RİSK YÖNETİMİ VE TEHDİT MODELLEME

Arş. Gör. Ecem İREN
Bilgisayar Müh. Bölümü
GEDİZ ÜNİVERSİTESİ

Yrd. Doç. Dr. Özgü CAN
Bilgisayar Müh. Bölümü
EGE ÜNİVERSİTESİ

IÇINDEKILER

1. RİSK NEDİR?

Risk, bir tehdit kaynağının potansiyel bir güvenlik açığı gerçekleştirme olasılığı ile bunun sonucunda kuruluş üzerinde ortaya çıkabilecek olumsuz etkinin bir fonksiyonu olarak nitelendirilebilir.

2. Neden risk yönetimi ve tehdit modelleme?

- Günümüzde bilgi sistemlerinin sağlıklı bir şekilde işleyip kullanıcılarına düzgün hizmet verebilmesi için sahip oldukları bilgi varlıklarını ve yürüttüğü görevi koruması şarttır.
- Bunu gerçekleştirmek için risk yönetimi ve tehdit modelleme yöntemlerine başvurulmaktadır.

3. RİSK YÖNETİMİ

- Risk yönetimi kuruluşun bilgi varlıklarına yönelik riskleri tanımlama, değerlendirme ve kontrol etme gibi faaliyetleri içeren bir süreçtir.
- Risk tanımlamada, kuruluşun karşılaştığı tehditlerin incelenip belgelendirilmesi gerçekleşmektedir.
- Risk tanımlama sonucunda güvenlik açıklarına yönelik önlemler alınmalıdır.

3. RİSK YÖNETİMİ

- Risk değerlendirmede, kuruluşa ait bilgi varlıklarının sahip olduğu risklerin dereceleri belirlenmekte,
- Risk kontrolünde ise, risk oluşumlarını kabul edilebilir bir düzeye indirgemek amacıyla mevcut riskleri azaltmak amaçlanmaktadır.

3.1. RİSK TANIMLAMA

- Organizasyonlar, sistemin ilişkili olduğu potansiyel tehdit ve riskleri belirleyebilmek için risk tanımlama faaliyetlerini uygularlar.
- Bu sürecin çıktısı, risk azaltma evresinde uygun kontrolleri belirlemede bize yardımcı olur.
- Risk tanımlama, sistemi tanıma, tehditleri belirleme ve önceliklendirme ve güvenlik açıklarını belirleme gibi 3 aşamadan oluşmaktadır.

3.1.1. SİSTEMİ TANIMLAMA

- Risk tanımlama sürecinde öncelikle söz konusu olan sistemi anlamak gerekir. Bu aşamada sistemin sınırları, sahip olduğu kaynaklar gibi bilgilere ihtiyaç duyulur.
- Bu kapsamda sistem hakkında bilgi edinmek için bazı tekniklere başvurulabilir.

3.1.1.1. SİSTEM HAKKINDA BİLGİ EDİNME

- Risk değerlendirme sürecini yönetecek olan kişinin sistem bileşenlerini iyi bilmesi gerekir. Sistem aşağıdaki şekilde sınıflandırılabilir:
- **Donanım:** Donanım, sistem cihazları olarak bilinir.
- **Yazılım:** Yazılım, uygulamalar, işletim sistemleri ve güvenlik bileşenleri olmak üzere 3 kategoride incelenebilir.

3.1.1.1. SİSTEM HAKKINDA BİLGİ EDİNME

- **Veriler:** Veriler bilginin işlenmesi, iletilmesi ve depolanmasından sorumludur.
- **Kişiler:** Kişiler, sistemi doğrudan kullanan ve doğrudan kullanmayan olarak ikiye ayrılır. Sistemi doğrudan kullananlar, güvenilir rolü olup daha fazla yetkiye sahip olan kişilerdir. Sistemi doğrudan kullanmayan kişiler ise organizasyonun güven ilişkisi içinde olduğu diğer organizasyon üyeleri vs. olarak düşünülebilir.
- Sistem görevi ve sistemin organizasyon açısından değeri

3.1.1.2. BİLGİ TOPLAMA TEKNİKLERİ

Aşağıdaki tekniklerden bazıları sistem ile ilgili bilginin toplanmasında kullanılabilir:

- Risk değerlendirme personeli sistemdeki yönetim ve kontroller konusunda bir anket hazırlayabilir.
- Yönetim ile görüşmeler yapılabilir.
- Sistem güvenliği ile ilgili belgeler güvenlik kontrolleriyle ilgili bilgiler sağlar.
- Bu aşama sonucunda elde edilen bilgiler tehditlerle ilişkilendirilerek tehdit modelleme bölümünde kullanılacaktır.

