Bilgi Sistemleri ve Güvenliği

Bilgi Güvenliği Yazılımları ve Kötücül Yazılım Türleri

Muhammet Baykara mbaykara@firat.edu.tr

1. **Saldırı Tespit Sistemleri**
2. **Saldırı Engelleme Sistemleri**
3. **Sıfır Gün Zararlı Yazılım Tespit Sistemi**
4. **Tuzak Sistemler**
5. **Güvenlik Duvarları**
6. **Web Uygulama Güvenlik Duvarı**
7. **Veritabanı Güvenlik Duvarı**
8. **Ağ Tabanlı Adli Bilişim Sistemi**
9. **İstemci Güvenlik Ürünleri**
10. **E-Posta Güvenliği**
11. **URL Filtresi ve Antivirüs**
12. **Web Cache Vekil Sunucu**
13. **Transparan İçerik Yönlendirici**
14. **Kayıt Toplama ve Korelasyon Sistemi**
15. **Ağ Erişim Kontrolü**
16. **Ağ İzleme ve Performans Analiz Sistemi**
17. **Tek Yönlü Veri Transfer Cihazları**
18. **Veri Kaçakları Önleme Sistemi**
19. **Risk Analiz Yönetim Sistemleri**
20. **Yük Dengeleyici**
21. **Zafiyet Tarama Sistemleri**

Bilgi Güvenliği Yazılımları

- Bilgi güvenliğinin sağlanması için çok çeşitli donanım ve yazılımlar kullanılmaktadır. Kişisel ya da kurumsal ihtiyaca göre bilgi teknolojileri yöneticileri, bu araçları temin ederek sistem üzerinde sürekliliğini ve güncelliğini sağlamak durumundadır. Bilgi güvenliği yazılımları, kurumsal ve kişisel anlamda öneme sahip kritik bilgilerin korunması açısından elzem araçlardır. Bu araçların birbirinin yerine kullanılamayacakları ve birbirini tamamlayıcı yapılar olduğu unutulmamalıdır [56]. Güvenlik ihtiyaç ve gereksinimlerine göre bu araçlar hibrit bir biçimde kullanılırlar.

1-Güvenlik Duvarları

- Güvenlik duvarları (firewall), temel ağ güvenliği sistemlerinden biri olup statik izleme kabiliyeti sayesinde üzerinden geçen trafik için belirlenen kurallara göre erişim denetimi yapmak amacıyla kullanılırlar. Güvenlik duvarları, sahip oldukları kural tablosu yardımı ile istenmeyen yere doğru giden veri geçişini engelleyebilmektedirler. Ağ içerisinde ana segmentler arasında kullanılabilmeleri sayesinde, segmentler arasında erişim kuralları uygulanabilmektedir. Güvenlik duvarları, dış dünya ile olan bağlantıyı sağladığından ve kullanıcıların şifreli bir şekilde bağlantı kurmalarına olanak verdiğinden verinin gizliliğinin korunmasına yardımcı olmaktadır.

2-Saldırı Tespit ve Engelleme Sistemleri

- STS'ler, saldırıları trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği raporlayarak, kritik durumlarda sistem yöneticisini uyarabilir. Saldırı engelleme sistemleri gibi ağ trafiğine müdahale etme özellikleri yoktur. Sonraki bölümde detayları ile birlikte ele alınacaktır.
- Saldırı engelleme sistemleri, korunmak istenen ağ segmentlerinin bağlantıları üstüne konularak zararlı trafiğin kesilmesini sağlar. Saldırı engelleme sistemleri, trafik üzerinde önceden belirlenmiş saldırı imzalarına uyan trafiği ararlar ve bulduklarında, paket düşürme, TCP bağlantısını sonlandırma gibi eylemlerde bulunabilirler. Bu özelliklere ek olarak servis dışı bırakma saldırılarına karşı (DoS, DDoS), istatistiksel ve manuel verilmiş sınırları işleterek koruma sağlayabilirler.

