Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri

Seda YILMAZ ve Şeref SAĞIROĞLU

***Özet*—Bu çalışmada, siber güvenlik konusunda uygulanması önerilen evrensel kurallar, siber kaynakların risk analizi, tehdit ve hazırlık seviyelerinin neler olduğu ve siber tehdit araçları üzerine bir inceleme ve analiz sunulmuştur.**

***Anahtar Terimler*— Siber güvenlik, risk analizi, tehditler, inceleme**

***Abstract*— In this study suggested international rules and applications about cyber security, risc analysis of cyber resources, what are the levels of threats and readiness and tools for cyber threats are reviewed, anaylised and presented.**

***Index Terms*— Cyber security, risk analysis, threats, review**

I. GİRİŞ

Cambridge üniversitesinde 1837 yılında Profesör Charles Babbage tarafından "Akıllı Motor" adıyla ilk bilgisayar tasarlanırken bu denli büyük bir devrim yaratacağı belki de bugünkü savaşların eşiğine gelineceği düşünülmemişti. Zaman içinde hızla gelişen bu teknoloji, artık bilginin sadece saklandığı değil işlendiği, kullanıldığı ve geliştirildiği en önemli ortam haline gelmiştir.

Kişisel kullanıcıların yanı sıra kurumsal kullanıcılar tarafından da etkin şekilde kullanılan bu dijital bilgi dünyasının internet ortamına taşınması, erişilebilirliği kolaylaştırmakla birlikte bilgiyi daha çekici ve hedeflenebilir bir hale getirmiştir. Bugün dünyada yaklaşık 2.28 milyar internet kullanıcısı, 19,2 milyar internet sayfası, 1,6 milyar resim ve 50 milyon ses-görüntü dosyasının olduğu tahmin edilmektedir [1]. Hem kişiler hem de kurumlar tarafından çok etkin kullanılan bu siber dünya giderek daha tehlikeli bir yer olmaya başlamıştır. Siber güvenlik, siber saldırı, siber savaş sözcükleri hem bireylerin hem devletlerin kelime dağarcıklarına yerleşmiş, gün geçtikçe daha vahim anlamlar içermeye ve çağrışımlar yapmaya başlamıştır.

Siber güvenlik, "siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitimler, en iyi uygulamalar ve teknolojiler bütünüdür" [1] şeklinde tarif edilebilir.

Siber saldırı, "hedef seçilen şahıs, şirket, kurum, örgüt, gibi yapıların bilgi sistemlerine veya iletişim altyapılarına yapılan planlı ve koordineli saldırılardır" [1].

Siber savaş, "Aynı saldırıların ülke veya ülkelere yönelik yapılmasıdır" [1]. Siber savaşta hedef ülkelerin güvenlik, sağlık, enerji, haberleşme, su ve kanalizasyon, bankacılık ve kamu hizmetleri gibi kritik altyapıları saldırı alanı olarak seçilmektedir [2].

Ülkeler siber güvenliklerini sağlamak için stratejiler ve politikalar belirlemektedirler. İngiltere Başbakanı Gordon Brown ülke güvenliği konusundaki anlayışın değiştiğini "19.yy da ulusal güvenliğimizi korumak için deniz ve hava güvenliğimizi sağlamak zorundayken 21.yy'da kamu kurum ve kuruluşlarımız ile işletmelerimizin sanal dünyadaki güvenliğini sağlamak zorundayız." sözleriyle ifade etmiştir [6].

Bu çalışmada ikinci bölümde siber güvenlik unsurları ve evrensel kurallar, üçüncü bölümde siber kaynak risk analizi, dördüncü bölümde siber tehdit ve hazırlık seviyeleri ile beşinci bölümde siber tehdit araçları konularından bahsedilmiştir.

II. SİBER GÜVENLİKTE EVRENSEL UNSURLAR VE KURALLAR

Bir ülkenin kurumlarına ya da ulusal güvenliğine yönelebilecek siber tehditlerin, dünya üzerindeki erişim kolaylıkları ve bağlantıları dikkate alındığında herhangi bir kaynaktan gelebileceği açıktır. Bu durum uluslar arası işbirliğini ve evrensel kuralların uygulanmasını zorunlu hale getirmektedir.

A. Siber Güvenlik Unsurları

Siber güvenliği sağlamak için alınacak her türlü tedbirde ve geliştirilecek uygulamalarda göz önünde bulundurulması gereken hususlar vardır. Bunlar hususlar [11]:

- Temel hak ve hürriyetlerinin korunması
- Demokratik toplum düzeninin gereklerine uyulması
- Ölçülülük İlkesine uyulması
- Karar alma süreçlerine tüm paydaşların katılımının sağlanması
- Bütüncül bir yaklaşımla hukuki, teknik, idari, ekonomik, politik ve sosyal boyutların ele alınması
- Güvenlik ile kullanılabilirlik arasında denge kurulması
- Diğer ülke mevzuatlarının göz önünde bulundurul-ması ve mümkün olabildiğince uyumluluğun sağlanması
- Uluslar arası işbirliğinin sağlanması

Bu hususların her yerde genel geçer önceliklere sahip olduğu bir gerçektir. Bunun yanı sıra siber güvenlik yaklaşımlarının belirlenmesinde dikkate alınması önerilen unsurlar aşağıda belirtilmiştir [11].

1) Ulusal Politika ve Stratejinin Geliştirilmesi: Siber saldırılar karşısında alınabilecek önlemlerin başarısı olması için ulusal politika ve stratejilerin geliştirilmesi gereklidir.

2) Yasal Çerçevenin Oluşturulması: Siber saldırılara karşı yüksek caydırıcılığı olan hukuki düzenlemelerin yapılması gereklidir.

3) Teknik Tedbirlerin Geliştirilmesi: Yazılım, donanım ve iş süreçlerinin güvenliğini arttırmak için güvenlik standartları dikkate alınarak teknik açıdan tedbirler geliştirilmelidir.

4) Kurumsal Yapılanmanın Belirlenmesi: Bireylerin, sivil toplum kuruluşları, özel sektör ile kamu kurum ve kuruluşlarının görev ve sorumluluklarının yasal çerçevesi belirlenmelidir.

