29.12.2022
Ödev No: 7

BM 359 İNTERNET PROGRAMLAMA

Web Güvenliği

Selin Cansu AKBAŞ
Bilgisayar Mühendisliği Bölümü – 191180005

Özet

İnternet güvenliği, internet üzerindeki etkinlik ve olay güvenliğini tanımlayan bir terimdir. Tarayıcı güvenliği, çevrimiçi davranış ve ağ güvenliği gibi konuları kapsayan daha geniş siber güvenlik ve bilgi güvenliği kavramlarının bir parçasıdır. Hayatımızın çoğunu internette geçiriyoruz. Tehditlerle dolu çevrimiçi bir mecrada, her web sitesi kendi güvenliğini sağlamalıdır. Özellikle kullanıcılarının kişisel verilerini saklayabilen ve güvende tutabilen web siteleri her zaman bir adım önde olacaktır. Güvenlik, internetteki en önemli faktörlerden biridir diyebiliriz.

Ödev İçeriği

Web Güvenliği Nedir?

Web sitesi güvenliği, web sitelerini ve sunucuları korumanın ve güvenliğini sağlamanın önemli bir parçasıdır. Web siteleri, web sitesi güvenlik yazılımı kullanılarak olası güvenlik açıkları ve kötü amaçlı yazılımlara karşı kontrol edilir.

Bu yazılım, arka kapı saldırılarını, yeniden yönlendirme saldırılarını, Truva atlarını ve diğer birçok tehdidi tarayabilir. Web sitesi güvenlik yazılımları, web sitesinde sorunlar olduğunda kullanıcıyı bilgilendirir ve bunları gidermek için çözümler sunar.

Kurumsal ağlar her zaman yüksek güvenlik açığı riskine sahiptir ve web sayfalarının güvenliğinin sağlanması çok önemlidir. Bir ağ tehdidi durumunda, sunucu ve web sitesi de tehlikeye girer. Bu, kötü amaçlı yazılımın şirket ağına girmesine ve kötü amaçlı yazılımın faaliyetlerini açığa çıkarmasına olanak tanır. [1]

İnternet güvenliği yalnızca İnternet ile ilgili değildir, genellikle tarayıcı güvenliği ve ağ ile ilgilidir, aynı zamanda ağ güvenliği, uygulamalar ve bir bütün olarak işletim sistemleri ile de ilgilidir. Amacı, İnternet saldırılarına karşı kurallar ve önlemler oluşturmaktır. İnternet, güvenli olmayan bir veri alışverişi kanalıdır; bu sizi, kimlik avı, web virüsü, truva atları, solucanlar ve diğerleri gibi yüksek saldırı veya dolandırıcılık riskine sokar.

Veri aktarımını korumak için şifreleme ve sıfırdan tasarım dahil birçok yöntem kullanılır. Şu anda, bilinen veya ortaya çıkan tehditlere karşı önleme ve gerçek zamanlı korumaya odaklanılmaktadır. [2]

İyi Bir Web Sitesi Güvenlik Planının Özellikleri

Kötü amaçlı yazılım taraması

Web Sitesi Kötü Amaçlı Yazılımları Kaldırma

Manuel kötü amaçlı yazılım ve bilgisayar korsanlığı kaldırma

Dosya değişikliği izleme

Kara liste / spam izleme

Kara listeyi kaldırma

Güvenlik izleme

Gelişmiş DDoS azaltma

Web Uygulaması Güvenlik Duvarı (WAF)

İçerik Dağıtım Ağı (CDN)

Site Mührü

İnternet Güvenlik Ürünleri

Antivirüs: Virüsten koruma yazılımı ve Internet güvenlik programları, programlanabilir bir aygıtı kötü amaçlı yazılımları algılayıp ortadan kaldırarak saldırılara karşı koruyabilir. Antivirüs yazılımı internetin ilk yıllarında ağırlıklı olarak shareware'di, fakat günümüzde bütün platformlar için internet üzerinde seçilebilecek pek çok ücretsiz antivirüs yazılımı bulunmaktadır.

Parola Yöneticileri: Parola yöneticisi, kullanıcının parolaları depolamasına ve düzenlemesine yardımcı olan uygulamalardır. Parola yöneticileri parolaları şifrelenmiş olarak saklar ve kullanıcının bir ana parola oluşturmasını gerektirir. Bu parola kullanıcıya tüm parola veri tabanlarına erişim sağlayan tek, ideal olarak çok güçlü bir parola olmalıdır.