3-Web Uygulama Güvenlik Duvarı

- Web uygulama güvenlik duvarları, saldırı engelleme sistemlerine benzer bir görev üstlenirler. Web hizmetlerinin çok yaygın kullanılması sebebi ile üretilen bu sistemler, web hizmetlerine ve web sunucularına gelebilecek saldırıları önleyecek trafik imzaları bulundururlar. Bu özelliklerine ek olarak yazılım geliştirilirken önlem alınmamış konularda ek koruma getirebilirler.

4-Veri Tabanı Güvenlik Duvarı

- Günümüzde hacimleri oldukça artan ve sayısız sorgunun çalıştırıldığı veri tabanlarına gelen sorguların incelenmesi ve olası kötücül faaliyetlerin önlemlerinin alınması gerekmektedir. Veri tabanı güvenlik duvarları bu amaçla kullanılmaktadır. Veri tabanı güvenlik duvarları, kullanıcıların genel davranışlarını öğrenerek bunların dışına çıkılması halinde uyarı üretebilen sistemlerdir. Veri tabanı güvenlik duvarı ile web güvenlik duvarlarının birlikte kullanılması sayesinde sistem kullanıcılarının web üzerinde gerçekleştirdiği eylemlerin izdüşümleri takip edilebilmektedir.

5-E-posta Güvenliği

- Kurum ve kuruluşların sistemlerine dışarıdan gelebilecek SPAM ve zararlı kod içeren e-postaların engellenmesi amacıyla kullanılırlar. E-posta güvenliği (gateway), ağ üzerinde İnternet erişimi olan bir mail sunucu (Mail Transfer Agent, MTA) görevi ile de kullanılabilmektedir. Ayrıca mail sunucular üzerinde çalışabilen çeşitleri de mevcuttur.

6-Yük Dengeleyici

- Bilişim sistemlerinde işlem hacmi oldukça kritik seviyelere ulaşabilmektedir. Yük dengeleyiciler, artan trafiği, yoğun istek gelen sunucular arasında yükü paylaştırarak rahatlatırlar. Örneğin söz konusu bir web sunucu ise yük dengeleyiciler, SSL'i kendi üzerinde sonlandırır ve diğer sunucuları şifreleme yükünden kurtarıp performans artışı sağlayabilmektedir.

7-URL Filtresi ve Antivirüs

- Bilgisayar ağlarında çalışan istemci makinelerin İnternet erişimlerinin düzenlenmesi için kullanılmaktadırlar. Kurum politakaları gereği erişim yasağı bulunan sitelerin engellenmesi gibi kritik işlemleri gerçekleştiren yapılardır. Bu eylemlerin yanı sıra bu yazılımlar eğer vekil sunucu olarak çalışıyorlarsa ağ üzerindeki gelen trafiği kontrol edip zararlı yazılım analizi de yapabilmektedirler.

8-Web Cache Vekil Sunucu

- Web Cache vekil sunucuları, URL filtreleri ile birlikte kullanılabildikleri gibi tek başlarına da kullanılabilmektedir. İnternet üzerinden aynı dosyanın birden çok kez indirilmesi durumunun önüne geçilmesi amacıyla kullanılmaktadır. Web Cache vekil sunucuları, indirilen dosyaları kendi üzerlerinde tutarak İnternet bant genişliği açısından tasarruf sağlamış olurlar.

9-Transparan İçerik Yönlendiriciler

- Transparan içerik yönlendiriciler, kompleks ağ yapılarında ağa bağlı istemcilerin URL filtrelemesi gibi trafik yönlendirmesi gerektiği durumlarda, kullanıcı tarafında herhangi bir ayarlama yapılmadan işlemin gerçekleştirilmesini sağlayabilirler. Böylece kullanım kolaylığı sağlanmış ve ayarların eksik yapılması durumu ortadan kalkmış olur. Ayrıca kullanıcıların istenilen vekil sunucuları kullanması garanti edilmiş olur.