5) Ulusal İşbirliği ve Koordinasyonun Sağlanması: Bütün sistem, şebeke ve altyapıların birbiriyle bağlantılı olduğu, her birinin güvenliğinin sağlanmadan tam bir güvenlikten bahsedilemeyeceği unutulmamalıdır. Bu nedenle belirlenen ulusal strateji ve politika çerçevesinde bütün unsurların tam bir koordinasyon ile çalışmasının sağlanması önemlidir.

6) Kapasitenin Geliştirilmesi: Teknolojinin sürekli gelişmesi siber tehdit araçlarının da değişmesine neden olmaktadır. Bu nedenle uygulama geliştirici teknik personel, yönetim birimleri, hukukçular ve kanun koyucuların teknolojiyi yakından takip ederek bu konudaki bilgi birikimlerini geliştirmeleri gerekmektedir.

7) Farkındalığın Artırılması: En zayıf halka olan kişisel kullanıcıların siber tehdit araçları ve korunma yolları konusunda bilgilendirilmesi gereklidir.

8) Uluslar Arası İşbirliği ve Uyumun Sağlanması: İnternet üzerinden bütün dünya ülkelerine rahatlıkla ulaşılabiliyor olması suç merkezlerinin farklı yerlerde olmasına imkan sağlamaktadır. Siber tehdidin bütün dünya için bir tehlike olduğu göz önünde bulundurularak hukuki mevzuatta uyum sağlanmalı ve bilgi paylaşımına önem verilmedir.

B. Evrensel Kurallar

2007 yılında Estonya'ya gerçekleştirilen siber saldırı, dünyanın siber tehdit efsanelerini dikkate almasını sağladı. 2010 yılında Çin'de Google ve diğer sitelere yapılan Aurora kod adlı saldırılar, 2008'de Microsoft ürünlerini hedefleyen Conficker adındaki solucan, İran nükleer programını hedefleyen Stuxnet solucanı ve daha birçok yeni saldırı yöntemi aslında soruna birkaç bilgisayar korsanının eğlence anlayışı olarak yaklaşmanın doğru olmadığını göstermiştir. 2007'de Estonya Siber Saldırılarından sonra ülkeler kendi varlıklarını ve vatandaşlarının bilgi güvenliğini korumak için daha etkin teknik ve hukuksal önlemler almaları gerektiğini görmüşlerdir. NATO, Birleşmiş Milletler, Avrupa Birliği, AGIT ve diğer birçok uluslar arası örgütün güvenlik politikaları bu sayede revize edilmeye başlanmıştır. Bu değişim sürecinde aşağıda belirtilen evrensel kurallar oluşmuştur [3]:

1) Bölgesellik Kuralı: Bir devletin toprakları içinde yer alan bilgi teknolojileri altyapısı devletin ulusal egemenlik unsurudur. Uluslar arası hukuk anlayışına göre; her devlet kendi ülkesinin bilgi teknoloji altyapısına karşı gerçekleştirilecek her türlü tehdit ve saldırıya karşı önlem almak ve bunlarla başa çıkabilmek için BT altyapısına yönelik her türlü iyileştirme yetkisine sahiptir [3].

2) Sorumluluk Kuralı: Bir devletin topraklarında bulunan bilgi sistem kaynağına düzenlenen siber saldırıların başka bir ülke kaynaklı olduğu varsayımı oluştuğunda sorumlu tutulan ülkenin konu ile ilgili soruşturma yapması, suçluların yakalanmasına yardımcı olması ve yargılanma sürecini desteklemesi beklenir [3].

3) İşbirliği Kuralı: Siber saldırı, bir devletin topraklarında bulunan bilgi sistemleri aracılığıyla başka bir ülkeyi hedef alarak gerçekleştirilmiş ise saldırı kaynakları kendi topraklarında olan devletin kurban devlet ile işbirliği yapma görevi vardır. Uluslar arası Siber Suçlar Sözleşmesine göre, tarafların cezai konularda uluslar arası araçlar ile hukuk kurallarının uygulanmasını ve elektronik kanıtların toplanmasını talep etme hakları vardır. Bunun yanı sıra Kuzey Atlantik Antlaşması uyarınca herhangi bir ülkenin toprak bütünlüğünü, siyasi bağımsızlığını ve güvenliği tehdit eden bir durum oluşması halinde diğer taraf ve müttefik ülkelerin işbirliği yapması zorunludur [3].

4) Öz-Savunma Kuralı: Uluslar arası ceza kanunlarına göre kişiler, yasaların kişisel özgürlüklerine karşı yasadışı olarak kullanıldığını düşündüğünde kendini korumak amacıyla gerçekleştirebilecekleri haksız eylemlerden sorumlu tutulamaz. Uluslar arası düzeyde eğer bir ülke bireysel ya da toplu olarak gerçekleştirilen bir saldırının güvenliğini tehdit ettiğini düşünürse silahlı güç de dahil olmak üzere belirlediği bir yöntemle saldırılara cevap verme hakkına sahiptir. Hatta NATO anlaşmasının 5.Maddesi uyarınca, NATO üyesi bir ülkeye gerçekleştirilen saldırıya karşı bütün üye ülkelerin cevap verme hakkı bulunmaktadır [3].

5) Veri Koruma Kuralı: Bir bireyin ağ üzerinde bulunan herhangi bir verisinin, verilerin gizliliği kapsamına girip girmediği hukuk uzmanları arasında halen bir inceleme ve tartışma konusudur. AB'nin Veri Koruma Yönergesi'ne göre tanımlanmış ya da tanımlanmamış gerçek kişilerin bilgileri kişisel veri olarak kabul edilir. Bu bakımdan bir kişinin ağ üzerindeki IP adresi yasa dışı yollardan elde edilirse hukuki olarak delil kabul edilemez. Yine aynı yönergeye göre bir kişi üçüncü bir ülkeye kişisel verilerini transfer ettiğinde ilgili ülkenin bu verileri koruma zorunluluğu vardır. Bu durumun suistimal edilmesi ihtimaline karşılık yasal mevzuatla ilgili olarak uluslar arası bir düzenlemeye ihtiyaç duyulmaktadır [3].