3.1.2. TEHDİTLERİ BELİRLEME VE ÖNCELİKLENDİRME

- Tehdit, bilgi varlıklarına zarar veren ve güvenlik ihlallerine neden olan her türlü eylem olarak kabul edilebilir.
- Doğal kaynaklı tehditler, sel, deprem, kasırga, çığ gibi felaketler olabilir.
- İnsan kaynaklı tehditler ise kasıtlı veya kasıtlı olmayan şeklinde incelenebilir:

  - Yanlış veri (Kasıtsız)

  - Ağ tabanlı saldırılar, kötü niyetli yazılım yükleme, yetkisiz şekilde gizli bilgilere erişim (Kasıtlı)

3.1.2.1. TEHDİT MODELLEME

- Tehdit modelleme, sistemde oluşabilecek tehditlerin belirlenip belgelendirilmesi ve önlemler alınarak tehditlerin azaltılması olarak gerçekleştirilen bir süreçtir.
- Bu süreç; güvenlik geliştirme takımlarının, uygulamaları potansiyel düşman gözünden inceleyerek sistemin tehdit profilini anlamalarına yardımcı olmaktadır.
- Sistemle ilişkili olabilecek risklerin saptanmasında önemli bir role sahiptir. Bu nedenle, tehdit modelleme risk yönetiminin bir girdisi olarak düşünülebilir.

3.1.2.1. TEHDİT MODELLEME

Tehdit modelleme uygulamayı ayrıştırma ve tehditleri belirleme gibi iki safhadan oluşmaktadır:

Uygulamayı ayrıştırma: ***U****ygulamanın* dış varlıklar ile nasıl etkileşime girdiği hakkında bilgi sahibi olmaktır. Aşağıdaki adımlarla bu aşama gerçekleştirilir:

- Potansiyel saldırganın, uygulama ile hangi noktalardan etkileştiğini tanımlamak gerekir. Saldırganın uygulamaya müdahale etmesi için mutlaka bir giriş noktası bulunması şarttır.

