

ÜCRETSİZ DERS NOTU ÖZETİ

Bilgi Sistemleri Güvenliği

Bağımsız Denetim Lisansı

Bilgi güvenliği yönetimi ve siber güvenlik

Bu PDF'teki bölüm	6 bölüm
Modüldeki toplam bölüm	18 bölüm
Formül sayısı	2 formül
Son güncelleme	17 Eylül 2026

Bu belge **Bilgi Sistemleri Güvenliği** modülünün ücretsiz bölümlerinden derlenmiştir. Tamamı ve güncel hâli:

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-guvenligi>

İçindekiler

1. Bilgi Güvenliđi Yönetimi ve Risk Deđerlendirme
2. Bilgi Güvenliđi Yönetimi ve Risk Deđerlendirme • Bilgi Sistemleri Güvenliđi, Varlık ve Risk Yönetimi
3. Bilgi Sistemleri Güvenliđi, Varlık ve Risk Yönetimi • Fiziksel, Çevresel ve Ağ Güvenliđi Kontrolleri
5. Fiziksel, Çevresel ve Ağ Güvenliđi Kontrolleri • Ağ Güvenliđi Temelleri, Topolojiler ve OSI Modelleri
6. Ağ Güvenliđi Temelleri, Topolojiler ve OSI Modelleri • OSI ve TCP/IP Ağ Modelleri ile Temel Protokoller

Bu PDF, **Bilgi Sistemleri Güvenliđi** ders notunun ücretsiz olarak yayımlanan ilk 6 bölümünü içerir. Modülün tamamı 18 bölümden oluşur; kalan 12 bölüm ile soru bankası, sesli anlatım ve deneme sınavları finlisans.com üzerinde yer alır.

Bölümler web sayfasında birbiriyle örtüşecek şekilde hazırlandıđı için, bu PDF’te aynı maddenin ikinci ve sonraki tekrarları ayıklanmıştır (180 yinelenen madde). Madde sırası ve bölüm numaraları web sayfasıyla aynıdır.

1. Bilgi Güvenliği Yönetimi ve Risk Değerlendirme

Temel Kavramlar

- **Bilgi Güvenliği:** Bilginin gizliliği, bütünlüğü ve erişilebilirliği ilkelerini korumak amacıyla uygulanan idari, teknik ve fiziksel kontrollerin tamamını kapsayan yönetim disiplini.
- **Siber Güvenlik:** İnternet üzerinden gelen tehditlere karşı siber uzaydaki varlıkların, ağların ve dijital altyapıların bütünsel güvenliğini ve korunmasını esas alan süreçtir.
- **Gizlilik (Confidentiality):** Bilgiye yetkisiz veya izinsiz erişimlerin engellenmesi ilkesidir; bilginin sadece erişim yetkisi verilmiş taraflarca görülmesini garanti altına almayı hedefler.
- **Bütünlük (Integrity):** Bilginin tam, doğru ve değiştirilmemiş olması halidir; verinin yetkisiz kişilerce bozulmasını, silinmesini veya manipüle edilmesini engellemeyi amaçlar.
- **Erişilebilirlik (Availability):** Bilginin ve ilgili sistemlerin, ihtiyaç duyulduğu her an yetkili taraflarca ulaşılabilir ve kullanılabilir durumda olması özelliğidir.
- **Siber Uzay:** İnternet, ağlar, sistemler ve dijital ortamdaki tüm etkileşimlerin oluşturduğu, fiziksel sınırları aşan küresel ve birbirine bağlı dijital bilgi ortamıdır.
- **Zafiyet (Vulnerability):** Bilgi sistemlerinde bulunan ve tehdit unsurları tarafından istismar edilerek sisteme zarar verilmesine yol açabilecek yapısal eksiklik veya güvenlik açıklarıdır.
- **İstismar (Exploit):** Bir sistemdeki mevcut zafiyetin, bir tehdit tarafından kullanılarak sisteme yetkisiz erişim sağlanması veya zarar verilmesi eyleminin gerçekleştirilmesidir.
- **Risk Yönetimi:** Bilgi sistemleri kullanımından kaynaklanan risklerin tespiti, analizi ve makul bir güvence sağlamak amacıyla kabul edilebilir seviyeye indirilmesi sürecidir.
- **Sızma Testi (Pentest):** Sistemlerdeki açıklıkların ve zafiyetlerin önceden tespit edilip düzeltilmesi amacıyla gerçekleştirilen, farklı yöntem ve araçların kullanıldığı güvenlik testidir.
- **Siyah Kutu Testi (Black Box):** Sızma testini gerçekleştirecek tarafa hedef sistemlere ilişkin önceden hiçbir bilginin verilmediği, dışarıdan bir saldırgan gözüyle yapılan test yöntemidir.
- **Beyaz Kutu Testi (White Box):** Test edilecek sistemlere yönelik mimari, kod ve altyapı gibi tüm teknik bilgilerin test ekibiyle paylaşıldığı kapsamlı güvenlik denetimi uygulamasıdır.
- **Gri Kutu Testi (Gray Box):** Sızma testi ekibine sistemler hakkında kısmi bilgi sağlandığı, hem iç hem de dış tehdit senaryolarının birlikte değerlendirildiği şeffaf kutu uygulamasıdır.
- **Bilgi Güvenliği Politikası:** Üst yönetimce onaylanan, kurumun güvenlik hedeflerini, rollerini ve risk yaklaşımını belirleyen, tüm çalışan ve paydaşlara duyurulan temel rehber belgedir.
- **CIA Üçlüsü:** Bilgi güvenliğinin üç temel unsuru: Gizlilik (Confidentiality), Bütünlük (Integrity), Erişilebilirlik (Availability).
- **Siber Uzay:** Ağların, sistemlerin, insanların ve dijital ortamların birbirine bağlı olduğu küresel alan.
- **Zafiyet (Vulnerability):** Bir varlıkta bulunan ve tehditler tarafından istismar edilebilecek zayıf nokta.
- **İstismar (Exploit):** Bir zafiyetten yararlanarak sisteme sızma veya zarar verme eylemi.
- **Sızma Testi (Pentest):** Sistemlerdeki açıklıkları önceden tespit etmek amacıyla yapılan kontrollü saldırı testi.