6) Bakım Kuralı: AB'nin Veri Koruma Yönergesi'ne göre, kişiler ağ üzerinden ya da yasal olmayan yollarla erişime karşı verilerin yanlışlıkla veya kasıtlı olarak yok edilmesini, değiştirilmesini, yetkisiz kişilere açıklanmasını önlemek amacıyla her türlü teknik ve organizasyonel önlemi almakla sorumludur. Aynı şekilde Avrupa Konseyi Sözleşmesi'nde (1981) kişilerin verilerini her türlü veri kaybı, yetkisiz kişilerin erişimi ve verilerin üçüncü kişilere açıklanması ile değiştirilmesini önlemek amacıyla gerekli önlemleri alması zorunluluğu hükmü 7.Maddede açıkça belirtilmiştir. Bu kapsamda siber saldırıların siyasi boyutları arttıkça toplumsal, askeri ve bilgi hizmetleri açısından verilerin bakım ve

korunmasına dair standartların geliştirilmesi gerekecektir [3].

7) Erken Uyarı Kuralı: Servis sağlayıcılar, e-Gizlilik Yönergesi EC/2002/58'e göre hizmetlerinin güvenliğini korumak için her türlü teknik ve organizasyonel önlemleri almakla yükümlüdür. Gerektiğinde kamu iletişim ağı sağlayıcısı ile benzer eylemleri koordine etmek yükümlülü-güne sahiptir. Ayrıca e-Ticaret Yönergesine göre servis sağlayıcılar yasadışı faaliyetleri üye devletlerin yetkililerine derhal bildirmek zorundadırlar [3].

8) Bilgileri Kuralı: Halkın yaşam, güvenlik ve refahına yönelik tehditler hakkında bilgi sahibi olma hakkı vardır. Avrupa'da toplumların kamusal yaşam ve refahlarına yönelik tehditleri ve bu tehditler karşısında alınan kararları öğrenmek konusunda devletlerin şeffaf olması gerektiğine dair bir yargı gün geçtikçe daha güçlü olarak varlığını hissettirmektedir. Tehditlerin ve bu durumlar karşısında alınan kararların erişime açık olması kamuoyunun bilgilen-dirilmesi ve siber güvenlik açısından bilinçlendirilmesini sağlarken istenmeyen bilgi ifşasına da neden olabilir. Buna rağmen yapılan saldırılar ve alınan tedbirlerin açıklaması yasal çerçevede stratejik iletişim ve kamu bilincinin arttırıl-ması bağlamında gereklidir [3].

9) Suçluluk Kuralı: Her ulusun kendi ceza hukukuna en yaygın siber suçları dâhil etme sorumluluğu vardır. Uluslar arası ceza kanuna göre bir durumun sonucu ulusal ya da uluslar arası yasalara göre bir suç sayılmadığı sürece siber saldırı yapan kişiye yönelik bir yaptırım uygulanması mümkün değildir. Bu durumlardaki anlaşmazlıkların giderilmesi ve bir uyum oluşturulması için esas alınabilecek olan Avrupa Birliği Siber Suçlar Sözleşmesi'ne göre bir bilgi-sayar sisteminin tamamına ya da herhangi bir parçasına haksız erişimler yasal yükümlülükler çerçevesinde değerlendirilmelidir [3].

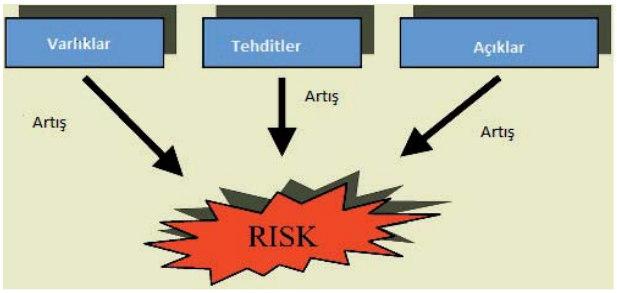
10) Manda Kuralı: Manda yönetimi siber güvenlik konusunda uluslar arası çabaların desteklenmesi ve koordinesini kapsamaktadır. Siber güvenlikle ilgili olarak yasal ve politik araçlar açısından uluslar arası koordinasyonu ve boşlukları ortaya koymayı hedeflemektedir. Bugün bu uyum sağlama çabası hali hazırda hala en az 6 uluslar arası örgütün çalışma planında yer almaktadır. NATO, üye ülkelere gerçekleştirilen siber saldırılara karşı hangi durumlarda silahlı saldırı gerçekleştirilebileceği konusunda net bir karara varamamıştır. Bu bağlamda ülkelerin ortaklaşa ve koordineli olarak çalışmaları ve strateji geliştirmeleri gerekliliği ortadadır [3].

III. RİSK ANALİZİ

Bir varlığın korunabilmesi için öncelikle değerinin bilinmesi ve hangi risklere maruz olduğunun tespiti gereklidir. Yapılan incelemelerde siber saldırıların her geçen yıl artış gösterdiği tespit edilmiştir. Bu nedenle güvenlik risklerinin analiz edilerek gerekli risk modellerinin oluşturulması hayati bir önem taşır noktaya gelmeye başlamıştır [5].

Risk analizinin başlıca faydaları aşağıda sıralanmıştır [5]:

- Güvenli bilgi yönetimini geliştirmek
- Organizasyonun kritik varlıkları izlenmesi ve etkili bir şekilde korunmasını sağlamak
- Karar vermede etkin bilgi güvenliği politikalarının desteklenmesini sağlamak
- Organizasyonlara yönelik pratik güvenlik politikalarının belirlenmesini sağlamak
- Gelecekteki tahminler için değerli analiz verilerinin teminini sağlamak



Şekil 1. Güvenlik Riski ve İlgili Öğeler [5].

Şekil 1'de görüldüğü gibi risk faktörü varlıklar, tehditler ve varolan açıklardan etkilenmektedir. Varlıklar, tehditler ya da açıklar arttıkça karşı karşıya olunan risk de artacaktır.