10-Zafiyet Tarama Sistemleri

- Bu yazılımlar, sistem üzerindeki açıklıkların tespit edilmesi amacıyla kullanılan yapılardır. Zafiyet tarayıcı sistemler, işletim sistemlerindeki ve işletim sistemi üzerinde çalışan uygulamalar içindeki açıklıkları otomatik taramalar ile bulabilmektedir. Bu sistemler ayrıca yama eksiklikleri ve kurum/kuruluş güvenlik politikalarına aykırı durumları tespit edebilme yeteneğine de sahiptirler.

11-Risk Analiz Yönetim Sistemleri

- Risk analiz yönetim sistemleri, ağ üzerinde bulunan zafiyet tarama sistemlerinden sistem açıklıklarını; güvenlik duvarı, anahtar ve yönlendirici gibi ağ aktif cihazlarından da yapılandırma ayarlarını toplayıp bir ağ modeli oluşturabilen yapılardır. Oluşturulan bu ağ modeli ile risk analizleri gerçekleştirilir ve bu riskler önceliklerine göre derecelendirilir. Böylece sınırlı iş gücü kaynaklarının nerede ve hangi durumda ilk önce kullanılması gerektiği ve en çok riske sahip olan sistemler gibi kritik bilgiler elde edilebilmektedir.

12-Kayıt Toplama ve Korelasyon Sistemi

Ağ üzerinde birçok cihaz ve sistem kendi üzerinde meydana gelen aktiviteleri barındıran olay kayıtlarını tutmaktadır. Bu kayıtlar, her sistem üzerinde ayrı ayrı formatlarda bulunabildiğinden bunların ilişkilendirilmesi çok zor olmaktadır. SIEM (Security Information and Event Management) adı verilen bu kayıt toplama ve korelasyon sistemleri sayesinde dağıtık halde bulunan bu kayıtlar, merkezi bir yerde toplanıp ilişkili hale getirilebilmektedir. Yazılan mantıksal kurallar sayesinde gerçek zamanlı korelasyon yapılabilir ve böylece normalde tespit edilemeyen güvenlik olayları tespit edilebilir.

13-Ağ Erişim Kontrolü

- Ağ erişim kontrolü sistemleri, kurum politikalarına uymayan sistemlerin ağa dahil olmalarını engellemek amacı ile kullanılır. Bu sayede yabancı sistemlerin ve güvenlik durumu uygun olmayan sistemlerin iç ağı tehdit etmesi önlenir.

14-Sıfır Gün Zararlı Yazılım Tespit Sistemi

- Kötüye kullanım tespiti mantığı ile çalışan imza tabanlı saldırı tespit sistemleri (antivirüs vb.), kendi imza veri tabanlarında olmayan zararlı yazılımları yakalayamamaktadır. Bu durum, özellikle günümüzde artan bir hacime sahip kötücül yazılımların varlığı düşünüldüğünde oldukça kötü sonuçlar doğurabilmektedir. Bugün ortaya çıkartılan yeni bir kötücül yazılımın, ilgili tespit sisteminin imza veri tabanında yer alması uzun süreler alabilmektedir. Arada geçen süre zarfında sistemler yeni çıkartılan kötücül yazılımlara karşı savunmasız kalmaktadır. Sıfırıncı gün zararlı yazılım tespit sistemi, şüpheli gördüğü yazılımları ağ seviyesinde yakalayıp test sistemlerinde çalıştırırlar [58]. Bu testler sonucunda imzasız olarak zararlı olduğu tespit edilen yazılımların engellenmesi sağlanmaktadır.

15-Ağ İzleme ve Performans Analiz Sistemi

- Bu sistemler, ağ üzerinde ağ trafiğini izleyip, uygulamalar ve ağ performansı hakkında bilgi toplayan yapılardır. Ağ izleme ve performans analiz sistemlerinin kullanım amacı, performans kaybı durumlarında sistem yöneticisini bilgilendirmek ve sorunun kaynağı hakkında detaylı bir raporlama sağlamaktır [59].

