

## Acil Durum Müdahalesi

### İbrahim Çalışır

Orta Doğu Teknik Üniversitesi  
icalisir@metu.edu.tr

Son zamanlarda artan güvenlik bilinci ile bilişim sistemlerinde ani oluşacak sorunlara karşısında kısa zamanda çözüm üretmek de güvenlik konusundaki çalışmalar arasında kendisine yer bulmaya başladı. Acil durum müdahalesi olarak isimlendirilen konu içinde ön plana çıkan önemli alt başlıklar risk analizi, öncül tedbirlerin belirlenmesi ve sorun anında çözüm aşamasıdır. Bu yazıda öncelikle birkaç risk analizi yöntemi tartışılacak, sonrasında da bilişim sistemlerinde oluşacak sorun anında çözüm aşamasında nelere ihtiyaç duyulacağı ortaya konacaktır. Öncül tedbirler şu anda konumuz dışında yer almaktadır.

#### Risk Analizi:

Soğuk savaş döneminde olası nükleer saldırıların hangi noktaları vuracağını öngörülmesi için çalışma sırasında ABD'de önem kazanan yöntem, dünyanın çevresine uydu yerleştirmeden ekonomiye kadar pek çok alanda kendine çalışma imkanı buldu. Son zamanlarda da bilişim sistemlerine adapte edilmeye çalışılmaktadır.

Risk analizi, varlıkların değeri ve tehditin gerçekleşme olasılığı kavramları üzerine kurulmaktadır. Bu kavramlar hakkında detaylı bilgiler kitaplarda ya da Internet ortamında bulunmaktadır. Ancak dikkat etmemiz gereken önemli noktalardan birisi bilişim alanında varlıkların belirlenmesi ve bu varlıklara verilen değer tamamen kuruma özel bir çalışma gerektirir. Bunun yanı sıra, tehditler ve gerçekleşme olasılıkları da yine kuruma özel bir çalışma gerektirmektedir.

Bu kuruma özel noktalara karşın bazı genel geçer kurallar da bulunmaktadır. Bilişim alanında risk analizi tehditin etkisini üç ana başlığa ayırmıştır.

- gizlilik
- bütünlük
- kullanılabilirlik

**Gizlilik**, kurum içi özel bilgiler ve kurumun servis verdiği kişilerin özel hayatı konularını kapsamaktadır. Örnek: kişisel epostaların herkes tarafından görülmemesi.

**Bütünlük**, kurumun sahip olduğu varlıklar üzerinde izinsiz değişiklik yapılmamasını kapsamaktadır. Örnek: Veritabanlarında yetkisiz değişiklik yapılmaması

**Kullanılabilirlik**, kurumun sahip olduğu varlıklara izin verilen kişilerin erişimini kapsamaktadır. Örnek: Kurum anasayfasının sürekli erişilebilir olması

Bilişim alanında risk analizi ile ilgili verilen üç örnek kavramlara açıklık getirmek için yardımcı olacaktır.

#### Örnek 1:

Bu örnekte bir tehdidin varlığa etkisi iki şekilde varsayılır:

- sistem üzerinde tam yetkili veya kısıtlı bir kullanıcının hakkını elde etme ile sonlanabilecek tehditlerin etkileridir.
- varlığın hizmetinin kısmen veya tamamen devre dışı bırakılmasıdır.

	Düşük	Orta	Yüksek	Çok Yüksek
Düşük	D	D,O	O	O,Y
Orta	D,O	O	O,Y	Y
Yüksek	O	O,Y	Y	Ç.Y
Çok Yüksek	O,Y	Y	Ç.Y	Ç.Y

Bu risk analizi yöntemi sadece merkezi sunucularda kullanıcı kodu özeli ile ilgilenmektedir, bilişim sisteminin tümünü kapsamamaktadır. Buna ek olarak tehditin etkisini gizlilik, bütünlük ya da kullanılabilirlik kavramları açısından incelemektedir.