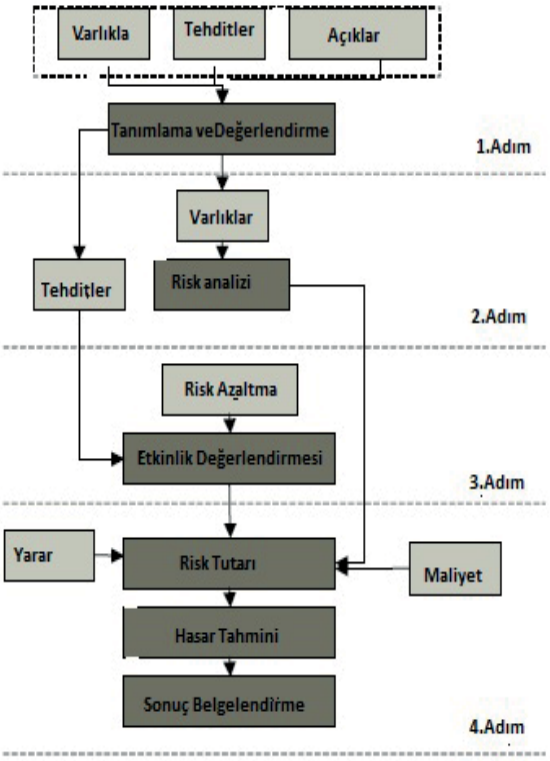
Varlıklar genel olarak bilgi/veri, evraklar, donanım, yazılım, insan kaynakları ve şartlardan oluşur. Tehditler insani/insani olmayan faktörler, ağ/fiziksel, teknik/çevresel, içerden/ dışarıdan ve kasıtlı/kazara kaynaklı tehditler olarak sınıflandırılabilir. Açıklar ise idari belgeler, personel, yönetmelikler, fiziksel koşullar ve imkânlar, teknik donanım, yazılım, iletişim/ağ kaynaklı açıklar şeklinde sınıflandırılabilir [6].

Matematiksel olarak risk, varlıkların herhangi bir açığa maruz kalması sonucunda değerlerinde oluşan azalma ile ilgili güvenlik açığına karşı tehdit oluşma olasılığının çarpımıyla hesaplanır [5].

Risk = Kayıp * Olasılık

Şekil 2'de gösterildiği gibi risk analiz işlemi genel olarak dört adımdan oluşmaktadır. Birinci adımda varlıklar, tehditler ve açıklar üzerinde bir tanımlama ve değerlendirme işlemi yapılmalıdır. İkinci adımda varlıklar, tehditler ve mevcut açıklar göz önüne alınarak sistemin toplam bir risk değerlendirmesi yapılmalıdır [6].

Üçüncü adımda mevcut tehditlerin riskinin azaltılması için gerekli yöntemin belirlenmesi ve etkinlik



Şekil 2. Güvenlik Riski Analiz Modeli [5].

değerlendirmesi yapılır. Organizasyon tarafından riskler belirlenip bu riskleri mümkün olduğunca minimize edecek yöntem seçilmelidir.

Bazı risk azaltma yöntemlerinde hangi uygulamaların kullanılabileceği aşağıda özetlenmeye çalışılmıştır [5]:

1) Erişim Kontrolü: Şifre tanımlamaya dayalı sistemler, fiziksel erişim ekipmanları (akıllı kart), kimlik doğrulama sistemi kullanılabilir.

2) Şifre Kontrolü: Açık anahtar altyapısı (AAA), vb şifreleme algoritmaları kullanılabilir.

3) İnternet Güvenlik Kontrolü: Saldırı tespit sistemi (Ids), güvenlik duvarı, vb önlemler alınabilir.

4) Uygulama Güvenlik Denetimi: Veri tabanı güvenliği, sistem dosyası güvenliği gibi uygulamaları kapsar.

5) Fiziksel/Çevresel Güvenlik Kontrolü: Tesisleri güvenliği, kurum güvenliği, giriş/çıkış kontrolü gibi uygulamaları kapsar.

Dördüncü adımda ikinci ve üçüncü adımda hesaplanan risk tutarına fayda ve maliyetler de eklenerek son risk tutarı elde edilir. Bu risk tutarı üzerinden hasar tespiti yapılarak ileriki çalışmalara zemin hazırlaması ve durumun daha net görülmesinin sağlaması için sonuç belgesi hazırlanır [5].

Toplam Maliyet = Maliyet + Operasyon Maliyeti + İş Fırsat Maliyeti

Maliyet, bir varlığı satın alma veya yükleme maliyetidir. Operasyonlu maliyet, hasarlı varlığı kurtarmak için yapılan maliyettir. İş fırsatı maliyeti ise parasal kazanç kazanmak için iş kaybıdır. Bu hesaplama dikkate alınarak organizasyon risk yönetim politikasına karar verilebilir [5].

A. Güvenlik Açığı Risk Analizi

Risk faktörlerinden birinci öncelikli olan güvenlik açıklarına daha yakından bakıldığında bir yaşam döngüsüne sahip olduğu fark edilebilir. Her sistemde bir açık vardır ve bu açığın saldırıya maruz kalması olasıdır. Eğer şanslı iseniz açıklar beyaz korsanlar tarafından keşfedilir ve kapatılması için bir fırsatınız olur. Açıkların ilk fark edildiği zamana keşif tarihi, açıkla ilgili ayrıntılı bilgi verildiği tarihe bilgilendirme tarihi, kamuoyuna açıklandığı tarihe tanıtım tarihi, açık için oluşturulan yararlanma kodunun web siteleri aracılığıyla yayınlandığı tarihe yararlanma tarihi, açığın kapatılması için ilgili yamanın yayınlandığı tarihi de yama tarihi denir. Yayınlanan her yama yeni bir açık keşfinin yani yeni bir

Şekil 3. Güvenlik Açığı Yaşam Döngüsü Olayları [8].

döngünün başlangıcı olabilir [8].

Şekil 3'de gösterilen döngü, güvenlik açığının yaşam döngüsüdür. Açıklara yönelik saldırılar bu tarihlere göre isimlendirilir [8].

- **Sıfır Gün Saldırısı**: Genellikle kötü niyetli korsanlar tarafından keşfedilen açığın, yama tarihinden önce kullanıldığı saldırılardır.
- **Sözde Sıfır Gün Saldırısı**: Piyasaya sürülen yamanın sisteme eklenmesi kaynaklı saldırılardır.
- **Olası Sözde Sıfır Gün Saldırısı**: Bu saldırı tipinde düzeltme yayınlanmış ama saldırıya uğrama olasılığı hala gündemdedir.
- **Saldırı Olasılığı**: Sistem açığının bulunmuş, ilgili yamanın hazırlanmış fakat dağıtımının yeterli yapılamadığı durumda gerçekleşme ihtimali olan saldırı tipidir.

- **Pasif**: Bu tip saldırılar henüz gerçekleşmemiş ya da kodları bile hazırlanmamış saldırılardır.

