Eğitim İçeriği

Network Security Training

Altyapı ve Sistem Güvenliği 8 modül

Ağ Güvenliği Nedir?

Ağ Güvenliği, bir işletmenin dijital altyapısını korumak, veri akışını güvence altına almak ve dış tehditlere karşı önlemler almak için kullanılan yöntem ve teknolojileri kapsar. Erişim kontrolü, güvenlik duvarları, izleme sistemleri ve şifreleme gibi unsurları içerir.

Ağ Güvenliği Eğitiminin Amacı Nedir?

Eğitim, ağ güvenliği prensiplerini öğretmeyi ve katılımcılara ağ altyapısını koruma, tehditlere karşı önlem alma ve güvenlik açıklarını gidermede gerekli bilgi ve becerileri kazandırmayı hedefler. Katılımcılar, güvenilir ve sürdürülebilir ağ sistemleri oluşturmayı öğrenir.

Ağ Güvenliği Eğitimini Neden Almalısınız?

Bu eğitim, işletmelerin dijital altyapısını güvence altına almak, veri ihlallerini önlemek ve ağ güvenliği tehditlerine karşı dayanıklılık oluşturmak isteyen profesyoneller için tasarlanmıştır. Ağ güvenliği bilgisi, işletmelere operasyonel verimlilik ve stratejik koruma sağlar.

Kimler Ağ Güvenliği Eğitimini Alabilir?

- IT uzmanları ve sistem yöneticileri
- Ağ altyapısı tasarımı ve yönetimi yapan profesyoneller
- Dijital güvenlik alanında kariyer yapmak isteyen bireyler
- Şirketlerin ağ güvenliğini sağlamakla sorumlu çalışanlar

Eğitim, ağ güvenliği süreçlerini etkin bir şekilde yönetmek isteyen herkes için uygundur.

Ağ Güvenliği Eğitiminin Kariyere Yararları Nelerdir?

- Ağ güvenliği yönetiminde uzmanlaşma sağlar.
- Veri ve sistem koruma süreçlerinde yetkinlik kazandırır.
- Şirketlerin ağ altyapısını tehditlere karşı koruma imkânı sunar.
- İş dünyasında artan ağ güvenliği talebine yanıt verme fırsatı sunar.
- Daha geniş iş olanakları ve profesyonel statü elde etme fırsatı sağlar.

Eğitim Sonunda Hangi Beceriler Kazanılır?

- Ağ güvenliği tehditlerini tespit etme ve analiz etme
- Güvenlik duvarları ve izinsiz giriş önleme sistemlerini yönetme
- Ağ altyapısında güvenlik politikaları oluşturma
- Veri akışını koruma ve güvenli ağlar oluşturma

Eğitim Programı

1. Giriş ve Temel Kavramlar

1. Giriş ve Temel Kavramlar

- Ağ Güvenliğine Giriş
- Temel Ağ Kavramları
- Siber Tehditler ve Saldırı Türleri

2. Ağ Protokolleri ve İletişim

2. Ağ Protokolleri ve İletişim

- TCP/IP ve UDP Protokolleri
- DNS Güvenliği
- HTTP/HTTPS ve Web Güvenliği

3. Ağ Cihazları ve Güvenlik

3. Ağ Cihazları ve Güvenlik

- Yönlendiriciler ve Anahtarlar
- Güvenlik Duvarları (Firewall)
- Saldırı Tespit ve Önleme Sistemleri (IDS/IPS)

4. Kimlik ve Erişim Yönetimi

4. Kimlik ve Erişim Yönetimi

- Kimlik Doğrulama ve Yetkilendirme
- Çok Faktörlü Kimlik Doğrulama (MFA)

5. Şifreleme ve Kriptografi

5. Şifreleme ve Kriptografi

- Temel Kriptografi Kavramları

- VPN ve Güvenli İletişim
- Sertifika Yönetimi ve PKI

6. Ağ İzleme ve Denetim

6. Ağ İzleme ve Denetim

- Ağ Trafiği Analizi
- Log Yönetimi ve Analizi
- Olay Müdahale ve Adli Bilişim

7. Güvenlik Politikaları ve Standartları

7. Güvenlik Politikaları ve Standartları

- Güvenlik Politikalarının Oluşturulması
- Uluslararası Güvenlik Standartları
- Yasal ve Etik Konular

8. Uygulamalı Çalışmalar

8. Uygulamalı Çalışmalar

- Güvenlik Duvarı Konfigürasyonu
- Penetrasyon Testleri
- Siber Saldırı Simülasyonları

Bu eğitimi kurumunuza özel planlayalım. İçerik, süre ve uygulama senaryoları ekiplerinizin rolüne ve seviyesine göre uyarlanabilir. www.impress.com.tr/iletisim