Önemli Noktalar

- Sızma testleri, BSY Tebliği uyarınca muaf olanlar hariç olmak üzere yılda en az 1 kere gerçekleştirilmek zorundadır.
- Bilgi güvenliği politikası üst yönetimce onaylanmalı ve her yıl düzenli olarak veya önemli değişikliklerde periyot dışında gözden geçirilmelidir.
- Risk işleme sürecinde bir kontrolün maliyeti, riskin olası maliyetini aşmamalıdır; ancak yasal mevzuat zorunluluğu bu kuralın istisnasıdır.
- Kurumda en az bir kişi 'bilgi sistemleri güvenliği sorumlusu' olarak belirlenmeli ve bu rol kurum organizasyon şemasında açıkça yer almalıdır.
- Bilgi güvenliği ekibinde kurumdaki her birimden en az bir temsilcinin bulunması, kararların birimlerde uygulanabilirliği açısından kritiktir.

Önemli Noktalar

- Risk değeriendirme sonuçlarında kabul edilebilir risk seviyesinin (risk iřtahı) üzerinde kalan tüm riskler için mutlaka risk iřleme çalıřması yapılmalıdır.
- Sızma testi raporları; her bir bulgunun tekil etkisini ve bulgular birleřtiđinde oluřan toplam etkiyi içerecek şekilde hazırlanmalıdır.
- Bilgi güvenliđi eğitimi, içeriđi hedef gruba ve güncel gelişmelere göre düzenlenerek tüm çalıřanlara düzenli aralıklarla verilmelidir.
- Bilgi güvenliđi üst yönetimin sorumluluğundadır ve teknik bir iřten ziyade bir yönetim sürecidir.
- ISO 27001:2013, her türden kurum için uygulanabilir en yaygın bilgi güvenliđi standardıdır.
- BSY Tebliđi (VII-128.10) uyarınca sızma testleri yılda en az bir kez yapılmalıdır.
- Risk iřleme seçenekleri: Azaltma, Engelleme, Paylařma ve Kabul Etme'dir.
- Sızma testleri siyah, beyaz veya gri kutu yaklařımlarıyla gerçekteřtirilebilir.

Sık Yapılan Hatalar

- Siber güvenlik ile bilgi güvenliđini tamamen aynı kavramlar sanmak (Bilgi güvenliđi fiziksel varlıkları da kapsar).
- Risk yönetiminde amacın 'sıfır risk' olduđunu düşünmek (Amaç riskin kabul edilebilir seviyeye indirilmesidir).
- Güvenlik eğitimlerini sadece bir kerelik bir faaliyet olarak görmek.