### Örnek 2:

Bu örnekte risk tehditin gerçekleşme olasılığı ile tehditin etkisinin çarpımı olarak ortaya konmaktadır. Tehditin gerçekleşme olasılığı ve tehditin etkisi 1 ile 5 arasında değerler atanarak belirlenmektedir.

Tehditin gerçekleşme ihtimali / Tehditin Etkisi	Çok Düşük {1}	Düşük {2}	Orta {3}	Yüksek {4}	Çok Yüksek {5}
Çok Düşük {1}	Düşük [1]	Düşük [2]	Düşük [3]	Orta (4)	Orta (5)
Düşük {2}	Düşük [2]	Orta (4)	Orta (6)	Yüksek [8]	Yüksek [10]
Orta {3}	Düşük [3]	Orta (6)	Yüksek [9]	Yüksek [12]	Kritik [15]
Yüksek {4}	Orta (4)	Yüksek [8]	Yüksek [12]	Kritik [16]	Çok Yüksek [20]
Çok Yüksek {5}	Orta (5)	Yüksek [10]	Kritik [15]	Çok Yüksek [20]	Çok Yüksek [25]

$$\text{Risk} = \text{Tehditin Gerçekleşme İhtimali} * \text{Tehditin Etkisi}$$

Bu analiz bilişim sistemleri için daha kapsayıcı olsa da hala tehditin etkisinin gizlilik, bütünlük ya da kullanılabilirlik kavramları açısından incelemektedir.

### Örnek 3:

Bu örnekte gizlilik, bütünlük ve kullanılabilirlik için risk ayrı ayrı hesaplanmaktadır. Hesaplama için her varlığın gizlilik, bütünlük ve kullanılabilirlik değerleri (VDg, VDb, VDK) ve olası tehditin gizliliğe, bütünlüğe ve kullanılabilirliğe etkisi (TEg, TEb, TEK) ayrı ayrı düşünülür. Her bir kavram için risk hesaplanırken tehditin olma olasılığı (To) da işin içine girmektedir.

Rg, Rb, Rk	1	2	3	4
1	1	2	3	4
2	2	4	6	8
3	3	6	9	12
4	4	8	12	16

$$R_g = V_{Dg} * T_{Eg} * T_o$$

$$R_b = V_{Db} * T_{Eb} * T_o$$

$$R_k = V_{Dk} * T_{Ek} * T_o$$

Risk seviyesi, her bir kavram için belirlenen risk değerlerinin kurum tarafından belirlenecek bir formüle yerleştirilmesi ile bulunur (örnek formüller: toplama, aritmetik orta, geometrik orta, vb).

### Risk Analizi Sonuçları Yorumlama:

Verilen her üç örnekte de sağ alt köşede bulunan risk değerinin – çok yüksek değerli bir varlığa tehditin etkisinin çok olması – ortadan kaldırılması önemlidir. Bu alanların analiz tablolarında olmaması gerekmektedir.

Diğer yandan sol üst köşedeki sonuçlar için alınacak önemlerin en az emek harcayan önlemler olduğunu da unutmadan öncelikle orta kısımdaki riskleri azaltacak önlemler alınması düşünülmelidir.

Bunu yanı sıra günümüzdeki saldırıların “düşük etki – sık görülme” yerine “yüksek etki – az görülme” alanına kaymakta olduğunu unutulmamalı ve sağ alt alandaki risklere özellikle dikkat edilmelidir

### Bileşik Yapı Yaklaşımı

Risk analizi varlıkları tek tek incelemesi nedeniyle bilişim sistemleri gibi karmaşık yapılarda tek başına kullanımı yeterli gözükmemektedir. Bir tehdit gerçekleştiği zaman sadece etkilediği varlığa değil, onun ilişkide olduğu varlıklara da etki etmektedir. Bu yan etkiler risk analizinde dikkate alınmamaktadır. Bu nedenle sistemi bileşik bir yapı olarak görmek ve uygun teo-

rilerden acil durum yaklaşımını incelemekte fayda vardır.

