

Risk Analizi

Hazırlayan:

Gürsoy DURMUŞ

Gursoy.Durmus@tikle.com

gdurmus@yahoo.com

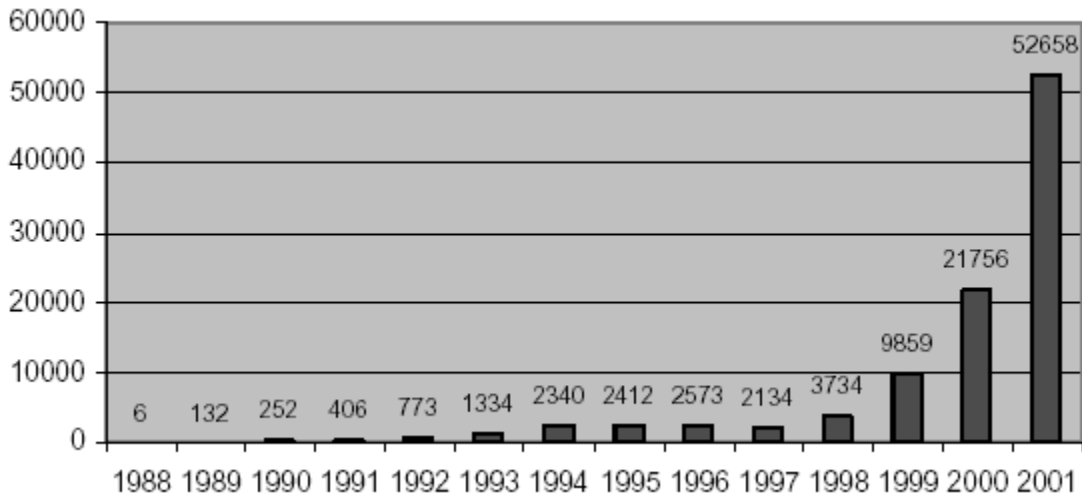
1.Giriş

Her şey insanoğlunun birbiri ile haberleşmesi ile başladı ve herşey bu amaçla geliştirildi dersek yanılmış olmayız. Isıkla, dumanla başlayan haberleşme teknolojinin ilerlemesi sayesinde bugünkü konumuna gelmiştir. Her ürlü haberleşmelerimizde kullandığımız sistemler ne kadar güvenli?

Haberleşme ile başlayan ve daha sonra kullanım kolaylığı ve rahatlığı sayesinde hayatimizin en önemli unsurlarından biri haline gelen veri paylaşımındaki güvenlik unsurlarını, icinde bulunduğumuz riskleri gözden geçireceğiz.

Bilişim sistemlerine olan bireysel ve toplumsal bağımlılığımız arttıkça bu sistemlerde meydana gelebilecek arıza ve saldırılara karşı duyarlılığımız da artmaktadır. Bilgisayar sistemlerine ve ağlarına yönelik saldırılar ciddi miktarda para, zaman, prestij ve değerli bilgi kaybına neden olabilir. Bu saldırıların hastane bilişim sistemleri gibi doğrudan yaşamı etkileyen sistemlere yönelmesi durumunda kaybedilen insan hayatı da olabilir.

Bilgisayar Güvenliği Enstitüsü (Computer Security Institute - CSI) ve Federal Araştırma Bürosu (FBI) tarafından geleneksel olarak gerçekleştirilen "Bilgisayar Suçları ve Güvenlik Araştırması"nın 2001 yılı raporuna göre bilişim suçları 1997- 2001 yılları arasında her yıl neredeyse ikiye katlanacak biçimde artmıştır [CSI-FBI, 2001]. Aynı araştırma, gizli bilgilerin çalınması ve finansal kayıtlarda değişikliklerin en çok maddi zarara neden olan iki saldırı biçimi olduğunu göstermektedir.



Cert/CC Yıllara Göre Rapor Edilen Olay Sayısı

Güvenlik ihlallerindeki bu artışın nedeni, iyi bilgilerin olduğu kadar kötü bilgilerinde hızlı bir şekilde yayılması, güvenlik açıklıklarını tespit edip seven kullanıcılar, maddi yada manevi hasar vermek isteyen kötü amaçlı kullanıcılar vs de ki artışı gösterebiliriz.

