Kurumsal BİLGİ Güvenliği

Teknik ve Yönetimsel Yönleriyle

Dr. Mehmet KARA

PAPATYA

© **PAPATYA YAYINCILIK EĞİTİM**
Ankara Caddesi, Prof. Fahreddin Kerim Gökay Vakfı İşhanı Girişi
No: 11/6, Cağaloğlu (Fatih) / İstanbul

Tel : (+90 212) 527 52 96 (+90 532) 311 311 0
Faks : (+90 212) 527 52 97
e-mail : admin@papatyabilim.com.tr
Web : www.papatyabilim.com.tr

Dağıtım : TDK Bilim – www.tdk.com.tr

Kurumsal Bilgi Güvenliği – Dr. Mehmet KARA

1. Basım Eylül 2018

Yayın Danışmanı : Toros Rifat ÇÖLKESEN (Ph. D)
Yayına Hazırlayan : Cengiz UĞURKAYA (Ph.D)
Üretim : Necdet AVCI
Pazarlama : Mustafa DEMİR
Satış : TDK Bilim ***www.tdk.com.tr***
Sayfa Düzenleme : Papatya ve Kelebek Tasarım
Basım ve Ciltleme : Özkaracan Matbaacılık (Sertifika No: 12228)
Evren Mah. Gülbahar Cad. No:62 Güneşli/İstanbul

Kara, Mehmet
Kurumsal Bilgi Güvenliği / Mehmet Kara - İstanbul: Papatya Yayıncılık Eğitim, 2018.
xvi, 344 s.; 24 cm.
Kaynakça ve Dizin var.
Sertifika No: 11218
ISBN 978-605-9594-50-9
1. OSI 2. Kriptografi 3. Ağ Güvenliği 4. Saldırı Atakları
I. Title

Bu kitabımı;
Yaşamın bütün zorluklarına karşı dimdik duran,
iyi yetişmemiz için her türlü fedakarlığı gösteren
Sevgili annem
Döndü KARA'ya
ithaf ediyorum.
Seni her geçen gün daha çok özlüyorum.

İÇİNDEKİLER

ÖNSÖZ

Bilgi güvenliğinin önemi her geçen gün daha çok anlaşılıyor. Ama bilişim uygulamaları hep bir adım önde gidiyor. Çünkü bilişim teknolojileri askeri, sağlık, enerji üretim ve dağıtımı, haberleşme, devlet uygulamaları, ticaret, bankacılık gibi hayatın her alanında yeni uygulamaları hizmete sunuyor. Bunu da klasik bir sunucu istemci uygulaması ile değil, bulut bilişim, nesnelerin İnternet'i, endüstriyel kontrol sistemler gibi değişik bakış ile sunuluyor. Bu da güvenliğin sürekli ve bütüncül bakış açısı ile ele alınmasını gerektiriyor. Önceki dönemlerde güvenlikten beklenilen iyi yönetilen bir güvenlik duvarı, aktif bir antivirüs programı, güncel işletim sistemi, güçlü kimlik doğrulama ve bunları yönetimiydi. Günümüzde ise hem teknik hem yönetimsel taraflarıyla güvenliği tümden ele alan yaklaşımlar gerekiyor. Hatta bu o kadar ileri gidiyor ki ağda kullanılan yazılım ve donanımların güvenli geliştirme metodolojileri ile geliştirilmesi, bağımsız laboratuvarlar tarafından test edilip sertifikalandırılması isteniyor. İstenilen güvenliğin sağlanması için bazen ülkedeki kurumlar arasında, bazen uluslararası düzeyde iş birliği ve koordinasyon gerekiyor.

Bu kapsamada bu kitapta bilgi güvenliği konusu hem yönetimsel hem teknik yönleriyle ele alındı. Bir kurumda bilgi sistemin güvenli olarak tasarlanması, kurulması ve işletilmesi için gerekli tüm adımlar anlatıldı. Ağ cihazları, sınır güvenliği cihazları, saldırı yöntem ve araçları, fiziksel güvenlik gibi teknik konular yanında, olay kayıtlarının değerlendirilmesi ve yönetilmesi, risk analizi, iş sürekliliği ve felaketten kurtarma, bilişim hukuku, personellerin eğitilmesi gibi yönetimsel konular da ele alındı. Uygulamaya yönelik teknik ve yönetimsel konuların yanısıra OSI referans modeli, kriptografi, erişim kontrolü, kimlik doğrulama gibi bilgi güvenliğiyle ilgili kavramlar derinlemesine anlatıldı. Bu bakış açılarıyla Üniversitelerde bilgi güvenliğinin tüm yönüyle el almak isteyen dersler için kaynak kitap olarak okutulabilir.

Kitap ISO/IEC 27001 Bilgi güvenliği Yönetim Sistemi standardının kurumda kurulup güvenli olarak işletilmesinde veya tüm dünyada bilgi güvenliği konusunda önemli prestiji olan CISSP (Computer Information System Security Professional) gibi sertifikasyon sistemlerinin konu ve kavramlarının anlaşılmasında önemli bir kaynak niteliğindedir.

Dr. Mehmet KARA

Kısaltmalar

AES Advanced Encryption Standard
AH Authentication Header
CISSP Computer Information System Security Professional
DDoS Distributed Denial Of Service
DoD Department of Defence
DoS Denial of Service
DSS Digital Signature Standard
EAL Evaluation Assurance Level
ESP Encapsulating Security Payload
GSM Global System for Mobile Communication
IDEA International Data Encryption Algorithms
ITSEC Information Technology Security Evaluation Criteria
OSI Open System Interconnection
PAP Password Authentication Protocol
PCI Payment Card Industry
RADIUS Remote Authentication Dial In User Service
RAID Redundant Array of Indipendent Disks
RFC Request For Comments
RSA Rivest, Shamir, Adleman
SDL Security Development Lifecycle
SHA Secure Hash Algorithms
SOME Siber Olaylara Müdahale Ekibi
SÖS Saldırı Önleme Sistemi
SSL Secure Socket Layer
TACACS Terminal Access Controller Access Control System
TCSEC Trusted Computer Security Evaluation Criteria
VPN Virtual Private Network
WEP Wired Equivalent Privacy
WPA Wi-Fi Protected Access