Hanseth bilişim sistemlerinin bu karmaşık yapısını ortaya koymak için sundukları teori sistemdeki bileşen sayısı ve bileşenler arasındaki bağlantı sayısını dikkate almaktadır. McLean bu yaklaşımı biraz daha geliştirerek farklı türde bileşen sayısını, bileşenler arası bağlantı türü sayısını ve bunun değişimini karmaşıklık tanımlamak için kullanmaktadır. Dikkat edilmesi gerek önemli noktalardan birisi farklı türde bileşen sayısı, veritabanı birimi, güvenlik birimi türleri değil, bilişimi sisteminin çalışmakta olduğu platform, uygulama gibi teknik yapılar ile organizasyon rutinleri, alışkanlıkları ve içyapısı bileşenlerinden hesaplanmaktadır.

McLean'in yaklaşımındaki bileşenler arasındaki bağlantının değişim hızına da önem verildiği dikkat çekmektedir. Bileşenler ve birbirleri ile ilişkileri hakkında bilgimiz her zaman eksiktir. Bunun nedeni de bilgimizin artma hızı, bileşenlerin değişim hızından her zaman daha az olmasıdır. Yeni bileşenin sisteme yerleştirilmesi ve diğer bileşenlerle ilişkilendirilmesi sırasında bileşenin yeteneklerinden sadece bir kısmını kullanılmakta olduğunu unutmamak gerekir.

Bir bileşenin özelliklerinin öğrenilmesi ve bilgi sahibi olmak konusu kurumlar tarafından önemsenmektedir. Ancak yaparak öğrenmek hiçbir zaman sözel aktarım ile öğrenmenin yerini tutmamaktadır. Öğrenmeye ilgini azalmasına neden olan ikinci yöntem çalışanların bilgi seviyelerinin yeterince hızlı artmasını da engellemektedir. Sonuçta sistem hakkında yeterli bilgiye sahip olmayan çalışanlar (yöneticiler) acil durumda müdahale etmek durumunda kalmaktadır.

## **Acil Durum Müdahalesi:**

Genelde panik ve ne yapacağını bilmeyen çalışanlarla karşılaşıldığında yöneticilerin aklına gelen acil durum müdahalesi konusu sistemler çalışırken dikkate edilmesi gerekmektedir. Bu konuda yukarıda da belirtilen bileşenlerin özeline inerek risk analizi ve biri sistem olarak bileşik yapı yaklaşımından çıkacak sonuçların değerlendirilmesi önemlidir ancak unutulmamalıdır ki, sistemin kurulmasını amacı kullanımdır. Bu kullanımı denetleyen ikincil sistemler kurulması ve bu sistemlerin doğru denetim yapıp yapmadıklarını denetleyen üçüncül sistemler kurulması söz konusu olmaktadır. İkincil sistemlerin yapması beklenenler üç aşamada sıralanabilir

- Sistem kontrolü
- Sorunun belirlenmesi
- Sorunun ortadan kaldırılması

Sistem kontrolü ve sorun belirlenmesi sırasında beklenen ve beklenmeyen sorunlarla karşılaşılabilir. Tabii ki risk analizi sonucunda olası tehditlere karşı, öncül önlemler almak elbetteki en iyi çözümdür, ancak bu tür önlemleri almanın iki sorunu olabilir. Bunlardan birisi önlem almanın maliyetin varlığın değerinden yüksek olması, diğeri ise sistemi çalışmaz hale getirecek çözümlerdir. Bu nedenle bazı durumlarda öncül tedbirler yerine tehdit gerçekleştiği zaman sorunu en kısa zamanda giderecek çözümlere yönelmek de gerekebilir. Beklenen risklere karşı izlenebilecek bu yolda iyi hazırlanmış güncel belgeleme sistemi ve iş içi eğitimlerin gerekliliği tartışılmazdır. Beklenmeyen riskler konusunda önerilebilecek tek çözüm, bilgili ve yaratıcı çalışanların istihdamıdır.