MITIGAZIONE DEL RISCHIO S2-L1

Traccia

Un'azienda di servizi finanziari gestisce un'applicazione web che consente ai clienti di accedere ai propri account e effettuare transazioni finanziarie online. L'applicazione web memorizza e gestisce dati sensibili dei clienti, come informazioni personali, dettagli finanziari e credenziali di accesso.

Il rischio principale è rappresentato da potenziali attacchi informatici volti a compromettere la sicurezza dell'applicazione web e a ottenere l'accesso non autorizzato ai dati dei clienti. Supponendo di aver già effettuato l'analisi del rischio per lo scenario identificato, l'azienda decide di non accettare il rischio e procedere con la mitigazione del rischio applicando degli ulteriori controlli.

Utilizzando NIST SP 800-53, seleziona 5 controlli, uno per ogni funzione di controllo (Deterrent, Preventive, Detective, Corrective, Compensating) e stabilisci come agisce il controllo sul rischio (può essere anche una combinazione):

• diminuendo la probabilità che un threat agent avvii una minaccia;

• diminuendo la probabilità che una minaccia sfrutti una vulnerabilità;

• diminuendo la vulnerabilità;

• diminuendo l'impatto se la minaccia riesce a sfruttura la vulnerabilità

Scopo del report

L'analisi del rischio è un processo fondamentale per garantire la continuità operativa, la protezione del patrimonio aziendale e la sicurezza dei nostri dipendenti, clienti e stakeholder.

L'identificazione e la valutazione dei rischi rappresentano un passo cruciale nel garantire la sostenibilità e la resilienza dell'azienda di fronte a potenziali minacce. Il presente documento fornisce una panoramica dei rischi individuati, valutati in base alla loro probabilità di manifestarsi e all'impatto potenziale sulle nostre attività commerciali. Inoltre, vengono presentati i controlli proposti per mitigare o gestire ciascun rischio, delineando chiaramente i ruoli e le responsabilità delle parti interessate coinvolte nell'implementazione e nel monitoraggio di tali controlli.

È fondamentale che questo documento sia considerato uno strumento dinamico e soggetto a revisioni periodiche, in linea con l'evoluzione delle condizioni operative interne ed esterne. Si prevede una regolare valutazione e aggiornamento dei rischi e dei relativi controlli per garantire l'efficacia continua nel gestire le sfide emergenti.

Identificazione del rischio

Dopo un attenta analisi del rischio gestita dal team di risk assessment è stato possibile identificare una serie di rischi per l’azienda. Ogni rischio è stato identificato, analizzato e valutato. In base ai risultati ottenuti sono stati identificati due rischi con criticità “Molto Alta”. L’azienda ha quindi deciso di ridurre questo rischio a proprie spese ed assegnare i rischi con criticità “Medio/Bassa” ad una azienda terzi.

Threat Actors

Il rischio identificato come criticità “Molto alta” coinvolge un Threat Actor esterno (individuo, gruppo criminale organizzato o hacktivisti) che possa ottenere l’accesso non autorizzato ai dati dei clienti. Seguiremo il workflow del rischio per riassumere il rischio trattato.

Threat

L’analisi ha individuato come possibili minacce a rischio “Molto Alto” le seguenti:

Ransomware: Il ransomware rappresenta una minaccia grave in termini di potenziale danno, poiché può crittografare i dati aziendali rendendoli inaccessibili e richiedere un pagamento per il ripristino. Ciò può causare perdite finanziarie, danni reputazionali e interruzioni delle operazioni aziendali.

Malware: Un malware con capacità di modifica o esfiltrazione dei dati rappresenta una seria minaccia per l’azienda. Questo potrebbe collezionare dati sensibili aziendali e dei clienti ed inviarli all’esterno dell’azienda. Questa comprometterebbe la riservatezza, l’integrità e la reputazione aziendale.

