iteratec

Security By Design

Best Practices und Erfahrungsberichte von den Requirements bis zum Deployment

Magdalena Tsolaki

26.06.2024 | Wien

Agenda

Über uns

Security By Design

Praxisbeispiel

iteratec

Über Uns

500
Kolleg:innen

100
Studierende

27+
Jahre Erfahrung

64
Mio. Euro Umsatz

7
Standorte

Ich bin Magdalena Tsolaki

iteratec

M.Sc. – IT Security

2022

Iteratec GmbH

Lead Software Security Engineer

2012

netzkontor nord gmbh

Senior Software Engineer Technical Lead

2009

Versatel Nord GmbH

IT specialist for system integration

Praxisbeispiel

Energieunternehmen - App zur Kosten-Effizienten-Ladung von Elektrofahrzeugen

iteratec
Security By Design

Designphase

Testphase

Anforderungsphase

Implementierungsphase

Deployment- und Carephase

Sicherheitsanforderungsanalyse

- Technische und regulatorische Anforderungen
- Management von Kundeninformationen, Energieverbrauchsdaten und die Einhaltung von Datenschutzgesetzen (z.B. DSGVO)

Risikobewertung

- Cybersicherheitsrisiken
- Technische Risiken
- Operative Risiken
- Reputationsschäden

Designphase

Testphase

Anforderungsphase

Implementierungsphase

Deployment- und Carephase

Secure Network Design

- Entwurf einer sicheren Netzwerkarchitektur, die es ermöglicht, Ladevorgänge sicher zu steuern und gleichzeitig kritische Systeme vor Angriffen zu schützen.
- Segmentierung
- Verschlüsslung

Privacy by Design

- Datenschutz und Datensicherheit von Beginn an in das Systemdesign integrieren
- Datenminimierung
- Verschlüsslung
- Anonymisierung

Designphase

Testphase

Anforderungsphase

Implementierungsphase

Deployment- und Carephase

Secure Coding Practices

- Anwendung von Best Practices, wie die Vermeidung von z.B. OWASP Top 10
- OWASP ZAP Automated Scanners zur Überprüfung
- Verwendung sicherer und aktueller Libs und Frameworks
- Validation

Integration von Sicherheitsmodulen

- Art und Weise wie spezielle Sicherheitsmodule, z.B. für die Authentifizierung und Autorisierung, in die Software integriert werden.

Designphase

Testphase

Anforderungsphase

Implementierungsphase

Deployment- und Carephase

Security Testing

- Einsatz von Penetrationstests
- Threat Modeling
- Vulnerability Scans zur Identifizierung von Schwachstellen

Resilienztests

- Bewertung der Systemfähigkeit, auch nach Sicherheitsvorfällen zuverlässig zu funktionieren.
- Testen von Strategien zur schnellen Wiederherstellung nach Ausfällen.

Designphase

Testphase

Anforderungsphase

Implementierungsphase

Deployment- und Carephase

Update-Patch-Management

- Manuelle sowie automatische Updates und Patches durchführen, um auf neue Sicherheitsbedrohungen zu reagieren.

Monitoring und Incident Response

- Art und Weise der Systemüberwachung, um auf Sicherheitsvorfälle schnell und effektiv zu reagieren.

iteratec

Bereit, digitaler Security Champion zu werden?

Magdalena Tsolaki

Lead Software Security Engineer

iteratec GmbH
Donau-City-Straße 11
1220 Wien

magdalena.tsolaki@iteratec.com

iteratec

Vielen Dank für Ihre Aufmerksamkeit!