2.Tanımlar

Risk analizinin tanımını yapmadan önce, ilerde sık sık bahsedeceğimiz konu ile ilgili bazı kavramların tanımlarına ve açıklamalarına öncelik verelim.

2.1.Genel Kavramlar

2.1.1 Risk

Belirli bir tehdidin, sistemin belirli bir zayıflığından faydalanarak sisteme zarar verme ihtimalidir.

2.1.2 Arta Kalan Risk

Güvenlik önlemleri uygulandıktan sonra kalan riskler.

2.1.3 Güvenlik

Art niyetli eylemlerden ve etkilerden korunmak üzere alınan ve sürdürülen koruyucu önlemlerin sonucunda oluşan durum.

2.1.4 Zayıflık

Bir sistemde yetkilendirilmemiş eylemlere izin veren zaafiyet.

2.1.5 Saldırı

- Yetkisiz biçimde bir takım sonuçlara ulaşmak amacıyla bir saldırgan tarafından gerçekleştirilen bir dizi adım.
- Bir kaynağın bütünlüğünü, gizliliğini yada bulunurluluğunu bozmayı hedefleyen her türlü eylem.

2.1.5 Saldırgan

Bir amaca ulaşabilmek üzere bir yada daha fazla saldırıyı deneyen kişi.

2.1.6 Kıymet

Korunması gereken herşey olarak tanımlayabiliriz. Temel olarak 4 gruba ayırabiliriz:

- Veri
- Kaynak
- Zaman
- Saygınlık

2.1.7 Açıklık

Bir kıymeti tehditlere karşı korumasız hale getiren unsurlardır.

2.1.8 Tehdit

Bir kıymetteki açıklıkları kullanarak kıymete kısmen yada tamamen zarar veren etkenlerdir. Tehditler insan ve doğal kaynaklıdır.

2.1.9 Risk Analizi

Güvenlik risklerinin, bu risklerin ölçüklerinin ve önlem alınması gereken alanların belirlenmesi süreci.

2.1.10 Risk Yönetimi

Sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreç. Risk analizi, fayda-maliyet analizi, seçim, gerçekleştirim, sınama, önlemlerin güvenlik değerlendirmesi komple güvenlik gözden geçirmesini içerir.

2.2 Risk Analizi

Güvenlik risklerinin, bu risklerin ölçeklerinin ve önlem alınması gereken alanların belirlenmesi sürecidir.

Risk analizinde, riskler belirlenirken mevcut kıymetler tek tek göz önüne alınır ve her bir kıymetin içinde bulunduğu tehditler belirlenir. Ayrıca, halihazırda mevcut olan karşı önlemler incelenir. Daha sonraki aşamada, ortaya konulmuş olan kıymet, açıklık, tehdit ve karşı önlemlerinin değerlendirilmesi işlemi yapılır. Değerlendirilmiş kıymet, açıklık, tehdit ve karşı önlem değerleri girdi olarak alınıp, matematiksel ve mantıksal metodlar kullanılarak risk değeri bulunur. Son olarak risk-kıymet eşleştirmesi yapılır.

Risk analizi karşı önlemlerin nasıl ve ne şekilde alınacağı üstünde durmaz. Bu işi, risk risk yönetimi prosesi yapmaktadır.

2.3 Risk Yönetimi

Sistem kaynaklarını etkileyebilecek belirsiz olayların belirlenmesi, denetlenmesi, yok edilmesi ya da en aza indirgenmesini kapsayan süreçtir. Risk analizi, fayda-maliyet analizi, seçim, gerçekleştirim, sınaama, önlemlerin güvenlik değerlendirmesi komple güvenlik gözden geçirmesini içerir.

Risk analizi ve yönetiminin amacı, kurum içinde olabilecek tehlikelere uygun cevap verebilecek, kasıtlı ya da kasıtsız tehditlerin etkisini ve olma ihtimalini azaltacak hazırlıkları, prosedürleri ve kontrolleri teşhis etmektir.

Risk analizi ve yönetiminin yararların başta gelenleri şu şekilde sıralanabilir.

