Endüstri Mühendisliği Dergisi
Cilt: 22 Sayı: 2 Sayfa: (14-32)

Makale

ŞİRKET YEREL ALAN AĞLARININ İNTERNET BAĞLANTILARINDA GÜVENLİĞİN SAĞLANMASI PROBLEMİNİN KISITLAR TEORİSİ YAKLAŞIMIYLA İNCELENMESİ

Gülşen AKMAN, Özkan URAL*

Kocaeli Üniversitesi, Endüstri Mühendisliği Bölümü, İzmit, Kocaeli
akmang@kocaeli.edu.tr, ozural@yahoo.com

Geliş Tarihi: 22 Eylül 2008; Kabul Ediliş Tarihi: 7 Nisan 2011
Bu makale 2 kez düzeltilmek üzere 40 gün yazarlarda kalmıştır.

ÖZET

Kısıtlar teorisi herhangi bir sistemin performansının artırılması için sistem performansını olumsuz etkileyen faktörlerin bulunması, yönetilmesi ve ortadan kaldırılması felsefesidir. Bu çalışmada: Kısıtlar teorisinin düşünce süreçlerinin bir şirket yerel alan ağının internet bağlantısında güvenliğin sağlanmasında dar boğazların tespiti, giderilmesi ve performansının artırılmasında nasıl kullanılacağının gösterilmesi amaçlanmıştır. Bu amaçla kısıtlar teorisi düşünce süreçleriyle bilgisayar ağlarında güvenlik probleminin çözülmesi konusunda genel bir çerçeve sunulmuştur. Öncelikle mevcut gerçeklik ağacı kullanılarak darboğazlar tespit edilmiş, buharlaşan bulut tekniğiyle bu darboğazların giderilmesine yönelik çözüm önerileri geliştirilmiştir. Gelecek gerçeklik ağacıyla darboğazlar ortadan kaldırıldıktan sonra arzu edilen durum tanımlanmış, geçiş ağaçlarıyla çözüm önerilerinin nasıl hayata geçirileceği açıklanmaya çalışılmıştır.

Anahtar Kelimeler: Kısıtlar teorisi, düşünce süreçleri, buharlaşan bulut, internet bağlantı güvenliği

INVESTIGATION OF SECURITY PROBLEM IN LOCAL AREA NETWORKS USING THEORY OF CONSTRAINTS

ABSTRACT

Theory of constraints (TOC) is finding, managing and eliminating factors which influence system performance negatively. This study presents how thinking process of the TOC is applied to determine and eliminate the bottlenecks in internet connection of local area networks in an institution or company to develop system performance of internet connections. For this purpose, a framework employing TOC thinking processes is defined. In the first stage, bottlenecks are determined by using current reality trees, then suggestions in order to eliminate this bottlenecks are developed by evaporating cloud method. Desired situation after eliminating bottlenecks are defined by future reality trees and transition tree method is applied to explain how these suggestions are accomplished.

Keywords: Theory of constraints, thinking process, evaporating cloud, internet connection security

* İletişim yazarı

1.GİRİŞ

Internet, bilişim ve iletişimi öne çıkarmaktadır. Telefon şebekeleri ya da radyo ağı gibi tek bir hizmet için işletilen iletişim ağları yerine, bilişimin gücünü kullanarak tek bir iletişim ağını birçok uygulama için kullanmaktadır. Bu sistem aynı anda mesajlaşma, genel yayın, ses ve video, gerçek zamanlı paylaşım ve daha birçok uzlaşma gerektiren uygulamayı desteklemektedir. Böylece, iletişim dünyasında büyük bir değişim yaşanmıştır ve bu kapsamda farklı iletişim hizmet sektörleri arasındaki sınırlar giderek belirginliğini yitirmeye başlamıştır (Heywood ve Heywood, 1999). Bunun sonucunda da bilgisayar ve bilgisayar ağı teknolojileri hayatımızın pek çok alanında "*olmazsa olmaz*"ları haline gelmiştir. İletişim, elektronik ticaret, para transferleri, kamu hizmetleri, askeri sistemler, elektronik bankacılık, savunma sistemleri, bu alanlardan bazılarıdır (Pro-G ve Oracle, 2003).

Bilginin ve kaynakların paylaşılması gereksinimi sonucunda kurumlar, bilgisayarlarını çeşitli yollardan birbirine bağlayarak kendi bilgisayar ağlarını kurmuşlar ve sonra dış dünyayla iletişim kurabilmek için bilgisayar ağlarını İnternet'e uyarlamışlardır (Ural, 2007). İnternet kullanımının artması ve yaygınlaşmasıyla birlikte, buna paralel olarak, güvenlik tehditleri ve riskleri aynı oranda artarak bilgisayar ağlarını ve sistemlerini bir saldırı aracı haline, kullandığımız sistemleri de açık birer hedef haline getirmiştir. Internet bir taraftan günlük yaşamı kolaylaştırırken, diğer taraftan bilginin güvenliğine yönelik yeni tehditleri de ortaya çıkarmaktadır (Ural ve Akman, 2006).

Teknolojik olarak güvenlik önlemlerinin gelismesine rağmen bilişim sistemlerine karşı yapılan saldırıların sayısının artması ve bilgi sistemleri üzerinde yüksek derecede etki yapan hasarlar oluşturması, teknik yöntemlerin bilgi güvenliğinin sağlanmasında yetersiz olduğunu göstermektedir (Tekerek, 2008). Özellikle, elektronik ticaret gibi gerçek zamanda yapılan ve para transferinin söz konusu olduğu işlerde; performansın, doğruluğun ve güvenliğin en üst düzeyde olması gerekir. Bu nedenle, bu tarz uygulamaların yapılacağı Internet bağlantısı olan Intranet'lerin olduğu her kuruluşta bilgisayar ağı yönetiminin öneminin en iyi şekilde anlaşılması; kolay, hızlı ve uygulanabilir olması gerekmektedir (Heywood ve Heywood, 1999). İnternet uluslararası veya ulusal arenada bir firmanın varlığını ve rekabet gücünü sürdürebilmesi için yenilikleri izleme, bilgi edinme, bilgi paylaşımı, haberleşme, pazar araştırması ve benzeri konularda en büyük yardımcısı olmasına rağmen, aynı zamanda firmanın tüm dünyaya açık, savunmasız bir penceresidir. Şirketlerin de kendilerine ait çok özel ve önemli sırları ve bilgileri mevcuttur (Ural, 2007).

Bir firmanın işlediği bilgiler (müşteri bilgileri, ürün bilgileri, imalat bilgileri ve benzeri) firmanın varlığının sürekliliği için çok önemli ve korunması gereken verilerdir. Bu bilgilerin firma içinde bile kasıtlı veya kasıt dışı yanlış kullanımı söz konusu olabildiği gibi, internet gibi sonsuz saldırıların gelebileceği bir ortama fiziksel bağlantısının bulunması, normal şartlarda kabul edilebilecek bir eylem gibi görünmemektedir. Ancak, bu noktayı çok iyi dengelemek ve internet ortamından gelecek zararlardan çok faydalarını ön plana çıkarabilecek bir güvenlik organizasyonunun oluşturulması gerekmektedir. Firmaların kendi içlerinde tuttukları verilere saldırı olabileceği gibi, çok basit bir şekilde firmaların kendi tanıtımlarını yaptıkları web sitelerine de saldırı yapılabilir. Bu da çok büyük mali kayıplara yol açabilmektedir (Ural, 2007). Bu makalede firmaların internet bağlantılarında yerel alan ağlarında karşılaşabilecekleri problemlerin tespiti, yönetilmesi ve ortadan kaldırılmasına yönelik öneriler geliştirme de kisitlar teorisi yaklaşimi kullanilacaktir.

2. BİLGİSAYAR AĞLARINDA GÜVENLİK UYGULAMALARI

İnternet, yasalarla kolaylıkla denetlenemeyen bir sanal dünyadır ve firmalar internet yoluyla birçok tehditle karşı karşıya kalmaktadır. Bu sanal dünyada saldırganlar bilgiye ulaşmak için ağların zayıf noktalarını kullanarak yasadışı yollar denemektedirler. Sadece yapılan saldırılarla değil, aynı zamanda kullanıcıların bilinçsizce yaptıkları hatalar nedeniyle birçok bilgi başka kişilerin eline geçmekte veya içeriği değiştirilmektedir (Karaaslan vd., 2003). Firmalar veri kaybı, finansal kayıplar, itibar kayıpları, hizmetlerin

sunulamaması veya aksaması, gizli bilgilerin çalınması gibi zararlarla karşı karşıya kalabilmektedirler (Tekerek, 2008).

Bilgi sistem güvenliğinin yüksek tutulması; var olan tehditlere karşı bilgi güvenliğine ilişkin gerekli tedbirlerin eksiksiz alınması ve alınan önlemlerin yeni tehditlere karşı sürekli olarak güncellenmesi sayesinde gerçekleştirilmektedir. Bilgi sistemlerinin güvenliğini artırmak için yapılan düzenlemelerin sağladığı avantajlardan yararlanırken, bilgi güvenliği zaafına düşülmemesi dikkat edilmesi gereken en önemli konulardan biridir (Ural, 2007).

2.1 Bilgisayar Ağlarında Güvenlik Tehditleri

Bilgisayar sistemleri ve ağlarındaki güvenliğin sağlanması, mevcut bilgi sistemleri zafiyetleri ile bunlara karşı olası tehditlerin bilinmesi ve karşı önlemlerin alınmasıyla mümkündür (Khatiwala vd., 2006).

Zafiyet, bir bilgisayar sisteminin ya da ağının saldırıya veya kasıtlı olmayan zarar verici eylemlere karşı yetersiz olmasıdır. Bir sistemin zafiyetini belirleyen faktörler; fiziksel zafiyet alanları, doğal zafiyet alanları, donanım ve yazılım zafiyetleri, ortam zafiyetleri, iletişim zafiyetleri, elektromanyetik yayılımdan kaynaklanan zafiyetler, kullanıcılardan kaynaklanan zafiyetlerdir (Khatiwala vd., 2006). Tehditler, bilgisayar sistem ya da ağına yönelik tehlike kaynaklarıdır. Bunlar doğal ve fiziksel tehditler olabileceği gibi (yangın, sel, elektrik kesintisi vb.), bilinçli ya da bilinçsiz olarak oluşan ve sistemin kullanımını ya da çalışmasını engelleyen durumlardır (Ural, 2007). Bilgisayar güvenliği ile ilgilenenlerin görevi, zayıf noktaları belirlemek ve olası tehditlere yönelik karşı önlemleri almaktır (Khatiwala vd., 2006).