2. Bilgi Güvenliği Yönetimi ve Risk Değerlendirme • Bilgi Sistemleri Güvenliği, Varlık ve Risk Yönetimi

Temel Kavramlar

- Sızma Testi (Penetration Test):** Sermaye Piyasası Kurulu BSY Tebliği uyarınca, muaf olanlar hariç yılda en az bir kez yapılması zorunlu olan, sistemdeki açıklık ve zafiyetlerin önceden tespiti faaliyetidir.
- Siyah Kutu (Black Box):** Sızma testini gerçekleştirecek tarafa test edilecek sistemlere ilişkin hiçbir ön bilginin verilmediği, dışarıdan bir saldırgan gözüyle yapılan test yöntemidir.
- Beyaz Kutu (White Box):** Testi gerçekleştirecek tarafa hedef sistemlere yönelik tüm teknik detayların ve iç bilgilerin sağlandığı, kapsamlı bir güvenlik değerlendirmesi sunan sızma testi türüdür.
- Bilgi Güvenliği İhlali:** Bilgi sistemlerinde sonucu itibarıyla bilgi veya ortamlarda zarara sebep olmuş veya olma ihtimali çok yüksek olan arıza, yanlış kullanım veya dış saldırı gibi olaylardır.
- Bilmesi Gereken İlkesi (Need to Know):** Bilgi güvenliği ihlali gerçekleştiğinde, iç ve dış bilgilendirmelerin sadece konuyla doğrudan ilgili ve yetkili kişilerle kısıtlı tutulması prensibidir.
- Varlık (Asset):** Kurum için potansiyel veya gerçek değeri olan, fiziksel veya dijital nitelikteki, sayılabilir veya sayılamayan her türlü unsur ifade eden geniş kapsamlı terimdir.
- Varlık Sahibi:** Varlığın envantere kaydından imhasına kadar geçen tüm yaşam döngüsü boyunca risk yönetimi, korunması ve bakımından sorumlu olan onaylı kişi veya birimdir.
- Varlık Yaşam Döngüsü:** Bir varlığın ihtiyaç olarak planlanmasıyla başlayan; alım, izleme, bakım süreçlerinden geçerek güvenli imha veya kullanımdan kaldırma ile sona eren aşamalar bütünüdür.
- Kritik Bilgi:** Güvenlik zafiyeti oluşması durumunda yasal yaptırımlara veya kurumda çok ciddi maddi/manevi zarara yol açabilecek, yetkisiz erişimi engellenmesi gereken hassas veridir.
- Bilgi İşleme Tesisi:** Bilgi işlem faaliyetlerinde kullanılan sistem, servis, altyapı ve bu bileşenlerin konuşlandırıldığı fiziksel mekanları kapsayan maddi veya maddi olmayan olanaklardır.
- Statik Sistemler:** Bina gibi sabit ortamlarda kurulan ve yer değiştirmeden çalıştırılan, fiziksel ve çevresel tehditlere karşı sabit koruma gerektiren bilgi sistemi bileşenleridir.
- USB 3.0 Standardı:** Saniyede 5 Gigabit (Gbps) veri aktarım hızına ulaşabilen, harici güç kaynağı gerektirmeyen ve tak-çalıştır özelliği sunan yüksek hızlı iletişim standardıdır.
- Sızma Testi (Pen Test):** Sistemlerdeki açıklıkların önceden tespiti için yapılan, yılda en az bir kez zorunlu olan teknik test.
- Varlık (Asset):** Kurum için değeri olan maddi veya gayrimaddi her türlü unsurdur (donanım, yazılım, veri vb.).
- Varlık Sahibi (Asset Owner):** Varlığın yaşam döngüsü boyunca (envanter, sınıflandırma, risk, imha) sorumluluğunu taşıyan kişi veya birim.
- Siyah Kutu Testi:** Sistem hakkında hiçbir ön bilgi verilmeden yapılan sızma testi türü.
- İhlal Yönetimi:** Güvenlik olaylarının tespiti, analizi, müdahalesi ve kanıt toplanması süreçlerinin bütünü.

Önemli Formüller

USB Veri Hızları

USB 2.0 = 480 Mbps | USB 3.0 = 5 Gbps | USB 3.1 = 10 Gbps

Mbps: Megabit per second · **Gbps:** Gigabit per second

Örnek: USB 3.0, USB 2.0'dan yaklaşık 10 kat daha hızlı veri aktarımı sağlar.

Önemli Noktalar

- Sızma testleri, BSY Tebliği (VII-128.10) uyarınca muaf olanlar hariç yılda en az 1 kere gerçekleştirilmek zorundadır.
- Bilgi güvenliği ihlal yönetimi kapsamında, tüm çağrılarının analizi ve geri bildirimi için en az bir çalışan bu işle görevlendirilmiş olmalıdır.