Il team di analisi ha individuato tre vettori di attacco:

Ignegneria sociale: Un utente malintenzionato potrebbe impersonare una figura rilevante dell’azienda e contattare un dipendente tramite e-mail riguardo una situazione urgente. Per poterla risolvere l’utente è spinto a cliccare su un link o ad aprire un file (un eseguibile solitamente) che installa il malware nel dispositivo.

Email di phishing: Gli attaccanti inviano e-mail fraudolente che sembrano provenire da fonti legittime, incoraggiando gli utenti a fare clic su link dannosi o scaricare allegati infetti.

Download di software dannoso: Gli utenti scaricano software da fonti non attendibili o pirata, senza rendersi conto che il software contiene malware.

Vulnerability

L’analisi di questo scenario di rischio ha permesso di individuare tre vulnerabilità dell’infrastruttura aziendale che possono essere sfruttate da un attaccante.

Debolezze nell'infrastruttura di rete: Le configurazioni di rete non sicure, come password deboli per dispositivi di rete o router mal configurati, possono essere sfruttate da attaccanti per eseguire attacchi di ransomware o per facilitare la propagazione di malware attraverso la rete.

Vulnerabilità umane: La poca sensibilizzazione dei dipendenti sulle tematiche di sicurezza aumenta drasticamente le probabilità di una campagna di phishing. Gli attaccanti possono sfruttare l'ingegneria sociale per indurre gli utenti a fornire informazioni di accesso sensibili o a scaricare e installare malware sui loro dispositivi.

Impatto

Per quanto riguarda questo scenario di rischio, l'impatto è valutato come "Molto Alto". Un attacco di tipo ransomware o malware potrebbe infliggere danni significativi e drastici all'organizzazione, compromettendo gravemente la continuità operativa e la missione aziendale. Questo potrebbe tradursi in gravi perdite finanziarie a causa della perdita di dati critici, dei costi di ripristino dei sistemi e dei possibili pagamenti di riscatto. Inoltre, l'azienda potrebbe subire danni reputazionali sostanziali, con conseguenze negative a lungo termine sulla fiducia dei clienti, sulle relazioni con gli stakeholder e sull'immagine pubblica dell'organizzazione.

Rischio

L’analisi qualitativa e semi-quantitativa effettuata dal team di Risk Assessment sulle minacce identificate, le vulnerabilità individuate e l'impatto potenziale sul nostro ambiente aziendale, siamo giunti alla conclusione che il rischio associato a questi scenari Malware/Ransomware e Code Injection sono valutati come "Molto Alto" in base alla verosimiglianza degli eventi .

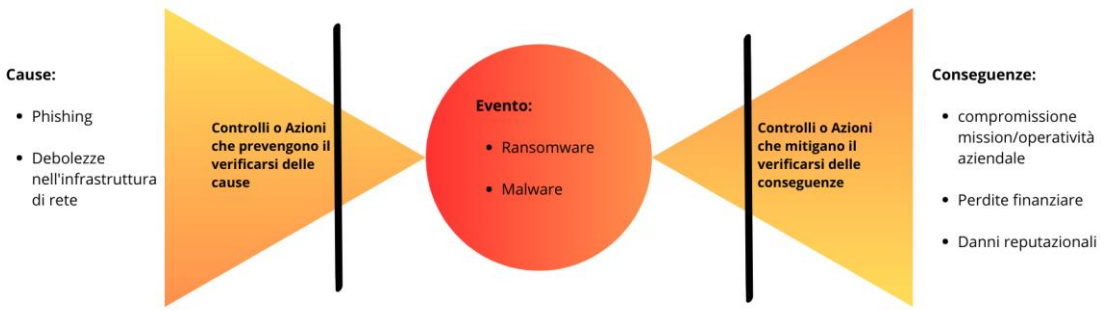
Questa valutazione è coerente con i criteri di valutazione del rischio delineati nelle tabelle del NIST SP800-30r, evidenziando la necessità di adottare misure di mitigazione efficaci per proteggere l'azienda da potenziali conseguenze dannose.