Her geçen gün yeni gelişen yazılım ve donanım olanakları sayesinde kötü niyetli kişilerce birçok saldırı ve sistemler üzerindeki güvenlik açıkları tespit edilmektedir. Son günlerde, bilgi sistemlerinde bilgi güvenliği konusunda zafiyet ve tehdit oluşturan ve her biri farklı amaçlara yönelik değişik yöntemler kullanan çok çeşitli kötü amaçlı yazılımın var olduğu tespit edilmiştir (Canbek ve Sağıroğlu, 2006). Bunlar; virüsler, solucanlar, Truva atları, arka kapılar, mesaj sağanakları, kök kullanıcı takımları, telefon çeviriciler, korunmasızlık sömürücüleri, klavye dinleme sistemleri, tarayıcı soyma ve casus yazılımların yanında, reklâm, parazit, hırsız, püsküllü bela yazılım, tarayıcı yardımcı nesnesi, uzaktan yönetim aracı, ticari RAT, bot ağı, ağ taşkını, saldırgan ActiveX, Java ve betik, IRC ele geçirme savaşı, nuker, paketleyici, ciltçi, şifre yakalayıcılar-soyguncular, şifre kırıcılar, anahtar üreticiler, e-posta bombardımanı, kitle postacısı, web böcekleri, aldatmaca, sazan avlama, web sahtekârlığı-dolandırıcılığı, telefon kırma, port tarayıcılar, sondaj aracı, arama motoru soyguncusu, koklayıcı, kandırıcı, casus yazılım ve iz sürme çerezleri, turta, damlatıcı, savaş telefon çeviricileri ve tavşanlar (Canbek ve Sağıroğlu, 2006).

Bilgi sistemini kullanabilecek, depolanmış, işlenen ve gönderilen bilgilere ulaşabilecek kişilere karşı kontrol mekanizmasının dikkatlice uygulanmaması da zafiyetlere yol açabilir. Bilgi sistemleri ve ağlarında bilginin depolanması, işlenmesi ve iletilmesinde doğruluğun sağlaması için otomatik kontrollerin yetersizliği veya işlemleri ve kontrolleri yapan sorumluların ihmalleri zafiyetin artmasına neden olur. Tasarım ve uygulama hataları, sistem kurma ve bakım sorunları, işletim sisteminde değişikliklere neden olan bilinçli sızmalar kullanıcılar için istenmeyen sonuçlar doğurabilir. Bilgi, bir yerden diğerine iletilirken kazayla ortaya çıkması halinde, yetkisiz kişilerce kasıtlı olarak kopyalanabilir veya üzerinde değişiklikler yapılabilir. Bilgisayar sistemini yönetenler ya da kullananlar, sistemle ilgili gizli bilgileri yetkisiz kişilere bilerek veya bilmeyerek verebilirler (Ural, 2007) . Yapılan araştırmalar dünya genelinde şirketlere yapılan saldırıların %70 ile %90 arasında şirket çalışanları tarafından yapıldığını ortaya koymaktadır. Bu bilgi hırsızlığından tutun da bilerek ya da bilmeyerek sistemlere verilen zararları da kapsamaktadır. Genelde işinden kötü şekilde ayrılan şirket çalışanları, sistemlere ait bilgilerini başkalarına verebilmekte ya da özellikle sistemleri sabote edebilmektedirler. Kendi bilgisayarlarına kurdukları “paket dinleyiciler” (sniffer) sayesinde başka kişilerin e-postalarını ya da gizli bilgilerini elde ede-

bilmektedirler. Ya da her türlü önleminizi dışarıdan gelebilecek saldırılara karşı almışken içeriden birisi kolaylıkla önemli sistemlere erişebilir kritik bilgileri silip değiştirebilir ya da rakip bir firmaya verebilir. Ya da meraklı bir kullanıcı yeni öğrendiği hacker araçlarını firma üzerinden başka firmalara girmek için kullanabilir (Kahya, 2007).

Koçnet tarafından yapılan Türkiye İnternet Güvenliği Araştırması Sonuçları’na göre (Koçnet, 2004); şirketlerin %27’sinin bilişim sistemlerinde çok yüksek seviyede açıklar olduğu görülmüştür. Özellikle ADSL geniş bant erişimlerinde şirket kullanıcılarını ve KOBİ’leri tehdit eden %70’lere varan oranda risk tespit edilmiştir. ADSL abonelerinin %72’sinin güvenlik duvarı konfigürasyonlarında ciddi açıklar görülmüştür. Şirketlerin %40’ının web sunucu bilgilerinin kolaylıkla çalınabileceği, ana sayfalarının değiştirilebileceği veya bir başka adrese yönlendirilebileceği tespit edilmiştir. Şirketlerin %29’unda isim çözmek için kullanılan DNS (Domain Name System) sunucularındaki açıklar nedeniyle şirket e-postalarının ele geçirilmesi ve çalışanların internet üzerinden eriştiği bankacılık gibi işlemlerde kullandıkları şifrelerin çalınması riski saptanmıştır. Şirketlerin %17’sinde bilgilerinin çalınmasına yol açan güvenlik konfigürasyonu problemi belirlenmiştir. Şirketlerde 2003 yılında %29 olan yüksek seviyeli açık oranı 2004 yılında yakın şekilde %27 olarak saptanmışken, 2005 yılında %19 olarak ortaya çıkmıştır.

Firmaların kendi içlerinde tuttukları verilere saldırı olabildiği ve korunması gerektiği gibi çok basit bir şekilde firmaların kendi tanıtımlarını yaptıkları web sitelerine yapılabilecek bir saldırı çok büyük mali kayıplara yol açabilmektedir. Bunu basit bir hesaplamayla incelediğimizde; genellikle bankacılık sektörünün sitelerinin yüksek güvenlik içerdiği ve maliyet açısından büyük yatırımlar yapıldığı; ancak onun haricinde diğer firmaların kendi sitelerine bu derece maliyetli yatırımları fazla gördükleri gözlenmiştir. Basit bir örnek olarak Borsada hisseleri işlem gören bir firmanın kendi tanıtım sitesine yapılan bir saldırıda sitenin ekran penceresinde kayan haber hattına firmanın bu yıl zarar açıkladığı ve yönetim kurulunun istifa ettiği bilgisinin kötü niyetli kişiler tarafından saldırı yapılarak yazılması durumudur. Bu durum, 10.000 $’lık güvenlik yatırımından kaçınan firmanın haberi fark edip düzeltinceye kadar 1 milyon $’lık bir kayba uğramasına neden olmaktadır (Apohan, 2004). Bir diğer örnek ise internet üzerindeki en iyi performansa sahip sitelerden biri olan Yahoo’ya 1999 yılında düzenlenen saldırıdır. Bir internet analiz servisi olan Keynote Systems’e göre Yahoo normalde %99,3 ‘lük erişim oranına sahipti. Fakat saldırı sırasında Yahoo portalı üç saat boyunca neredeyse erişilmez hâle gelmiş ve bu zaman aralığındaki erişim oranı sadece %0 ile %10 aralığında gerçekleşebilmiştir. Erişilemeyen süre boyunca 100 milyon gibi çok sayıda sayfa görüntüsünün kaybedilmiş olabileceği ve muhtemel reklam ve elektronik ticaret geliri kaybının yaklaşık olarak 500.000 $ olduğu belirtilmiştir (Apohan, 2004).

Günümüz acımasız rekabet koşullarında kurumların ülkelerin ve organizasyonların varlıklarının temeli olan stratejik bilgilerin üretildiği, işlendiği, saklandığı, iletildiği ve işlem yapıldığı bilişim sistemleri bu bilgi ile çıkar, rant, ekonomik avantaj ve rekabet gücü sağlayacak kişi kurum ve hatta ülkeler tarafından potansiyel hedef olarak değerlendirilmektedir (TBD, 2008). Özellikle elektronik iş uygulamalarının artmasıyla birlikte firmalar virüs ve hackerların saldırılarına maruz kalmaktadırlar. Bu durum gerek firmalar ve kamu sektörü gerekse vatandaşlar için önemli bir risk oluşturmaktadırlar. Virüs ve Hacker’ların uluslararası ve ulusal ekonomilere verdikleri zararlar milyar dolar düzeylerini bulmaktadır (Kelleci, 2003). Taylor (2003), örneğin SirCam ve LoveBug virüslerinin iş alemine maliyetinin sırasıyla 1,5 ve 8,75 milyar dolar olduğunun tahmin edildiğini ifade etmektedir. Dünyada bu sorunu aşmak için internet güvenlik sistemleri önem kazanmaktadır.

2.2 Bilgisayar Ağlarında Güvenlik Önlemleri

Şirket yerel alan ağlarının internet bağlantılarında güvenliğin sağlanması belki de şirketin var olması kadar önemlidir (Ural ve Akman, 2006). Görüldüğü gibi Internet güvenli bir ortam değildir. Bu nedenle Internet’e bağlı olan Intranet’ler nedeniyle hem ilgili

kurumlar hem de kurumların kullanıcıları her an Internet'deki saldırılara maruz kalabilirler ve bu saldırıların bir kısmı başarılı da olabilir. Bu gibi saldırılara anında cevap verebilmek için bilgi güvenliği yönetimi konusunda bilgi sahibi olmak, uygulanabilmesi için politikalar oluşturmak ve gerekli önlemleri almak gereklidir. Bu noktada alınacak güvenlik tedbirlerinin aslında politik birer kısıt olduğu karşımıza çıkmaktadır. Bilgisayar teknolojisi güvenlik politikası olmalı, politikanın arkasında yönetim olmalı, politika dışında insiyatif kullanımı yok edilmeli ve yönetim politikanın uygulanması talimatını yazılı vermelidir (Ural, 2007).

Sistemde bulunan zafiyetleri engellemek veya en aza indirmek amacıyla birçok üretici firma yama yayımlamakta ve hatta bazıları kullanıcı etkileşimine bile gerek duymadan otomatik olarak kendini güncellemektedir. Sistemde bulunan zafiyetlerin dışında sosyal mühendislik ve şifre atakları sayesinde de güvenlik mekanizmaları aşılabilmektedir (Ural, 2007). Sistemlerin güvenliğini artırmak için işletim sistemi politikaları daha da güçlendirilebilmekte, kişisel ve kurumsal güvenlik duvarı yazılımları yüklenebilmekte, gelen giden dosyalar ve kullanıcılar bazında anti virüsler yüklenebilmektedir. Ağ bazında güvenliği artırmak için Honey pot, IDS, Erken uyarı sistemleri, Otomatik imza olmak üzere pasif ve erişimi bloklama (Spam filtreleri, White/Black listeleri, güvenlik duvarı, ACL, Dinamik karantina), aldatma, yavaşlatma olmak üzere aktif önlemler alınabilmektedir (Khatiwala vd., 2006).

