Gizlilik ve Güvenlik

GÜVENLIK AÇIKLARININ OLUSUMU

ODTÜ

ÖNSÖZ

Bu kitapçık;

Orta Doğu Teknik Üniversitesi

Bilgisayar ve Öğretim Teknolojileri Eğitimi Bölümü

Öğretim Materyali Tasarımı ve Kullanımı Dersi Kapsamında

Prof. Dr. Zahide YILDIRIM rehberliğinde

Muhammed Ali ÖZER tarafından

Kasım 2023 tarihinde hazırlanmıştır.

ÖZET

Gizli, kişisel veya hassas bilgilerin izinsiz kişilerle paylaşılmamasını sağlama sürecidir. Mahremiyeti koruyarak, kullanıcıların özel verilerini sızıntılardan ve istismardan korur.

Güvenlik, bilgi, sistem veya ağların korunmasını ifade eder. Yetkisiz erişimleri, veri kaybını veya hasarını, kötü amaçlı yazılımları ve diğer tehditleri engellemek için alınan önlemleri içerir. Şifreleme, kimlik doğrulama, güvenlik duvarları gibi yöntemlerle sağlanır.

Güvenlik açıkları, sistemlerin veya yazılımların savunmasız olduğu noktaları ifade eder. Bu açıklar, kötü niyetli kişilerin sistemlere sızmasına veya zararlı faaliyetlerde bulunmasına izin verebilir. Yazılım hataları, zayıf yapılandırma veya eksik güvenlik önlemleri bu açıklara yol açabilir.

Bu konular, dijital dönemde kişisel ve kurumsal verilerin korunmasının temelini oluşturur. İnternetin yaygınlaşmasıyla birlikte, gizlilik ve güvenlik daha da önem kazanmış, şirketler sürekli olarak yeni tehditlere karşı önlemler geliştirmiştir. Sonuç olarak, gizlilik, güvenlik ve güvenlik açıklarının yönetimi, dijital dünyada bireyleri ve kurumları daha güvende tutmak için hayati bir rol oynamaktadır.

SÖZLÜK

Güvenlik Açığı: Bir sistemdeki zayıf noktalar veya hatalar. Bu açıklar, kötü niyetli kişilerin sistemlere izinsiz erişmesine veya istenmeyen sonuçlara yol açabilir.

Yazılım Hatası: Bir programın veya yazılımın hatalı kodlanması sonucu oluşan güvenlik açıkları veya istenmeyen davranışlar.

Donanım Eksikliği: Bir cihazın tasarım veya üretim aşamasında oluşan hatalar veya eksiklikler. Bu eksiklikler, cihazın güvenliğini etkileyebilir.

Tasarım Eksikliği: Bir sistemin veya ürünün güvenlik açıklarıyla ilgili tasarım aşamasında meydana gelen hatalar veya eksiklikler.

Uygulamalı Sorular: Kitapta yer alan teorik bilgilerin pratikte nasıl kullanılacağını gösteren, okuyucuların becerilerini sınayan sorular.

Şifreleme: Bilginin başkalarının erişimine karşı korunması için kullanılan matematiksel veya algoritmik yöntemler.

Biometrik Kimlik Doğrulama: Parmak izi, retina taraması gibi fiziksel özelliklerin kullanılarak kişinin kimliğinin doğrulanması süreci.

Phishing (Oltalama): İnsanları kandırmak için yapılan bir tür dolandırıcılık. E-posta veya mesaj gibi yerlerden sahte bilgilerle insanları aldatmaya çalışma.

Ağ Güvenliği: Bilgisayar ağlarının kötü niyetli saldırılara karşı korunması için alınan önlemler.