- Kurumun yazılı prosedür ve politikalarının olmasını ya da olgunlaşmasını sağlar.
- Kurum çalışanlarının ve bilgi işlem personelinin bilgi güvenliği konusunda bilgi sahibi olmasını sağlar.
- Bir kurum yönetiminin de bilgi teknolojileri güvenliği konusunda bilgi sahibi olmasını ve bu konularda karar vermesini sağlar.
- Risk analizi prosesinin ilk kısmında yapılan kıymet analizi sonuçlarının kurumun yazılım ve donanım envanterlerinin yenilenmesinde yardımcı olur.

Risk analizi ve yönetiminin yapılmadığı bir bilgi sisteminde aşağıdaki gibi durumlar olabilir.

- Bu bilgi sisteminde hiç güvenlik olmayabilir ya da çok az güvenlik olabilir
- Kullanılabilirliği oldukça azaltan çok fazla güvenlik olabilir
- Yanlış güvenlik önlemleri alınmış olabilir
- İnsanlarda yanlış güvenlik bilinci olabilir.

Bütün bunları maddi olarak ve zaman olarak kayıplara yol açan durumlardır.

Kurum içi risk yönetimi sırasında, riskler karşısında alınacak kararlar şunlar olabilir:

- Kabul: Korunacak kıymetin varlığı önemsiz, buna karşı alınacak tedbirin maliyeti yüksek ise bu durumda risk kabul edilebilir.
- Devretme: Riski göz önüne alıp riskin başka birine devredilmesidir. Bu sayede riski önlemek için gerekli maliyet düşürülür ve sorumluluk başkasına verilir.
- Kaçınma: Güvenlik riski mevcut olan ancak saldırı riski olmayan kıymetler için risk maliyetine girmek yerine, riski göz ardı etmektir.

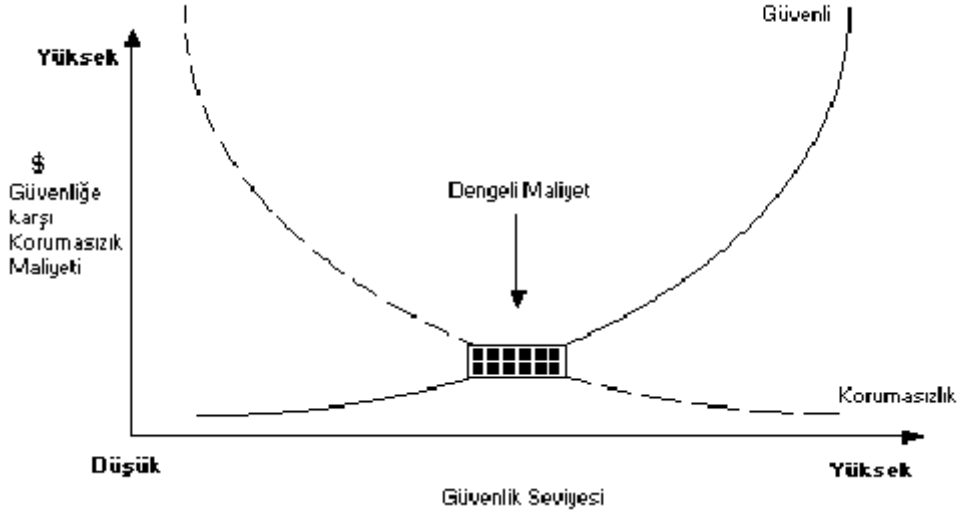
İki temel risk analizi yöntemi mevcuttur. Bunlar, nicel ve nitel yöntemlerdir.

- Nicel risk analizi, riski hesaplarken sayısal yöntemlere başvurur. Nicel risk analizinde, kıymet, açıklık, tehditin olma ihtimali, tehditin etkisi gibi değerlere sayısal değerler verilir ve bu değerler matematiksel ve mantıksal metotlar ile proses edilip risk değeri bulunur.
- Nitel risk analizi riski hesaplarken ve ifade ederken numerik değerler yerine *yüksek*, *çok yüksek* gibi tanımlayıcı değerler kullanır.