Zafiyetlerin engellenmesi ve tehditlerin en aza indirilmesi için bilgi güvenliği politikaları bilgisayar ağları için çok önemli bir yer tutmaktadırlar. Bilgi güvenliği politikaları, organizasyonlarda uygulanacak olan bilgi güvenliğinin sağlanması için gerekli olan önlemlerin alınmasını sağlayan kurumsal faaliyetlerdir (Kararslan vd., 2003) ve her organizasyon için farklılık gösterse de, tipik olarak çalısanın sorumluluklarını, kontrol mekanizmalarını, amaç ve hedefleri içeren genel ifadelerden olusur (Tekerek, 2008). Başka bir deyişle bilgi güvenliği politikaları güvenli bir sistemin nasıl olması gerektiğini tanımlarlar ve hangi durumlarda sistemde güvenlik açıkları meydana geleceğini belirtirler. Bilgi güvenliği politikaları oluşturulurken sisteme gelebilecek bütün tehditler göz önünde bulundurulmalıdır. Ayrıca, güvenlik tehditleri zamanla değiştiğinden, güvenlik politikaları da devamlı kontrol edilip güncellenmelidir (Doğantimur, 2009). Bilgi ve ağ güvenlik politikalarından söz edildiğinde birçok alt politikadan söz etmek mümkündür. Bunun nedeni, politikaların konuya veya teknolojiye özgü olmasıdır. Ağ güvenliğinin sağlanması için gerekli olan temel politikalar şu şekilde sıralanabilir (Cambazoğlu, 2008); 1. Kabul edilebilir kullanım (acceptable use) politikası, 2. Erişim politikası, 3. Ağ güvenlik duvarı (Firewall) politikası, 4. İnternet politikası, 5. Şifre yönetimi politikası, 6. Fiziksel güvenlik politikası, 7. Sosyal mühendislik politikası.

Yapılacak kötü niyetli saldırıları, risk analizleri temelinde oluşturulan güvenlik politikaları sayesinde engellemek ise ciddi yatırım gerektirmektedir. Güvenlik konusunda yapılacak harcamaların, çok hızlı olarak gelişen teknoloji paralelinde her geçen gün daha da fazla artması gerektiği değerlendirilmektedir (Heywood ve Hewwood, 1999). Ayrıca alınan güvenlik önlemlerinin maliyetinin, korumaya çalıştığımız hizmet ya da kaynağın değerinden daha düşük olması gereklidir. Uygulanacak güvenlik önlemleri işletmeden işletmeye, kurumdan kuruma, organizasyondan organizasyona farklılık gösterir. Örneğin bir ticaret işletmesi için uygulanacak güvenlik önlemleriyle bir eğitim kurumunda, örneğin bir üniversitede, bir bankada uygulanacak güvenlik önlemleri farklı olacaktır. Güvenlik sağlamak için satın alınacak yazılımların niteliği, kurulacak donanımın özellikleri de aynı olmayacaktır. Bu nedenle şirketler, kurumlar ve organizasyonlar için gereğinden fazla donanım yatırımı yapılmasının bir bedeli vardır. Ne kadar güçlü bir donanım gerekiyorsa o büyüklükte yatırım yapılmalıdır. 100 kişinin çalıştığı yere 10.000 kişinin trafiğini kaldıracak bir sistem kurmanın veya günde 1000 hit alacak bir web sunucusunu korumakla yüzbinlerce hit alacak bir sunucuyu korumak için alınacak donanım maliyeti iyi düşünülmelidir. Aksi takdirde güvenlik hizmetleri işletmenin verdiği servisin maliyetini arttıracak, bu da bilgisayar ağının kuruma kazandırdıklarının kurumdan aldıklarından daha az olmasına neden olacaktır (Ural, 2007).

Çözüm için ister ticari bir ürün kullanılsın, isterse açık sistemler kullanılsın kuruma bir maliyeti olacaktır. Burada eldeki bütçenin alabileceği en iyi sistemin kurulması söz konusudur. Konulacak sistemin sadece bugünü kurtarması hedeflenmemeli; birkaç yıllık ağın genişleme durumu da dikkate alınarak buna göre bir seçim gerçekleştirilmelidir. Sahip olma maliyeti de dikkate alınmalı ve uzun vadede bu ürünün yıllık yenilemeleri, yama ücretleri de planlanmalıdır. Teknik destek ücreti de düşünülmelidir. Daha yüksek fiyatlar her zaman daha iyi güvenlik anlamına gelmemektedir (Karaaslan, 2009).

3. KISITLAR TEORİSİ

İşletmeyi bağımsız süreçler topluluğu yerine bütün bir sistem olarak gören Kısıtlar Teorisi (Theory of Constraints) büyük bir kısmı Goldratt (1990)'ın çalışmalarına dayanan bir teoridir. Aynı zamanda, sistem kısıtlarının belirlenerek, amaçlara ulaşılabilmesi için bu kısıtlar arasındaki ilişkinin ortaya konmasını sağlayan bütünleşik bir yönetim felsefesidir (Coldratt ve Cox, 2004). Kısıtlar Teorisi (KT), zaman içinde üzerine yapılan araştırmaların artmasıyla daha yaygın bir kullanım alanı kazanmıştır. KT herhangi bir sistemin performansının arttırılması için, sistem performansını olumsuz yönde en çok etkileyen faktörün bulunması, yönetilmesi ve ortadan kaldırılması konusunda oluşturulmuş; yönetim felsefeleri, disiplinleri ve sektörlere özel en iyi uygulamaları içeren bir felsefedir (Rahman, 1998; Akman ve Karakoç, 2005).

Birçok organizasyon için amaç, şimdi ve gelecekte daha yüksek verimlilik sağlamak ve sonuçta kârlılığı artırmaktır. Amaç kârlılık olduğu için sistemin daha yüksek düzeyde kâr elde etmesini engelleyen kısıtlar ortadan kaldırılmalıdır. Her organizasyon kendi içerisinde bir sistemdir. KT de bu sistemi geliştirmek ve daha iyiye ulaştırmak amacıyla kullanılmaktadır. Ancak sistemin herhangi bir bölümünü geliştirmeden önce sistemin bütünsel amacı ve bu amacın üzerinde etkili olabilecek alt sistemlerle kararları tanımlanmalıdır (Corbett, 1999) . KT, kısıtların bir firmanın performansını belirlediği ve her sistemin en az bir kısıta sahip olduğu gerçeğinden yola çıkmaktadır. Eğer böyle bir durum söz konusu olmasaydı, kar amaçlı bir örgütün sonsuz miktarda kâr elde etmesi mümkün olabilirdi (Goldratt, 1990). Kısıt, " bir sistemin para kazanma hedefini başarmasını engelleyen herhangi bir unsur" olarak tanımlanabilmektedir. Bir diğer deyişle kısıt " bir sistemin hedefiyle ilgili olarak, performansı sınırlayan her şey " olup, KT sistemdeki kısıtların yönetilmesi yoluyla gelişmeye odaklanan bir yönetim yaklaşımıdır (Atwater ve Gagne, 1997). KT'nin temel noktası ise; geleneksel düşüncenin tersine, her kısıtın aslında birer ilerleme fırsatı olmasıdır. KT, kısıtları pozitif olarak değerlendirir, çünkü kısıtlar bir sistemin performansını tanımlarlar ve sistem kısıtlarının aşama aşama ortadan kaldırılması sistemin performansını artırır (Spencer ve Cox, 1995). Özellikle üretim sürecinde yaşanan her sorunun elbette ki belli bir önem derecesi vardır; ancak, işletmenin kısıtları bu sorunlar içerisinde gerçekten önemli bir paya sahiptir. Her kısıt, yeni bir darboğaz ve giderilmesi ya da uygun değer hâle dönüştürülmesi gereken bir problem olarak karşımıza çıkmaktadır (Goldratt ve Cox, 2004). Kısıtlar firmanın içinden (örneğin şirkette kolaylıkla kontrol edilebilen veya değiştirilebilen bir şey) veya dışından (örneğin firmanın kontrol edemediği, fakat firmanın çözmek için orta ve uzun vadede çeşitli önlemler alacağı bir kısıt) kaynaklanabilir. Tablo 1'de çeşitli kısıt örnekleri görülmektedir. Tablo 2'de ise kısıtlar teorisi uygulama örnekleri görülmektedir.

KT performansı sınırlayan kısıtları belirlemek ve onların performansını artırarak tüm sistemi iyileştirebilmek için genel bir yaklaşım ve çeşitli araçlar sunmaktadır. Bu araçlar, değişimin yönetilmesi, politika kısıtlarının tanımlanması ve çözülmesi sürecinde sağduyu, sezgisel bilgi ve mantıksal yaklaşım kullanmaktadır. Bu yaklaşımların kullandığı çeşitli tekniklerden biri düşünce süreçleridir. Bu teknik, kısıtların ortadan kaldırılmasına yönelik olarak sistemin ana problemleri üzerine yoğunlaşmakta ve alternatif çözümler sunmaktadır (Akman ve Karakoç, 2005). Düşünce süreçleri (DS), sistemin performansını

Tablo 1. Kısıt Türü Örnekleri

Kısıtın Türü	Kısıtın Tanımı
Pazar Kısıtları	Dengesiz pazar talebi üretim yapabilmesi için işletmelerin kapasitesini kısıtlayabilir.
Kaynak Kısıtlan	İşletme kaynakları pazar talebi karşısında yetersiz kalabilmektedir.
Politik Kısıtlar	Yöneticiler fırsatlar karşısında basiretsiz tutumlarda bulunabilirler.
Davranış Kısıtları	İşletmedeki tüm çalışanların davranışlarının, çalışanlar ile üst yöneticilerdeki genel eğilimler.
Lojistik Kısıtlar	Uygulanan prosedürler işletmelerin faaliyetlerini sınırlayabilmektedir.

