Cosa faremo al riguardo?	6
Abbiamo fatto un buon lavoro?	7
GAP Analysis	8
Road Map	9

Traccia

Utilizzando il framework di modellizzazione delle minacce di Adam Shostack, identifica una minaccia per un'azienda di sviluppo software.

Su cosa stiamo lavorando?

Cosa può andare storto?

Che cosa faremo al riguardo?

Abbiamo fatto un buon lavoro?

Ripeti il processo, eseguendo una gap analysis per trovare i punti di miglioramento.

Su cosa stiamo lavorando?

La start-up Bonny, Fiorils & Mino Cyber è nata con lo scopo di sviluppare un e-commerce intuitivo e userfriendly che sia allo stesso tempo di facile fruizione per i nostri clienti (lato back end).

Tramite lo sviluppo di un prototipo innovativo di software, dettagliato e frutto di approfonditi anni di ricerca siamo in grado di fornire una piattaforma facilmente customizzabile e modulabile su esigenze specifiche del cliente.

Siamo convinti dell'importanza di supportare la customer experience a 360° e pertanto ci impegniamo nel garantire non solo la costruzione del vostro e-commerce ideale ma anche un servizio di assistenza post vendita sempre disponibile.

Scopo del Report

I nostri tre soci fondatori condividono i valori della trasparenza, informazione, sicurezza e controllo che ritengono essenziali per sviluppare una solida relazione di business che possa perdurare nel tempo.

Sulla base di queste credenze si è deciso di pubblicare il seguente report relativo al Risk Management del nostro prodotto affinché tutti - potenziali acquirenti, clienti e investitori – possano visionare il processo di messa in sicurezza del software.

Infatti la Bonny, Fiorils & Mino Cyber affonda le proprie radici nell'esperienza dei suoi componenti nel mondo della sicurezza informatica, di cui una componente fondamentale è la sicurezza delle applicazioni Web.

Come si vedrà il nostro è un processo di mitigazione dei rischi in continuo divenire vista la natura evolutiva dell'innovazione digitale e quella mutevole delle minacce informatiche.

Treath Modelling

Utilizzeremo i framework di Shostack's 4 e STRIDE per effettuare il Threat modelling, cioè il processo di identificazione dei rischi che prevede l'esame di ogni possibile attore malevolo, azione o evento, vettore di attacco e vulnerabilità per un determinato sistema, bene o processo.

Cosa potrebbe andare storto?

Durante l'elaborazione del nostro software abbiamo proceduto ad effettuare l'identificazione delle vulnerabilità che potrebbero essere sfruttate da minacce, cioè eventi che, qualora dovessero verificarsi, avrebbero un impatto negativo sulle organizzazioni dei nostri acquirenti. Si procede, quindi, all'identificazione delle minacce stesse e alla loro analisi.

Vulnerabilità

Software

- Mancata sanificazione input utente, sia nella casella di input sia nel modulo web
- Utilizzo di librerie obsolete o pericolose poiché pubblicamente sfruttate per exploit
- Mancata previsione di un sistema di gestione degli errori
- Errori nelle configurazioni di sistema
- Mancanza di Patch di sicurezza
- Assenza o difetto nel processo di autenticazione per l'accesso
- Mancanza di un sistema di gestione delle sessioni utente

Dati

- Gestione inadeguata dei dati
- Mancata crittografia dei dati sensibili
- Assenza di meccanismi di ripristino dei dati

Processi

- Mancanza di adeguata Registrazione e monitoraggio delle attività dell'applicazione in tempo reale
- Assenza di formazione e conoscenza circa le minacce informatiche

Fisiche

- Mancanza di adeguate barriere architettoniche in caso di disastri ambientali
- Mancanza di adeguate misure di protezione fisica dei dispositivi, quali i server della società

Minacce

Per l'individuazione e classificazione delle minacce informatiche alla sicurezza dell'e-commerce si è deciso di utilizzare il Framework **STRIDE** che è l'acronimo per le sei principali minacce informatiche. In più sono state aggiunte **ulteriori minacce** che ricomprendano anche le altre vulnerabilità rilevate, in particolare quelle sui processi e fisiche.

Spoofing: tecnica ingannevole utilizzata per falsificare l'identità di un mittente o di una fonte di informazioni, al fine di trarre in inganno il destinatario, per esempio mascherando il proprio indirizzo IP con quello della macchina vittima (Autenticazione). **4/5**

Tampering: minaccia che consiste nella manipolazione non autorizzata di dati o configurazioni di sistema, ad esempio sfruttando la mancanza di crittografia o errori nell'architettura del software.

In tal modo un aggressore potrebbe cambiare la descrizione di un prodotto o aumentare l'importo di una transazione finanziaria sull'e-commerce. **2/5**

Repudiation: questa minaccia significa letteralmente negazione di un'azione.