Mitigazione del rischio

In questa sezione, proporremo le strategie e le azioni proposte per mitigare il rischio identificato attraverso l'analisi condotta dal team di valutazione del rischio. Utilizzando i dati raccolti durante l'analisi delle minacce, delle vulnerabilità e dell'impatto, ci concentreremo sull'identificazione di soluzioni proattive e preventive volte a ridurre al minimo l'esposizione dell'azienda a potenziali eventi dannosi.

Per comprendere meglio lo scenario di rischio utilizziamo la tecnica di analisi Bow-tie, L'analisi Bow-Tie è uno strumento utilizzato nell'analisi del rischio e il suo nome deriva dalla forma a farfalla che assume il diagramma utilizzato per rappresentare le relazioni tra cause, eventi pericolosi e conseguenze. Si tratta quindi di uno strumento che aiuta a comprendere come un pericolo possa concretizzarsi e quali azioni possono essere messe in atto per evitarlo.

Rischio Ransomware/Malware:



La seguente tabella elenca alcuni controlli preventivi e di mitigazione basati sulle tabelle della normativa NIST SP800-53r per affrontare lo scenario di rischio Ransomware/Malware:

Controllo	Descrizione	Fonte NIST	Tipo di controllo
AC-2	**Backup dei dati** Effettuare il backup regolare e sicuro dei dati aziendali critici per garantire la disponibilità e l'integrità delle informazioni in caso di attacco ransomware o perdita di dati.	SP800-53r	Preventivo, Corrective
AC-3	**Controllo dell'accesso** Implementare meccanismi di controllo dell'accesso basati su ruoli, privilegi minimi e autenticazione multi-fattore per limitare l'accesso non autorizzato ai sistemi e ai dati sensibili.	SP800-53r	Preventivo, Deterrente
AC-6	**Sessione di accesso** Gestire e monitorare le sessioni di accesso degli utenti per identificare e prevenire comportamenti anomali o attività sospette, riducendo così il rischio di accesso non autorizzato.	SP800-53r	Rilevamento, Preventivo
CM-2	**Controllo delle configurazioni** Applicare e gestire le configurazioni di sicurezza standard su tutti i dispositivi e i sistemi aziendali per ridurre le vulnerabilità e mantenere un ambiente IT sicuro e affidabile.	SP800-53r	Preventivo, rilevamento, deterrente
CM-3	**Patch e aggiornamenti** Applicare tempestivamente le patch e gli aggiornamenti di sicurezza rilasciati dai fornitori per correggere le vulnerabilità note e proteggere i sistemi da attacchi di malware e ransomware.	SP800-53r	Preventivo, Deterrente
CM-7	**Aggiornamenti software** Implementare un processo di gestione degli aggiornamenti software per garantire che tutte le applicazioni e i sistemi siano aggiornati con le versioni più recenti, riducendo così il rischio di esposizione a vulnerabilità note.	SP800-53r	Preventivo, rilevamento
CP-2	**Monitoraggio dei dispositivi** Monitorare costantemente l'attività e le prestazioni dei dispositivi di rete e dei sistemi informatici per identificare e rispondere prontamente a comportamenti anomali o attività sospette.	SP800-53r	Rilevamento, Compensativo
CP-9	**Protezione dei dati sensibili** Implementare misure di protezione avanzate per i dati sensibili, come crittografia e controllo degli accessi basati sui principi del bisogno di sapere, per garantire la riservatezza e l'integrità delle informazioni.	SP800-53r	Preventivo, rilevamento