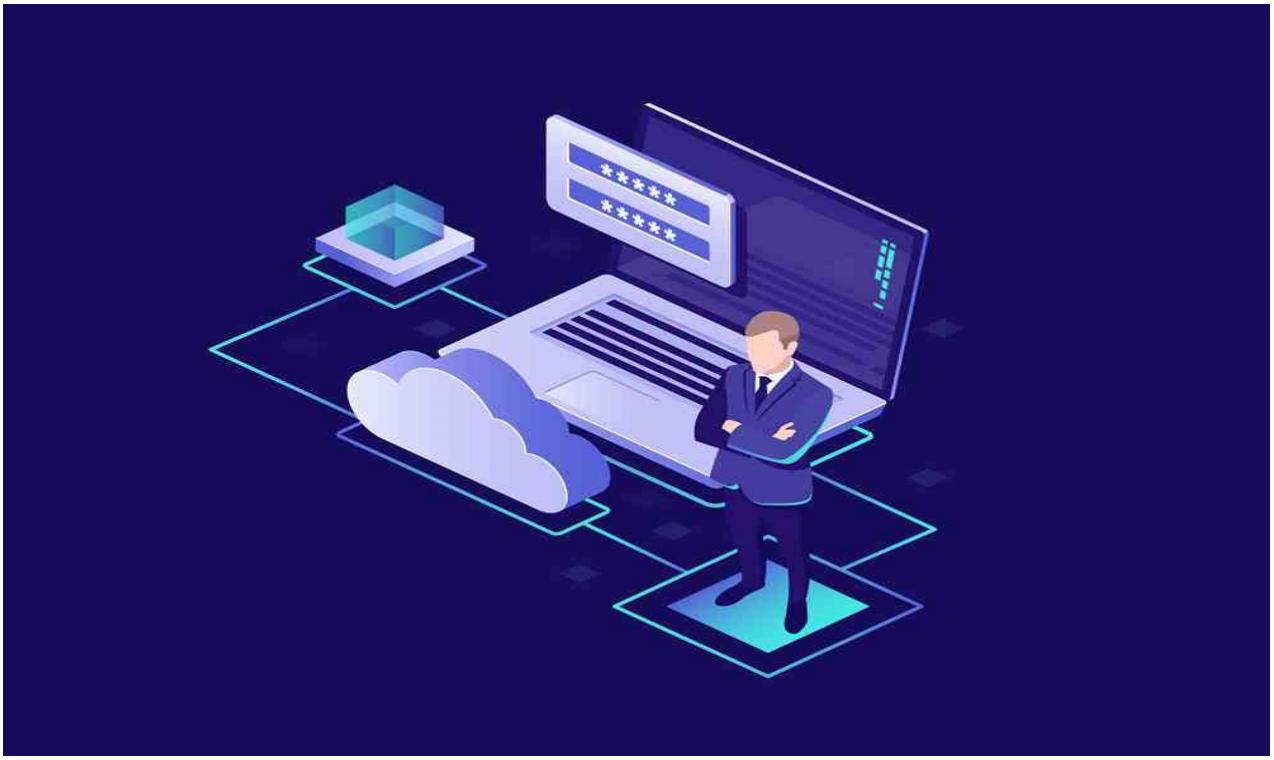
Two-Factor Authentication (2FA): İki aşamalı kimlik doğrulama yöntemi; genellikle şifre dışında bir ek kimlik doğrulama adımı daha gerektirir.

İÇİNDEKİLER

KAZANIMLAR

- Gizlilik ve güvenlik bilinci kazanmak
- Güvenlik açıklarını tanıma ve önleme yetisi kazanmak
- Yazılım, donanım ve kullanıcı hatalarını ayırt edebilmek
- Tasarım ve uygulama güvenliğini anlamak
- Pratik uygulamalar ve çözüm odaklı düşünme yeteneklerini güçlendirmek
- Sistemlerde güvenlik analiz yeteneğini geliştirmek
- Siber tehditleri tanıma ve karşı tedbir alma becerisi kazanmak
- Gizlilik politikalarının önemini kavrayabilmek
- Yasal ve etik konuları kavrayabilmek
- Güvenlik bilincinin yayılmasına katkıda bulunabilmek

Güvenlik ve Gizlilik



Dijital gizlilik ve veri güvenliği, bireylerin ve kurumların dijital ortamlarda gizliliklerini ve veri güvenliklerini korumak için aldıkları önlemleri ifade eder. Dijital gizlilik, kişisel bilgilerin ve iletişimlerin dijital ortamlarda korunması anlamına gelir. Bu, izinsiz erişime, kullanıma veya ifşaya karşı korunmayı, gizli iletişimlerin şifrelenmesini ve bilgilerin kullanıcının kontrolünde paylaşılmasını içerir. Kişisel verilerin, finansal bilgilerin ve sağlık verilerinin korunması amaçlanır.