Si tratta del caso in cui non sia possibile verificare l'autenticità di un'azione e colui che la compie per via dell'assenza di meccanismi di monitoraggio e controllo delle attività dell'applicazione. **1/5**

Information disclosure: è la rivelazione di informazioni riservate operata da aggressori che sfruttano l'assenza o difetti nell'autenticazione o l'assenza di adeguata crittografia per rubare dati attraverso sniffing del traffico di rete con Man in the middle. **3/5**

Denial of service: questa minaccia consiste nell'Interruzione del servizio per gli utenti legittimi, impedendo loro di accedere al servizio di e-commerce.

In questo caso un aggressore potrebbe utilizzare una botnet, un insieme di dispositivi infetti, per inviare un ingente quantità di traffico al fine di sovraccaricare il server. **5/5**

Elevation of privileges: consiste nell'ottenere l'accesso non autorizzato a un livello superiore di diritti di accesso o autorizzazioni all'interno di un sistema.

Ciò consente agli aggressori di eseguire azioni che non dovrebbero essere in grado di compiere, come modificare le impostazioni di sistema o eliminare file critici di sistema.

Un caso è quello in cui un aggressore sfrutti vulnerabilità del software per ottenere l'accesso da amministratore, utilizzare credenziali rubate per accedere a un account con privilegi elevati, o indurre un utente a concedere più autorizzazioni del necessario. **4/5**

Altre minacce

Errore umano: questa minaccia va intesa in senso ampio come errore nella programmazione del software da parte degli sviluppatori ed errore nella gestione dei sistemi della startup. **4/5**

Disastri naturali: eventi naturali che possono impattare la start up creando danni di vario tipo ma la cui verifica è più complessa e non facilmente ripetibile a livello di frequenza **1/5**

Danneggiamento o furto dei dispositivi (server): In caso di compromissione dei dispositivi è il danno per la start up potrebbe essere ingente con conseguenze economiche importanti.

Cosa faremo al riguardo?

Una volta individuate le vulnerabilità e le relative minacce che possono sfruttarle, abbiamo stilato un elenco di azioni di mitigazione al fine di ridurre il rischio, inteso come probabilità che le minacce si verifichino e producano impatti dannosi.

Sanificazione dell'input utente:

Validare e sanificare rigorosamente tutti i dati di input, sia da form che da caselle di input, per prevenire attacchi di injection come SQL injection, cross-site scripting (XSS) e injection di directory traversal.

Questo implica la creazione di filtri o funzioni di sanificazione che rimuovono caratteri dannosi o non consentiti dagli input dell'utente. Inoltre, è importante validare i dati inseriti per assicurarsi che rispettino i formati previsti e non contengano dati dannosi.

Aggiornamento software e utilizzo di librerie sicure:

- Evitare l'utilizzo di librerie obsolete o note per essere vulnerabili a exploit conosciuti preferendo invece librerie sicure, rimanendo aggiornati sugli avvisi di sicurezza per i prodotti e le librerie web più utilizzati.
- Implementare e distribuire versioni più recenti e patch di sicurezza del software, monitorando costantemente le vulnerabilità pubblicate relative a web application.

Gestione degli errori:

Implementare un sistema di gestione degli errori robusto che registra e gestisce correttamente gli errori, evitando di esporre informazioni sensibili o dettagli di implementazione nei messaggi di errore.

Configurazione sicura del sistema:

- Indurire le configurazioni di sistema e dei server web per ridurre la superficie di attacco da parte di malintenzionati.
- Disabilitare servizi e funzionalità non necessari.
- Applicare i principi di "difesa in profondità" con più livelli di sicurezza.

Autenticazione robusta e Gestione delle sessioni utente:

- Implementare un processo di autenticazione forte che richieda credenziali univoche e robuste per l'accesso.
- Utilizzare l'autenticazione a due fattori (2FA) per un ulteriore livello di sicurezza.
- Evitare l'utilizzo di meccanismi di autenticazione basati su token o cookie.

Gestione sicura dei dati:

- Limitare l'accesso ai dati sensibili solo agli utenti e ai sistemi autorizzati.

Crittografia dei dati:

- Utilizzare protocolli sicuri di comunicazione come HTTPS.
- Crittografare i dati utilizzando algoritmi di crittografia forti.
- Utilizzare crittografia asimmetrica.

Recupero dei dati:

- Implementare un piano di ripristino dei dati completo e testato regolarmente.
- Effettuare backup regolari dei dati sensibili.
- Avere procedure per il ripristino rapido dei dati in caso di incidente informatico.

Registrazione e monitoraggio:

- Registrare e monitorare tutte le attività dell'applicazione web in tempo reale.
- Analizzare i log regolarmente per identificare attività sospette o anomale.
- Implementare un sistema di alerting per notificare gli eventi di sicurezza critici.