Güvenlik Süitleri: Sözde güvenlik süitleri ilk olarak 2003 yılında (McAfee) satışa sunuldu ve bir dizi güvenlik duvarı, antivirüs, anti-spyware ve daha fazlasını içeriyordu. Ayrıca hırsızlığa karşı koruma, taşınabilir bellek güvenlik kontrolü, özel internet taraması, bulut anti-spam, bir dosya parçalayıcı ya da açılır pencerelerin yanıtlanması gibi güvenlikle ilgili kararlar sunmaktaydılar ve bunların bazıları ücretsizdir. [2]

Web uygulaması güvenliği, güvenlik ilkeleri olarak da adlandırılan dört güvenlik koşulunu ele almayı ve yerine getirmeyi amaçlamaktadır:

Gizlilik: Web uygulamasında saklanan hassas verilerin hiçbir koşulda ifşa edilmemesi gerektiğini belirtir.

Dürüstlük: Web uygulamasında bulunan verilerin tutarlı olduğunu ve yetkisiz bir kullanıcı tarafından değiştirilmediğini belirtir.

Kullanılabilirlik: Web uygulamasının, isteğe bağlı olarak belirli bir süre içinde gerçek kullanıcı tarafından erişilebilir olması gerektiğini belirtir.

Reddetme: Gerçek kullanıcının Web uygulamasında yer alan verileri değiştirmeyi reddedemeyeceğini ve Web uygulamasının kimliğini gerçek kullanıcıya kanıtlayabileceğini belirtir. [4]

Web Servislerinin Güvenliği

Web servisleri, diğer dağıtık uygulamalar gibi farklı seviyelerde korunur:

• SOAP mesajları, kablolardan, gizli olarak ve üzerinde değişiklik yapılamadan dağıtılmalıdır.

• Sunucu kimin konuştuğu ve konuşan istemcilerinin hakları konularında emin olmalıdır.

• İstemciler doğru sunucu ile konuştuklarından ve bir balık ağına yakalanmadıklarından(phishing) emin olmalıdırlar.

• Sistem mesajlarının kayıtları olaylar zincirinin güvenilebilir bir şekilde tekrar edilebilmesi ve kimliği doğrulanmış ziyaretçileri takip edebilecek kadar yeterli bilgiye sahip olmalıdırlar. [3]

Yapılan çalışmaların sonuçlarında, internet sitelerinde gezinti yaparken bilgisayarımıza virüs ve tehlikeli yazılım bulaştırma ihtimali yüksek olan siteler genellikle şunlardır:

- çok fazla bilinmeyen siteler,
- bahis siteleri,
- pornografik siteler,
- korsan yazılım indirilen siteler.

Web güvenliğinde öncelikli olarak:

- Tuzak web sitelerine dikkat etmek ve güvenilmeyen web sitelerini ziyaret etmemek,
- E-posta mesajları ile gönderilen bağlantılara dikkat etmek,
- Sık kullanılanlar listesi oluşturmak,
- Web sitelerinde gezerken yayılabilen zararlı programlardan korunmak için açılır pencere engelleyicisi kullanmak (Yukarıda bahsedilen ayarlar),
- Arama motorlarını kullanırken özellikle çocuklu ailelerin yüksek düzeyli filtreleme araçları sayesinde özellikle müstehcen sitelerin arama sonuçlarında engellenmesini ve bu sayede güvenli arama sağlamaları gerekmektedir. [5]

Sonuç

Bu ödev araştırmasında Web güvenliği hakkında genel bir araştırma yapılmıştır. Genel bir bilgi sahibi olunmuştur. Web sitesi güvenliği, web sitelerini ve sunucuları korumanın ve güvenliğini sağlamanın önemli bir parçasıdır. Web siteleri, web sitesi güvenlik yazılımı kullanılarak olası güvenlik açıkları ve kötü amaçlı yazılımlara karşı kontrol edilir. Bilinmeyen web sitelerinde dolaşmamak gerekir ve çok dikkatli olmak gerekir. Birçok web sitesi çeşitli tuzaklar içerebilir. Bu nedenle, güvendiğimiz ve itimat ettiğimiz web sayfalarını tavsiye etmemiz ve web sayfalarından bu web sayfalarının bilmediğimiz bölümleri hakkında bilgi/iletişim bilgileri gibi bilgiler toplamamamız gerekiyor. Ayrıca sık kullanılan web siteleri için tarayıcıda sık kullanılanlar oluşturmak, tuzağa düşen web sitelerinden kendimizi koruyabilmemiz için önemlidir.

Kaynakça

1- https://siberdagitim.com/Web-Sitesi-Guvenligi-nedir-a3
2- https://tr.wikipedia.org/wiki/%C4%B0nternet_g%C3%BCvenli%C4%9Fi
3- https://www.webguvenligi.org/wp-content/uploads/2007/09/Web%20ServicesTRK.pdf
4- https://tr.theastrologypage.com/web-application-security
5- https://www.guvenliweb.org.tr/dokuman-detay/web-guvenligi