16-Veri Kaçakları Önleme Sistemi

- Kurumsal açıdan önem arz eden hassas verilerin izinsiz olarak kurum dışına çıkartılmasına engel olan sistemlerdir. İstemci ve ağ düzeyinde çalışan farklı modelleri mevcuttur. İstemci üzerinde çalışan sistemlerde, taşınabilir cihazlardan oluşabilecek veri kaçaklarının önlenmesi için aygıtsal kontrol yapan bileşenler bulunmaktadır.

17-Ağ Tabanlı Adli Bilişim Sistemi

- Bu sistemler pasif olarak ağ trafiğini yakalayarak trafik üzerinde derin paket incelemesi yapabilme imkânı sağlarlar [60]. Bu sistemler, bilişim sistemlerindeki bilgilerin mahkemede suçluluğun veya suçsuzluğun ispatında kullanılmak üzere incelenmesini sağlamaktadır. Ağ tabanlı adli bişim sistemleri, sayısal verilerin elde edilmesi, korunması ve analiz edilmesi işlemlerinin kanıtın gereklerine uygun olarak adli makamlara sunulması aşamasına kadar uygulanması sürecini yönetir.

18-Tek Yönlü Veri Transfer Cihazları

- İnternet erişimi olmayan ağlara veri transferi yapıldığı zaman dış dünyaya veri sızmasını engellemek amacı ile kullanılan cihazlardır. Donanım tabanlı tek yönlü veri transfer cihazları, kullanılan protokolü her iki tarafa da çalışırmış gibi gösterip donanım üzerinde bir yön dışında ters tarafa veri iletişimini fiziksel olarak engelleyen yapılardır [61].

19-İstemci Güvenlik Ürünleri

- İstemci tarafında çalışan güvenlik ürünleri, ağ seviyesinde çalışan araçlara destek niteliğindeki yapılar olup ek bir katman gibi görev yaparlar. İstemci güvenlik ürünlerine örnek olarak, antivirüs, saldırı engelleme sistemleri, veri kaçakları önleme yazılımları ve disk şifreleme yazılımları örnek olarak verilebilir [56].

Kötücül Yazılım Türleri

Bilgi Güvenliği
WEB AÇIKLIKLARI

Muhammet Baykara mbaykara@firat.edu.tr

Web Güvenlik Açıklıkları

- Web uygulamalarının güvensiz olması; uygulamanın kaynak kodu, uygulamanın üzerinde çalıştığı sunucu veya sunucu istemci arasındaki iletişim altyapısının üzerindeki açıklardan kaynaklanmaktadır.
- Literatür incelendiğinde güvenlik riskleri hakkında en kapsamlı çalışan kuruluş olarak OWASP göze çarpmaktadır. OWASP dünya çapında yazılım güvenliğini geliştirmeye odaklanmış bir kuruluştur.
- Kuruluşun misyonu, dünya çapında birey ve kuruluşların gerçek yazılım güvenlik riskleri hakkında bilinçli karar verebilmesi için yazılım güvenliğini öne çıkarmaktır. Kuruluş web uygulama güvenliğinde farkındalığı arttırmak için en bilindik web uygulama açıklıklarını yayınlamaktadır.

OWASP 10

Web Güvenlik Açıklıkları

Sıra Nu.	Açıklıklar	Kaynak	Etkilenen
1	Enjeksiyon (Injection)	Uygulama	Sunucu
2	Kırık Kimlik Doğrulama ve Oturum Yönetimi (Broken Authentication and Session Management)	Uygulama	İstemci
3	Siteler Arası Betik Çalıştırma (Cross-Site Scripting -XSS)	Uygulama	Sunucu/ İstemci
4	Güvensiz Doğrudan Nesne Başvurusu (Insecure Direct Object References)	Uygulama	Sunucu
5	Güvenlik Yanlış Yapılandırma (Security Misconfiguration)	Sunucu	Sunucu
6	Hassas Veriyi Açıkta Bırakma (Sensitive Data Exposure)	Uygulama	Sunucu
7	İşlev Seviyesi Erişim Kontrolü Eksikliği (Missing Function Level Access Control)	Uygulama	Sunucu
8	Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery (CSRF))	İletişim Altyapısı	İstemci
9	Bilinen Açıklık Bileşenlerini Kullanma (Using Known Vulnerable Components)	Uygulama	Sunucu
10	Doğrulanmayan Yönlendirme ve İletme (Unvalidated Redirects and Forwards)	Uygulama	Sunucu/ İstemci