Önemli Noktalar

- Varlık envanterinde mutlaka sahiplik bilgisi, varlığın sınıfı ve hangi kullanıcıda/nerede olduğuna dair güncel bilgiler yer almalıdır.
- Varlık sahipliği sorumluluğu, varlığın işletmeye kabulü veya geliştirilmesinin tamamlanmasıyla başlar ve imha aşamasında sona erer.
- Varlıklar sınıflandırılırken, işlediği, sakladığı veya koruduğu bilginin sahip olduğu en yüksek kritiklik ve hassasiyet derecesi esas alınmalıdır.
- USB 2.0 özellikleri saniyede 480 Mbps veri aktarımını desteklerken, USB 3.1 standardı 10 Gbps hıza kadar erişebilmektedir.
- Fiziksel varlıklar bakım için kurum dışına çıkarılmadan önce üzerindeki veriler güvenli şekilde silinmeli veya depolama ortamları sökülmelidir.
- Kurumdaki tüm personel bilgi güvenliği konusunda en az bir kere eğitim almış olmalı ve bu eğitimlerin kayıtları denetim için saklanmalıdır.
- BSY Tebliği uyarınca sızma testleri yılda en az 1 kez yapılmalıdır.
- Varlık yönetimi fiziksel alımla değil, talebin oluşması ve planlama ile başlar.
- İhlal yönetiminde 'kanıt toplama' süreci hukuki ve teknik açıdan en kritik aşamadır.
- Tüm personel (sadece BT değil) bilgi güvenliği eğitimi almalıdır.
- Taşınabilir cihazlar (USB) şifrelenmeli ve merkezi olarak yönetilmelidir.

Sık Yapılan Hatalar

- Hata: Varlık yönetiminin varlığın fiziksel olarak satın alınmasıyla başladığının sanılması. Doğrusu: Süreç, varlığa olan ihtiyacın veya talebin oluştuğu planlama aşamasında başlar.
- Hata: Varlık sahibinin günlük işler için bir çalışanı görevlendirdiğinde sorumluluğunun sona erdiğinin düşünülmesi. Doğrusu: Görevlendirme yapılsa dahi varlık sahibinin sorumluluğu azalmaz.
- Hata: Bilgi güvenliği politikasının sadece bilgi sistemleri birimine duyurulmasının yeterli görülmesi. Doğrusu: Politika tüm çalışanlara duyurulmalı ve her an erişilebilir olmalıdır.
- Hata: Tüm varlıklara aynı güvenlik kontrollerinin uygulanması. Doğrusu: Kontroller, varlığın sınıfına ve taşıdığı bilginin önemine göre maliyet ve risk dengesi gözetilerek farklılaştırılmalıdır.
- Hata: Varlığın yer değiştirmesinin veya kullanıcısının değişmesinin imha süreci olarak değerlendirilmesi. Doğrusu: Yer değiştirme kullanım aşamasının bir parçasıdır, imha ise yaşam döngüsünün sonudur.
- Varlık sahipliğinin sadece BT birimine ait olduğunu sanmak (Sahiplik iş birimlerine de dağıtılabilir).
- Varlık imhasında üzerindeki veriyi silmeden cihazı elden çıkarmak.
- Sızma testini sadece dış ağdan ibaret sanmak (İç ağ, sosyal mühendislik ve mobil uygulamalar da kapsama dahildir).