Kaynak: Atwater ve Gagne, 1997

Tablo 2. Kısıtlar Teorisi Uygulamalarına Şirket Bazlı Örnekler

İşletme	Kısıt	Sonuç
General Motor's	Kitlesel üretim sonucunda üretim hattında çok fazla işin birikmesi.	Ulaştırma süresi %30 azaltılmış ve üretim kalitesi arttırılmıştır.
General Electric	Stoklar ve faaliyetler ile ilgili yönetsel kısıtlar.	Stok ve direkt işçiliğe bağlı devir zamanında azalma sağlanmıştır.
American Lighting Standard Corp.	Verimlilik ve standart maliyet konularında gereğinden fazla odaklanma ve zaman kaybı.	Dönemlik işletme hasılatında %40, nakit akışında %60 artış sağlanmıştır.
Southwestern Ohio Steel	Değişken kapasite.	Kapasiteye bağlı faaliyetlerde iyileşme görülmüştür.

Kaynak: Louderback ve Patterson, 1996

Tablo 3. Düşünce Süreçleri Adımları ve Kullanılan Yöntemler (Akman ve Karakoç, 2005)

SORULAR	AMACI	YÖNTEMLER	AÇIKLAMA
Ne değişecek?	Temel problemlerin tanımlanması	Mevcut gerçeklik ağacı	Bir sistemin mevcut durumunu analiz etmek ve problemleri daha iyi anlamak için oluşturulur ve sistemin performansını azaltan istenmeyen etkilere sahip temel problemleri tanımlar.
Neye Dönüşecek?	Basit ve pratik çözümler geliştirmek	Buharlaşan Bulut	Problemlerin ayrı olarak ele alınmasını, karşılaşılan çatışmaların ve varsayımların belirlenmesini ve çözüm amacıyla incelenmesini içerir.
		Gelecek Gerçeklik Ağacı	Mevcut sistemde yapılacak değişiklikleriyle meydana gelebilecek sonuçlar arasındaki neden sonuç ilişkisini gösterir.
Dönüşüm Nasıl gerçekleşecek?	Çözümlerin uygulanması	Ön gereksinim ağacı	Çözüm fikrinin önündeki tüm engellerin üstesinden gelmek için gerekli olan ikincil çözüm kümelerinin oluşturulması için mantıksal bir yol sunar.
		Geçiş ağacı	Amaca ulaşmak için gerekli faaliyetlerin tanımlanmasında kullanılır. Arzu edilmeyen sonucun tanımlanmasından, değişimin gerçekleşmesine kadar adım adım süreçleri ortaya koymak için tasarlanmış bir sebep-sonuç zinciridir.

Kaynak: Akman ve Karakoç, 2005

sınırlandıran kısıtın incelenmesi, çözüm önerilmesi, çözümlerin önkoşullarının bulunması ve uygulanması sırasında karşılaşılabilecek güçlüklerin DS yöntemleri kullanılarak ortadan kaldırılmasını içerir (Köksal ve Karşılıklı, 2000). Yapılan araştırmalar, örgütsel değişim sürecinin başarılması en zor süreç olduğunu göstermektedir. DS, gerekli değişimleri kolaylıkla ve başarılı bir şekilde gerçekleştirebilmek için geliştirilmiştir. DS'nin amacı, bir organizasyonun mevcut durumunu geliştirmek için gerekli faaliyetleri tanımlamak, belirsiz durumlara çözüm üretmektir (Stein, 1997). Düşünce süreçlerinin temelinde üç soru bulunmaktadır; *Ne Değişecek? Neye Dönüşecek? Dönüşüm Nasıl Gerçekleşecek?* (Mabin ve Balderstone, 2003). Bu sorular problem çözme tekniklerinin de esasını oluşturur. Bu soruları cevaplamak için temel olarak neden-sonuç diyagramlarına dayanan araçlar kullanılır. Tablo 3'te bu sorular ve kullanılan yöntemler hakkında detaylı bilgi verilmektedir.

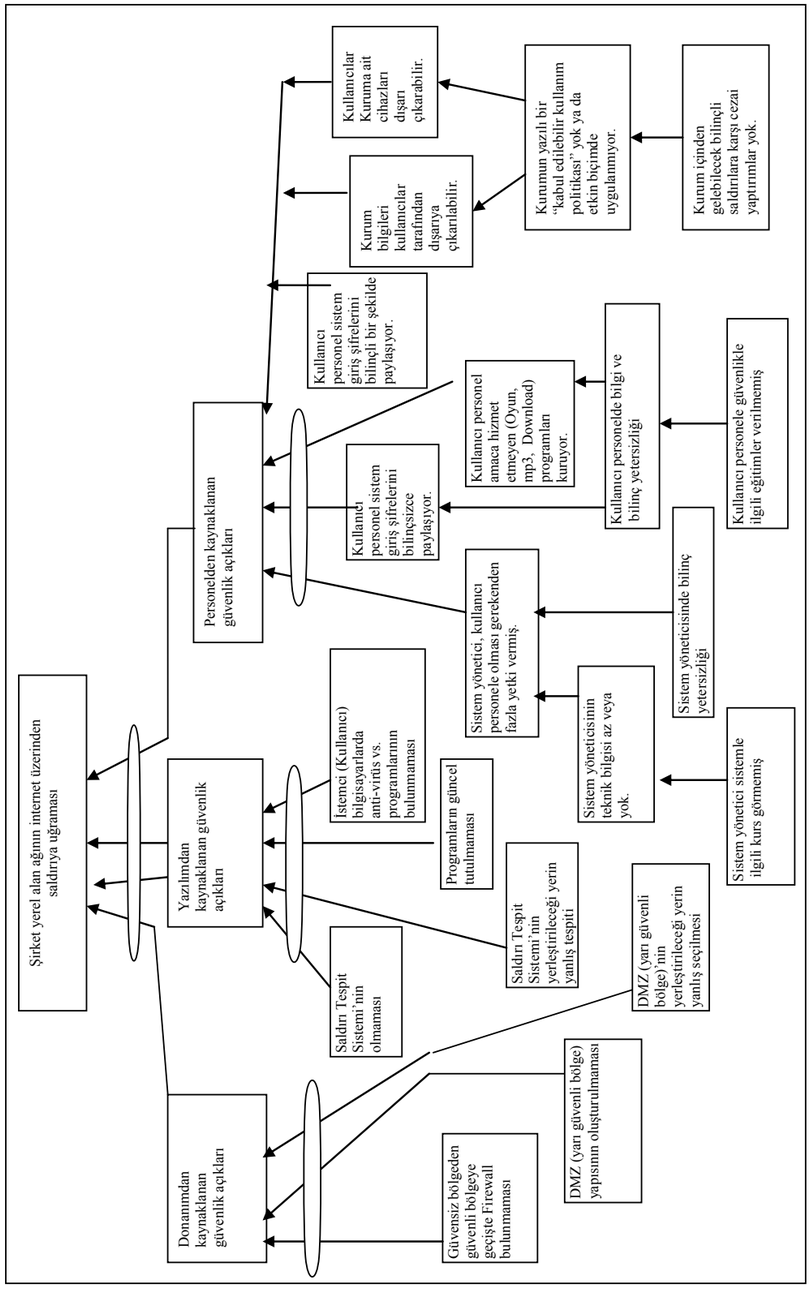
4. AĞ GÜVENLİĞİNDE KARŞILAŞILAN PROBLEMLERE KISITLAR TEORİSİYLE ÇÖZÜM ÖNERİLERİ GELİŞTİRİLMESİ

Bu makalede, firmaların kendi yerel alan ağlarında işlenen bilginin ve veri tabanının güvenliğinin sağlanması ve internet ortamından gelebilecek bilinçli veya istem dışı saldırılara karşı mevcut sistemin korunmasında kısıtlar teorisi düşünce süreçlerinin kullanımı incelenmiştir. Bir firmanın yerel alan ağının içeriden ve/veya dışarıdan gelebilecek tehlikelere karşı savunabilmesi ve tam güvenli bir alt yapıya kavuşabilmesi için, öncelikle mevcut durumun değerlendirilmesi gerekir. Bunun için düşünce süreçlerinin birinci adımı olan *Ne Değişecek?* sorusuna cevap aranmıştır. Bu sorunun cevabı ise *Mevcut Gerçeklik* Ağacının oluşturulması ile verilmektetir. Yerel alan ağlarının internet bağlantısında karşılaşılan ana kısıtlar; donanımdan kaynaklanan güvenlik açıkları, yazılımdan kaynaklanan güvenlik açıkları ve personelden kaynaklanan güvenlik açıkları olarak sıralanabilir. Şekil 1'de mevcut gerçeklik ağacında şirket yerel alan ağlarının internet üzerinden saldırıya uğramasındaki nedenler ortaya konmuştur.

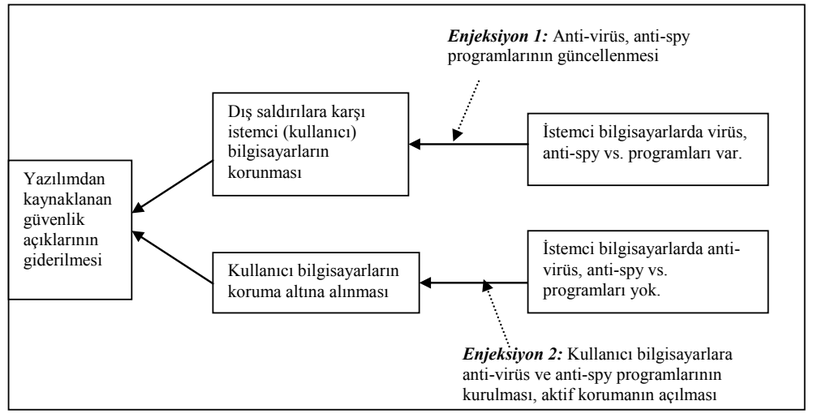
Mevcut gerçeklik ağacını oluşturduktan sonraki aşama *"neye dönüşecek?"* sorusunun cevaplanmasıdır. Bu soruya buharlaşan bulut ve gelecek gerçeklik ağacı ile cevap verilir. İstenmeyen sonucu ortadan kaldırmak için önerilen çözümlerle temel ve ön gereksinimlerin tanımlandığı, çözümler arasındaki çatışmanın ortaya konduğu ve bu çatışmanın yok edilmesi için enjeksiyonun yapıldığı araç olan buharlaşan bulutları oluşturulur. Bu araç, tek bir problemin ayrı olarak ele alınmasını, karşılaşılan çatışmaların ve varsayımların belirlenmesini ve çözüm amacıyla incelenmesini içerir (Köksal ve Karşılıklı, 2000). Buharlaşan bulut yöntemi problemin yaşandığı mevcut durumdan arzulanan gelecek duruma geçişte, problemlerin ortadan kaldırılmasına katkıda bulunarak etkili bir köprü görevi görmektedir (Davies vd., 2005). Çoğu zaman çatışmada ortaya atılan varsayımlar sözlü hâle getirildiğinde, çatışan taraflar yanlış varsayımlar altında çatıştıklarını fark ederler ve çatışma bir buhar bulutu gibi dağılır (Yaralıoğlu, 2007).

