

LU03h - Ebenenmodell für Websicherheit

Immer mehr Geschäftsprozesse stehen und fallen mit der Verfügbarkeit entsprechender Webanwendungen. Deren Sicherheit sollten Unternehmen systematisch angehen und nicht auf die leichte Schulter nehmen.

1. Klassifizierung von Schwachpunkten

Ein Ebenenmodell wie die Klassifizierung von Schwachpunkten soll bei der Strukturierung des weiten Feldes der Web Application Security helfen. Das Modell erweitert die Netzwerkebene um fünf weitere Schichten.

| Klassifizierung von Schwachpunkten | | | |
|------------------------------------|-------------------|--|---|
| | Ebene | Inhalt | Beispiele |
| 5 | Semantik | Schutz vor Täuschung und Betrug | Phishing-Schutz, Schutz vor Informationspreisgabe |
| 4 | Logik | Absicherung von Prozessen und Workflows als Ganzes | „Passwort vergessen“-Funktion, Benutzer-Lock-Out |
| 3 | Implementierung | Vermeiden von Programmierfehlern, die zu Schwachstellen führen | Cross-Site Scripting, SQL-Injection |
| 2 | Technologie | richtige Wahl und sicherer Einsatz von Technologie | Verschlüsselung, Authentifizierung |
| 1 | System | Absicherung der auf der Systemplattform eingesetzten Software | Known Vulnerabilities, Konfigurationsfehler |
| 0 | Netzwerk und Host | Absicherung von Host und Netzwerk | |

- **1:** Die Systemebene befasst sich mit der Sicherheit der zur Realisierung der Webanwendung benötigten Software.
- **2:** Die Technologieebene behandelt Fragen wie die Wahl des richtigen Authentifizierungsverfahrens und der Softwarearchitektur.
- **3:** Diese Ebene betrifft den Bereich der Kodierung und damit der Programmierfehler. Hier sind so namhafte Schwachstellen wie Cross-Site Scripting und SQLInjection angesiedelt.
- **4:** Auf der Logikebene geht es um die Art, wie die Fachprozesse in der Anwendung abgebildet sind.
- **5:** Auf der semantischen Ebene geht es um den Schutz vor Täuschung und Betrug.

In der rechten Spalte sind jeweils Beispiele für typische Schwachstellen oder Angriffstechniken genannt.

2. Zuständigkeiten

Die zu verteilenden Verantwortlichkeiten im Unternehmen lassen sich anhand des Ebenenmodells bestimmen.

| Zuständigkeiten in den Entstehungsphasen | | | | |
|--|-------------------|--|--------------------------------------|----------|
| | Ebene | Fähigkeiten/Kenntnisse | Stelle | Funktion |
| 5 | Semantik | Corporate Identity und Unternehmenskommunikation | Fachabteilung (fordert an), Zentrale | Plan |
| 4 | Logik | Kenntnisse der Geschäftsprozesse | Fachabteilung (fordert an), Zentrale | Plan |
| 3 | Implementierung | Softwareentwicklungskenntnisse | Entwickler (setzt um) | Build |
| 2 | Technologie | allgemein IT-Sicherheit | Fachabteilung, Entwickler, Betrieb | Build |
| 1 | System | Netzwerk- und Systemadministration | Betrieb | Run |
| 0 | Netzwerk und Host | Netzwerk- und Systemadministration | Betrieb | Run |

- **Ebene 1** ist Sache des Betriebs, Netzwerk- und Systemkenntnisse sind die benötigten Fähigkeiten.
- **Ebene 2** wird von der Fachabteilung und Entwicklern mit Unterstützung des Betriebs verantwortet.
- Um **Ebene 3** kümmert sich die Entwicklungsabteilung.
- Um **Ebene 4** ist vorwiegend von der Fachabteilung, die eine Anwendung benötigt, zu steuern.
- **Ebene 5** ist hinsichtlich der allgemeinen Grundsätze von der Zentrale und in puncto anwendungsspezifische von der Fachabteilung zu verantworten.

Die rechte Spalte fasst die Zuständigkeiten für Planung, Umsetzung und Betrieb (Plan, Build, Run) einer Anwendung zusammen.

Quellennachweis Bilder

- https://insights.mgm-tp.com/wp-content/uploads/2016/05/Best_Practices_fuer_sichere_Webanwendungen_ix0703.pdf



Daniel Garavaldi

From:

<https://wiki.bzz.ch/> - **BZZ - Modulwiki**

Permanent link:

<https://wiki.bzz.ch/modul/m183/learningunits/lu03/08?rev=1767980488>

Last update: **2026/01/09 18:41**

