Secure Development – Starter Guideline

Protect7
your application security experts

Sicherheit gehört zum Software Development Prozess

Die Entwicklung robuster Applikationen ohne Schwachstellen ist keine einfache Aufgabe und absolute Sicherheit kann unmöglich erreicht werden. Viele funktionale Anforderungen, enge Zeitpläne und Kosten führen schnell dazu, dass Sicherheit und Qualität vernachlässigt werden. Dies hat zur Folge, dass die meisten Applikationen über Schwachstellen im Design und in der Implementierung verfügen.

Durch die Einhaltung einiger grundlegender Vorgaben lassen sich Applikationen bereits während der Implementierungsphase sicher gestalten und haben viel bessere Chancen eine Sicherheitsüberprüfung zu bestehen.

Machen Sie den ersten Schritt und etablieren Sie eine Secure Development Guideline in Ihrem Unternehmen.

Um den Start zu erleichtern, können unsere Kunden die technologieneutrale „Secure Development Starter Guideline" von Protect7 1:1 übernehmen oder auf interne Bedürfnisse anpassen. Darin sind die relevantesten Sicherheitsanforderungen formuliert und Massnahmen gefordert, die bei der Entwicklung von Applikationen umgesetzt werden müssen.

Mit dieser Starter Guideline lässt sich mit geringem Aufwand eine für Ihr Unternehmen spezifische Guideline erstellen, welche die wichtigsten Themen adressiert.

Vorgehen

Interessiert? Sprechen Sie mit uns über die Möglichkeiten, diese Starter-Guideline für Ihr Unternehmen zu nutzen.

Weitere Dienstleistungen

Im Zusammenhang mit der Sicherheit im Software Development Lifecycle bieten wir weitergehende Dienstleistungen an:

- Security-Architektur & Konzepterstellung
- Unterstützung bei der Entwicklung von Applikationen
- Sicherheits-Überprüfungen (Source Code Reviews & Penetration Tests)
- Risiko-Analysen

Nehmen Sie mit uns Kontakt auf für ein unverbindliches Gespräch.

Sie erhalten

- Eine Guideline die alle relevanten Themen enthält
- Einfacher Start zu einem eigenen Secure Development Lifecycle
- Nach Bedarf angepasste Guideline
- Dokument zur freien Verfügung in Ihrem Unternehmen

Ihr Vorteil

- Technologieneutrales Dokument
- Reduzierung von Mängeln während der Entwicklung
- Sicherheit als integraler Bestandteil der Software Entwicklung
- Gewährleistung von Compliance-Anforderungen

Preis

- Nutzungslizenz der Starter-Guideline beträgt CHF 5'000.-
- Anpassungen nach Aufwand

BERATUNG & ENGINEERING

Protect7 GmbH | Schaffhauserstrasse 418 | 8050 Zürich | Tel. +41 44 515 68 68 | www.protect7.com | info@protect7.com

Managed Web Application Vulnerability Scanning

Protect7
your application security experts

Inhalt der Starter Guideline

- Einleitung
    - Abgrenzung
    - Referenzen
    - Nutzungsrechte (Lizenz)
- Sichere Applikationsentwicklung
    - Allgemeine Sicherheitsanforderungen
    - Applikationssicherheit (application security)
        - Benutzerverwaltung (user management)
            - Benutzer, Benutzerkonto, Rollen und Profile
            - Rechte
            - Integration in das Unternehmens-Repository
            - Passwort speichern
            - Initiale Wahl des Passworts
            - Passwort-Qualität
            - Passwort ändern
            - Passworteingabe (login)
            - Vertrauliche Zustellung von Passworten
            - Generieren von Passworten und Schlüsseln
            - Passwort zurücksetzen (Passwort vergessen)
            - Erstellung eines neuen Benutzerkontos
            - Anpassen von Benutzerdaten im Benutzerkonto
            - Benutzerlöschung
        - Authentisierung (authentication)
            - Endbenutzer-Authentisierung
            - System-Authentisierung
            - Privilegierte Aktionen
            - Delegation und Proxy
        - Autorisierung und Zugriffskontrolle (authorization and access control)
            - Rollen basiert
            - Rechte basiert
            - Attribut basiert
        - Session-Verwaltung (session management)
            - Session erstellen (first contact)
            - Session ändern (login, re-login)
            - Session löschen (logout)
            - Cookies
        - Daten-Validierung: Injection und CSRF Schutz (validation and CSRF)
            - Eingabeprüfung (input validation)
            - Ausgabeprüfung und Escaping (output validation)
            - Verhinderung von CSRF (CSRF prevention mechanism)
        - Fehlerbehandlung (error and exception handling)
        - Logging und Monitoring
            - Logging
            - Monitoring
        - Datenintegrität (message integrity)
        - Datenvertraulichkeit (confidentiality protection)
            - Vertraulichkeit bei Speicherung (data at rest)
            - Vertraulichkeit bei Übermittlung: Schutz auf Transport-Stufe (data in transit: transport layer protection)
            - Vertraulichkeit bei Übermittlung: Schutz des Inhalts (data in transit: message layer protection)
    - Dokumentation architekturrelevanter Sicherheitsfunktionalität
    - Kryptographie
- Überprüfung
    - Manuelle Source Code Analyse
    - Statische Source Code Analyse
    - Manueller Application Penetration Test
    - Automatischer Application Penetration Test
    - Analyse Sicherheitsdokumentationen
- Versionskontrolle

BERATUNG & ENGINEERING