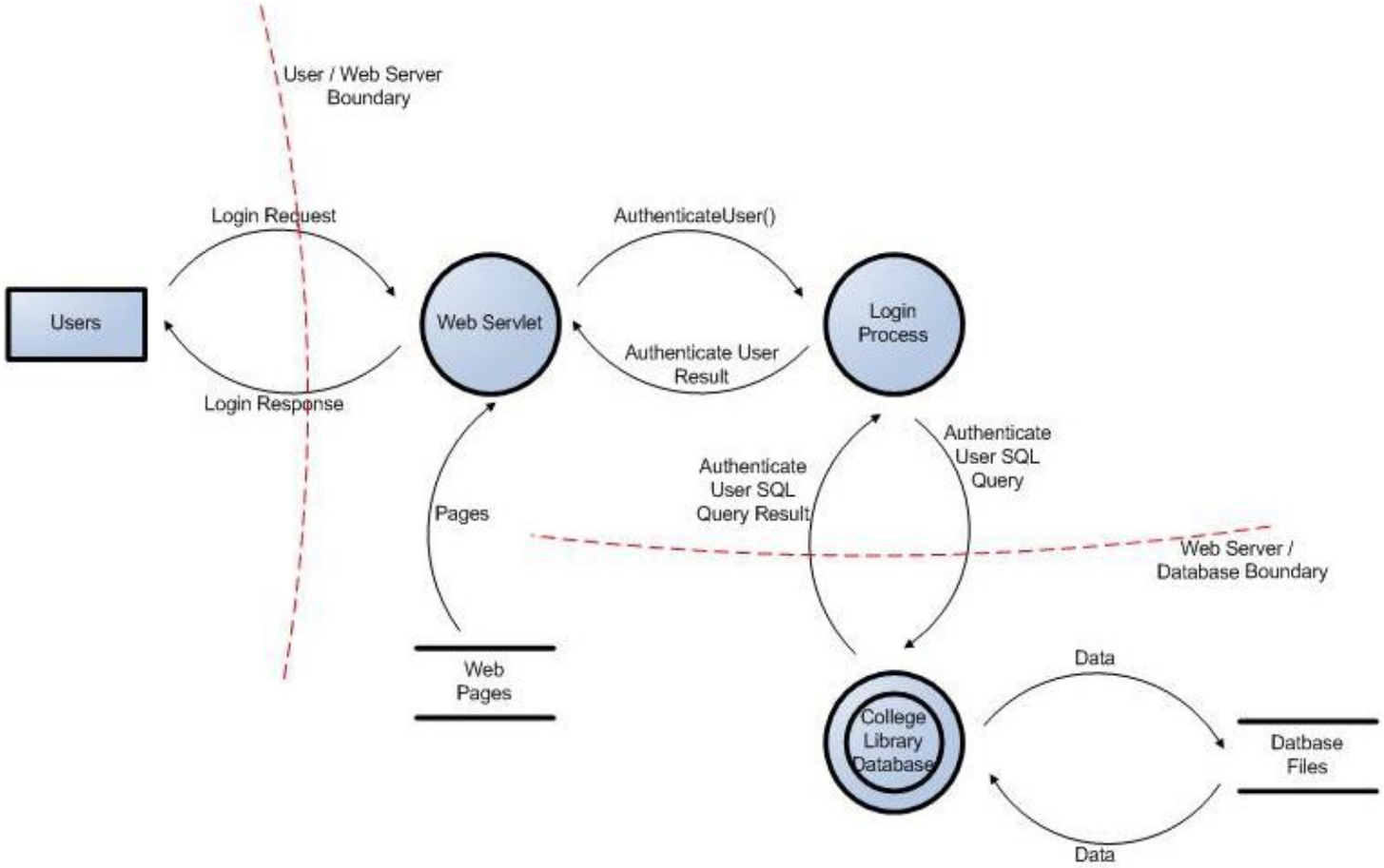
3.1.2.1. TEHDİT MODELLEME

- Uygulamayla etkileşen kullanıcıların erişim haklarını temsil eden güven düzeyleri tanımlanır. Bu tanımlama, giriş noktalarında ihtiyaç duyulan erişim haklarının ve yetkilerinin belirlenmesinde büyük rol oynar.
- Uygulamada kötü niyetli kişinin ilgilenebileceği bilgi varlıkları ayrıştırılır. Örnek; müşteri bilgileri.

3.1.2.1. TEHDİT MODELLEME

- Uygulamanın nasıl kullanıldığını anlamak amacıyla veri akış şemaları çizilir. Bir kullanıcının kütüphane sistemine giriş yapmasına ilişkin veri akış şeması Şekil 1'deki gibidir.

3.1.2.1. TEHDİT MODELLEME



ŞEKIL 1. KULLANICI GİRİŞ ŞEMASI

3.1.2.1. TEHDİT MODELLEME

Tehditleri Belirleme: Uygulama analiz edildikten sonra tehditlerin gruplandırılıp belirlenmesi gerekir. Bu noktada insan kaynaklı tehditlerin incelenmesi faydalı olacaktır. İnsan kaynaklı tehditler STRIDE olarak da gruplandırılabilir:

- **Bilgi Sızdırma (Spoofing):** Bir başkasıymış gibi davranmaktır. Burada amaç, yasadışı erişim dahilinde bir başkasına ait kullanıcı adı ve şifre gibi kimlik bilgilerinin kullanılmasıdır.

3.1.2.1. TEHDİT MODELLEME

- ***Sabotaj (Tampering):*** Yetkisiz bir şekilde bilgiyi değiştirmektir. Burada amaç, veritabanında bulunan bir veri ya da iki bilgisayar arasında akan veri gibi bilgilerin kötü niyetle değiştirilmesidir.

- ***Yadsıma (Repudation):*** Yasaklanmış işlemleri takip ve tespit etme yeteneğinden sistemi mahrum bırakarak sistemde yasadışı işlemler gerçekleştirmek amaçlanmıştır.

