1. Record Nr. UNINA9910460187803321

Autore	Eckert Claudia
Titolo	IT-sicherheit : Konzepte - Verfahren - protokolle / / Claudia Eckert ; Lektorat, Angelika Sperlich ; Herstellung, Tina Bonertz
Pubbl/distr/stampa	Munich, Germany : , : De Gruyter Oldenbourg, , 2014 ©2014
ISBN	3-11-039910-5 3-486-85916-1
Edizione	[9. Auflage.]
Descrizione fisica	1 online resource (1004 p.)
Classificazione	ST 276
Disciplina	005.8
Soggetti	Cloud computing - Security measures Information technology Information technology - Security measures Electronic books.
Lingua di pubblicazione	Tedesco
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	Frontmatter -- Vorwort -- Inhaltsverzeichnis -- 1. Einführung -- 2. Spezielle Bedrohungen -- 3. Internet-(Un-)Sicherheit -- 4. Security Engineering -- 5. Bewertungskriterien -- 6. Sicherheitsmodelle -- 7. Kryptografische Verfahren -- 8. Hashfunktionen und elektronische Signaturen -- 9. Schlüsselmanagement -- 10. Authentifikation -- 11. Digitale Identität -- 12. Zugriffskontrolle -- 13. Sicherheit in Netzen -- 14. Sichere mobile und drahtlose Kommunikation -- Literaturverzeichnis -- Abkürzungsverzeichnis -- Index
Sommario/riassunto	Gesundheit, Mobilität, Handel oder Finanzen: moderne IT-Systeme sind heute in nahezu allen Bereichen von zentraler Bedeutung und mögliche Sicherheitsrisiken dieser Systeme von unmittelbarer Brisanz.Claudia Eckert stellt in diesem Standardwerk die zur Umsetzung der Sicherheitsanforderungen benötigten Verfahren und Protokolle detailliert vor und erläutert sie anschaulich anhand von Fallbeispielen. Im Vordergrund steht dabei, die Ursachen für Probleme heutiger IT-Systeme zu verdeutlichen und die grundlegenden Sicherheitskonzepte mit ihren jeweiligen Vor- und Nachteilen zu präsentieren. Der Leser entwickelt nicht nur ein Bewusstsein für IT-Sicherheitsrisiken, sondern

erwirbt auch ein breites und grundlegendes Wissen zu deren Behebung. - Sicherheitsbedrohungen durch unsichere Programmierung, Schadcode, Apps - Internet- (Un)Sicherheit- Security Engineering Vorgehen mit Bedrohungs- und Risiko-Analysen, Bewertungskriterien und Sicherheitsmodellen - Kryptografische Verfahren und Schlüsselmanagement - Authentifikation und digitale Identität - Zugriffskontrolle in zentralen und serviceorientierten (SOA) Systemen - Kommunikationssicherheit mit SSL/TLS, IPSec und sicherer Mail- Sichere mobile und drahtlose Kommunikation mit GSM/UMTS/LTE sowie, WLAN und Bluetooth Ein Muss für jeden, der sich mit dieser hochaktuellen Problematik beschäftigt!