Şekil 2'de yazılımdan kaynaklanan güvenlik açıklarına neden olan ve kullanıcı bilgisayarlarında koruyucu programların bulunması ya da bulunmamasının sorgulandığı çatışma ile olası enjeksiyonları göstermektedir. Buradaki çatışma kullanıcı bilgisayarlarda virüs, anti-spy programlarının bulunup bulunmamasının güvenlik açığına neden olmasıdır. Bu çatışmanın ortadan kaldırılmasına yönelik enjeksiyonlar, "Anti-virüs, anti-spy programlarının güncellenmesi" ve "Kullanıcı bilgisayarlara anti-virüs ve anti-spy programlarının kurulması, aktif korumanın açılması"dır.

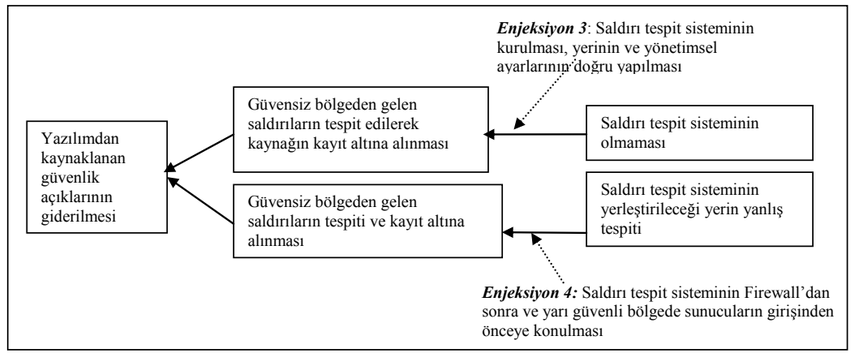
Şekil 3'te yazılımdan kaynaklanan güvenlik açıklarına neden olan ve saldırı tespit sisteminin olmaması veya var ise de Saldırı Tespit Sistemi (STS)'nin yerinin yanlış yapılandırılmasının yarattığı çatışma ve çözüm için olası enjeksiyonlar gösterilmektedir. Burada yaşanan çatışma saldırı tespit sisteminin olmaması veya var ise de STS'nin yerinin yanlış yapılandırılmasıdır. Bu çatışmaların ortadan kaldırılmasına yönelik enjeksiyonlar "saldırı tespit sisteminin kurulması, yerinin ve yönetimsel ayarlarının doğru yapılması" ve "STS'nin



Şekil 1. Mevcut Gerçeklik Ağacı



Şekil 2. Buharlaşan Bulut-1

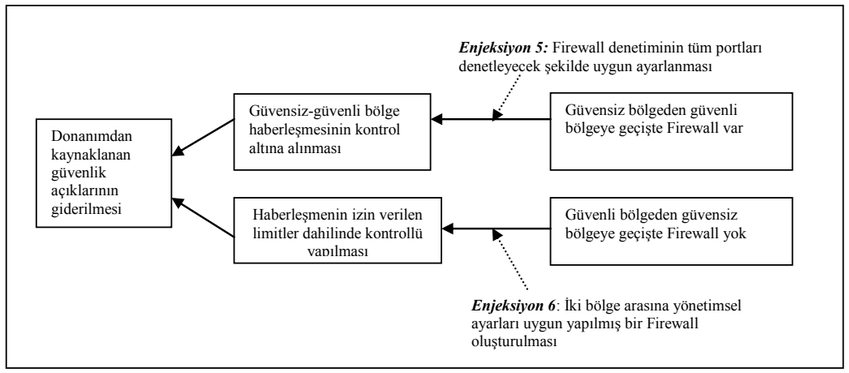


Şekil 3. Buharlaşan Bulut-2

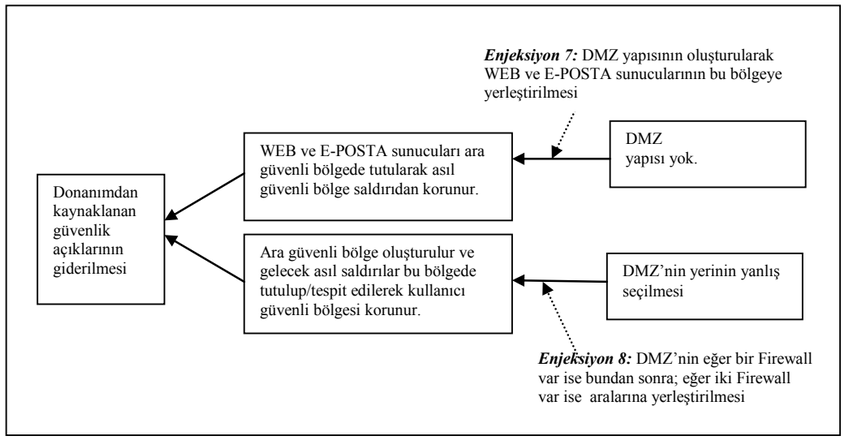
güvenlik duvarıdan sonra ve yarı güvenli bölgede (DMZ, demilitarized zone) sunucuların girişinden önce yapılandırılması"dır.

Şekil 4'te donanımdan kaynaklanan güvenlik açıklarına neden olan ve güvensiz bölgeden güvenli bölgeye geçişte güvenlik duvarı (Firewall) olması veya olmamasıyla var ise de güvenlik duvarının ayarlarının yarattığı çatışma ve çözüm için olası enjeksiyonlar gösterilmektedir. Burada yaşanan çatışma güvensiz bölgeden güvenli bölgeye geçişte Firewall olması veya olmamasıyla var ise de güvenlik duvarının yönetimsel ve donanımsal ayarlarının uygun yapılmasıdır. Bu çatışmaların ortadan kaldırılmasına yönelik enjeksiyonlar "güvenlik duvarı denetiminin tüm portları denetleyecek şekilde uygun ayarlanması" ve" iki bölge (güvenli-güvensiz) arasına yönetimsel ayarları uygun yapılmış bir güvenlik duvarı oluşturulması"dır.

Şekil 5'te donanımdan kaynaklanan güvenlik açıklarına neden olan ve DMZ yapısının olmamasıyla eğer var ise yerinin yanlış seçilmesinin sorgulandığı çatışmalardan bir tanesini ve çözüm için olası enjeksiyonlar gösterilmektedir. Burada yaşanan çatışma DMZ yapısının olmamasıyla eğer var ise yerinin yanlış seçilmesidir. Bu çatışmaların ortadan kaldırılmasına



Şekil 4. Buharlaşan Bulut-3

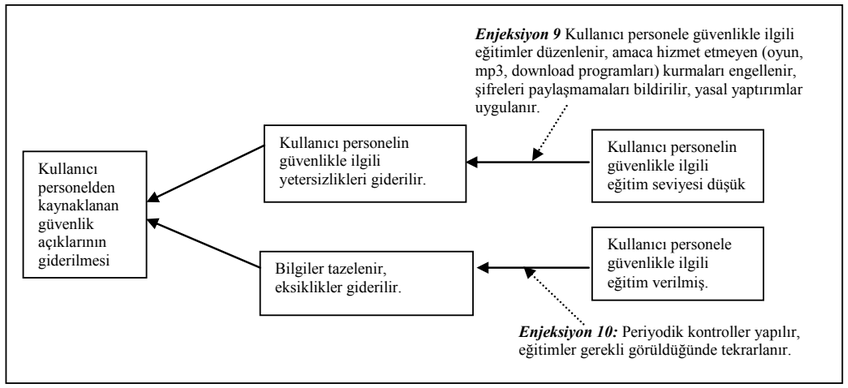


Şekil 5. Buharlaşan Bulut-4

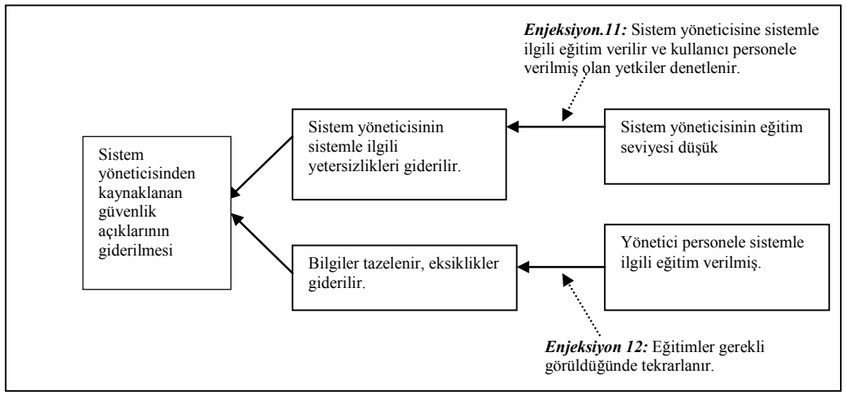
yönelik enjeksiyonlar "DMZ yapısının oluşturularak WEB ve E-POSTA sunucularının bu bölgeye yerleştirilmesi" ve "eğer bir güvenlik duvarı var ise DMZ'in bundan sonra; iki güvenlik duvarı var ise aralarına yerleştirilmesi"dir.

Şekil 6, kullanıcı personelden kaynaklanan güvenlik açıklarına neden olan ve kullanıcı personelin güvenlikle ilgili eğitimlerinin düşük veya olmamasıyla eğitimler verilmiş; ancak güncelliğini yitirmiş olmasının sorgulandığı çatışmalarla olası enjeksiyonları göstermektedir. Burada yaşanan çatışma; kullanıcı personelin güvenlikle ilgili eğitimlerinin düşük veya olmamasıyla eğitimler verilmiş; ancak güncelliğini yitirmiş olmasıdır. Bu çatışmaların ortadan kaldırılmasına yönelik enjeksiyonlar, "kullanıcı personele güvenlikle ilgili eğitimler düzenlenmesi, amaca hizmet etmeyen (oyun, mp3, download programları) kurmaları engellenmesi, şifreleri paylaşmamalarının bildirilmesi, yasal yaptırımlar uygulanması" ve "periyodik kontroller yapılarak, eğitimlerin gerekli görüldüğünde tekrarlanması"dır.