- ***Bilginin İfşa Olması (Information Disclosure):*** Bilginin yetkisi olmayan kişilere karşı açıkta bırakılmasıdır. Mesela, yetkisi olmayan insanların bir dosyayı okuması bu tehdite örnek olarak verilebilir.

3.1.2.1. TEHDİT MODELLEME

- ***Servis Reddi (Denial of Service):*** Sistemi çökerterek, yavaşlatarak veya sistemin depolama birimlerini doldurarak sistemi hizmet vermekten alıkoymak amacıyla yapılan saldırılardır. Bir web sunucusunun geçici olarak kullanılamaz hale getirilmesi ve kullanıcı erişimlerinin reddedilmesi bu tehdite örnek olarak gösterilebilir.

- ***Ayrıcalıkların Artması (Elevation of Privilege):*** Kaynaklara yetkisiz erişim sağlamak amacıyla erişim ayrıcalıklarının arttırılmasıdır.

3.1.2.1. TEHDİT MODELLEME

- Kuruluşlarla ilişkili olabilecek tehditlerin detaylıca değerlendirilmesi gerekmektedir. Bu değerlendirme ancak birtakım sorulara cevap vererek yapılabilir.

  -Hangi tehditler kuruluş için tehlike teşkil eder?

  -Hangi tehditler çok riskli olarak değerlendirilir?

  -En çok harcamayı gerektiren tehditler hangileridir?

- Bu aşama sonucunda kuruluşta var olan tehditlerin bir listesi ortaya çıkar.

3.1.3. GÜVENLİK AÇIKLARINI BELİRLEME

- Güvenlik açıkları, tehditlerin bilgi varlıklarına saldırma amaçlı kullandığı özel durumlardır.
- Her bir bilgi varlığıyla ilişkili olan tehditleri gözden geçirerek güvenlik açıklarını belirlemek gerekir.
- "Mevcut tehditlerin gerçekleşmesi hangi güvenlik açıklarının var olması durumunda mümkün olur" sorusu ile belirlenebilir.

3.1.3. GÜVENLİK AÇIKLARINI BELİRLEME

- Risk tanımlama süreci sonunda varlıklara ait güvenlik açıklarını ön planda tutan bir liste elimizde bulunmuş olur. Bu aşamadan sonra söz konusu güvenlik açıklarını önlemek için bazı kontrollere ihtiyaç duyulur.

3.1.3. GÜVENLİK AÇIKLARINI BELİRLEME

- Bu kontrollerden bazıları aşağıda listelenmiştir:

Doğrulama Kontrolleri Örnekleri

-Tüm iç ve dış bağlantıların uygun ve yeterli derecede kimlik doğrulamasından geçtiğinden,

-Sistemdeki tüm web sayfalarında kimlik doğrulaması yapıldığından,

Yetki Kontrolleri Örnekleri

-Yetki mekanizmalarının uygulandığından ve mekanizmaların doğru bir şekilde çalıştığından,

-Uygulamadaki kullanıcı tiplerinin ve haklarının açıkça tanımlandığından,

3.1.3. GÜVENLİK AÇIKLARINI BELİRLEME

Loglama ve Denetleme Kontrolleri

-Uygulamanın veri değiştirme (güncelleme, yaratma ya da silme) gibi kullanıcı eylemlerini denetlediğinden,

-Uygulama hatalarının kaydedildiğinden emin olunmalıdır.

3.2. RİSK DEĞERLENDİRME

- Risk değerlendirme süreci riskin gerçekleşme olasılığını belirleme, riskin doğurabileceği olumsuz etkinin derecesini analiz etme ve bu verileri kullanarak genel riski belirleme gibi 3 evreden oluşmaktadır.

3.2.1. OLASILIĞA KARAR VERME

- Riskin gerçekleşme olasılığı “yüksek”, “orta” ve “düşük” düzeyleri ile ifade edilmektedir.

  Yüksek Seviye Olasılık: Tehdit kaynağının güçlü olduğu ve güvenlik kontrollerinin yetersiz olduğu durumda riskin gerçekleşme olasılığı yüksek olarak nitelendirilir.