3. Bilgi Sistemleri Güvenliği, Varlık ve Risk Yönetimi • Fiziksel, Çevresel ve Ağ Güvenliği Kontrolleri

Temel Kavramlar

- **Bilgi İşleme Tesisi:** Bilgi işlem faaliyetlerinde kullanılan her türlü sistem, servis, altyapı ve bu bileşenlerin konuşlandırıldığı fiziksel mekanları kapsayan maddi veya maddi olmayan varlıklardır.
- **Statik Sistemler:** Bina gibi sabit ortamlarda kurulan ve çalıştırılan, yer değişikliği öngörülmeleyen bilgi sistemleri sınıfıdır.
- **Mobil Sistemler:** Sabit bir yapının işlevini yerine getiren ancak araç gibi sabit olmayan ortamlarda çalışan hareketli sistemlerdir.
- **Taşınabilir Sistemler:** Herhangi bir mekana bağlı kalmaksızın açıkta veya farklı konumlarda çalışabilen, dizüstü bilgisayar gibi cihazları kapsayan sistemlerdir.
- **Emniyet Kapısı (Deadman Door):** İki kapılı bir mekanizma ile yetkili tek bir kişinin geçişine izin veren, yancı geçiş (piggybacking) riskini azaltan yüksek güvenlikli giriş sistemidir.
- **Yancı Geçiş (Piggybacking/Tailgating):** Yetkisiz bir kişinin, yetkili bir kişiyi fiziksel olarak takip ederek güvenli alana izinsiz giriş yapması riskini ifade eder.
- **Islak Borulu Yağmurlama:** Borularında her an su bulunan, yangına anında tepki veren ancak sızıntı durumunda teçhizata zarar verme riski taşıyan söndürme sistemidir.
- **Kuru Borulu Yağmurlama:** Normalde borularında su bulunmayan, yangın anında su pompalanan ve sızıntı riskini ortadan kaldıran ancak su verilememe riski olan sistemdir.
- **FM-200 Gazı:** Halon gazına alternatif olarak geliştirilen, ozon tabakasına zarar vermeyen ve insanlar için zararsız olması nedeniyle en çok tercih edilen temiz söndürücü gazdır.
- **Tam Arıza (Blackout):** Doğal afetler veya şebeke kaynaklı olarak geniş bir bölgeyi veya binayı etkileyen tam elektrik kesintisi durumudur.
- **Düşük Gerilim (Brownout):** Elektrik dağıtım şirketinin kabul edilebilir seviyelerin altında güç sağlaması sonucu teçhizatın zorlanmasına ve hasar görmesine neden olan durumdur.
- **Elektromanyetik Enterferans (EMI):** Elektrikli aletlerin veya fırtınaların oluşturduğu gürültü nedeniyle sistemlerin çökmesine veya gerilim dalgalanmalarına yol açan girişim türüdür.
- **Ağ (Network):** Paylaşılan bir ortam aracılığıyla bilgi paylaşımı ve donanım kullanımı amacıyla birbirine bağlı iki veya daha fazla uç nokta cihazı kümesidir.
- **Ağ Protokolü:** Uç nokta cihazların birbiriyle iletişim kurabilmesi için uyması gereken standartlar ve kurallar dizisidir.
- **Bilgi İşleme Tesisi:** Bilgi işlem faaliyetlerinde kullanılan sistem, servis, altyapı ve mekanların genel tanımı.
- **Mantrap (Emniyet Kapısı):** Yetkisiz kişilerin yetkili birini takip ederek içeri sızmasını önleyen iki kapılı güvenlik mekanizması.
- **EMI (Elektromanyetik Girişim):** Elektrikli aletlerin veya dış kaynakların oluşturduğu parazit nedeniyle sistemlerin çökmesine yol açan gürültü.
- **Hassas Kontrollü Klima:** Sistem odalarında sıcaklık ve nemi çok dar aralıklarda sabit tutan özel iklimlendirme ünitesi.
- **UPS (Kesintisiz Güç Kaynağı):** Enerji kesintilerinde anlık güç sağlayan ve voltaj dalgalanmalarını düzenleyen cihaz.

Önemli Noktalar

- Sistem odası ideal sıcaklığı 21°C (+/-1), ideal nem oranı ise %50 (+/-5) RH olarak kabul edilmektedir.
- Sistem odası duvarları, tavanı ve zemini en az iki saatlik yangına dayanıklılık derecesine sahip olmalıdır.
- Fiziksel erişim kontrolleri ile can güvenliği hedefleri çeliştiğinde, her zaman can güvenliği öncelikli tutulmalıdır.
- Sistem odaları su baskını ve deprem riskine karşı binanın en alt (bodrum) ve en üst katlarında konumlandırılmamalı, orta katlar tercih edilmelidir.

Önemli Noktalar

- Halon gazı kullanımı çevreye verdiđi zararlar nedeniyle yasaklanmıřtır; Karbondioksit ise insan bulunan ortamlarda kullanılmamalıdır.
- Güç kabloları ile haberleşme kabloları, elektriksel yangın ve parazit riskine karşı birbirinden ayrı kanallardan geçirilmelidir.
- Sistem odası enerji beslemesi şebekeden deđil, UPS (Kesintisiz Güç Kaynađı) üzerinden sağlanmalı ve jeneratörle yedeklenmelidir.
- Sistem odasında yiyecek, içecek ve sigara kullanımı teçhizat güvenliđi için kesinlikle yasaklanmalıdır.
- Can güvenliđi her zaman fiziksel güvenlik kontrollerinden önceliklidir.
- Sistem odası ideal koşulları: 21°C (+/-1) sıcaklık ve %50 (+/-5) bađıl nemdir.
- Fiziksel erişim sağlandığında mantıksal kontroller (şifre vb.) etkisiz hale getirilebilir.
- Yangın söndürmede FM-200 insan dostu ve ozon dostu olduđu için tercih edilir; CO2 ise insanlı ortamda tehlikelidir.
- Güç ve haberleşme kabloları EMI riskine karşı fiziksel olarak ayrılmalıdır.

Sık Yapılan Hatalar

- Islak borulu ve kuru borulu sprinkler sistemlerini karıştırmak (Islak boruda su her an hazır ve sızıntı riski yüksektir).
- Sistem odasının yerini tabela ile belirtmenin iyi bir şey olduđunu sanmak (Aslında gizli kalmalıdır).
- UPS'in jeneratörün yerini tutacađını düşünmek (UPS kısa süreli, jeneratör uzun süreli koruma sağlar).

