EPICODE

S4 L4 Risk Assesment Report

Gestione del rischio informatico per un caso aziendale specifico

22 maggio 2024

Team

- Davide Di Turo
- Lisa Bonato
- Manuel Di Gangi
- Maria Flavia Minotti
- Oliviero Camarota

INDICE

Valutazione dei Controlli SC-7:

Firewall Perimetrale e sistemi di rilevamento

Data di Valutazione - 22 Maggio 2024

Valutatore: Responsabile della Sicurezza Informatica

Descrizione del Controllo:

Il firewall perimetrale è installato e configurato per proteggere la rete interna dagli accessi non autorizzati e dagli attacchi esterni.

Step 1: Verifica dell'Implementazione del Firewall

Risultato:Il firewall è fisicamente installato e correttamente posizionato secondo l'architettura di rete.

Step 2: Verifica della Configurazione del Firewall

Risultato: Le regole del firewall sono configurate per permettere solo il traffico autorizzato basato sui criteri di sicurezza aziendali.

Step 3: Test di Funzionamento del Firewall

Risultato: Il penetration test esterno ha confermato che il firewall blocca i tentativi di intrusione. Le porte non autorizzate sono chiuse.

Step 4: Monitoraggio e Logging del Traffico

Risultato: Il firewall sta generando log dettagliati del traffico e li sta inviando al sistema SIEM.

Step 5: Revisione Periodica delle Regole e delle Configurazioni

Risultato: La revisione trimestrale è stata completata e le regole del firewall sono state aggiornate secondo le nuove minacce identificate.

Step 6: Valutazione dell'Efficacia dei Controlli

Risultato: Non sono stati rilevati accessi non autorizzati attraverso il firewall negli ultimi sei mesi. I risultati dei penetration test mostrano un miglioramento rispetto ai test precedenti.

Conclusione:

I controlli implementati per il firewall perimetrale sono correttamente configurati e funzionano come previsto. Producono i risultati desiderati in termini di protezione del perimetro della rete, soddisfacendo i requisiti di sicurezza e privacy dell'organizzazione.

Raccomandazioni:

- Continuare il monitoraggio costante e la revisione periodica delle regole del firewall.

- Aggiornare regolarmente il sistema firewall per proteggere contro nuove minacce.

- Eseguire penetration test semi-annuali per verificare l'efficacia continua del firewall.

Valutazione dei Controlli SC-05:

Denial of Service Protection

Data di Valutazione - 22 Maggio 2024

Valutatore: Responsabile della Sicurezza Informatica

Descrizione del Controllo:

Implementazione di contromisure per proteggere i servizi, le risorse e i sistemi informativi dagli attacchi di denial of service (DoS) e distributed denial of service (DDoS), inclusa l'adozione di tecnologie e politiche per rilevare, mitigare e rispondere tempestivamente agli attacchi al fine di garantire la disponibilità continua dei servizi e delle risorse digitali.

Step 1: Identificazione dei Tipi di Attacchi DoS/DDoS

Definizione degli Eventi di Denial of Service da Proteggere

Risultato: Gli eventi DoS/DDoS sono definiti e documentati, compresi attacchi volumetrici, attacchi a livello di protocollo, e attacchi a livello applicativo.

Step 2: Scelta dei Valori di Protezione

Selezione dei Parametri di Protezione

Risultato: È stata scelta la protezione contro gli attacchi DoS/DDoS (valore selezionato: "protect against").

Step 3: Definizione dei Controlli

Definizione dei Controlli per Tipo di Evento DoS

Risultato: I controlli per proteggere contro i vari tipi di attacchi DoS/DDoS sono definiti e implementati, inclusi firewall, sistemi di rilevamento e prevenzione delle intrusioni (IDS/IPS), e soluzioni di mitigazione DDoS.

Step 4: Implementazione dei Controlli

Implementazione delle Misure di Protezione

Risultato: Le misure di protezione sono state implementate come segue:

Firewall e IDS/IPS: Configurati per rilevare e bloccare traffico sospetto e malevolo.

Soluzioni di Mitigazione DDoS: Implementate a livello di rete per deviare e mitigare attacchi volumetrici.

Rate Limiting e Throttling: Applicati per prevenire abusi a livello applicativo.

Step 5: Monitoraggio e Logging

Monitoraggio delle Attività

Risultato: Sono stati implementati sistemi di monitoraggio per rilevare tempestivamente tentativi di attacco DoS/DDoS.