İşletim Sistemi / Saldırı Tipi	Linux		Windows	
	Açık	Oran	Açık	Oran
Sıfır Gün Saldırısı	0	0	21	8.79
Sözde Sıfır Gün Saldırısı	5	2.49	20	8.37
Olası Sözde Sıfır Gün Saldırısı	133	66.17	78	23.64
Olası Saldırı	1	0.5	5	2.09
Pasif Saldırı	62	30.84	115	48.12
Toplam	**201**	**100%**	**239**	**100%**

Şekil 4. Saldırıların İşletim Sistemlerine Göre Oranları [8].

Şekil 4'de bir fikir oluşturulması amacıyla her bir saldırı tipinin işletim sistemlerinde görülen açık sayısı ve görülme oranları ifade edilmiştir [8].

Bir açığın hedef olmasını etkileyen faktörler 3 alanda kategorize edilebilir. Bu alanlar aşağıda açıklanmıştır [8]:

1) Her uygulama güvenlik açığı yaşam döngüsü boyunca mutlaka saldırıya hedef olma olasılığına sahiptir. Bir uygulamanın ya da sistemin saldırıya maruz kalması, güvenlik açığı yaşam döngüsünün hangi aşamada sekteye uğradığına veya ne kadarının gerçekleştirildiğine bağlıdır. Döngünün tamamlanma olasılığı arttıkça açık cazip bir hedef olmaktan uzaklaşır [8].

2) Açığın popülerliği ve piyasa payının büyük olması saldırı hedefi olmasını arttıran faktörlerdendir. Pazar payı ve popülerlik oranı %60'dan büyükse yüksek risk grubunda, %30'dan küçükse düşük risk grubunda değerlendirilebilir [8].

3) Açığın yaşı, yamayı aldığı son tarih ve açığın tanıtım tarihleri de etkili faktörler arasındadır. Bir açık keşif tarihinden itibaren bir yıl içinde genç, 1-3 yıl içinde orta yaşlı, 3 yıldan sonra ise yaşlı olarak değerlendirilir. Açık, keşfinin üzerinden zaman geçtikçe değerini kaybeder. Yaralanma ile yama tarihi arasındaki fark 20 günü geçtiyse ya da yama henüz yayınlanmadıysa risk yüksek, 1 günden azsa veya yararlanma kodu yayınlanmadıysa risk düşüktür. Aynı şekilde tanıtım tarihi ile yama tarihi arasındaki fark 80 günden büyükse risk yüksek, küçükse risk düşüktür [8].

B. Güvenlik Risk Değerlendirme Yöntemleri

Güvenlik risk değerlendirmesi yapılırken bazı yöntemlerden faydalanılır. Bunlardan başlıcaları; Bilgi Güvenliği Değerlendirme Metodolojisi (IAM), Güvenlik Açığı Değerlendirme Çerçevesi (VAF) ve Operasyonlu Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE) dir [5].

1) Bilgi Güvenliği Değerlendirme Metodolojisi (IAM), NSA ve ABD Savunma Bakanlığı tarafından kullanılan, yapısal güvenlik açıklarını analiz ederek güvenlik risklerini değerlendiren bir yöntemdir [5].

2) Güvenlik Açığı Değerlendirme Çerçevesi (VAF), 1998'de ABD Kritik Altyapı Güvencesi Ofisi Komisyonu ile KPMG Marwick LLP tarafından geliştirilen, ilgili kuruluşun asgari temel altyapısı ile seçilen varlıklarının açıklarını analiz ederek değerlendirme sonucunda güvenlik notunu hesaplayan bir yöntemdir [5].

3) Operasyonel Kritik Tehdit, Varlık ve Güvenlik Açığı Değerlendirmesi (OCTAVE), ABD'de Carnegie Mellon Üniversitesi Yazılım Mühendisliği Enstitüsü tarafından geliştirilen, varlığa dayalı tehdit senaryolarının oluşturulması, önemli tesisler hakkında açıklarını tanımlanması ve risk değerlendirilmesi ile güvenlik stratejilerinin geliştirilmesi olmak üzere üç aşamadan oluşan bir güvenlik değerlendirme yöntemidir [5].

IV. SİBER TEHDİT VE HAZIRLIK SEVİYELERİ

Siber savunma hazırlık süreci birbirini takip eden dört aşama şeklinde özetlenebilir. Birinci aşamada siber tehditlere karşı kurumun misyonu kategorize edilmeli, ikinci aşamada misyonun başarısının sağlanması için hazırlık düzeyi belirlenmeli, üçüncü aşamada hazırlık hedefleri belirlenerek siber güvenlik için strateji planı geliştirilmeli ve dördüncü aşamada gerekli güvenlik yatırımları planlanmalı ve kararlar alınmalıdır [13]. Bu başlık altında siber savunmanın birinci ve ikinci aşamasını oluşturan tehdit ile hazırlık seviyelerindeki adımlardan bahsedilmiştir.

A. Tehdit Seviyeleri

Siber savunmanın temel adımı tehdit seviyelerinin belirlenmesidir. Tehdit seviyelerinin belirlenmesi süreci beş aşamalı bir süreçtir. Ek A'da verilen Tablo 1'de tehdit seviyeleri, bu seviyelerdeki saldırgan tipleri, hedefler, strateji ve yöntemleri listelenmiştir [13].

B. Hazırlık Seviyeleri

Siber savunmanın ikinci adımı hazırlık seviyelerinin belirlenmesidir. Hazırlık seviyelerinin belirlenmesi süreci beş aşamalı bir süreçtir. Ek B'de verilen Tablo 2'de hazırlık seviyeleri, amaçları, alınacak tedbirler ve çözüm önerileri listelenmiştir [13].

V. SİBER TEHDİT ARAÇLARI

Siber tehditlerin etkilerini kısa ve uzun vadeli olarak ayırmak mümkündür. Kısa vadeli tehditler, hedef aldığı organizasyonun, hükümet, işletme ve son kullanıcıların günlük faaliyetlerini etkileyen tehditlerdir. Dolandırıcılık faaliyetleri, müşteri veri ihlalleri, ATM den usulsüz nakit çekimi gibi günlük faaliyetler örnek verilebilir. Uzun vadeli tehditler ise daha çok etkileri uzun süre devam eden, ülkenin ve toplumun dengelerini değiştirmeyi hedefleyen, endüstriyel ve askeri casusluk, sosyal hoşnutsuzluk ve huzursuzluk yaratma, ulusal güvenlik ihlali gibi tehditlerdir [4].