5. Fiziksel, Çevresel ve Ağ Güvenliği Kontrolleri • Ağ Güvenliği Temelleri, Topolojiler ve OSI Modelleri

Temel Kavramlar

- Ağ (Network): İki veya daha fazla uç nokta cihazının bilgi paylaşımı ve donanım kullanımı amacıyla bir iletişim ortamı üzerinden birbirine bağlanmasıdır.
- İnternet (Büyük Harf): IAB protokollerini ve ICANN adres alanlarını paylaşan, dünya çapında birbirine bağlı ticari ve resmi ağlardan oluşan en büyük sistemdir.
- Surface Web (Yüzey Ağ): Arama motorları tarafından dizinlenebilen ve herhangi bir web tarayıcısı ile herkesin erişebildiği web dünyasının görünen kısmıdır.
- Deep Web (Derin Ağ): Parola korumalı veya özel sunucularda olduğu için arama motorlarınca dizinlenemeyen; bankacılık ve e-posta gibi yasal ama kapalı içeriklerdir.
- Dark Web (Karanlık Ağ): Sadece TOR gibi özel yazılımlarla erişilebilen, anonimlik sağlayan ve genellikle yasadışı faaliyetlerin yürütüldüğü şifreli ağ katmanıdır.
- Intranet: İnternet standartlarını kullanan ancak güvenlik duvarları ile dış dünyadan izole edilmiş, sadece kurum içi yetkili kullanıcılara açık özel ağıdır.
- Extranet: İş ortakları ve tedarikçiler gibi belirli dış paydaşlara, kurumun iç ağındaki sınırlı kaynaklara güvenli erişim imkanı tanıyan özel ağ yapısıdır.
- Fiziksel Topoloji: Bir ağındaki cihazların konumunu, kabloların kurulumunu ve bileşenlerin fiziksel yerleşim düzenini tanımlayan ağ tasarım şemasıdır.
- Mantıksal Topoloji: Fiziksel yapıdan bağımsız olarak, bilginin ağ içindeki akış yolunu ve cihazlar arası iletişim mantığını ifade eden kavramdır.
- Ortak Yol (Bus) Topolojisi: Tüm düğümlerin tek bir ana hat üzerinden bağlandığı, merkezi hiyerarşisi olmayan ve ağ kapasitesinin tüm cihazlarca paylaşıldığı yapıdır.
- Örgü (Mesh) Topolojisi: Düğümlerin birbirine noktadan noktaya bağlı olduğu, hatalı düğümlere karşı alternatif yollar sunarak yüksek yedeklilik sağlayan ağ yapısıdır.
- Yıldız (Star) Topolojisi: Tüm düğümlerin merkezi bir dağıtıcıya (switch/AP) direkt bağlı olduğu, günümüzde en yaygın kullanılan ve performansı merkeze bağlı olan yapıdır.
- OSI Referans Modeli: Ağ iletişimini 7 katmana ayıran, işlevlerin nasıl yapılacağından ziyade ne yapılması gerektiğini tanımlayan kavramsal ve standart bir modeldir.
- PDU (Protokol Veri Birimi): OSI modelinde her katmanın işlediği veriye verilen isimdir; katman 3'te paket, katman 2'de çerçeve (frame), katman 1'de ise bit adını alır.
- Ağ (Network): İki veya daha fazla uç nokta cihazın bilgi ve donanım paylaşımı amacıyla birbirine bağlanması.
- Intranet: Güvenlik duvarı ile dış dünyadan izole edilmiş özel kurumsal iç ağ.
- Extranet: İş ortakları ve tedarikçiler gibi yetkili dış unsurlara sınırlı erişim sağlayan özel ağ.
- OSI Modeli: Ağ iletişimini 7 katmana ayıran kavramsal referans modeli.
- Deep Web: Arama motorları tarafından dizinlenemeyen, parola korumalı içeriklerin bulunduğu web katmanı.
- Dallanma Faktörü: Ağaç topolojisinde bir ebeveyn düğüme bağlı alt düğüm sayısı.

Önemli Noktalar

- Bir yapının ağaç topolojisi sayılabilmesi için hiyerarşinin en az üç derinlik seviyesinden oluşması zorunludur.
- İnternet (büyük harf) küresel sistemi, internet (küçük harf) ise sadece farklı ağlar arası bağlantıyı (inter-network) ifade eder.
- OSI modelinde ilk 4 katman (1-4) donanımla, üst 3 katman (5-7) ise yazılımla ilgili işlevleri yerine getirir.
- Dallanma faktörü 1 olan bir ağaç yapısı, fiziksel olarak doğrusal bir topolojiye karşılık gelir.
- Dark Web erişimi için TOR (The Onion Router) gibi trafiği çoklu sunucular üzerinden şifreleyerek yönlendiren özel tarayıcılar gereklidir.