Errore umano e Formazione sulla sicurezza informatica:

- Fornire una formazione regolare e aggiornata sulla sicurezza informatica a tutti gli sviluppatori, gli amministratori e gli utenti, sensibilizzando anche sui rischi comuni delle web application e su come prevenirli.
- Incoraggiare la segnalazione di potenziali vulnerabilità o incidenti di sicurezza.

Furto e danneggiamento:

Introduzione di videocamere di sorveglianza e di un sistema di controllo perimetrale (sensori intorno alla società).

Disastri naturali

Previsione di adeguate misure architettoniche per la tutela dei beni tangibili della start up e sistema.

Abbiamo fatto un buon lavoro?

Dopo un'attenta analisi del NIST SP 800-53 Rev. 5, abbiamo identificato i controlli di sicurezza necessari da implementare nel sistema della start up.

Valutazione dell'efficacia dei controlli implementati

Monitoraggio continuo dell'ambiente di sviluppo per identificare e rispondere alle minacce alla sicurezza.

Esecuzione di scansioni periodiche per identificare e correggere vulnerabilità nel software in fase di sviluppo.

Piano di formazione del personale circa minacce e rischi informatici.

Eseguire procedure di gestione del rischio periodiche per individuare nuove minacce e sviluppare innovative azioni di rimedio.

Procedura di controllo degli accessi basata sulla protezione dei dati, che assicuri la disponibilità degli stessi solo ai soggetti aventi diritto.

Sviluppare una procedura di Gestione del rischio in caso di calamità naturali.

Sviluppare una procedura di controllo circa la manutenzione, riparazione e sostituzione dei dispositivi.

Controllo periodico della validità degli strumenti di registrazione e monitoraggio delle attività aziendali, in particolare relativi all'e-commerce.

GAP Analysis

Si procede ora ad effettuare il processo di valutazione delle discrepanze o delle lacune tra la situazione attuale e quella desiderata in termini di gestione del rischio cui può essere sottoposta la Bonny, Fiorils and Mino Cyber.

Dati e account:

Attuale: Manca un sistema che preveda l'eliminazione dei dati sensibili una volta che non siano più necessari e che determini la rimozione degli account inattivi.

Desiderato: Implementare un sistema che possa garantire una gestione più completa dei dati.

Sviluppo Software

Attuale: fallimento parziale nell'evitare che gli sviluppatori usino librerie non sicure.

Desiderato: Sviluppare il codice in modo che possa avvertire gli sviluppatori dell'utilizzo di una libreria non sicura

Configurazione sicura del sistema:

Attuale: errori nelle configurazioni di sistema

Desiderato: Implementare controlli prevedendo regolari Pentesting che verifichino le vulnerabilità in tal senso.

Gestione delle sessioni

Attuale: Riscontrati casi di sfruttamento delle sessioni utenti per compromettere la sicurezza del prodotto.

Desiderata: Impostare tempi di time-out di sessione appropriati e invalidare le sessioni inattive e implementare il codice per evitare l'archiviazione di dati sensibili nelle sessioni utente.

Gestione degli Errori

Attuale: fallimento nella completa gestione degli errori per mancata previsione della casistica di gestione degli errori del software stesso.

Desiderata: Sviluppare una strategia di fallback per gestire i casi in cui il sistema di gestione degli errori stesso fallisca.



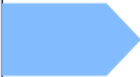


Furto e danneggiamento e tutela fisica dei dispositivi e dei dati in esso contenuti:

Attuale: manca un sistema di controllo fisico degli accessi ai locali in cui si trovano i dispositivi con l'ulteriore rischio di attacchi da parte di insider o esterni malintenzionati.

Desiderato: Prevedere sistema di accessi con badge che permetta l'accesso solo al personale autorizzato e che possa registrare gli accessi in modo da dissipare il rischio di Repudiation.

Road Map

Di seguito è consultabile una tabella che detta gli step da implementare per garantire un ulteriore mitigazione dei rischi emersi in seguito allo svolgimento della Gap Analysis.

ROAD MAP	Month 1	Month 2	Month 3	Month 4	Month 5	Month 6
Step 1: Implementare un sistema che possa garantire una gestione più completa dei dati.						
Step 2: Sviluppare il codice in modo che possa avvertire gli sviluppatori dell'utilizzo di una libreria non sicura.						
Step 3: Implementare regolari Pentesting che verifichino le vulnerabilità.						
Step 4: Impostare tempi di timeout di sessione appropriati e invalidare le sessioni inattive e implementare il codice per evitare l'archiviazione di dati sensibili nelle sessioni utente.						
Step 5: Sviluppare una strategia di fallback per gestire i casi in cui il sistema di gestione degli errori stesso fallisca.						
Step 6: Prevedere sistema di accessi con badge che permetta l'accesso solo al personale autorizzato e che possa registrare gli accessi in modo da dissipare il rischio di repudiation.						