  Orta Seviye Olasılık: Tehdit kaynağının güçlü olduğu fakat güvenlik kontrollerinin başarılı ve etkili olduğu durumda riskin gerçekleşme olasılığı orta olarak adlandırılır.

  Düşük Seviye Olasılık: Tehdit kaynağının zayıf olduğu ve güvenlik kontrollerinin etkili olduğu durumda riskin gerçekleşme olasılığı düşük olarak nitelendirilir

3.2.2. ETKİ DERECESİNİ ANALİZ ETME

- Güvenlik açığından doğacak tehlikenin yarattığı olumsuz etkiyi analiz etmektir.
- Bu analizi yapmak için sistem hassasiyetinin incelenmesi gerekir.
- Bu analizlerde kuruluş varlıkları, nitel ya da nicel bir değerlendirmeye tabi tutulup bu değerlendirme sonucuna göre etki düzeyleri ile ilişkilendirilirler. Bu düzeylere göre öncelikleri belirlenir.

3.2.2. ETKİ DERECESİNİ ANALİZ ETME

- ***Gizlilik açısından düzeyler:*** Bilginin yetkisiz olarak açığa çıkarılmasının kuruluş üzerinde yarattığı etki sınırlı düzeyde ise bu etki ***düşük,*** ciddi düzeyde ise ***orta*** ve felaket düzeyinde ise ***yüksek*** olarak nitelendirilir.
- ***Bütünlük açısından düzeyler:*** Bilginin yetkisiz olarak değiştirilmesinin kuruluş üzerinde yarattığı etki sınırlı düzeyde ise bu etki ***düşük,*** ciddi düzeyde ise ***orta*** ve felaket düzeyinde ise ***yüksek*** olarak nitelendirilir.
- ***Kullanılabilirlik açısından düzeyler:*** Erişim bozukluklarının kuruluş üzerinde yarattığı etki sınırlı düzeyde ise bu etki ***düşük,*** ciddi düzeyde ise ***orta*** ve felaket düzeyinde ise ***yüksek*** olarak nitelendirilir

3.2.3. RİSK MATRİSİ

- Risk düzeyi hesaplanırken, tehdidin gerçekleşme olasılığına atanan değer ile tehdit etkisine atanan değeri çarpılır.
- Risk seviyeleri düşük, orta ve yüksek olmak üzere üç seviyeden oluşmaktadır.
- Tabloya göre risk seviyesi 50 ile 100 arasında ise yüksek, 10 ile 50 arasında ise orta, 1 ile 10 arasında ise düşük olarak değerlendirilir.

3.2.3. RİSK MATRİSİ

Tehdit Olasılığı	Etki Dereceleri		
	Düşük (10)	Orta (50)	Yüksek (100)
Yüksek (1,0)	Düşük 10x1.0=10	Orta 50x1.0=10	Yüksek 100x1.0=100
Orta (0,5)	Düşük 10x0.5=5	Orta 50x0.5=25	Yüksek 100x0.5=100
Düşük (0,1)	Düşük 10x0.1=1	Orta 50x0.1=5	Yüksek 100x0.1=10

TABLO 2. RİSK MATRİSİ

3.2.3. RİSK MATRİSİ

- ***Düşük Düzey:*** Risk düşük düzeyde gözlemlenmişse, sistem yöneticisi düzeltici eylemlerin gerekip gerekmediğini analiz edebilir veya riski kabul edebilir.
- ***Orta Düzey:*** Risk orta düzeyde gözlemlenmişse, düzeltici eylemler gereklidir ve bu eylemlerle bütünleşecek bir planın en kısa zamanda geliştirilmesi zorunludur.
- ***Yüksek Düzey:*** Risk yüksek düzeyde gözlemlenmişse, düzeltici eylemlere büyük oranda ihtiyaç vardır. Mevcut sistem bu şekilde çalışmaya devam edebilir fakat en kısa zamanda önlemleri uygulamaya koymak gerekir

3.3. RİSK AZALTMA

- Bu bölümde risk azaltma teknikleri incelenecektir.
- Risk azaltma süreci aşağıda sıralanmış yöntemler ile yapılır:

-***Riski Kabul Etme:*** Riski kabul edip sistemin çalışmasına devam etmesi veya isteğe göre mevcut risklere kontroller uygulanmasıdır.

