



Einfach Sicher(er) Entwickeln



About me

Steve Gerstner

Lead Architect for Cloud Solutions

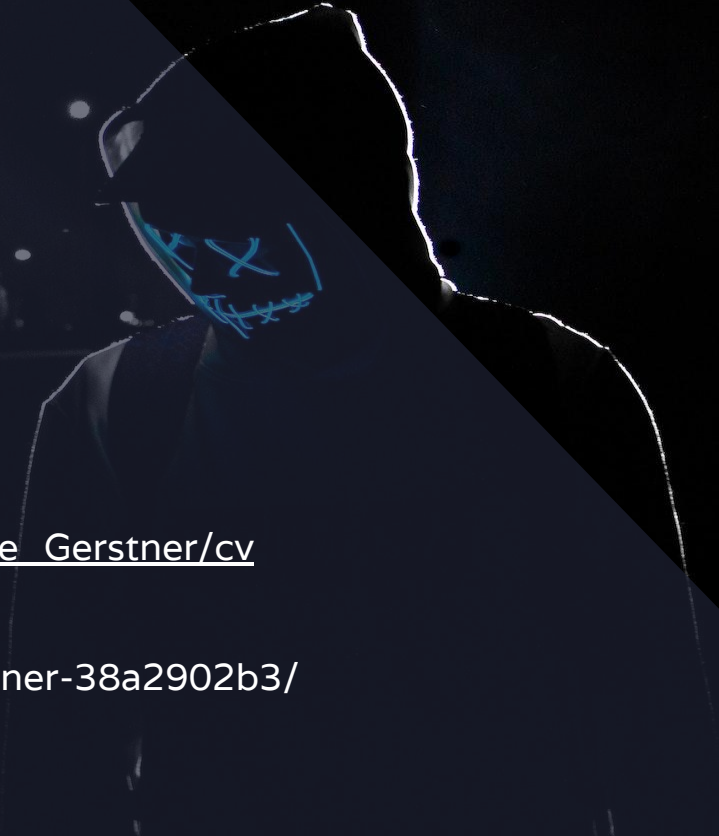
bridgingIT GmbH

Twitter: [@steve.gerstner](https://twitter.com/steve.gerstner)

Xing: https://www.xing.com/profile/Steve_Gerstner/cv

LinkedIn:

<https://www.linkedin.com/in/steve-gerstner-38a2902b3/>



Disclaimer



Agenda

- Motivation
- Security für Architekten
- Security in der Entwicklung




Nach globalem IT-Ausfall

BSI-Chefin will stärker auf Qualität von Produkten achten

Ein fehlerhaftes Update führte weltweit zu Chaos. Die Chefin des Bundesamts für Sicherheit in der Informationstechnik, Claudia Plattner, kündigt Maßnahmen an. Ganz werde man derartige Ausfälle aber nicht verhindern können.

20.07.2024, 05.28 Uhr

Artikel zum Hören • 2 Min

 [Anhören](#)



Entwickelt IHR sicher?



Habt ihr schon einmal
eine Sicherheitslücke
gefunden?



Habt ihr schon einmal
eine Sicherheitslücke
verursacht?





Motivation

Softwarecraftsmanship

Motivation

- Vorgaben im Unternehmen
 - OWASP TOP 10
 - OWASP ASVS
 - plus eigene Vorgaben & Prozesse
- Regulatorik / Gesetze (nur die wichtigsten):
 - ISO 27000
 - B3S (wenn Kritis)
 - BSIG (Kritische Infrastrukturen & NIS2)
 - Cyber Resilience Act
 -

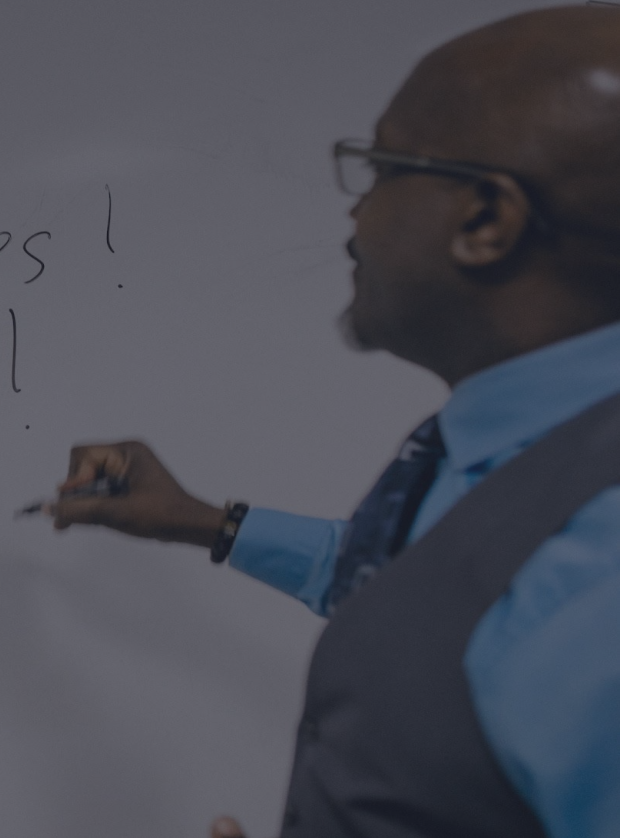
Rules

NO

heating !!!