Web Güvenlik Açıklıkları

- **A. Uygulama Kodu Kaynaklı Açıklıklar**
- **Enjeksiyon (Injection):** Enjeksiyon açıklıkları komutun ya da sorgunun bir kısmında güvenilmeyen verinin yorumlayıcıya gönderilmesiyle meydana gelmektedir.
- **Kırık Kimlik Doğrulama ve Oturum Yönetimi (Broken Authentication and Session Management),** Uygulama fonksiyonlarının kimliklendirme ve oturum yönetimiyle ilgili fonksiyonlarının uygulanmaması sonucu meydana gelmektedir.
- **Siteler Arası Betik Çalıştırma (Cross-Site Scripting (XSS)),** Siteler Arası Betik Çalıştırma açıklığı uygulamaların web tarayıcı üzerinden, güvenilmeyen verinin alınması ya da gönderilmesi sırasında, verilerin düzgün doğrulanmaması sonucu meydana gelmektedir. Bu açıklık saldırganlara, kurbanının tarayıcısı üzerinde betik çalıştırmasını sağlamaktadır.

Web Güvenlik Açıklıkları

- **Güvensiz Doğrudan Nesne Başvurusu (Insecure Direct Object References),** Doğrudan nesne başvurusu, uygulamayı geliştiren kişinin uygulama içerisinde kullanılan dâhili uygulama nesnelerinin referanslarına uygun erişim kontrolü yapılmaması sonucu meydana gelmektedir.

- **Hassas Veriyi Açıkta Bırakma (Sensitive Data Exposure),** Web uygulamaların birçoğunda kredi kartları, vergi numaraları ve kimliklendirme bilgilerini düzgün olarak korumamaktadır.

- **İşlev Seviyesi Erişim Kontrolü Eksikliği (Missing Function Level Access Control),** Web uygulamalarının birçoğunda kullanıcı ara yüzü kullanılabilir olmadan önce erişim hakları seviyesinde fonksiyonlar doğrulanmaktadır.

Web Güvenlik Açıklıkları

- **Bilinen Açıklık Bileşenlerini Kullanma (Using Known Vulnerable Components),** Yazılım modülleri, çerçeveler (frameworks) ve kütüphaneler gibi bileşenler, genellikle tam yetkiyle çalışmaktadırlar. Eğer bu bileşenlerin açıklıkları istismar edilebilir ise, saldırganlar açıklıklar üzerinden sistem üzerinde, veri kaybına yol açmasına ya da sunucuyu ele geçirmesini kolaylaştırabilir.
- **Doğrulanmayan Yönlendirme ve İletme (Unvalidated Redirects and Forwards),** Web uygulamaları sık sık kullanıcıları diğer sayfa ve web sitelerine yönlendirmekte ve hedef sayfalara karar vermek için güvenilmeyen veri kullanmaktadırlar. Bu saldırı türünde, saldırganlar kullanıcıları sahte ya da kötücül sitelere yönlendirebilir ya da yetkisiz sayfalara erişim için iletebilirler.

Web Güvenlik Açıklıkları

- **Siteler Arası İstek Sahteciliği (Cross-Site Request Forgery (CSRF)),** Bu saldırılar sisteme kendini tanıtmış kullanıcının tarayıcısını web uygulaması üzerinde açıklık oluşturmak amacıyla, kullanıcının oturum çerezi ya da diğer otomatik olarak eklenen kimliklendirme bilgisini içeren, sahte HTTP istekleri göndermesine zorlamaktadır.
- Bu da saldırganlara, açıklık bulunan web uygulamasının gelen istekleri kullanıcıdan gelen meşru istek olarak görmesini sağlamaktadIR.