A. Kötü Amaçlı Yazılımlar

Truva atı, virüs, klavye dinleme, casus yazılımlar, önemsiz e-posta gibi kötücül yazılımlar, açıkları kullanarak verileri elde etme, değiştirme ya da yok etme gibi amaçlarla kullanılırlar. Kötü amaçlı yazılımlar gerek kullanım kolaylıkları gerekse hızlı sonuç verebilmeleri açısından sıkça tercih edilen, hükümet, işletme ve son kullanıcılar için en tehlikeli siber saldırı araçlarından sayılmaktadırlar. Kötü amaçlı uygulamalar yazılımsal olduğu kadar donanımsal da olabilirler. Donanımsal olarak

işlem yapan klavye dinleme cihazları buna bir örnektir. Kimi zaman cihazın içine yerleştirilen küçük bir aygıt ile klavyeden girilen her türlü bilgi (şifreleriniz, dosya isimleriniz, dosya içerikleriniz v.b.) kaydedilebilir [4].

Saldırılar mutlaka ağ üzerinden yapılmak zorunda değildir. Kötü amaçlı yazılımları ağ bağlantısı olmayan cihazlara yüklenerek veri hırsızlığı yapılabilir. ATM ve POS cihazlarına yüklenen casus yazılımlar sayesinde kullanıcının verileri yasadışı olarak ele geçirilebilir ya da maddi kayıplara neden olunabilir [4].

B. Güvensiz Ortamlar

Ağ güvenliği, omurgayı oluşturan ağ elemanların güvenliğine bağlıdır. Ürünün güvenlik açıklarından faydalanı-larak sistemlere saldırı gerçekleştirmek ve bilgilere erişmek mümkündür. Bunun örneği Stuxnet adlı virüs tarafından gerçekleştirilmiştir. Belli bir ürün markasının PLC rootkit indeksindeki açıklardan faydalanılarak geliştirilen bu virüs endüstriyel sistemi tamamen durma noktasına getirmiştir [4].

C. Kimlik Hırsızlığı

Bu tür saldırılarda saldırgan erişim izni olan bir kullanıcının kimliğine bürünerek sisteme sızmayı başarır. Ağ saldırıları, mesaj tekrarları, yazılım ve sömürü saldırıları kimlik saldırılarına örnek olarak verilebilir [7].

D. DOS Saldırıları

DOS(*Denial of Service – Sistem Engelleme*) ve DDOS(*Distributed Denial of Service* - Dağıtık Hizmet Engelleme) saldırıları direk olarak sistemi hedef alan saldırılardır. Bu saldırılar sistemleri durdurarak ya da aksatmaya uğratarak ciddi zararlara yol açarlar [7]. DDOS saldırıları bilginin erişilebilirlik kuralını hedef alan, işletim sistemi, sunucu ya da uygulamanın cevaplayabileceğinden fazla sayıda istek göndererek sistemi durma noktasına getirirmeyi hedefleyen saldırılardır [12].

E. Şifre Ele Geçirme Saldırıları

Gizlilik ihlali kapsamında değerlendirilen bu saldırılarda kullanılan başlıca yöntemler sosyal mühendislik atakları, sözlük saldırıları ve parola tahmin uygulamalarıdır. Daha çok sosyal mühendislik atakları ve sosyal beceriler ile kişilerin bilgileri elde edilerek sisteme nüfus etmeye çalışılır [7].

F. Yan Kanal Saldırıları

Yan kanal saldırıları sistemlerin güç analizine, elektromanyetik uygulamalarına ve zamanlanmış görevlerine yönelik saldırılardır. Bu saldırılarda asıl amaç şifreleme anahtarını ele geçirecek bir casus uygulamayı sisteme sızdırmaktır. Birçok Akıllı Sistem maalesef bu saldırıların sonucunda müşteri bilgilerini, kullanım bilgilerini ve şifrelerini kaybetmiştir [7].

G. HTML Enjeksiyonu

Bu açık, programcıların kodlama sırasında yaptığı hatalı kodlamadan faydalanır. Web yazılımlarımda veri tabanına giren verilerin ya da veri tabanından çekilen verilerin bir kontrol mekanizmasından geçirilmemesi açığa neden olmaktadır. XSS olarak da bilinen açıktan faydalanılarak session ve cookie çalması yapılır [10].

Uygulamalarda sayfaya gönderilen bir isteğe bir cevap döndürülmesi mantığı kullanılır. Sayfaya gönderilen istek sunucuda değerlendirilip bir cevap döndürülür. Ama eğer giriş yaptığınız sayfa kötü amaçlı bir url adresine yönlendirildiyse ya da Truva atı gibi araçlar yerleştirtildiyse aldığınız yanıt beklenenden farklı olacaktır. Bu saldırı tipinde amaç web uygulamasına zarar vermek değil daha çok uygulamayı ziyaret eden kullanıcılara erişmektir [9].

H. SQL Enjeksiyonu

SQL enjeksiyonu veri tabanından yapılan sorgulama işlemini hedef alan bir saldırı şeklidir. Bu saldırı şeklinde sorgulama dili yapısı kullanılarak saldırı gerçekleştirilir [14,15].

Bir web uygulamasının kullanıcı adı ve şifre ikilisi veri tabanına

*"SELECT * FROM TABLE_PERSONEL WHERE username = '" +Kullanıcı + "' AND password= '" +Şifre + "'"*

şeklinde gönderildiğinde ("") işaretleri içindeki veri bir filtrelemeye tabi tutulmazsa kullanıcının buraya yazacağı (OR "1=) şeklinde bir ifade sorguyu

*"SELECT * FROM TABLE_PERSONEL WHERE username = '' OR "1=1" AND Password = '' OR "1=1'"*

haline getirir. Bu durumda sorgudan var olan bütün kayıtlar dönecektir [14,15].

I. Komut Enjeksiyonu

Genellikle komut(shell) enjeksiyon saldırıları SQL enjeksiyon ve XSS saldırılarının aksine doğrudan sunucuları hedefleyen bir saldırı tipidir. Web uygulamasının komut satırını kullanarak uzaktan erişimle işletim sistemi, veri tabanı yönetim sistemi ve sunucudaki bilgilere erişimi hedefler [9].