Önemli Noktalar

- Halka topolojisinde veriler, çakışmaları önlemek amacıyla alıcı veriyi kabul edene kadar tek bir yönde hareket eder.
- WAN (Geniş Alan Ağı) ülkeler ve kıtalar arası mesafeleri kapsayan en geniş ağ türüdür; en büyük örneđi İnternet'tir.
- Arama algoritmaları, doğrusal veya örgü topolojilere kıyasla hiyerarşik ağaç yapısında daha verimli çalışmaktadır.
- İnternet (büyük İ) dünya çapındaki sistemi, internet (küçük i) ise farklı ağlar arası bağlantıyı temsil eder.
- Yıldız topolojisi günümüzde en yaygın kullanılan fiziksel topolojidir ve merkezde bir switch/hub bulunur.
- OSI modelinde PDU isimleri: Bit (K1), Çerçeve (K2), Paket (K3), Segment (K4), Veri (K5-7).
- Ağaç topolojisi için en az 3 seviye gereklidir.
- Mesh topolojisi, hatalı düğümlere karşı yedeklilik ve alternatif yollar sunar.

Sık Yapılan Hatalar

- Deep Web ile Dark Web'i karıştırmak (Deep Web bankacılık gibi yasal ama gizli içerikleri de kapsar, Dark Web ise anonim ve şifreli özel ağlardır).
- OSI katman numaralarını karıştırmak (Fiziksel katman her zaman 1. katmandır).
- TCP/IP'yi referans modeli sanmak (TCP/IP bir protokol modelidir, OSI referans modelidir).

6. Ağ Güvenliği Temelleri, Topolojiler ve OSI Modelleri • OSI ve TCP/IP Ağ Modelleri ile Temel Protokoller

Temel Kavramlar

- OSI Referans Modeli: Ağ iletişimini yedi ayrı katmana ayıran, IBM'in SNA mimarisinden esinlenerek geliştirilen ve günümüzde ağ iletişimini anlamak için teorik bir soyutlama olarak kullanılan modeldir.
- TCP/IP Modeli: İnternet'in temelini oluşturan, dört katmanlı bir yapıya sahip olan ve gerçek dünya ürünlerinde baskın standart olarak kullanılan pratik uygulama modelidir.
- Üç Yollu El Sıkışma (Three-way Handshake): TCP protokolünde veri iletimi başlamadan önce istemci ve sunucu arasında senkronizasyon ve onay mesajlarıyla bağlantının kurulmasını sağlayan güvenli yöntemdir.
- UDP (Kullanıcı Veri Bloğu Protokolü): Bağlantısız ve onay mekanizması içermeyen, hızın kritik olduğu ses akışı ve VoIP gibi uygulamalarda tercih edilen 'en iyi çabalı' aktarım protokolüdür.
- DNS (Alan Adı Sistemi): Kullanıcıların IP adresleri yerine alan adlarını kullanmasına imkan tanıyan, 53 numaralı port üzerinden çalışan hiyerarşik ve dağıtılmış bir ad çözümleme sistemidir.
- İyi Bilinen Bağlantı Noktaları (Well-known Ports): 1 ile 1023 aralığında yer alan ve IANA tarafından HTTP, SMTP gibi yaygın ağ uygulamalarına ayrılmış olan standart bağlantı noktalarıdır.
- DHCP (Dinamik Ana Bilgisayar Konfigürasyon Protokolü): Ağdaki cihazlara IP adresi, alt ağ maskesi ve varsayılan ağ geçidi gibi yapılandırma bilgilerini otomatik olarak atayarak manuel yapılandırma ihtiyacını ortadan kaldıran protokoldür.
- Soket (Socket): Bir IP adresi ile bir bağlantı noktası (port) numarasının birleşimiyle oluşan, ağ üzerindeki spesifik bir uygulama sürecini tanımlayan benzersiz uç noktadır.
- HTTP (Hiper Metin Transfer Protokolü): Web istemcileri ile sunucuları arasında 80 numaralı port üzerinden iletişim kuran, web sayfalarının ve kaynaklarının iletilmesini sağlayan uygulama katmanı protokolüdür.
- SSH (Güvenli Kabuk): Uzaktaki bir bilgisayara 22 numaralı port üzerinden şifreli ve güvenli bir kanal aracılığıyla erişim sağlayarak komut yürütülmesine imkan tanıyan kriptografik protokoldür.
- IPv4: Cihazları tanımlamak için kullanılan, 32 bit uzunluğunda, dört sekizliden oluşan ve noktalı ondalık formatta gösterilen mantıksal adresleme sistemidir.
- ICMP (İnternet Kontrol Mesajı Protokolü): Ağdaki cihazların birbirlerine hata bildirimleri ve kontrol mesajları göndermesi için kullanılan, ana bilgisayarın veya ağın erişilebilirliğini denetleyen protokoldür.
- OSI Modeli: 7 katmanlı teorik ağ referans modeli (Fiziksel, Veri Bağlantısı, Ağ, Taşıma, Oturum, Sunum, Uygulama).
- TCP/IP Modeli: 4 katmanlı pratik ağ modeli (Ağ Erişimi, İnternet, Taşıma, Uygulama).
- TCP: Bağlantı odaklı, güvenilir, üç yollu el sıkışma kullanan taşıma protokolü.
- UDP: Bağlantısız, hızlı, onay mekanizması olmayan 'en iyi çabalı' taşıma protokolü.
- DNS: Alan adlarını IP adreslerine çözümleyen hiyerarşik sistem (Port 53).
- DHCP: Cihazlara otomatik IP ve yapılandırma atayan protokol.