-***Riskten Kaçınma:*** Güvenliğin sağlanması için gerekli olan gereksinimleri veya sistem özelliklerini değiştirerek risk faktörünü ortadan kaldırmaktır

3.3. RİSK AZALTMA

-***Riski Sınırlandırma****:* Bazı kontroller uygulayarak risk nedeniyle oluşabilecek etkiyi azaltmaktır.

-***Risk Planlama:*** Riskle başa çıkabilmek için risk azaltma planının hazırlanmasıdır.

-***Risk Transferi:*** Risk nedeniyle oluşabilecek kaybın telafisini başka bir kuruluşa devretmektir.

3.3. RİSK AZALTMA

- Riski azaltmada kontrollerin uygulanması için bazı adımların izlenmesi gerekmektedir:

-**Eylemlerin Önceliklendirilmesi**

Önlemler önceliklendirilir. Çok yüksek risk seviyesine sahip tehditlere yüksek öncelik verilmelidir.

-**Kontrol Seçeneklerini Değerlendirme**

Kontrollerin fizibiliteleri (yapılabilirlik, uyumluluk vs.) analiz edilmektedir.

3.3. RİSK AZALTMA

-<u>Maliyet-Fayda Analizini Gerçekleştirmek</u>

Risk yönetiminin sağladığı faydaların, süreç boyunca ortaya çıkan toplam maliyetten daha büyük olup olmadığını belirlenir. Bu analiz aşağıdaki formüle göre hesaplanmaktadır:

Analiz Sonucu = (Azaltılmadan önceki risk-Azaltıldıktan sonraki risk) / Toplam Maliyet

3.3. RİSK AZALTMA

- **Önlemin Seçilmesi**

  En etkili önlemler belirlenir. Önlemlerin sistem için yeterince faydalı olduğundan emin olunmalıdır.
- **Sorumlulukların Dağıtılması**

  Belirlenen kontrollerin uygulanmasında yardımcı olacak yetkin kişilerin tanımlanması ve bu kişilere sorumluluklar dağıtılmasıdır.

3.3. RİSK AZALTMA

- **Güvenlik Planının Geliştirilmesi**

Güvenlik planı, önceki adımlarda edinilen bilgileri (riskler, önlemler, sorumlu kişiler) ve ayrı olarak planın başlama tarihi, bitiş tarihi ve kaynaklar gibi bilgileri içeren bir dokümandır.

- **Kontrollerin Uygulanması**

Kontroller uygulanmaya başlar ve şartlara bağlı olarak riski azaltabilir fakat riski tam olarak ortadan kaldırmaz.

KAYNAKLAR

1) G. Stoneburner, A. Goguen, A. Feringa, "Risk Management Guide for Information Technology Systems", National Institute of Standards and Technology (2002).

2) Whitman M. E., Mattord H. J., 2011, "Principles of Information Security", 4th Edition, Course Technology.

3) Application Threat Modelling, https://www.owasp.org/index.php/Application_Threat_Modeling#Threat_Categorization (Son Erişim Aralık 2015).

4) Shostack A., 2014, "Threat Modeling: Designing for Security", John Wiley & Sons, ISBN

5) Pfleeger C. P.,Pfleeger S. L., Margulies J., 2015, "Security in Computing", 5th Edition, Prentice Hall, ISBN 13 978-0-13-408504-3

KAYNAKLAR

6) Nayak U.,Rao U. H., 2014, "The Info Sec Handbook An Introduction to Information Security", ISBN 13 978-1-4302-6382-1

7) Risk Management, http://agile.csc.ncsu.edu/SEMaterials/RiskManagement.pdf (Son Erişim Aralık 2015).

8) Lee R. B., 2013, "Security Basics for Computer Architects", Morgan & Claypool, University of Wisconsin, Madison.

9) E. A. Oladimeji, S. Supakkul, L. Chung, "Security Threat Modelling and Analysis: A Goal-oriented Approach", in Proceedings of the 10th International Conference on Software Engineering and Applications, Dallas, Texas, USA, 2006.

TEŞEKKÜRLER