VI. SONUÇ

Bilgi varlıklarımızın siber dünyadaki bütünlüklerinin ve doğruluklarının korunabilmesi için siber güvenliğin unsurlarının özümsenmesi büyük önem taşımaktadır. Yapılan bu inceleme çalışmasının da gösterdiği gibi siber güvenliğin sağlanabilmesi için bilgi varlıkları üzerinde bir risk analizi yapılmalı, yapılan analizler ve siber süreçlerin gelişimi dikkate alınarak mevcut ve olası tehditlerin tespiti yapılmalı, tehditler karşısında uygulanması gereken hazırlık seviyeleri ve çözümleri belirlenerek popüler siber tehdit araçları konusunda önlem alınmalıdır.

EKLER

Ek A. Siber Tehdit Seviyeleri
Ek B. Siber Hazırlık Seviyeleri

KAYNAKLAR

[1] ALKAN Mustafa," Siber Güvenlik ve Siber Savaşlar" , Siber Güvenlik Siber Savaşlar TBMM İnternet Komisyonu, Mayıs 2012
[2] EMRE Bâkır, "Siber Savaşlar – Başlangıç", http://www.siberguvenlik.org.tr/ makaleler/siber-savaslar-i/, Aralık 2012
[3] TIKK Eneken, "Ten Rules for Cyber Security", Survival: Global Politics and Strategy, Mayıs 2011,(119-132)

[4] CHOO Kim-Kwang Raymond , "The cyber threat landscape: Challenges and future research directions", Computers and Security, Kasım 2011, (719-731)
[5] IN Hoh Peter, KİM Young-Gab, LEE Taek, MOON Chang-Joo, JUNG Yoonjung, KİM Injung, "A Security Risk Analysis Model for Information Systems", http://www.luisolis.com/seminario2011/papers/A Security Risk Analysis Model for Information Systems.pdf, 2011
[6] WİLLS David Barnard, ASHENDEN Debi, "Securing Virtual Space: Cyber War, Cyber Terror, and Risk" ,Space and Culture, Mayıs 2012, (110-123)
[7] YANG Y., LİTTLER Tim, SEZER S., MCLAUGHLİN K. , WANG H. F.,"Impact of Cyber-Security Issues on Smart Grid", Innovative Smart Grid Technologies (ISGT Europe),Aralık 2011,(1 – 7)
[8] JUMRATJAROENVANIT A. , TENG-AMNUAY Y., " Probability of Attack Based on System Vulnerability Life Cycle", Electronic Commerce and Security, 2008 International Symposium on, Ağustos 2008, (531 – 535)
[9] DWEN-REN Tsai; CHANG A.Y., PEİCHİ Liu, HSUAN-CHANG Chen, "Optimum Tuning of Defense Settings for Common Attacks on the Web Applications", Security Technology, 2009. 43rd Annual 2009 International Carnahan Conference on ,Ocak 2009, (89 – 94)
[10] ÇİTİL Ferhat, "HTML Injection Tehlikesi", http://www.cyber-security.org.tr/Madde/220/HTML-Injection-Tehlikesi- ,2009
[11] ÜNVER Mustafa, CANBAY Cafer , "Ulusal ve Uluslar Arası Boyutlarıyla Siber Güvenlik",EMO- elektrik mühendisliği, Mart 2010, (94-103)
[12] .ALTUNDAL Ömer Faruk, "DDoS nedir, ne değildir?", http://www.siberguvenlik.org.tr/makaleler/ddos-nedir-ne-degildir/, Ağustos 2012
[13] BODEAU Deborah J., GRAUBART Richard, FABİUS-GREENE Jennifer," Improving Cyber Security and Mission Assurance Via Cyber Preparedness (Cyber Prep) Levels", 2010 IEEE Second International Conference on Social Computing (SocialCom), Ağustos 2010 ,(1147 – 1152)
[14] OWASP," SQL Injection" , https://www.owasp.org/index.php/SQL_Injection, 2010
[15] OWASP "Reviewing Code for SQL Injection", https://www.owasp.org/index.php/Reviewing_Code_for_SQL_Injection, 2010

Seda YILMAZ Gazi Üniversitesi Bilgisayar Bilimleri Bölümünde yüksek lisans eğitimine devam etmektedir. Araştırma konuları arasında kablosuz sensor ağlarda güvenlik, web yazılım güvenliği, siber güvenlik, bilgi ve bilgisayar güvenliği yer almaktadır.

Şeref SAĞIROĞLU Gazi Üniversitesi Mühendislik Fakültesi Bilgisayar Mühendisliği Bölümü öğretim üyesidir. Zeki sistem kimliklendirme, tanıma ve modelleme, ve kontrol; yapay sinir ağları ve yapay zeka uygulamaları; sezgisel algoritmalar; endüstriyel robotlar; zeki anten analizi ve tasarımı; internet, web ve bilişim sistemleri ve uygulamaları; yazılım mühendisliği; bilgi ve bilgisayar güvenliği; biometri, elektronik ve mobil elektronik imza ve açık anahtar altyapısı; kötücül ve casus yazılımlar gibi konularda çalışmaktadır. 50'nin üzerinde SCI tarafından taranan uluslar arası dergilerde yayınlanmış makalesi, 50'nin üzerinde ulusal dergilerde yayınlanmış makalesi, 100'ün üzerinde uluslar arası konferans ve sempozyum bildirisi ile ulusal sempozyum, konferans ve çalıştaylarda sunulmuş100'e yakın bildirisi bulunmaktadır. 3 adet alınmış patenti vardır. 5 adet yayınlanmış kitabı, 2 adet kitapta bölüm yazarlığı bulunmaktadır. 4 kitabın da editörlüğünü yapmıştır.

Ulusal ve uluslar arası pek çok proje yürütmüş ve konferanslar düzenlemiş olup akademik çalışmalarına devam etmektedir.

