

Mehrere Studien haben ergeben, dass die Vielzahl aller Hacker-Angriffe über Webanwendungen stattfinden. Häufig weisen Webanwendungen Sicherheitslücken auf, die leicht auszunutzen sind. Die Folgen sind für das betroffene Unternehmen nicht kalkulierbar, insbesondere dann, wenn personenbezogene Daten einsehbar waren oder gestohlen wurden, und dieser Vorfall in der Öffentlichkeit diskutiert wird. Die sukzessive Erörterung von mehreren Fragestellungen bildet den Kern des Buchs. Die Wesentlichen sind: Wieso finden computerbasierte Angriffe statt und aus welcher Motivation heraus? Lassen sich die Angriffe bestimmten Interessengruppen zuordnen, und wie wirken sich bestimmte Motivationen auf ein Unternehmen oder ein Projekt aus? Was zeichnet das methodische Vorgehen eines solchen Angriffs aus? Welches sind die am weitesten verbreiteten Schwachstellen von Webanwendungen? Wie lassen sie sich von Angreifern ausnutzen? Schließlich: Wie können solche Schwachstellen während der Entwicklungsphase vermieden werden? Das Buch richtet sich an Projektverantwortliche, Software-Architekten und Software-Entwickler, die Sicherheitsaspekte vor, während und nach der Entwicklung von Webanwendungen beachten wollen.

Alexios Fakos, Fachinformatiker (IHK) und Diplom-Wirtschaftsinformatiker (FH).
Seit 1999 in der Computerindustrie tätig.
Zurzeit IT Security Consultant bei der n.runs AG, Oberursel/Berlin; unter anderem mit den Schwerpunkten: Penetrationstests und Quellcodeanalysen.
Ferner als freier Autor aktiv.



ISBN: 978-3-8364-0902-5

A. Fakos

Sichere Webanwendungen

VDM



Alexios Fakos

Sichere Webanwendungen

Grundlagen,
Schwachstellen und Gegenmaßnahmen

VDM Verlag Dr. Müller