Dijital gizlilik ve veri güvenliği, kişisel ve kurumsal bilgilerin güvenliğini sağlayarak kötü niyetli kişilerin, siber saldırıların veya veri ihlallerinin neden olduğu riskleri en aza indirir. Bu kavramlar, kullanıcıların çevrimiçi ortamlarda güvenle faaliyet göstermesini ve bilgilerinin kötüye kullanılmasından korunmasını hedefler.

Güvenlik Açıkları Nedir?

Güvenlik açıkları, bilgisayar sistemlerinde veya yazılımlarda bulunan zayıf noktalar veya hatalardır. Bu noktalar, kötü niyetli kişilerin sisteme girmesine, veriye zarar vermesine veya sistemi manipüle etmesine olanak tanır. Bunlar, genellikle tasarım eksiklikleri, yazılım hataları veya yanlış konfigürasyonlardan kaynaklanabilir. Örneğin, bir yazılımın doğrulama sürecinde yetersiz kontrol mekanizmaları olması, bir saldırganın sistemdeki hassas verilere erişmesine yol açabilir.

Güvenlik Açıklarının Türleri

Güvenlik açıkları internet dünyasında önemli bir konudur. Güvenlik açıkları farklı şekillerde karşımıza çıkabilir ve bizi etkileyebilir.Örneğin İnternette hesaplarımızı korumak için kullandığımız şifreler bazen başkaları tarafından bulunabilir veya çözülebilir. Bir diğer konu ise virüsler ve zararlı yazılımlar. Bilgisayarlarımıza veya telefonlarımıza bu zararlı yazılımlar bulaşabilir ve bilgilerimizi çalabilir veya cihazlarımızın çalışmasını engelleyebilirler. Phishing adı verilen bir dolandırıcılık yöntemi de var. Bu, insanları kandırmak için yapılan bir tür hile. Örneğin, sahte bir e-posta aracılığıyla insanları banka gibi göstererek kişisel bilgilerini çalmaya çalışabilirler. Cihazlarımızı düzenli olarak güncellemek de önemli bir adım çünkü güncellemeler güvenlik açıklarını kapatır ve cihazlarımızı kötü niyetli kişilerden korur.

Güvenlik Açıklarının Oluşumu

Güvenlik açıklarının oluşumu, genellikle yazılım, donanım veya kullanıcı hataları gibi çeşitli faktörlerin bir kombinasyonu sonucunda gerçekleşir. İşte bu faktörleri daha detaylı bir şekilde açıklayan bazı ana konular:

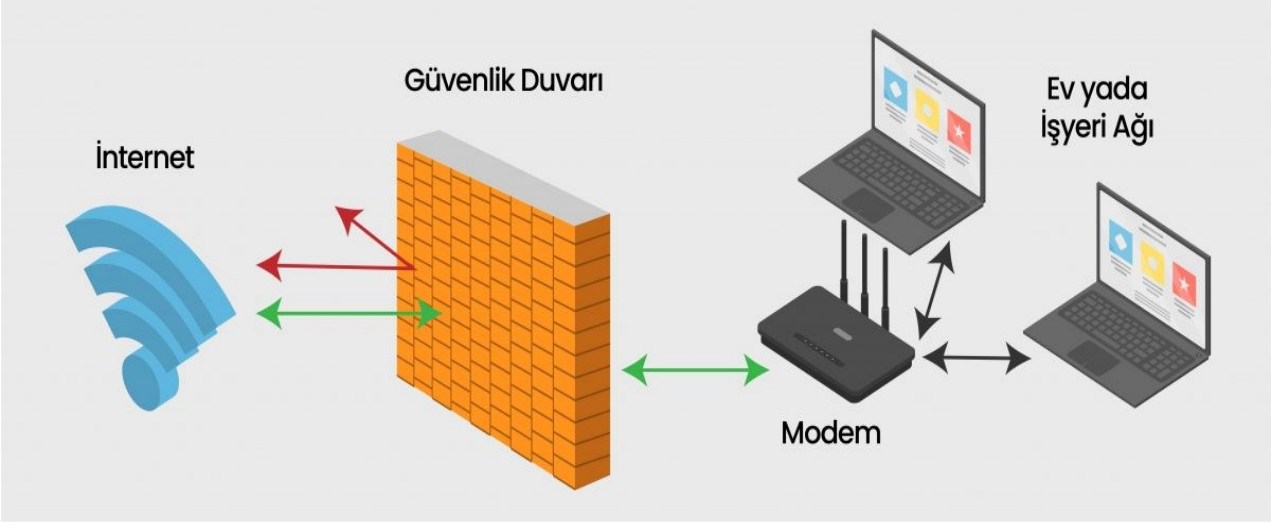
1. Yazılım Hataları:

Programlama Hataları: Yazılım geliştiricilerin yazılım kodlarını oluştururken yaptıkları hatalar, güvenlik açıklarına neden olabilir. Bu hatalar genellikle kodun anlamındaki bir eksiklik, yanlış bir mantık veya beklenmeyen bir durumun ele alınmaması gibi durumları içerebilir.

Zayıf Şifreleme veya Güvenlik Kontrolleri: Yazılımların içinde kullanılan şifreleme algoritmalarının zayıf olması veya güvenlik kontrollerinin yetersiz olması da güvenlik açıklarına neden olabilir.

2. Donanım Hataları:

Güvenlik Duvarı Eksiklikleri: Ağ güvenliği için kullanılan güvenlik duvarlarının yanlış yapılandırılması veya eksik olması, yetkisiz erişimlere neden olabilir.



Güçlü Kimlik Doğrulama Eksikliği: Donanımın kullanıcı kimlik doğrulama süreçlerinde zayıf olması, yetkisiz kişilerin sistemlere giriş yapmasına olanak tanır.

3. Kullanıcı Hataları:

Güvenlik Politikalarına Uyumsuzluk: Kullanıcıların güvenlik politikalarına uymaması veya bu politikaların yeterince açık olmaması, güvenlik açıklarına zemin hazırlar.

Bilinçsiz Kullanım: Kullanıcıların bilinçsizce kötü amaçlı bağlantılara tıklaması veya güvenlik uyarılarını dikkate almamaları, siber tehditlere yol açabilir.

4. Tasarım Eksiklikleri:

İstismar İmkanı Yaratan Tasarım Hataları: Sistem tasarımındaki eksiklikler veya yanlışlıklar, siber saldırganların bu zayıf noktaları istismar etmelerine olanak tanır.

İşlevsellik ve Güvenlik Dengesi: Tasarım aşamasında, işlevsellik ve güvenlik arasında doğru bir denge kurulmaması, sistemde güvenlik açıklarının ortaya çıkmasına neden olabilir.

Güvenlik açıklarının oluşumu genellikle bu faktörlerin bir kombinasyonundan kaynaklanır. Bu nedenle, güvenlik açıklarını en aza indirmek için yazılım geliştirme süreçlerinde güvenlik kontrolleri, güvenlik eğitimleri, düzenli güvenlik testleri ve güvenlik politikalarının etkin bir şekilde uygulanması önemlidir.