IR-4	**Risposta agli incidenti** Definire e implementare un piano di risposta agli incidenti che stabilisca procedure e protocolli chiari per rilevare, rispondere e recuperarsi da attacchi di ransomware o malware, minimizzando così l'impatto sugli affari.	SP800-53r	Correttivo, rilevamento
IR-10	Analisi degli incidenti Condurre un'analisi dettagliata degli incidenti di sicurezza per identificare le cause radicate e le lezioni apprese, al fine di migliorare continuamente le misure di sicurezza e prevenire futuri attacchi.	SP800-53r	rilevamento, Correttivo
PM-5	**Gestione dei rischi** Effettuare una valutazione periodica dei rischi per identificare e valutare le minacce emergenti e le vulnerabilità, e adottare misure di mitigazione appropriate per ridurre al minimo l'esposizione dell'azienda a potenziali eventi dannosi.	SP800-53r	Deterrente, Preventivo
SA-11	**Verifica di sicurezza** Condurre regolarmente verifiche di sicurezza e test di penetrazione per identificare e correggere le vulnerabilità e le debolezze del sistema prima che vengano sfruttate dagli attaccanti.	SP800-53r	rilevamento, Preventivo
SI-4	**Integrità dei dati** Implementare controlli di integrità dei dati per proteggere l'integrità e l'affidabilità delle informazioni aziendali, garantendo che i dati critici non vengano alterati o compromessi da attacchi di ransomware o malware.	SP800-53r	rilevamento, Preventivo
SI-7	**Protezione delle informazioni personali** Applicare misure di protezione avanzate per le informazioni personali degli utenti, come la pseudonimizzazione e l'anonimizzazione dei dati, per garantire la riservatezza e la conformità alle normative sulla privacy.	SP800-53r	Preventivo, Compensativo

Inoltre, il PCI DSS è uno standard che racchiude una serie di requisiti di sicurezza ed è obbligatorio per le organizzazioni che elaborano, archiviano o trasmettono dati delle carte di pagamento, e fornisce linee guida specifiche per proteggere le informazioni delle carte di pagamento contro frodi e violazioni della sicurezza.

Dato lo scenario in esame, i seguenti controlli compensativi dello standard PCI DSS dovrebbero essere utilizzati:

PCI DSS 1.1.3 - Installazione e manutenzione regolare di un firewall per proteggere la rete aziendale da accessi non autorizzati, inclusi i tentativi di intrusione da parte di malware.

PCI DSS 5.1 - Utilizzo di software antivirus e antispyware aggiornati e funzionanti su tutti i sistemi di accesso all'ambiente cardholder data per proteggere contro il malware.

PCI DSS 5.2 - Assicurarsi che tutti i software antivirus siano attivi, aggiornati regolarmente e capaci di rilevare, rimuovere e proteggere contro tutti i malware noti e emergenti.

PCI DSS 6.1 - Implementazione e mantenimento di controlli per garantire che tutti i sistemi e le applicazioni critici siano protetti da vulnerabilità note tramite l'applicazione regolare di patch di sicurezza.

PCI DSS 6.2 - Garanzia di protezione contro l'inserimento di codice malevolo tramite vulnerabilità nota del software tramite l'applicazione regolare di patch di sicurezza.

PCI DSS 8.1.4 - Protezione delle password e dei dati crittografici utilizzati per accedere all'ambiente cardholder data da attacchi di malware tramite crittografia forte e sicura.

PCI DSS 10.5.5 - Monitoraggio e gestione dei file di registro per rilevare, prevenire e rispondere prontamente a eventuali attività sospette o anomalie associate a malware.

PCI DSS 12.9 - Implementazione e manutenzione di un programma di gestione dei rischi che comprenda il monitoraggio e la gestione del rischio associato al ransomware/malware e altre minacce informatiche.

Monitoraggio e Revisione

Le procedure di monitoraggio e revisione devono essere progettate per valutare l'efficacia dei controlli implementati nel mitigare i rischi identificati. Ciò include il monitoraggio costante delle attività di sicurezza, l'analisi degli incidenti di sicurezza, l'audit dei controlli di sicurezza e la verifica delle politiche e delle procedure aziendali.

Inoltre, è importante pianificare revisioni periodiche del documento di controllo del rischio per garantire che sia aggiornato e rifletta le nuove minacce o i cambiamenti nell'azienda. Queste revisioni dovrebbero coinvolgere tutte le parti interessate e includere un'analisi approfondita dei rischi e delle vulnerabilità attuali, nonché la valutazione dell'efficacia delle misure di mitigazione attuate.