EPICODE

S3 - L3

Reporting e comunicazione del rischio

14 maggio 2024

Team

- Davide di Turo
- Manuel Di Gangi
- Marco Fasani

INDICE

Traccia

Un’azienda ha richiesto la raccolta di informazione per la conduzione di un risk assessment. Lo scenario da valutare è la gestione dei controlli di accesso.

- Prepara un elenco di persone chiave da intervistare nell'azienda e i potenziali argomenti di discussione per ciascuna di esse.
- Identifica i tipi di documentazione che dovresti rivedere per raccogliere informazioni su processi, sistemi e controlli di sicurezza.
- Descrivi i test che potresti eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti.

Ricordatevi delle risorse utilizzate nell’esercizio di ieri e del materiale relativo ai controlli.

Persone chiave da intervistare:

1. Responsabile della sicurezza informatica: Discutere delle politiche di accesso attualmente in vigore, dei processi di monitoraggio e delle eventuali violazioni di sicurezza recenti.
2. Responsabile IT: Esaminare l'infrastruttura IT e i controlli di accesso implementati sui sistemi e sulle reti.
3. Amministratori di sistema: Ottenere informazioni dettagliate sui livelli di accesso attribuiti agli utenti, sui permessi di accesso e sui protocolli di autenticazione utilizzati.
4. Gestori dei dipartimenti chiave: Valutare le esigenze di accesso specifiche dei dipartimenti e le politiche di accesso attualmente in atto.
5. Rappresentante legale: Esaminare le normative locali e le normative settoriali relative alla gestione dei dati e dei controlli di accesso.
6. Responsabile delle risorse umane: Ottenere informazioni sul processo di onboarding e offboarding dei dipendenti, inclusa la gestione degli account utente.
7. Comitato esecutivo: Coinvolto nell' orientazione strategica generale dell'organizzazione e potrebbe essere interessato a tutti gli aspetti dell IT che supportano gli obiettivi aziendali.
8. Direttore tecnico: Coinvolto nello sviluppo e nell'implementazione delle strategie tecnologiche aziendali, potrebbe essere interessato a una vasta gamma di servizi e infrastrutture IT.

9. Consiglio di governance I&T: Coinvolto nella governance dell'IT e potrebbe essere interessato a tutte le aree dell'IT che influenzano le decisioni strategiche dell'organizzazione.
10. Comitato Rischi Imprese: Coinvolto nella gestione dei rischi aziendali a livello strategico e potrebbe essere interessato a rischi legati alla tecnologia dell'informazione.

Potenziali argomenti di discussione:

- Politiche di accesso attuali e loro efficacia.
- Processi di monitoraggio degli accessi e di gestione delle identità.
- Procedure di autenticazione e autorizzazione.
- Protocolli di sicurezza per la gestione delle password.
- Audit e controlli interni relativi all'accesso.
- Formazione dei dipendenti sulla sicurezza informatica.
- Procedure di risposta agli incidenti legati agli accessi non autorizzati.
- Procedure di onboarding e offboarding dei dipendenti.
- Gestione delle password e autenticazione a più fattori.
- Ruoli e responsabilità nell'amministrazione dei controlli di accesso.
- Adesione alle normative di sicurezza e conformità.
- Risposta agli incidenti legati agli accessi non autorizzati.

Tipi di documentazione da rivedere:

- Politiche e procedure interne sulla gestione degli accessi.
- Politiche e procedure di sicurezza aziendale.
- Registri di accesso e di autenticazione/autorizzazione.
- Rapporti di audit e di conformità precedentemente svolti.
- Documentazione relativa alla configurazione dei sistemi e delle reti.
- Documenti legali e normativi relativi alla sicurezza informatica.
- Documentazione tecnica relativa alla configurazione dei sistemi e dei controlli di accesso.
- Documenti di formazione dei dipendenti sulla sicurezza informatica.

Test da eseguire per raccogliere dati sulla configurazione dei sistemi IT e sulla sicurezza delle reti:

1. Penetration testing: Testare la robustezza delle reti e dei sistemi contro potenziali attacchi esterni o interni.
2. Vulnerability scanning: Identificare e risolvere eventuali vulnerabilità presenti nei sistemi e nelle reti.
3. Scansione delle Configurazioni di Sistema: Analizzare le configurazioni di sicurezza dei dispositivi e dei software per identificare eventuali errori o lacune.
4. Access control testing: Verificare l'efficacia dei controlli di accesso attraverso test di autenticazione e autorizzazione.

5. Social engineering tests: Valutare la resilienza dei dipendenti agli attacchi di phishing o di ingegneria sociale.
6. Assessment della sicurezza delle password: Verificare la complessità delle password e la presenza di politiche di rotazione regolari.
7. Simulazioni di attacco: Testare la robustezza dei sistemi e delle reti contro scenari di attacco simulati.
8. Auditing dei privilegi utente: Analizzare i privilegi assegnati agli utenti e identificare eventuali sovra-privilegi o anomalie.
9. Valutazione della conformità normativa: Verificare se i controlli di accesso soddisfano i requisiti normativi applicabili.
10. Analisi dei log di accesso: Esaminare i log di accesso per individuare eventuali attività sospette o tentativi di accesso non autorizzati.
11. Monitoraggio del Traffico di Rete: Analisi dei log di accesso per individuare pattern sospetti o accessi non autorizzati. Rilevamento di attività anomale o tentativi di intrusione.