Şekil 7, yönetici personelden kaynaklanan güvenlik açıklarına neden olan ve yönetici personelin eğitim seviyesi düşük veya düşük olmamasıyla eğitimler ve-



Şekil 6. Buharlaşan Bulut-5

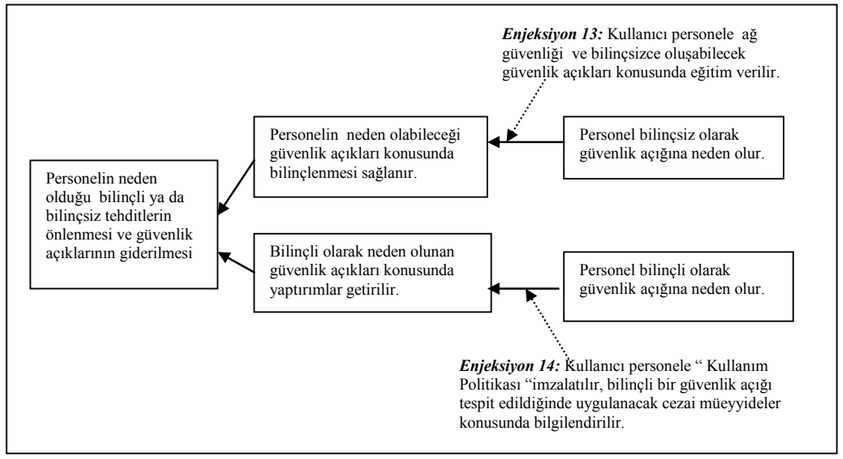


Şekil 7. Buharlaşan Bulut-6

rilmiş; ancak güncelliğini yitirmiş olmasının sorgulandığı çatışmalarla olası enjeksiyonları göstermektedir. Burada yaşanan çatışma; yönetici personelin eğitim seviyesi düşük veya olmamasıyla eğitimler verilmiş ancak güncelliğini yitirmiş olmasıdır. Bu çatışmaların ortadan kaldırılmasına yönelik enjeksiyonlar, "yönetici personele sistemle ilgili eğitim verilmesi" ve "kullanıcı personele verilmiş olan yetkiler denetlenmesi, Gerekli görüldüğünde eğitimlerin tekrarlanması"dır.

Şekil 8, kullanıcı personelden kaynaklanan güvenlik açıklarına neden olan ve kullanıcı personelin bilinçli ya da bilinçsiz olarak güvenlik açığına neden olduğunun sorgulandığı çatışma ile olası enjeksiyonları göstermektedir. Buradaki çatışma kullanıcı personelin bilinçli olarak ve bilinçsiz olarak güvenlik açığına neden olmasıdır. Bu çatışmanın ortadan aldırılmasına yönelik enjeksiyonlar," Kullanıcı personele ağ güvenliği ve bilinçsizce oluşabilecek güvenlik açıkları konusunda eğitim verilmesi" ve "kullanıcı personele *Kullanım Politikası* imzalatılması, bilinçli bir güvenlik açığı tespit edildiğinde uygulanacak cezai müeyyideler konusunda bilgilendirilmesi"dir.

Buharlaşan bulut yöntemiyle problemin neye dönüşeceği, çatışmalar ve enjeksiyonlarla tespit edilmeye



Şekil 8. Buharlaşan Bulut-7

çalışılmıştır. Sonraki aşamada geleceği hayal etmek, canlandırmak ve tahmin etmek için gelecek gerçeklik ağacı kullanılır. Gelecek gerçeklik ağacı bir organizasyon için strateji, vizyon veya bir planın resminin görülmesini sağlar. İstenen etkiyi oluşturma aracıdır.

Bu çalışmada istenilen etki "*her türlü güvenlik önlemi alınmış internet bağlantılı şirket yerel alan ağ*"dır. Şekil 9'daki gelecek gerçeklik ağacında, tam olarak güvenliği sağlanmış bir yerel alan ağında donanımdan, yazılımdan ve personelden kaynaklanan güvenlik açıkları giderilmiş ve bunlara neden olan istenmeyen tüm etkiler istenen etkiye dönüştürülmüştür.

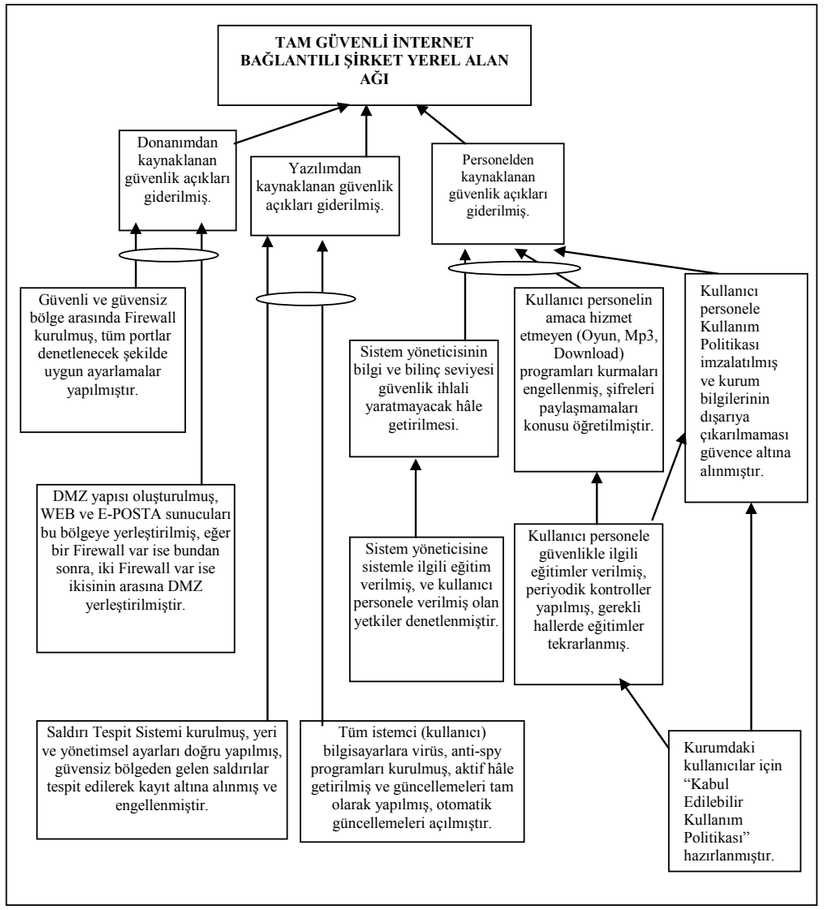
Düşünce Süreçlerinin son aşaması ve temelinde bulunan son soru da "*nasıl değiştireceğiz?*" sorusudur. Bu aşamada Geçiş Ağacı, amaca ulaşmak için gerekli faaliyetlerin tanımlanmasında kullanılır. Arzu edilmeyen sonucun tanımlanmasından değişimin tamamlanmasına kadar adım adım süreçleri ortaya koymak için tasarlanmış bir sebep-sonuç zinciridir. Geçiş ağacı, adım adım uygulama planıdır. İncelenen süreç, var olan durumundan arzulanan duruma bu yapıyla geçirilir.

Şekil 10'da tüm kullanıcı (istemci) bilgisayarlara anti-virüs, anti-spy programlarının kurulumuna ilişkin geçiş ağacı görülmektedir. İhtiyaca yönelik bir faaliyet planıdır. Varsayım olarak yapılan faaliyet ihtiyacı neden belirlemeyecek ve sonuç üretmeyecek tespit edilir. Buna yönelik ikinci bir faaliyet uygulanır ve istenen sonuca ulaşıncaya kadar adım adım ilerlenir. Burada istenen sonuç tüm kullanıcı (istemci) bilgisayarlara anti-virüs, anti-spy programlarının kurulmasıdır.

Şekil 11'de STS'nin kurulumuna ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç STS'nin kurulması, yeri ve yönetimsel ayarlarının doğru yapılması, güvensiz bölgeden gelen saldırıların tespit edilerek kayıt altına alınması ve engellenmesidir.

Şekil 12'de güvenlik duvarı kurulumuna ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç güvenli ve güvensiz bölge arasında Firewall kurulması, tüm portların denetlenecek şekilde uygun ayarlamaların yapılmış olmasıdır.

Şekil 13'te güvenli bölgeye direk saldırıları önlemek için DMZ mimarisinin kurulumuna ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç DMZ yapısı oluşturulması, WEB ve E-POSTA sunucularının bu bölgeye yerleştirilmesi; eğer bir güvenlik duvarı varsa bundan sonra, iki güvenlik duvarı varsa ikisinin arasına DMZ yerleştirilmesidir.