Uygulama Soruları

1. Hangisi yazılım güvenlik açıklarını düzeltebilmek için genellikle kullanılan bir yöntem değildir?
    a) Kod revizyonu ve güncelleme
    b) Otomatik güvenlik taramaları ve düzeltmeler
    c) Manuel güvenlik testleri ve düzeltmeler
    d) Hata ayıklama ve performans optimizasyonu
2. Güvenlik açıkları yazılım geliştirme sürecinde hangi aşamalarda ortaya çıkabilir?
3. Hangisi genellikle ağ güvenliği açıklarını keşfetmek için kullanılan bir yöntem değildir?
    a) Ağ trafiği izleme ve analiz
    b) Güvenlik duvarı kullanımı
    c) Penetrasyon ve sızma testleri
    d) Fiziksel erişim denetimleri
4. Web uygulamaları ve sitelerde sıkça görülen güvenlik açıkları nelerdir?
5. Mobil uygulamalarda en sık karşılaşılan güvenlik açıkları hangisidir?
    a) Kötü niyetli yazılım yükleme
    b) Zayıf şifreleme yöntemleri
    c) Veri sızıntısı
    d) Doğrulanmamış kullanıcı girişleri
6. Veri güvenliği açıkları hangi tür hatalar sonucunda ortaya çıkabilir?
7. Hangisi en etkili güvenlik farkındalığı oluşturmanın yolu değildir? ?
    a) Eğitim ve farkındalık programları
    b) Günlük güvenlik uygulamaları
    c) Gerçek zamanlı saldırı gösterimleri
    d) Gerçek hayat örnekleri ve başarı hikayeleri paylaşımı
8. Kullanıcıların güvenlik konusunda daha bilinçli olmalarını sağlamak için hangi yöntemler kullanılabilir?
9. Güvenlik açıkları için düzenli güncellemelerin önemi nedir?
10. Kötü niyetli uygulamaların kullanıcı cihazlarına verebileceği zararlar nelerdir?
11. Sosyal mühendislik saldırıları hangi yöntemlerle gerçekleştirilir ve nasıl önlenebilir?

Cevap Anahtarı

1. d) Hata ayıklama ve performans optimizasyonu
2. Yazılım geliştirme sürecinde güvenlik açıkları her aşamada ortaya çıkabilir. Genellikle tasarım, kodlama, test ve dağıtım aşamalarında görülebilir.
3. d) Fiziksel erişim denetimleri
4. Kimlik doğrulama ve oturum yönetimi hataları, hassas verilerin eksik korunması, zararlı kodlarla dolu mesajlarla insanları kandırma gibi.
5. a) Kötü niyetli yazılım yükleme
6. Veri güvenliği açıkları genellikle zayıf şifreleme, yanlış yapılandırılmış izinler, kötü kodlama uygulamaları gibi hatalar sonucunda ortaya çıkabilir.
7. b) Günlük güvenlik uygulamaları
8. Eğitim, farkındalık programları, gerçek zamanlı saldırı gösterimleri ve gerçek hayat örnekleri paylaşımı gibi yöntemler kullanılabilir.
9. Düzenli güncellemeler, yeni keşfedilen güvenlik açıklarını kapatmak, sistemleri ve uygulamaları korumak için hayati öneme sahiptir.
10. Kötü niyetli uygulamalar, kullanıcı cihazlarına zarar verebilir; örneğin, kişisel verilerin çalınması, cihazın kontrolünün ele geçirilmesi, kötü amaçlı yazılımın yayılması gibi zararlar verebilir.
11. Sosyal mühendislik saldırıları genellikle manipülatif taktiklerle gerçekleştirilir. Önlemek için kullanıcıların farkındalığını artırmak, eğitimlerle sosyal mühendislik taktiklerini tanımalarını sağlamak önemlidir. Ayrıca güvenlik politikalarına uygun davranılması ve güvenlik bilincinin sürekli olarak taze tutulması gerekir.

KAYNAKÇA

- https://www.bgasecurity.com/2019/01/guvenlik-mi-gizlilik-mi/#:~:text=Gizlilik%20ve%20g%C3%BCvenlik%20yukar%C4%B1da%20da,verilerini-zin%20nas%C4%B1l%20korunmas%C4%B1%20gerekti%C4%9Fini%20belirtir.
- https://safety.google/intl/tr/security-privacy/
- https://www.siberkavram.com/2022/04/owasp-top-10.html
- https://www.infinitumit.com.tr/guvenlik-acigi/
- https://www.delfpanel.com.tr/delfpanel/uploads/images/gizlilik-ve-guvenlik-cledec.jpg
- https://indigodergisi.com/wp-content/uploads/2017/11/siber-guvenlik-nedir-2-e1512203459906.png
- https://www.cybermagonline.com/img/sayfa/phishing-saldirisi-nedir-nasil-korunulur5afea6a3c5385.png
- https://paymentap.co.uk/wp-content/uploads/2022/12/phishing-saldirisi.png
- https://www.technopat.net/wp-content/uploads/2019/09/gizlilik.jpg