
Inhaltsverzeichnis

Vorwort	V
---------------	---

I. Einführung

Informationstechnik als Risikopotential der Informationsgesellschaft: Erfahrungen der Anwender

Günther Cyranek, Zürich	3
-------------------------------	---

II. Sicherheit und Bedrohungspotential

Über die Verletzlichkeit der Informationsgesellschaft

Klaus Brunnstein, Hamburg	11
---------------------------------	----

Sicherheitskonzepte für »offene« IT-Anwendungen

Eckart Raublöd, Darmstadt	35
---------------------------------	----

Hacking als Grenzüberschreitung

Frank Simon, Oldenburg	45
------------------------------	----

Technikfolgenabschätzung zur Sicherheit der Informationstechnik

Günther Cyranek, Zürich	53
-------------------------------	----

III. Informationssicherheit in Unternehmen

Informationssicherheit: Bedeutung und Durchsetzung von Sicherheitsstandards im Unternehmen

Daniel von Stockar, Winterthur75

Durchsetzung von Sicherheitsstandards in einer Grossbank

Walter Widmer, Zürich99

Erfahrungen aus der Arbeit eines Sicherheitsberaters

Peter Popp, Landschlacht109

Sicherheit in der Informationstechnik: Risikoanalyse in der Praxis

Erhard Berger, Zürich123

Methodische Informatik-Sicherheitsanalyse und Massnahmenplanung mit MARION

Adolf Dörig und Herbert Tomaschett, Zürich127

IV. Staatliche Massnahmen zur Sicherheit in der Informationstechnik und das juristische Umfeld

Neue Aufgabenstellungen des Bundesamtes für Sicherheit in der Informationstechnik

Heinrich Kersten, Bonn141

Die Informatik-Sicherheit in der öffentlichen Verwaltung – Der Weg zu angemessenen Sicherheitsmassnahmen

Bernhard Schmid, Bern153

Datenschutz und seine Konsequenzen für die Datensicherheit – mit schweizerischen Beispielen

Carl August Zehnder, Zürich171

Aus der praktischen Arbeit eines Datenschutzbeauftragten

Ürs Belser, Bern191

Autorenverzeichnis203