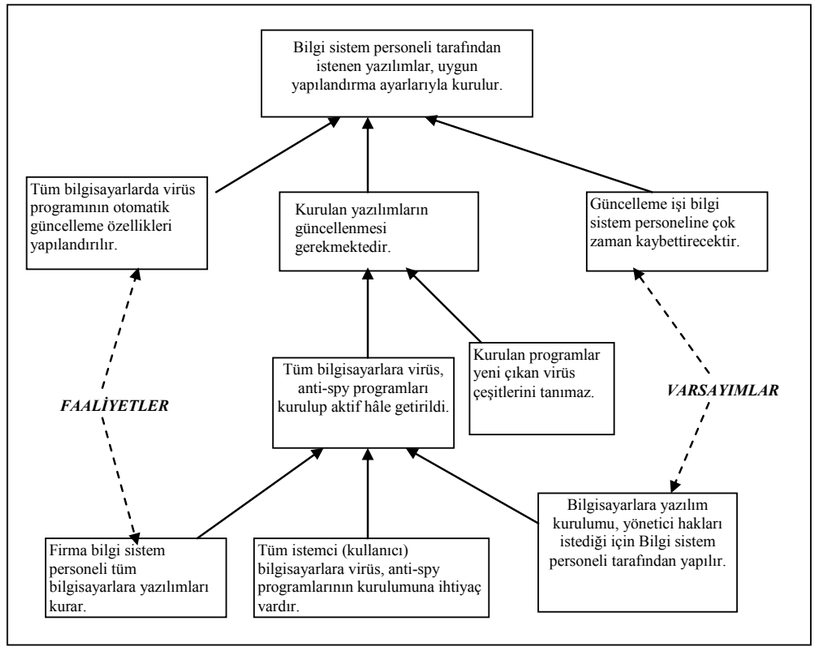


Şekil 9. Gelecek Gerçeklik Ağacı

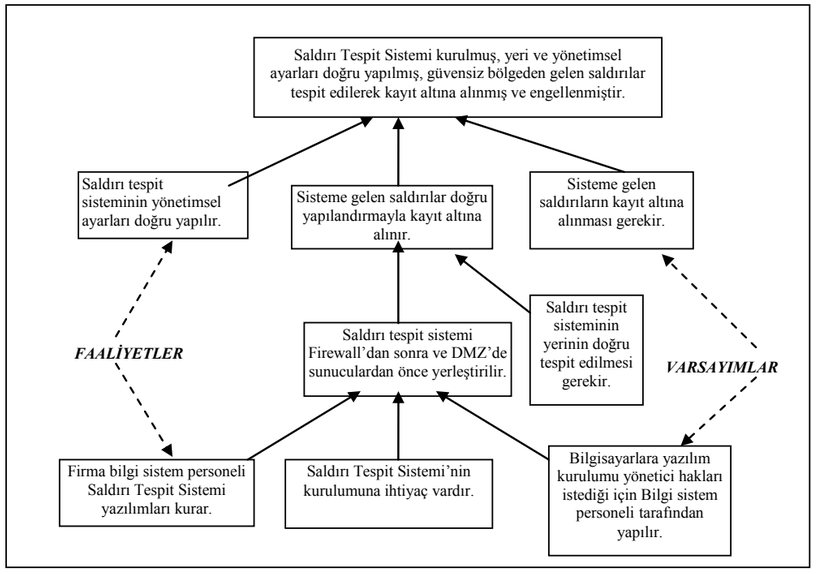
Şekil 14'te yönetici personelin sistemle ilgili kurs ihtiyacıyla bu personelin bilinç seviyesinde duyulan gelişmeye ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç yönetici personelin bilgi ve bilinç seviyesinin güvenlik ihlali yaratmayacak hâle getirilmesidir.

Şekil 15'te kullanıcı personelin sistemle ilgili kurs ihtiyacıyla bu personelin bilinç seviyesinde duyulan gelişmeye ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç kullanıcı personelin bilgi ve bilinç seviyesinin güvenlik ihlali yaratmayacak hâle getirilmesi ve amaca hizmet etmeyen (Oyun, Mp3, Download) programları kurmalarının engellenmesi, şifreleri paylaşmamaları konusunun öğretilmesidir.

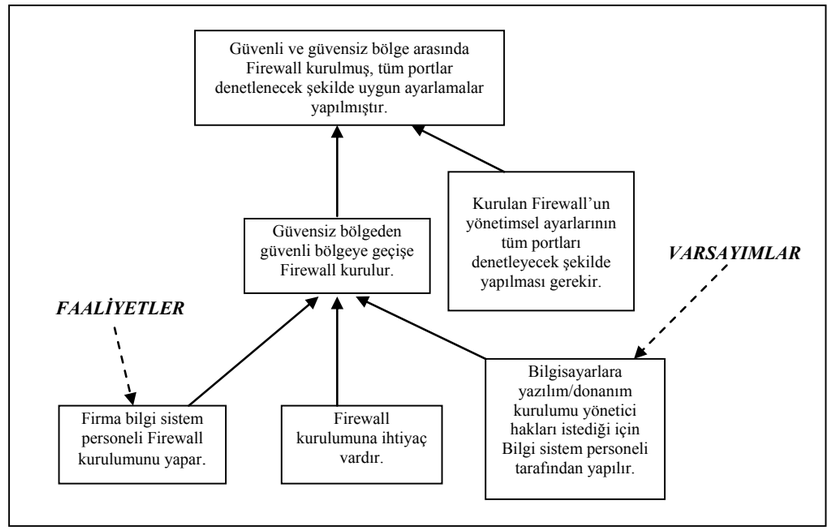
Şekil 16'da kullanıcı personelin sisteme bilinçli olarak zarar verildiğinin tespiti durumuna ilişkin geçiş ağacı görülmektedir. Burada istenen sonuç kullanıcı personelin bilinçli olarak sisteme zarar vermesinin engellenmesidir.



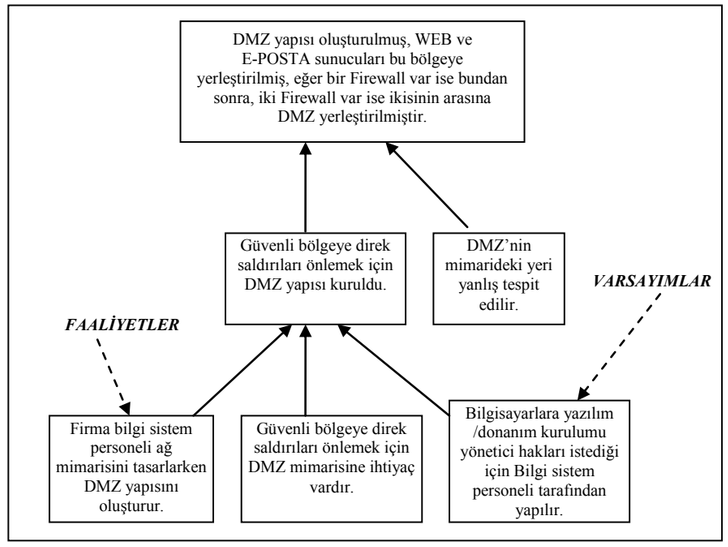
Şekil 10. Geçiş Ağacı-1



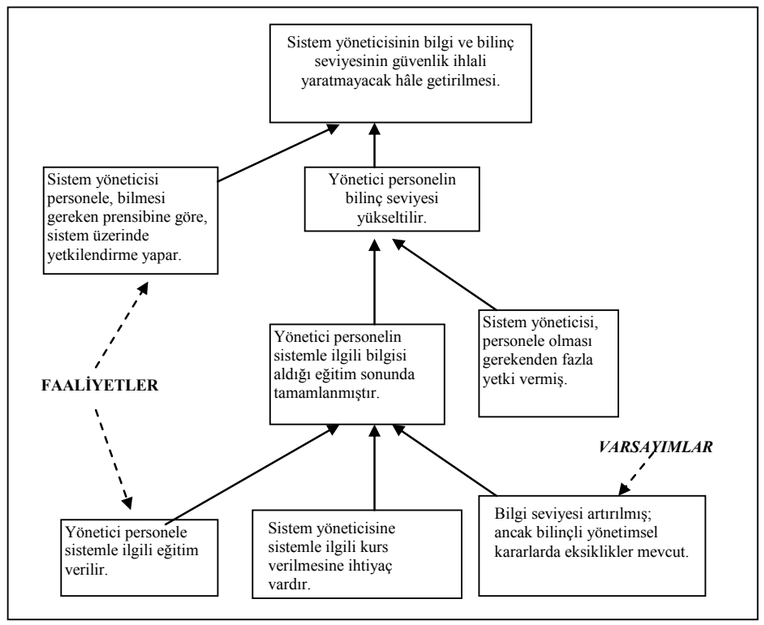
Şekil 11. Geçiş Ağacı-2



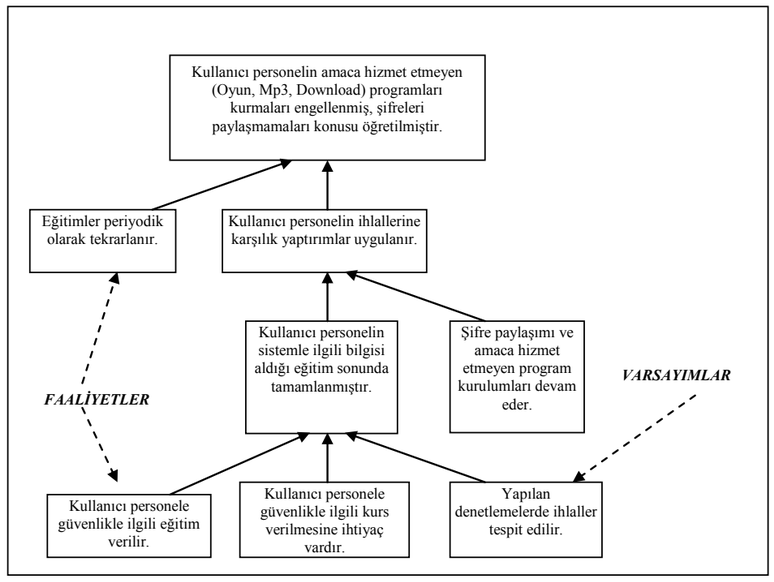
Şekil 12. Geçiş Ağacı-3



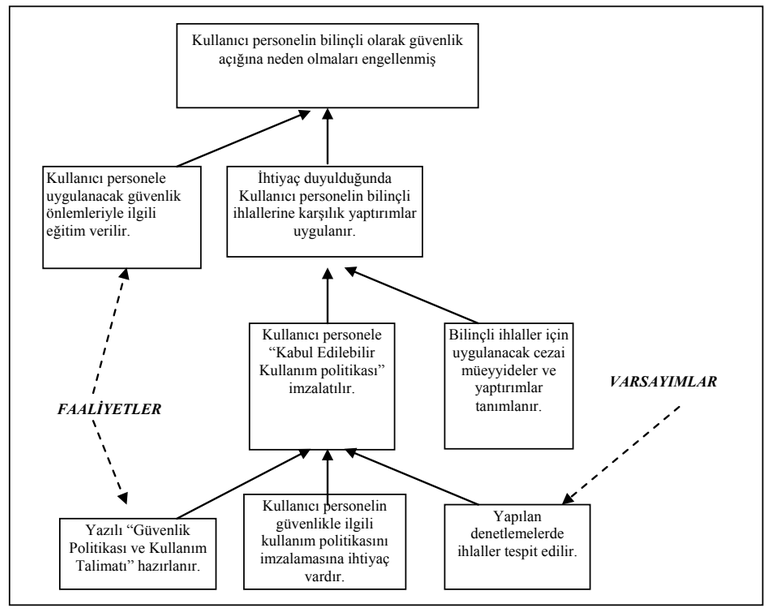
Şekil 13. Geçiş Ağacı-4



Şekil 14. Geçiş Ağacı-5



Şekil 15. Geçiş Ağacı-6



Şekil 16. Geçiş Ağacı-7

5. DEĞERLENDİRME VE SONUÇ

Şirket yerel alan ağlarının internet bağlantılarında güvenliğin sağlanması belki de şirketin var olması kadar önemlidir. Bu noktada alınacak güvenlik tedbirlerinin aslında politik birer kısıt olduğu karşımıza çıkmaktadır. Bilgisayar teknolojisi güvenlik politikası olmalı, politikanın arkasında yönetim olmalı, politika dışında insiyatif kullanımı yok edilmeli ve yönetim politikanın uygulanması talimatını yazılı vermelidir. Güvenlik politikaları oluşturulurken kurumun en alt düzeylerine kadar inerek gereksinimler belirlenmelidir. Ayrıca politikalar dikkatli bir şekilde uygulanmalıdır. Güvenlik politikasının etkinliği için üst yönetimin desteği sağlanmalı ve çalışanlar kullanılan politika konusunda bilgilendirilmelidir. Güvenlik politikası değişen tehditlere, zayıflıklara ve kurum politikalarına göre yeniden değerlendirilmeli ve gerekli değişiklikler yapılmalıdır.