Log degli Eventi: Conservati e analizzati regolarmente per identificare pattern di attacco.

Step 6: Risposta agli Attacchi

Piano di Risposta agli Incidenti

Risultato: Un piano di risposta agli incidenti è stato sviluppato e testato. Include procedure per:

Isolamento delle risorse attaccate.

Comunicazione con il team di sicurezza e gli stakeholder.

Ripristino dei servizi colpiti.

Step 7: Test e Validazione

Test delle Misure di Protezione

Risultato: Sono stati condotti test periodici per verificare l'efficacia delle misure di protezione DoS/DDoS.

Simulazioni di Attacco: Eseguite per testare le risposte automatiche e manuali agli attacchi.

Step 8: Formazione e Sensibilizzazione

Formazione del Personale

Risultato: Il personale ha ricevuto formazione specifica su come riconoscere e rispondere agli attacchi DoS/DDoS.

Sessioni di Training: Organizzate regolarmente per aggiornare le conoscenze del personale.

Conclusione:

I controlli implementati per la protezione contro gli attacchi DoS/DDoS sono correttamente configurati e funzionano come previsto. Producono i risultati desiderati in termini di disponibilità

continua dei servizi e delle risorse digitali, soddisfacendo i requisiti di sicurezza dell'organizzazione.

Raccomandazioni:

Continuare il monitoraggio costante e le revisioni periodiche delle soluzioni di mitigazione DoS/DDoS.

Migliorare ulteriormente la formazione del personale sulla gestione degli attacchi DoS/DDoS.

Integrare nuove tecnologie di rilevamento e mitigazione per migliorare la sicurezza complessiva.

Valutazione dei Controlli RA-3:

Risk Assessment

Data di Valutazione - 22 Maggio 2024

Valutatore - Responsabile della Gestione del Rischio

Descrizione del Controllo:

La valutazione periodica dei controlli di sicurezza è effettuata per identificare e mitigare le vulnerabilità, comprese quelle relative alla privacy.

Step 1: Definizione del Processo di Valutazione del Rischio

Risultato: Il processo di valutazione del rischio è documentato e approvato. È stato comunicato a tutte le parti interessate.

Step 2: Identificazione delle Risorse e dei Rischi Associati

Risultato: L'inventario delle risorse aziendali è stato creato. I potenziali rischi associati sono stati identificati tramite brainstorming con il team di sicurezza.

Step 3: Valutazione delle Minacce e delle Vulnerabilità

Risultato: Le minacce e le vulnerabilità sono state valutate utilizzando la metodologia NIST SP 800-30. Sono state condotte interviste con gli stakeholder e raccolti dati sugli incidenti passati.

Step 4: Analisi del Rischio

Risultato: Una matrice di rischio è stata applicata per classificare i rischi. Sono stati utilizzati strumenti di analisi quantitativa e qualitativa per valutare l'esposizione al rischio.

Step 5: Mitigazione del Rischio

Risultato: Sono state implementate misure di sicurezza come firewall, MFA, e crittografia dei dati. Le politiche di sicurezza e le SOP sono state aggiornate.

Step 6: Monitoraggio e Riesame Continuo

Risultato: È stato implementato un sistema di monitoraggio continuo. Le valutazioni del rischio sono programmate annualmente.

Step 7: Documentazione e Reporting

Risultato: Tutti i passi del processo di valutazione del rischio sono documentati. I risultati sono stati comunicati al management e agli stakeholder rilevanti.

Conclusione:

Il processo di valutazione del rischio è correttamente implementato e funziona come previsto. I controlli di sicurezza sono adeguati per identificare e mitigare le vulnerabilità, soddisfacendo i requisiti di sicurezza e privacy dell'organizzazione.

Raccomandazioni:

- Continuare il monitoraggio continuo e le valutazioni periodiche del rischio.

- Migliorare la formazione del personale sulla gestione del rischio.

- Integrare nuovi strumenti di valutazione del rischio per aumentare l'efficacia del processo.

Valutazione dei Controlli SC-13

Use of Cryptography

Data di Valutazione - 22 Maggio 2024

Valutatore: Responsabile della Sicurezza Informatica

Descrizione del Controllo:

L'organizzazione implementa la protezione fornita dalla crittografia in conformità alle leggi federali, ordini esecutivi, direttive, politiche normative, standard e linee guida pertinenti.