Risk analizi ve yönetimi ile birlikte gelen bir takım problemler ve ideal olmayan durumlar vardır. Bunlar,

- Risk analizinin kendisinin maliyetinin yüksek olmasıdır. Risk analizini kurumun kendisi bile yapsa zaman ve para kaybına yol açabilmektedir.
- Risk analizi sonuçlanana kadar geçen süre diğer bir problemdir. Güvenlik önlemlerinin biran evvel uygulanması gerekirken, risk analizi sonucu beklemek zorundadır. Bunun zararlı etkileri olabilmektedir. Bu nedenle bir çok yerde, risk analizi yapılmadan güvenlik önlemleri alınmaktadır.
- Risk analizi sonuçlarının nesnel olması beklenirken daha çok öznel olabilmektedir. Özellikle nitel risk analizinde bu problem daha çok görülebilir. Çünkü, nitel risk analizinde risk, sayısal değerlerden çok tanımlar ile ifade edilmektedir.
- Risk analizi ve yönetimi prosesi, önceden belirlenmiş kesin adımları olan prosesler değildir. Nitel ve nicel risk analizi yöntemlerinin çatısı altında, bir çok risk analizi metodolojisi mevcuttur. Bu methodlar, riski yorumlama aşamasında birbirinden ayrılırlar.
- Tüm kurumlara uyan bir risk analizi metodolojisi mevcut değildir. Çünkü, her organizasyonun kendine özel bir kıymet listesi, bu kıymetlere göre farklı farklı tehditleri vardır. Bütün bunları dışında, kurumdan kuruma güvenlik anlayışı ve güvenlik gereksinimleri de değişim göstermektedir. Risk analizi ve yönetimi yapılacak olan bir kurumda, öncelikle ne tip bir risk analizi ve yönetimi metodunun uygulanması gerektiği belirlenmelidir.
- Günümüzde, kıymetlerin, buna bağlı olarak açıklıkların ve tehditlerin artması ile beraber, risk analizi ve yönetiminin sahasına giren, kıymet tanımla, açıklık belirleme, tehdit tanımla ve karşı önlem belirleme safhaları çok geniş nesnelere kapsadığından dolayı, bir çok risk analizi ve yönetimi metodu her nesneyi örtemeyebilmekte ve bazı nesnelere gözardı edilebilmektedirler.

Aşağıdaki grafikete risk yönetimi maliyeti ve güvenlik arasındaki ilişki ele alınmıştır. Bizim için risk yönetimi aşamasında önemli olan ne kadar güvenlik istediğimizdir, buna karar verirken kıymetlerimizin değerini göz önüne almalıyız.



3. Güvenlik Uygulama Döngüsü

Uluslar Arası Bilgisayar Acil Durum Müdahale Ekipleri Koordinasyon Merkezi (Computer Emergency Response Teams Coordination Center - CERT/CC), ağları ve sistemleri korumak için gerçekleştirilmesi gereken faaliyetleri beş ana başlık altında toplamıştır. CERT/CC, bu gruplandırmayı yaparken geçmiş yıllarda rapor edilen saldırıları ve zayıflıkları temel almıştır ve bu gruplandırma çerçevesinde tanımlanan faaliyetlerin güvenlik ihlallerinin yüzde seksenini engelleyeceğini öngörmektedir.

CERT/CC tarafından öngörülen bu beş adımlık güvenlik uygulaması firma, ürün ya da teknolojiye bağımsız olarak düzenlenmiştir. Tüm adımlarda, firmanın güvenlik ihtiyaçları için zemin oluşturacak kurumsal hedeflerinin ve kurumsal güvenlik programı ve politikasının önceden oluşturulmuş olduğu varsayılır. CERT/CC tarafından öngörülen güvenlik uygulamalarının beş adımlık döngüsü aşağıdaki adımlardan oluşur; ilk adım hariç her adıma izleyen adımlardan geri dönüşler sağlanır:

- **Koruma ve Sağlama:** Bu ilk adımda, sistemlerin ve ağın güvenliğini arttırmaya yönelik faaliyetler gerçekleştirilir. Yaygın biçimde bilinen saldırılara karşı önlemler alınır ve bu önlemler denetlenerek işler hale getirilir. Diğer tüm adımlar bu adımın sonucunda ulaşılan düzeye göre geliştirileceğinden bu adımın etkin bir biçimde planlanması ve gerçekleştirilmesi son derece önemlidir.
- **Hazırlık:** Hazırlık aşamasında, bilinmeyen saldırıların tespit edilebilmesi ve bu saldırılara müdahale edilebilmesi için gerekli hazırlıklar gerçekleştirilir. Bilindik saldırılar için alınan önlemler ile bu adımda gerçekleştirilen faaliyetler karıştırılmamalıdır. Bilindik saldırılara karşı alınan önlemler koruma ve sağlama adımının konusudur. Bu adımda önemli olan bilinmeyeni tespit edebilmek ve gerçekleştiğinde müdahale edebilmek için gerekli zeminin oluşturmaktır.
- **Tespit:** Bu adımda, ağ ve sistemler üzerinde yetkisiz ya da şüpheli olayları tespit etmek için gerekli işlemler gerçekleştirilir. Ağ trafiğinin, kullanıcı davranışlarının, dosya ve dizinlerin ve yazılımların izlenmesi bu bağlamda ele alınmalıdır. Bir

yetkisiz erişim ya da şüpheli olay tespit edildiğinde ilk inceleme de bu adım kapsamında gerçekleştirilir.

- **Müdahale:** Şüpheli bir olayın tespit edilmesi durumunda olayın gerçekten bir saldırı olup olmadığının belirlenmesi, saldırı ise en kısa sürede saldırının etkilerinin yok edilerek sistemlerin tekrar sıkıntısız biçimde çalışır hale getirilmesi ve uygun ise saldırganlar aleyhine hukuki girişimlerin başlatılması bu adım kapsamında ele alınır.
- **İyileştirme:** Saldırlara müdahale edilmesinden sonra benzer türde saldırıların muhtemel etkisini azaltmak ve mümkün ise bu tür saldırıların gerçekleşmesini önlemek üzere ağ ve sistem güvenliğini artırıcı önlemlerin alınması bu adım kapsamında ele alınır. Müdahale sonrasında alınan önlemlerin genele yaygınlaştırılmasını sağlamak yapılabilecek bir çalışma da bu adım bağlamında değerlendirilir.

4. Değerlendirme ve Sonuç

Bilişim sistemlerinin ve bu sistemler tarafından işlenen bilgilerin güvenliğinin sağlanması ancak tüm kurum çalışanlarının kolektif çabası ile mümkün olabilir. Kurumsal güvenlik politikasının belirlenmesi ve bu doğrultuda yönetsel, operasyonel ve teknik denetimlerin yerleştirilmesi ve tüm kurum çalışanların düzenli ve kesintisiz eğitiminin sağlanması bilişim güvenliğinin sağlanması için en uygun yaklaşım olacaktır.

Bu yazıda, bilişim güvenliğinin sağlanması için ağ ve sistem yöneticileri tarafından kullanılacak yaklaşımların ve teknolojilerin bir özeti sunulmaktadır. Kurum hedeflerinin ve kurumsal güvenlik politikasının belirlenmesinden sonra CERT/CC tarafından önerilen güvenlik uygulamaları döngüsü ve bu çerçevede sunulan çözüm bileşenlerinin uygun bir biçimde bir araya getirilmesi anlamlı olacaktır. Unutulmaması gereken bilişim güvenliğinin bir son durum değil, hiç bitmeyen bir süreç olduğudur. Bilişim güvenliğinin sağlanmasına yönelik çabalar bitmeyen ve devamlı iyileştirmeler ile güncel tutulması gereken bir faaliyet olmalıdır.

6. Kaynaklar

- CERT– <http://www.cert.org> <http://www.cert.org>
- SANS– <http://www.sans.org> <http://www.sans.org>
- Security Focus – <http://www.securityfocus.com>
- Siyah Şapka – <http://www.siyahsapka.com>
- Dikey8– <http://www.dikey8.com>
- Olympos– <http://www.olympus.org>
- Güvenlik Haber – <http://www.guvenlikhaber.com>
- http://www.enderunix.org/documents/risk_analizi/
- <http://www.ietf.org/rfc/rfc2828.txt>
- http://www.fda.gov/ora/inspect_ref/igs/gloss.html
- <http://packetstormsecurity.org/docs/rainbow-books/NCSC-TG-004.txt>