Bir işletmede yerel alan ağ güvenliği konusunda ortaya çıkabilecek olası problemler genel hatlarıyla ele alınmaya çalışılmıştır. Çözüm önerileri geliştirilirken genel bir çerçeve çizilmeye çalışılmıştır. Alınacak ve uygulanacak önlemler, yapılacak yatırımlar, alınacak donanımlar ve yazılımlar organizasyonun özelliğine, firmanın/kurumun yapısına, kamu ya da özel oluşuna, firmanın/kurumun büyüklüğüne, firmanı/kurumun kritik öneme sahip olup olmamasına göre değişir. Her firma/kurum kendi bünyesine ve özelliklerine uygun güvenlik kurallarını ve politikalarını oluşturmalıdır. Bankalarda farklı güvenlik önlemleri alınması gerekir. Bir eğitim kurumunda, örneğin üniversitelerde uygulanacak güvenlik önlemleri farklı olacaktır. Örneğin genellikle bankacılık sektörünün sitelerinde yüksek güvenlikli önlemler alınırken ve maliyet açısından büyük yatırımlar yapılırken, bankalar haricinde diğer firmaların kendi sitelerine bu derece maliyetli yatırımların fazla görüldüğü gözlenmiştir.

Bu çalışmada kısıtlar teorisi düşünce süreçleri yaklaşımının bu makalede anlatılan türde problemlerin çözümünde ve çözüm önerileri geliştirilebileceği vurgulanmaya çalışılmıştır. Öncelikle mevcut durum analizi yapılarak güvenlik ağı problemlerinin sebepleri ortaya konmaya çalışılmıştır. Güvenlik ağındaki ana problem "*Şirket Yerel Alan Ağı'nın internet üzerinden*

saldırıya uğraması" olarak belirlenmiştir. Bu problemin nedenleri üç grupta toplanmıştır; donanımdan kaynaklanan güvenlik açıkları, yazılımdan kaynaklanan güvenlik açıkları, personelden kaynaklanan güvenlik açıkları. Daha sonra bu problemlerle ilgili çözüm önerileri geliştirilmiştir. Bunun için buharlaşan bulut tekniği kullanılmıştır ve yedi çözüm önerisi için on dört enjeksiyon tanımlanmıştır. Sonraki aşamada istenmeyen durumlar ve olumsuzluklar ortadan kalktıktan sonra arzu edilen durum tanımlanmıştır. Arzu edilen durum ve istenilen etki "*her türlü güvenlik önlemi alınmış internet bağlantılı şirket yerel alan ağ*" olarak tanımlanmıştır. En son olarak çözüm önerilerinin nasıl hayata geçirileceği konusunda yedi tane geçiş ağacı tanımlanmıştır. Görüldüğü gibi kısıtlar teorisinin düşünce süreçleri sistem analizi yaklaşımını kullanan bir metodolojidir. Çeşitli problemlerin analiz edilmesinde kolaylıkla uygulanabilir.

KAYNAKÇA

1. Akman, G., Karakoç, Ç. 2005. "Yazılım Geliştirme Prosesinde Kısıtlar Teorisinin Düşünce Süreçlerinin Kullanılması," İstanbul Ticaret Üniversitesi Fen Bilimleri Dergisi, 4 (7), 103-121.
2. Atwater, B., Gagne, M. 1997. "The Theory of Constraints Versus Contribution Analysis for Product Mix Decisions," Journal of Cost Manegement, 11 (1), 6-15.
3. Apohan, M. 2004. "Why is Security Policy Needed?," ICT Security 2004, 24-25 Mayıs 2004, İstanbul.
4. Cambazoglu, T. 2008. "Bilişimde Güçlü Güvenlik Politikalarından Ne Anlıyorsunuz? (I-II)" Http://Www.Bilisimrehber.Com.Tr. Son erişim tarihi:11.08.2008.
5. Canbek, G., Sağıroğlu, Ş. 2006. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme," Politeknik Dergisi, 9 (3), 165-174.
6. Corbett, T. 1999. "Making Better Decisions," CMA Magazine, November, 33-37
7. Davies, J., Mabin, V.J., Balderstone, S.J. 2005. "The Theory of Constraints : A Methodology Apart? – A Comparison with Selected OR/Msmethodologies," Omega, 33(6), 506-524.
8. Doğantimur, F. 2009. ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği, Maliye Bakanlığı Strateji Geliştirme Başkanlığı Mesleki Yeterlik Tezi, Ankara
9. Goldratt, E. M., Cox, J. 2004. The Goal: A Process of Ongoing Improvement, 3nd Revised Edition, North River Pres Inc., USA., 45-48.
10. Goldratt, E.M. 1990. What is This thing Called Theory of Constraints and How Should It Be Implemented, North River Pres, Great Barrington, 3rd ed.
11. Heywood, N., Heywood, M. 1999. "Internet Ağı Yönetimi, Bileşenleri ve Önemi," V. Türkiye'de İnternet Konferansı, 19-21 Kasım 1999, http://inet-tr.org.tr/inetconf5/oneri/zincir.doc. Son erişim tarihi: 20.12.2010.
12. Kahya, E. 2007. Bilgisayar Ağ Sistemleri Güvenliği, Akademik Bilişim 2007, 31 Ocak - 2 Şubat 2007, Dumlupinar Üniversitesi, Kütahya, http://ab.org.tr/ab07/bildiri/ab07-32-erhan_kahya.doc. Son erişim tarihi: 15.12.2009.
13. Karaarslan, E., Teke A., Sengonca H. 2003. Bilgisayar Ağlarında Güvenlik Politikalarının Uygulanması. Akademik Bilisim, Çukurova Üniversitesi, 1s.
14. Karaaslan, E. 2009. "Ag Güvenlik Duvarı Çözümü Olustururken Dikkat Edilmesi Gereken Hususlar," http://csirt.ulakbim.gov.tr/dokumanlar/GuvenlikDuvariCozumuOlusturma Sureci.pdf. Son erişim tarihi: 19.12.2009
15. Khatiwala, T., Swaminathan, R. Venkatakrishnan, V.N. 2006. "Data Sandboxing: A Technique for Enforcing Confidentiality Policies," Information systems security applications, Technological developments and the last techniques, ACSAC 2006-Annual Computer Security Applications Conference, Florida/USA, 11-15 December.
16. Kelleci, M.A. 2003. Bilgi Ekonomisi, İş Gücü Piyasasının Temel Aktörleri ve Eşitsizlik: Eğilimler, Roller, Fırsatlar ve Riskler Yayın No: DPT. 2674
17. Koçnet. 2004. Koç.net Türkiye İnternet Güvenliği Araştırması Sonuçları, Bilgisayar Bilimleri Araştırma ve Uygulama Merkezi, http://bilisim.istanbul.edu.tr/guvenlik/index.asp?grp=gDuyurular&no=8. Son erişim tarihi: 15.12.2009.
18. Köksal, G., Karşılıklı, K.U. 2000. "Kısıtlar Teorisi ve Toplam Kalite Yönetimi Yoluyla Etkin Performans Yönetimi ," 9. Ulusal Kalite Kongresi Toplam Kalite Yönetimi ve Kamu Sektörü, İstanbul, 21-22 Kasım.
19. Louderback, J., Patterson, J.W. 1996. " Theory of Constraints Versus Traditional Management Accounting," Accounting Education, 1 (2),189-196.
20. Mabin, V.J., Balderstone, S.J. 2003. "The Performance of The Theory of Constraints Methodology, " International Journal of Operations and Productionn Management, 23, 5/6, 572.
21. Pro-G ve Oracle. 2003. Bilişim Güvenliği v-1, Pro-G Bilişim Güvenliği ve Araştırma Ltd. ve Oracle, http://www.pro-g.com.tr/whitepapers/bilisim-guvenligi-v1.pdf. Son erişim tarihi: 15.02.2011
22. Rahman, S. 1998. " Theory of Constraints: A Review of The Philosopy and its Applications," International Journal of Operations and Productionn Management, 18, 336-355.
23. Spencer, M.S., Cox, J.F. 1995. " Master Production Scheduling Development in a Theory of Constraint Environment, " Production and Inventory Management Journal, First Quarter, 8-15.
24. Stein, R. E. 1997. The Theory of Constraints Aplications in Quality and Manufacturing, 2nd Edition, Marcel Dekker Inc., New York, USA 1,13-16, 306.
25. Taylor, P. 2003. Virtual Vulnerability, Financial Times, April 2, 2003.
26. TBD. 2008. Bilişim Sektörü Güvenlik Grubu, http://www.tbd.org.tr/genel/bsgg.php. Son erişim tarihi: 21.06.2008
27. Tekerek, M. 2008. "Bilgi Güvenliği Yönetimi," KSÜ Fen ve Mühendislik Dergisi, 11(1), 132-137
28. Ural, Ö., Akman, G. 2006. "Using of Thinking Processes of TOC to Define and Eliminate Bottlenecks of Company Local Area Network Internet Connection," ISEECE 2006-3rd International Symposium on Electrical, Elektronic and Computer Engineering, Near East University, 23-25 Kasım (2006), Nicosia, Northern Cyprus.
29. Ural, Ö. 2007. "Yerel Alan Internet Bağlantılarında Güvenliğin Sağlanmasında Kısıtlar Teorisinin Düşünce Süreçlerinin Kullanılması," Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Basılmamış Yüksek Lisans Tezi
30. Yaralıoğlu, K. 2007. Kısıtlar Teorisi, Dokuz Eylül Üniversitesi, http://www.deu.edu.tr/userweb/k.yaralioglu/dosyalar/kis_teo.doc. Son erişim tarihi:18.12.2007