Önemli Formüller

IPv4 Yapısı

$$32 \text{ bit} = 4 \times 8 \text{ bit (octet)}$$

32 bit: Toplam adres uzunluğu • **4:** Sekizli sayısı • **8 bit:** Her bir sekizlinin uzunluğu

Örnek: 192.168.1.1 (Noktalı ondalık gösterim)

Önemli Noktalar

- TCP/IP modelindeki Uygulama katmanı; OSI modelindeki Uygulama, Sunum ve Oturum katmanlarının işlevlerini tek başına kapsar.

Önemli Noktalar

- Bağlantı noktaları (portlar) 1 ile 65535 aralığındadır; 49152-65535 arası özel portlar IANA'ya kayıtlı değildir ve rastgele seçilebilir.
- FTP protokolü iki port kullanır: Kontrol bağlantısı için 21 numaralı port, veri dosyası aktarımı için ise 20 numaralı port görev yapar.
- POP3 protokolünde e-postalar istemciye indirildikten sonra sunucudan silinirken, IMAP protokolünde e-postalar sunucuda tutulmaya devam eder.
- DNS hiyerarşisinin en tepesinde dünyaya dağılmış 13 adet kök sunucu (root server) bulunur ve bunlar yetki devri (delegation) esasıyla çalışır.
- IPv4 adreslerinde her bir sekizli (octet) 0 ile 255 arasında bir değere sahip olabilir; bu değerler 32 bitlik ikili sistemin onluk karşılığıdır.
- TCP protokolü akış kontrolü (flow control) ve tıkanıklık kontrolü (congestion control) mekanizmalarıyla güvenilir iletim sağlar.
- OSI modelinin 1. ve 2. katmanları (Fiziksel ve Veri Bağlantısı), TCP/IP modelinde tek bir 'Ağ Erişim' katmanı olarak eşleşir.
- İyi bilinen portlar 1-1023 aralığındadır.
- TCP üç yollu el sıkışma: SYN -> SYN+ACK -> ACK.
- HTTP Port 80, HTTPS Port 443 kullanır.
- SSH (Port 22) güvenlidir, Telnet (Port 23) şifresizdir.
- IP protokolü bağlantısızdır ve Ağ katmanında çalışır.

Sık Yapılan Hatalar

- POP3 (110) ve IMAP (143) portlarını karıştırmak.
- TCP'nin 4 katmanlı, OSI'nin 7 katmanlı olduğunu unutmak.
- UDP'nin 'güvensiz' olmasını 'kullanışsız' olarak algılamak (Hız gereken yerde UDP şarttır).

Formül Tablosu (hızlı bakış)

Formül adı	Formül
USB Veri Hızları	USB 2.0 = 480 Mbps USB 3.0 = 5 Gbps USB 3.1 = 10 Gbps
IPv4 Yapısı	32 bit = 4 × 8 bit (octet)

Devamı ücretsiz kayıtle

Bilgi Sistemleri Güvenliđi modülünün **18 bölümünün 6 tanesi** bu PDF'te. Kalan 12 bölüm, konu anlatımı ve çıkmış soru tarzındaki soru bankası FinLisans'ta.

- ✓ Ücretsiz üyelikle soru çözmeye hemen başla — kredi kartı istemiyoruz.
- ✓ Tüm SPK/SPL dersleri için ders notu, özet ve formül kartları.
- ✓ Konu bazlı soru bankası, deneme sınavı ve yanlış analizi.
- ✓ Sesli ders anlatımı ile yolda/işte tekrar imkânı.
- ✓ İlerlemeni takip eden panel ve sınav geri sayımı.

Bu modülün güncel ve tam sayfası

<https://www.finlisans.com/ders-notlari/bilgi-sistemleri-guvenligi>

Ücretsiz kayıt ol → <https://www.finlisans.com/auth/signup>

Son güncelleme: **17 Eylül 2026** · Kaynak: finlisans.com ders notları

Bu doküman sınavlara hazırlık amaçlı bir özettir; resmî kaynak yerine geçmez. SPL'nin yayımladığı güncel çalışma notlarını da takip ediniz.