Step 1: Definizione delle Politiche di Crittografia

Risultato:Le politiche di crittografia sono documentate, approvate e comunicate a tutto il personale.

Step 2: Implementazione della Crittografia per i Dati in Transito

Risultato: Le comunicazioni via email sono protette tramite TLS e le connessioni VPN utilizzano IPsec.

Step 3: Implementazione della Crittografia per i Dati a Riposo

Risultato: I database e i dispositivi di archiviazione utilizzano AES-256 per la crittografia dei dati a riposo.

Step 4: Gestione delle Chiavi di Crittografia

Risultato: È implementato un sistema di gestione delle chiavi (KMS) e le chiavi sono regolarmente ruotate e protette.

Step 5: Conformità agli Standard e Normative

Risultato: L'uso della crittografia è conforme agli standard FIPS 140-2 e ISO/IEC 27001, e alle direttive GDPR e HIPAA.

Step 6: Formazione e Sensibilizzazione

Risultato: Sono stati organizzati workshop e sessioni di training periodiche. Linee guida sulla crittografia sono state distribuite.

Step 7: Monitoraggio e Audit dei Sistemi Crittografici

Risultato: Sono stati implementati strumenti di monitoraggio e condotti audit annuali sui sistemi crittografici.

Conclusione:

I controlli implementati per l'uso della crittografia sono correttamente configurati e funzionano come previsto. Producono i risultati desiderati in termini di protezione delle informazioni sensibili, soddisfacendo i requisiti di sicurezza e privacy dell'organizzazione.

Raccomandazioni:

- Continuare il monitoraggio costante e le revisioni periodiche dei sistemi crittografici.

- Migliorare ulteriormente la formazione del personale sulla gestione sicura della crittografia.

- Integrare nuove tecnologie di crittografia per migliorare la sicurezza complessiva.

Valutazione dei Controlli SC-28

Protection of Information at Rest

Data di Valutazione - 22 Maggio 2024

Valutatore: Responsabile della Sicurezza Informatica

Descrizione del Controllo:

Implementare la crittografia corretta e sicura per proteggere le informazioni sensibili e le comunicazioni da accessi non autorizzati o compromessi quando i dati sono a riposo.

Step 1: Definizione delle Politiche di Protezione dei Dati a Riposo

Risultato: Le politiche di protezione dei dati a riposo sono documentate, approvate e comunicate a tutto il personale.

Step 2: Implementazione della Crittografia per i Dati a Riposo

Risultato: I database aziendali utilizzano la crittografia AES-256 per proteggere i dati sensibili e i dispositivi di archiviazione sono crittografati.

Step 3: Gestione delle Chiavi di Crittografia

Risultato: È implementato un sistema di gestione delle chiavi (KMS) e le chiavi sono regolarmente ruotate e protette.

Step 4: Controllo degli Accessi ai Dati Crittografati

Risultato: I permessi di accesso ai file e ai database crittografati sono configurati in base ai ruoli degli utenti e l'MFA è utilizzata per l'accesso ai dati crittografati.

Step 5: Monitoraggio e Logging delle Attività sui Dati a Riposo

Risultato: Sono implementati sistemi di logging per tracciare le attività di accesso ai dati crittografati e le analisi dei log non hanno rilevato comportamenti sospetti significativi.

Step 6: Test e Validazione della Crittografia

Risultato: Sono stati condotti test di penetrazione e valutazioni della sicurezza che hanno confermato l'efficacia della crittografia implementata. Gli audit di sicurezza confermano il rispetto delle politiche e delle pratiche di crittografia.

Step 7: Formazione e Sensibilizzazione del Personale

Risultato: Sono stati organizzati workshop e sessioni di training periodiche. Linee guida sulla protezione dei dati a riposo sono state distribuite.

Conclusione:

I controlli implementati per la protezione dei dati a riposo sono correttamente configurati e funzionano come previsto. Producono i risultati desiderati in termini di protezione delle informazioni sensibili, soddisfacendo i requisiti di sicurezza e privacy dell'organizzazione.

Raccomandazioni:

- Continuare il monitoraggio costante e le revisioni periodiche dei sistemi di crittografia.

- Migliorare ulteriormente la formazione del personale sulla gestione sicura dei dati a riposo.

- Integrare nuove tecnologie di crittografia per migliorare la sicurezza complessiva.