

## Vorwort

Für die IT-Industrie gab es in den letzten Jahren ein unsanftes Erwachen. Fast ein Jahrzehnt lang wurde Unternehmen von den Medien und Beratern nahe gelegt, dass sie Firewalls, Einbruchserkennungssysteme und Netzwerk-Scanner bräuchten, um die Flut von Cyber-Attacken, über die wir täglich lesen, aufzuhalten. Hacker stehlen Kreditkarten, buchen kostenlos Flüge an exotische Reiseziele und laden persönliche Informationen über die letzten Affären von Politikern mit Filmstars herunter. Wir alle haben die Geschichten gesehen, und die Wissbegierigeren unter uns haben sich wahrscheinlich gefragt, wie das alles eigentlich passieren kann.

Als der Markt für Informationssicherheit zu einer riesigen kommerziellen Maschinerie heranwuchs und Technologien für Netzwerk- und Betriebssystemsicherheit als Allheilmittel anpries, entwickelte sich die IT-Industrie selbst in eine neue Richtung. Geschäfts- und Marketingmanager entdeckten, dass der Web-Browser der kleinste gemeinsame Nenner von (potenziellen) Benutzern ist. Und mal ganz ehrlich, weshalb um alles in der Welt sollten sie nicht alle möglichen Kunden ansprechen wollen? Warum sollten sie die Zielgruppe für ihre Dienste einschränken wollen? Unternehmensdaten und ganze Anwendungen ins Web zu bringen ist nicht nur ein Trend, sondern ein Phänomen. Heute weisen fast alle wichtigen Anwendungen Web-Schnittstellen auf – von verteilten Entwicklungsumgebungen über Gehaltsabrechnungssysteme bis hin zu Vertriebsdatenbanken. Wenn wir im Web surfen und das örtliche Wetter praktischerweise gleich im Seitenmenü erscheint, wurde es von einer Web-Anwendung dort hingestellt. Wenn wir unseren Kontostand online prüfen, steht ein System komplexer Web-Anwendungen dahinter, das den Saldo berechnet und anzeigt.

Derart komplexe technische Systeme zu erstellen ist keine triviale Aufgabe. Was die darunter liegende Technologie angeht, führen Microsoft und Sun die Entwicklung an. Sie geben die Plattformen und Sprachen vor, die die flexible Grundlagen für Web-Entwicklungen bilden. Mit der Flexibilität geht die Qual der Wahl einher. Obwohl diese Plattformen hervorragende Sicherheitsfunktionalität bieten können, liegt das Sicherheitsniveau im Ermessen der Designer und Entwickler. Alle heute auf dem Markt erhältlichen Plattformen können gleichermaßen sichere und unsichere Anwendungen hervorbringen, und wie

bei vielen Dingen im Leben steckt der Teufel auch hier im Detail. Bei der Entwicklung einer Web-Anwendung liegen die Details fast ausnahmslos im Verantwortungsbereich des Entwicklers.

Dieses Buch basiert auf einem einzigartigen und höchst effektiven Ansatz zur Wissensvermittlung, denn es spricht diejenigen an, die tatsächlich für das Schreiben von Code verantwortlich sind, die also etwas ändern können – die Entwickler selbst. Es wurde von einem Entwickler für Entwickler geschrieben, was bedeutet, dass es die Sprache der Entwickler spricht und Themen so erklärt, dass Entwickler sie verstehen können. In einem pragmatischen Ansatz vermittelt der Autor den Lesern eine Übersicht über die Themen und geht dann näher auf die teuflischen Details ein. Illustriert wird dies mit Beispielen und Szenarien aus der Praxis, welche leicht verständlich sind und vom Entwickler in seinem eigenen Code umgesetzt werden können.

Dieses Buch ist eine Pflichtlektüre für alle Entwickler, die Websites bauen. Ich weiß, dass Sie es genauso wie ich genießen werden.

*Mark Curphey*<sup>1</sup>

---

1. Mark Curphey hat einen Master in Informationssicherheit und leitet das Open Web Application Security Project ([www.owasp.org](http://www.owasp.org)). Er moderiert die mit Bugtraq verwandte Sicherheits-Mailingliste namens webappsec, die auf Web-Anwendungssicherheit spezialisiert ist. Er war früher Leiter für Informationssicherheit bei Charles Schwab und Consulting-Manager für Internet-Sicherheitssysteme. In dieser Zeit hat er so viele Banken und Consulting-Kunden beraten, dass er sich an deren genaue Zahl gar nicht mehr erinnern kann.

## Danksagungen

Ohne die Hilfe einer Hand voll kluger Freunde und Kollegen wäre dieses Buch nicht so gut lesbar, weniger konsistent und mit mehr Fehlern gespickt. Ich habe ihnen lediglich ein Bier und die ehrenwerte Nennung in diesem Abschnitt versprochen, und schon legten sie los und verbrachten Stunden und Tage (und einige sogar Wochen) damit, mir zu helfen.

Vor allem investierte Jan Ingvoldstad unwahrscheinlich viel Zeit in das Lesen und Kommentieren und schlug zu fast jedem Absatz Verbesserungen vor.

Zusätzlich haben folgende Personen viel Zeit aufgewendet, um frühe Versionen des Buchs zu lesen und zu kommentieren: Lars Preben S. Arnesen, Erik Assum, Jon S. Bratseth, Per Otto Christensen, Per Kristian Gjermshus, Morten Grimnes, Leif John Korshavn, Rune Offerdal, Frode Sandnes, Frank Solem, Rune Steinberg, Kent Vilhelmsen und Sigmund Øy.

Kjetil Valstadsve brachte mich dazu, einige Abschnitte zu überdenken, und Tore Anderson, Kjetil Barvik, Maja Bratseth, Lasse G. Dahl, Dennis Groves, Jan Kvile, Filip van Laenen, Glenn T. Lines, Kevin Spett, Thorkild Stray und Bjørn Stærk lieferten mir wertvolle Kommentare und Ideen zu Teilen des Buchs.

Man beachte, dass keine der Personen auf dieser Dankesliste für irgendwelche Fehler oder Unterlassungen in diesem Buch einzustehen hat. Ich war dumm genug, nicht auf alle Ratschläge zu hören, die mir diese netten, erfahrenen Leute gaben. Die Schuld trifft also ganz allein mich, wenn Sie das Gefühl haben, jemanden für etwas (was dieses Buch betrifft) zur Verantwortung ziehen zu müssen.

Ich möchte auch meiner Lektorin Gaynor Redvers-Mutton und ihren Freunden bei Wiley dafür danken, dass sie an meinen Buchvorschlag glaubten, obwohl die meisten Reviewer aus dem Buch ein traditionelles Infrastruktursicherheitsding machen wollten. :-)

Ich halte Buchwidmungen für ziemlich bedeutungslos und sage deshalb in diesem Abschnitt lieber »Hallo« zu Markus und Matilde. Danke für die vielen guten Erinnerungen, während ihr mich tagsüber beschäftigt habt.

Und last, aber sicherlich nicht least verneige ich mich tief vor meiner geliebten Frau Hanne S. Finstad. Sie schafft es immer, mir ein Gefühl der Sicherheit und Sorglosigkeit zu vermitteln. Ohne ihre Unterstützung (der sie sich vielleicht nicht einmal bewusst ist) wäre ich nie in der Lage gewesen, ein Buch zu schreiben (Klischee, stimmt aber trotzdem). Sie ist die kreativste, intelligenteste, schönste... oh, sorry. Ich sage ihr das lieber von Angesicht zu Angesicht.

*S. H. H.*