Sorgu Enjeksiyonu (SQL Injection)

- SQL Injection saldırıları, hedef web sitesinin kullandığı veri tabanında yetki olmadan sql sorguları çalıştırmaktır. İzinsiz sorgu çalıştırmalar sonucu veri tabanından hassas bilgiler çalınabilir. Veri tabanı sunucusuna sızılabilir.

Çapraz Betik Sorgulama (XSS)

- XSS yani Cross Site Scripting tehlikeli bir güvenlik açığıdır. Farklı programlama dilleri ile geliştirilen bir çok web uygulamasında bulunabilmektedir.
- Cross Site Scripting, saldırganın zararlı kodlarını web uygulamasına dahil etmesi ile başlar.
- Daha önce de belirttiğim gibi web uygulamalarına saldırılar kullanıcı girdileri ile yapılabilmektedir.
- XSS'de aynı şekildedir. Yazılımınızda ki bir html formu, arama modülü, XSS barındıran potansiyel noktalardır.

Çapraz Betik Sorgulama (XSS)

```
<?php
$gelen =  $_REQUEST['gelen'];
echo $gelen;
?>
```

- Yukarıda çok basit 2 satır php kodu bulunmaktadır. Bu kodlar bir web uygulamasının arama modülünden ufak bir kısımdır. İlk satırda kullanıcıdan $gelen değişkenine değer girilmesi beklenmekte, ikinci satırda ise bu girilen değer ekrana yazdırılmaktadır.
- Sizin arama satırına yaptığınız girdi, arama sonucunda dönen sayfada "aradığınız kelime : " şeklinde, bu mantıkla yazdırılmaktadır. Demek ki burada yaptığınız girişler hem veri tabanına sorgu olarak gitmekte, hem de ekrana yazdırılmaktadır. Doğal olarak SQL Injection ve XSS zafiyetlerinin aynı yerde bulunmasının en olası olduğu noktalar buralar olmaktadır.

Alınabilecek Önlemler

1. Web uygulama güvenliğinde açıklıkların uygulama kodu, sunucu ve iletişim altyapısından oluştuğu ve bu çalışmada özetlenen açıklıkların kontrol edilmesi ve açıklıkların kapatılması,
2. 2. Güvenlik çözümlerinin çeşitlilik gösterdiği ve bu güvenlik çözümlerinin seçilmesinde;

    a. Uygulamanın geliştirildiği yazılım dili,

    b. Uygulamanın üzerinde çalıştığı sunucu sayısı,

    c. Uygulamanın üzerinde çalıştığı sunucunun yazılım ve donanım özellikleri,

    d. Uygulamanın üzerinde çalıştığı web sunucu programı.

gibi kriterlere dikkat edilmesi,

Alınabilecek Önlemler

3. Açıklıkların büyük bir bölümünün uygulama kodu kusurlarından dolayı oluştuğu,

4. Web uygulama geliştiricileri yansıra web uygulamalarını kullanan kişilerin bilgi güvenliği farkındalık seviyesinin de büyük önem taşıdığı,

5. Web uygulama güvenliğini arttırmaya yönelik olarak bu çalışmada sunulan uygulama kod güvenliği yöntemlerinden mutlaka faydalanılması,

Alınabilecek Önlemler

6. Uygulama güvenliğinin sağlanabilmesi için saldırıların zamanında tespit edilmesinin çok önemli olduğu ve bilinen tespit yöntemlerinin mutlaka kullanılması,

7. Güncel açıklıkların takip edilmesi ve giderilmesi gerektiği görülmüştür.

Kaynaklar

- **F.Ü., Fen Bilimleri Enstitüsü, Yazılım Mühendisliği Anabilimdalı, Doktora Tezi, Muhammet Baykara, 2016.**
- **http://dergipark.gov.tr/download/issue-file/2820**
- https://dl.packetstormsecurity.net/papers/web/webappsec-101.pdf