Sicherheitsmassnahmen Webdienste

Generelle Anforderungen

* Wird eine Web Application Firewall[[1]](#footnote-2) zwischen den Internetnutzerinnen respektive Internetnutzern und dem Webserver eingesetzt? Liegt der Webserver in einer DMZ (demilitarisierten Zone)?
* Wurde der Quellcode durch eine unabhängige Stelle überprüft oder ein Penetration Test durchgeführt? Wenn ja, durch wen?
* Existieren wirksame Massnahmen im Bereich des Verfügbarkeitsschutzes (z.B. Clustering, Redundanz)? Wenn ja, welche?
* Werden Updates zuerst in einer Testumgebung getestet?

Anforderungen an Webanwendungen nach OWASP Top Ten,
Open Web Application Security Project[[2]](#footnote-3)

* Welche wichtigen programmiertechnischen Massnahmen wurden getroffen gegen die nachfolgenden Bedrohungen?
	+ «A01:2021 – Fehler in der Zugriffskontrolle / Broken Access Control»
	+ «A03:2021 – Injection»
	+ «A04:2021 – Insecure Design»
	+ «A07:2021 – Fehler in der Identifizierung und Authentifizierung / Identification and Authentication Failures»
	+ «A08:2021 – Software- und Datenintegritätsfehler / Software and Data Integrity Failures»
* Werden sensitive Daten wie Passwörter sicher verschlüsselt?
	+ «A02:2021 – Fehler in der Verschlüsselung / Cryptographic Failures»
* Ist der Webdienst und -server «gehärtet» und bspw. unnötige Dienste und Benutzer deaktiviert, unnö­tige Software deinstalliert, sicherheitsrelevante Einstellungen aktiviert etc. Wenn ja, welche Vorgaben wurden beachtet und welche Massnahmen wurden getroffen?
	+ «A05:2021 – Sicherheitsrelevante Fehlkonfiguration / Security Misconfiguration»
	+ « A10:2021 – Fälschung von Anfragen / Server Side Request Forgery (SSRF)»
* Werden Aktualisierungen und Sicherheitsupdates für Server, Anwendungen und externen Komponen­ten (z.B. Net- oder Java-Bibliotheken) regelmässig eingespielt? Wenn ja, in welchen Abständen?
	+ «A06:2017 – Nutzung von Komponenten mit bekannten Schwachstellen / Vulnerable and Outdated Components»
* Werden der Zustand des Servers sowie die Verfügbarkeit und Sicherheitsevents in Echtzeit (Protokollie­rung und Monitoring) überwacht?
	+ «A09:2021 – Unzureichendes Logging & Monitoring / Security Logging and Monitoring Failures»)

Anforderungen an API nach OWASP API Top Ten, Open Web Application Security Project

* Welche programmiertechnischen Massnahmen und spezifischen sicherheitsrelevanten Konfigurationen wurden an der API gegen die nachfolgenden Bedrohungen getroffen? Werden die API gehärtet? Wenn ja, welche Vorgaben wurden beachtet und welche Massnahmen wurden getroffen?
	+ «A1:2019 – Broken Object Level Authorization»
	+ «A2:2019 – Broken User Authentication»
	+ «A3:2019 – Excessive Date Exposure»
	+ «A4:2019 – Lack of Resources and Rate Limiting»
	+ «A5:2019 – Broken Function Level Authorization»
	+ «A6:2019 – Mass Assignment»
	+ «A7:2019 – Security Missconfiguration»
	+ «A8:2019 – Injection»
	+ «A9:2019 – Improper Asset Management»
* Wird der Zustand der API überwacht (Protokollierung und Monitoring) sowie die Verfügbarkeit und Vollständigkeit der Log-Daten der API gewährleistet?
* «A10:2019 – Insufficient Logging & Monitoring»

V 3.0 / August 2022

1. Web Application Firewall (WAF): <http://de.wikipedia.org/wiki/Web_Application_Firewall> [↑](#footnote-ref-2)
2. Open Web Application Security Project (OWASP): [OWASP Top Ten | OWASP Foundation](https://owasp.org/www-project-top-ten/) [↑](#footnote-ref-3)