



# Vorwort zur zweiten Auflage

Die erste Auflage dieses Buches wurde ein großer Erfolg. Bereits nach etwa 18 Monaten war sie fast vollkommen vergriffen. Viel ist jedoch seit der Veröffentlichung im November 2002 geschehen. Statt nun das Buch lediglich nachzudrucken, bot es sich daher an, es in wesentlichen Teilen zu überarbeiten.

Die auffälligste Änderung ist sicherlich der Verlagswechsel vom Markt+Technik Verlag zum Addison Wesley Verlag.

Aber auch inhaltlich hat sich vieles geändert. Viele bereits in der ersten Auflage vorgestellten Programme wurden von ihren Entwicklern stark weiterentwickelt. Außerdem sind einige neue und sehr aufregende Produkte hinzugekommen. Die wichtigsten Neuerungen möchte ich kurz vorstellen.

Das Linux-Intrusion-Detection-System LIDS wurde stark überarbeitet und um neue Funktionen erweitert. Die neuen Funktionen wurden in das Buch aufgenommen und erklärt.

Die erste Auflage beschreibt noch Snort in der Version 1.8.x. Snort wurde von seinen Entwicklern für die Version 2.0 komplett überarbeitet und intern neu aufgebaut. Neben einigen zusätzlichen Funktionen bedeutet dies für den Anwender bei geschickter Konfiguration eine bis zu 10-fache Geschwindigkeitssteigerung.

Auch die Verwaltung eines Netzwerkes von Intrusion-Detection-System-Sensoren wurde überarbeitet und um neue Produkte erweitert.

Als neues Intrusion-Detection-System (IDS) werden nun in dieser Auflage auch Samhain und Prelude besprochen. Samhain ist eine Tripwire-Alternative, während Prelude ein Open-Source-Projekt ist, welches sowohl HIDS- als auch NIDS-Funktionen anzubieten versucht.

Des weiteren versucht diese Auflage nicht nur den Bereich der Einbruchserkennung sondern auch den der Prävention (Intrusion Prevention) abzudecken. Stellenweise wurde dies gerade im Zusammenhang mit LIDS und Snort bereits in der ersten Auflage angesprochen. Diese Auflage behandelt den Einsatz von Systrace und Snort-Inline zu diesem Zweck.

Außerdem berücksichtigt diese Auflage erstmals auch Wireless LANs und behandelt hier das Werkzeug Snort-Wireless.

Schließlich werden die Werkzeuge Sleuthkit und Autopsy zur forensischen Analyse von kompromittierten Systemen ausführlicher und mit mehr Beispielen dargestellt.

Ich hoffe, dass es mir mit diesem Buch gelungen ist, Ihren Geschmack zu treffen und Ihnen wertvolle Informationen zu liefern. Falls Sie bereits die erste Auflage kennen und schätzen, wird dieses Buch Ihnen die Möglichkeit geben, Ihr Wissen auf den aktuellen Stand zu bringen.

Sollten Sie Fragen oder Kritik zu diesem Buch haben, würde ich mich über Ihre Mail an [info@pearson.de](mailto:info@pearson.de) freuen. Der Verlag wird Ihre Nachricht an mich weiterleiten.

Ich wünsche Ihnen viel Spaß beim Lesen und viel Erfolg beim Einsetzen der beschriebenen Methoden.

*Ralf Spenneberg, Oktober 2004*