Trattamento del rischio

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 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 sfruttare la vulnerabilità;

Deterrent

AC-8 SYSTEM USE NOTIFICATION

Control:

a. Display [Assignment: organization-defined system use notification message or banner] to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:

1. Users are accessing a U.S. Government system;

2. System usage may be monitored, recorded, and subject to audit;

3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and

4. Use of the system indicates consent to monitoring and recording;

Questo tipo di controllo agisce sul rischio mostrando degli avvisi preventivi all'utente dove viene specificato che l'utilizzo inappropriato del sistema avrà cause legali.

Preventive

IA-2 IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS)

Control: Uniquely identify and authenticate organizational users and associate that unique identification with processes acting on behalf of those users.

Control Enhancements:

(1) IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | MULTI-FACTOR AUTHENTICATION TO PRIVILEGED ACCOUNTS

Implement multi-factor authentication for access to privileged accounts.

Discussion: Multi-factor authentication requires the use of two or more different factors to achieve authentication. The authentication factors are defined as follows: something you know (e.g., a personal identification number [PIN]), something you have (e.g., a physical authenticator such as a cryptographic private key), or something you are (e.g., a biometric). Multi-factor authentication solutions that feature physical authenticators include hardware authenticators that provide time-based or challenge-response outputs and smart cards such as the U.S. Government Personal Identity Verification (PIV) card or the Department of Defense (DoD) Common Access Card (CAC). In addition to authenticating users at the system level (i.e., at logon), organizations may employ authentication mechanisms at the application level, at their discretion, to provide increased security. Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk. Organizations can add additional security measures, such as additional or more rigorous authentication mechanisms, for specific types of access.

Questo tipo di controllo agisce sul rischio utilizzando un sistema MFA per prevenire l'accesso a utente non autorizzati verso account privilegiati.

Detective

SI-3 MALICIOUS CODE PROTECTION

c. Configure malicious code protection mechanisms to:

1. Perform periodic scans of the system [Assignment: organization-defined frequency] and real-time scans of files from external sources at [Selection (one or more): endpoint; network entry and exit points] as the files are downloaded, opened, or executed in accordance with organizational policy; and

2. [Selection (one or more): block malicious code; quarantine malicious code; take [Assignment: organization-defined action]]; and send alert to [Assignment: organizationdefined personnel or roles] in response to malicious code detection;

Questo tipo di controllo agisce sul rischio scansionando in tempo reale la web app per la presenza di codice malevolo e bloccandolo/segnalandolo prima che possa essere eseguito.

Corrective

IR-8 INCIDENT RESPONSE PLAN

Control:

a. Develop an incident response plan that:

1. Provides the organization with a roadmap for implementing its incident response capability;

2. Describes the structure and organization of the incident response capability;

3. Provides a high-level approach for how the incident response capability fits into the overall organization;

4. Meets the unique requirements of the organization, which relate to mission, size, structure, and functions;

5. Defines reportable incidents;

6. Provides metrics for measuring the incident response capability within the organization;

7. Defines the resources and management support needed to effectively maintain and mature an incident response capability;

8. Addresses the sharing of incident information;

9. Is reviewed and approved by [Assignment: organization-defined personnel or roles] [Assignment: organization-defined frequency]; and

10. Explicitly designates responsibility for incident response to [Assignment: organizationdefined entities, personnel, or roles].

Questo tipo di controllo agisce sul rischio creando un Incident Response Plan che andrà ad attivarsi al riscontro della presenza di una minaccia.

Compensating

AC-17 REMOTE ACCESS

Control:

a. Establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and

b. Authorize each type of remote access to the system prior to allowing such connections.

Control Enhancements:

(2) REMOTE ACCESS | PROTECTION OF CONFIDENTIALITY AND INTEGRITY USING ENCRYPTION

Implement cryptographic mechanisms to protect the confidentiality and integrity of remote access sessions.

Discussion: Virtual private networks can be used to protect the confidentiality and integrity of remote access sessions. Transport Layer Security (TLS) is an example of a cryptographic protocol that provides end-to-end communications security over networks and is used for Internet communications and online transactions.

Questo tipo di controllo agisce sul rischio restringendo gli accessi da remoto e criptando i dati per proteggere la confidenzialità e l'integrità di questi ultimi, servendo quindi da ulteriore misura di sicurezza compensativa.