No Cell Phones!

No Gum!



ISO 27001 A8.25

Rules for the secure development of software and systems should be established and applied.



Welche Security Bugs kennt ihr?

RAW Hammer Log4shell
Unsafe deserialization
Buffer overflow
SQL injection Log4j
XSS Xxs
1242375
Unsanitized inputs
Talkshow

OWASP Top 10

1. Injection
2. Authentication-Fehler
3. Verlust der Vertraulichkeit sensibler Daten
4. XML External Entities (XXE)
5. Fehler in der Zugriffskontrolle
6. sicherheitsrelevante Fehlkonfiguration
7. XSS
8. unsichere Deserialisierung
9. Nutzung von Komponenten mit bekannten Schwachstellen
10. Unzureichendes Logging und Monitoring



OWASP Application Security Verification Standard

	Applicability	Building			Building, Configuration, Deployment Assurance and Verification			Assurance and Verification	
Level 1	All apps		Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Penetration Testing	DAST
Level 2	All apps	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Level 3	High Assurance	Security Architecture and Reviews	Secure Coding	Standards and checklists	Secure & Peer Code Review	DevSecOps	Unit and Integration Tests	Hybrid Reviews	SAST
Legend		Acceptable	Suitable						

Figure 1 - OWASP Application Security Verification Standard 4.0 Levels

Security für Architekten



Welche Security-Themen berücksichtigt ihr in der Entwicklung?

Least privilege

Security Header (CORS etc)

Zugriff auf Endpunkte

Talaho Rbac XXE

Escaping Input sanitizing

Valid inputs

Penetration Testing

Input validation

Zero Trust

- Least Privilege Principle
- Traue niemandem
- Geh davon aus, du wurdest bereits gehackt



Verteidigung in der Tiefe



Checkliste Architektur

- Architekturdokumentation
- Infrastruktur
- Qualitative Anforderungen
 - ISO 25000
 - Arc42 Quality Model
- sicherer Entwicklungsprozess
 - Reviews
 - Code sicher halten
 - Umgang mit Sicherheitslücken
 - Security-Infrastruktur für die Entwicklung
 - Threat Model
 - SAST/DAST

Sichere Datenübertagung

- ❑ Daten im Transfer sind verschlüsselt
- ❑ vertrauliche und/oder persönliche Daten im Storage sind verschlüsselt
- ❑ nicht genutzte Methoden und Content-Types sind blockiert
- ❑ alle relevanten HTTP-Header sind gesetzt (OWASP ASVS)
- ❑ Sessions im Webserver sind sicher konfiguriert



Schreibt ihr für eure
Security-Funktionen
Tests inkl. aller
Fehlerfälle?



Security für Entwickler










Checkliste Review

- Ist der Code verständlich?
- Sind Security-Good-Practices umgesetzt worden?
- Sind keine Sicherheitslücken ersichtlich?
- Werden die definierten Entwicklungs-Konzepte eingehalten?
- Gibt es keine Findings aus der Security-Analyse?
- Sind alle Unit-, Integrations-, Akzeptanz-, Last- und Security-Tests auf dem Testsystem grün?
- Sind alle Buildschritte auf den CI-Umgebungen erfolgreich durchlaufen?

Verteidigung im Code

- Authentication
- Authorization am Endpoint
- Input Validation
- Authorization auf dem Objekt
- Persistenz
- Output Encoding
- keine Informationen über den Code an Nutzer

Was war die spannendste Lücke, die ihr schon selbst gefunden habt?

-  Anonymous
Authentication im Frontend
-  Anonymous
XXE bei xml config upload
-  Anonymous
?bestellnummer= in der URL
-  Anonymous
Passwort vergleich mit toLowerCase
-  Anonymous
Shell with root
-  Anonymous
Prompt injection
-  Anonymous
Logonmaske username=* suchte alle user

Zusammenfassung

A collection of wooden Scrabble tiles is arranged on a dark grey background. The tiles are dark brown with black letters and numbers. They are arranged in a grid-like pattern, spelling out the word 'DONESTHEATER' in a slightly irregular, staggered fashion. The letters are: D (2), O (1), N (1), E (1), S (1), T (1), H (4), A (1), R (1), E (1), P (3), E (1), R (1), F (4), C (3), T (1). The tiles are scattered across the frame, with some overlapping and others standing alone.

- ✓ arbeitet professionell und lebt eure Werte
- ✓ kennt eure Sicherheitsrichtlinien
- ✓ kennt eure eigenen Architekturvorgaben
- ✓ kennt eure Tools
- ✓ versetzt euch in die Sicht eines Angreifers

What's next

- Kryptografie
- AI
- Pentesting
- ...



Entwickelt IHR sicher?

Hat sich eure Sicht auf die
Frage geändert?



DANKE!
THANK YOU!
MERC I!
GRAZIE!
GRACIAS!
DANK JE WEL!

.....