EK A

TABLO 1
SİBER TEHDİT SEVİYELERİ [13]

Seviye	Saldırgan Tipleri	Saldırgan Hedef/Amacı	Yöntemleri
1.Seviye (Siber Vandalizm)	-Küçük saldırgan grupları	-Kurum organizasyon yapısını bozmak -İtibarını zedelemek	-Hassas verilere erişmek -Giriş denemeleri gerçekleştirmek -Genel erişime sahip sistemler üzerindeki dosyaları hedef almak -Ağ yapısına yönelik keşif saldırıları yapmak -Kurum çalışanlarına yönelik sosyal mühendislik faaliyetleri uygulamak
2.Seviye (Siber Hırsızlık)	-Bireysel ya da küçük saldırgan grupları	-Siyasi-ideolojik amaçlar -Endüstiriyel casusluk -Kar edinme	-Kurum içi yardım ile fiziksel erişim sağlama -Siber saldırı için kullanılan bilgilere açık kaynaktan erişim -Veri trafiğini izleme -Bilgi sistem cihazlarını çalma -Dış bilgi sistemlerini ve ağları izleme -IIS bağlantılarına erişmek için açıklardan ayarlanma
3.Seviye (Siber Gözetleme)	-Büyük saldırgan gruplar -Sofistik terör örgütleri -Profesyonel organize suç örgütleri	-Siber kaynakları elde etmek -Genel altyapı bilgisine sahip olmak -Büyük çaplı saldırılara temel olacak verileri elde etmek	-Veri transferini kolaylaştırmak için örgütsel yapıya casus kod parçaları yerleştirmek -Dahili ağlara genel amaçlı bilgi toplayıcıları ekleme -Haritalama ve organizasyon ağlarını tarama -Bilgi sistem ortamları ve operasyonlara keşif gerçekleştirme -Yaygın kullanılan yazılımı ele geçirme -Hedefli sıfır gün saldırıları gerçekleştirme -Yetkili kişilerin verilerini ele geçirme
4.Seviye (Siber Casusluk)	-Profesyonel istihbarat örgütleri	-Ülkelerin özel misyon ve programları	-Sahte donanım tedarik zinciri ekleme -Oturum bilgisini ele geçirme -İzleme içeriklerini kurumsal bilgi sistemleri ve ağları üzerine yükleme -Örgüt içine casus yerleştirilmesi -Ana bilgisayarlar ve kritik noktaları hedefleme -Sıfır gün saldırılarıyla kurumsal bilgi sistemlerini hedefleme -Hedef kuruluşun ISSini hedefleyen, kuruluş tarafından kullanılmasını sağlamak üzere kötü amaçlı yazılımlar tasarlama -Kablosuz algılayıcıları hedef yapı içine gizlice eklemek
5.Seviye (Siber Savaş)	-Terörist gruplar	-Hedefin bilgi altyapısını yok etmek	-Kritik bilgi sistem bileşenleri ve işlevlerini hedef alma -Tasarım, üretim ve/veya dağıtım bileşenlerini kullanarak bilinen organizasyonu tehlikeye atmak -İç, dış ve tedarik zinciri saldırını koordineli şekilde kullanarak kuruluşa saldırılar düzenlemek -Kuruluşun tedarik zincirine kötü niyetli yazılımlar enjekte ederek yanlış-açık organizasyonları yaratmak -ISSe yanlış ama inandırıcı veri enjekte etmek -ISS içine sistem yapılandırmalarına dayalı özel, sıradan olmayan, kötü amaçlı yazılım eklemek -Kablosuz iletişim sistemine erişim sağlamak -Kuruluş içindeki ayrıcalıklı pozisyonlara casus yerleştirilmek

EK B

TABLO 2
HAZIRLIK SEVİYELERİ [13]

Seviye	Amaç	Tedbirler	Çözümler
1.Seviye (Çevre Savunması)	-Dış çevreden gelecek saldırılara karşı genel hazırlık	-Ticari güvenlik ürünleri ve masaüstü uygulamaları	-Güvenlik duvarı oluşturmak ve saldırı tespiti yapmak -Kimlik doğrulaması yapmak -E-posta sunucuları ve istemci sistemlerine anti-virüs yazılımları yüklenmesi -Denetim günlüğü ile açıkları ve çevre sistemlerini izlemek
2.Seviye (Kritik Bilgileri Koruma)	-Kritik yada hassas verilere erişimi engellemek	-Gelişmiş kimlik doğrulama -Erişim kontrol sistemleri -Şifreleme -Kritik verilerin bağımsız sistemlerde saklanması	-Dış ve iç sistemler arasında güvenilir şifreli uygulamaların kullanımı (SSL, VPNs) -Kurumsal ağlarda ayrılmış ve arındırılmış bölge oluşturulması -Taşınabilir sistemlerin (dizüstü bilgisayarlar, flaş sürücüler, vb) iç ağa yeniden bağlanmadan önce taranması -Kötü niyetli iç erişimleri önlemek için kritik sistemlere güçlü bir fiziksel güvenlik kontrolünün oluşturulması -Periyodik açık arama ve bilgi savunma ayarlarının yapılması -Riskli kullanıcı davranışlarını daha iyi kontrol edebilmek için masaüstü bilgisayarlarının sanallaştırılması -Tasarım/mimariyi ek güvenlik yazılımları ile geliştirmek
3.Seviye (Farkındalık)	-Bilgi sistem altyapısını korumak	-Penetrasyon testleri	-Saldırıları algılamak için kritik noktalara alıcıları dağıtmak -Anormal koşulları ve sıra dışı akışları izlemek için ağ trafiğini analiz etmek -İçeriden çıkan dağılımı izlemek -Siber ve fiziksel erişim analizi yapmak -Yasadışı veri aktarımı için çevre iletim kanallarını izleme
4.Seviye (Mimari Esneklik)	-Saldırı geçmişini incelemek	-Bilgi sistem altyapısının yedeklenmesi -Erişimlerin sınırlandırılması -Saldırılar karşısında esnek bir mimari oluşturulması	-Kritik bilgi sistemlerine güçlü erişimler kullanmak -İç yapıyı kontrol etmek ve yeniden konfigürasyonları hızlı bir şekilde yapmak için sistemi alt bölümlere bölmek -Sipariş ve tedarik zinciri arasındaki süreyi en aza indirmek -Kuruluşdaki yapılara fiziksel güvenlik uygulamak (Penetrasyon Testi) -Güvenilir aygıtlar kullanmak -Sık sık yazılım yapılandırmalarında küçük değişiklikler yapmak
5.Seviye (Çeviklik)	-Direk organizasyon yapısını hedef alan saldırılara hazırlık	-Sistemlerin mümkün olduğunca bağımsız tasarlanması -Esnek ve uyarlanabilir mimari seçilmesi	-Anahtar bileşenleri için birden çok tedarikçi kullanmak -Kuruluş adına kritik bileşenleri güvenilir aracılar yoluyla elde etmek -Penetrasyon testlerini kullanmak -Hizmetleri sanallaştırmak -Periyodik olarak saldırgan yeteneğini azaltmak için kritik işlevleri yeniden oluştumak -Gelecekteki saldırılara cevap verebilmek için yakın zamanlı saldırıların yapısal incelemesini ve analizini yapmak