GU J Sci, Part C, 6(3): 507-523 (2018)

Gazi Üniversitesi

Fen Bilimleri Dergisi

PART C: TASARIM VE TEKNOLOJİ

dergipark.gov.tr/http-gujsc-gazi-edu-tr

Kurum İçi Saldırıların Tespiti ve Önlenmesi için Sunucu İzleme Uygulaması

Halil İbrahim ULUS[1], Mehmet DEMİRCİ[2,*]

[1]*Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Bilgi Güvenliği Mühendisliği Anabilim Dalı, 06500, Yenimahalle/ANKARA*

[2]*Gazi Üniversitesi, Mühendislik Fakültesi, Bilgisayar Mühendisliği Bölümü, 06570, Maltepe, Çankaya/ANKARA*

Makale Bilgisi

Başvuru: 12/11/2017
Düzeltme: 08/04/2018
Kabul: 10/04/2018

Anahtar Kelimeler

Kurum İçi Saldırı
İç Tehdit
Veri Sızdırma

Keywords

Insider Attack
Insider Threat
Data Leakage

Öz

Son yıllarda büyük bir hızla artan kurum içi saldırılar, çok büyük zararlara sebep olsa da, bu problemi araştıran ve çözüm önerisi getiren çok az sayıda akademik çalışma bulunmaktadır. Bu saldırıların pek çoğu prestij kaybı, rakip firmaların avantaj sağlaması gibi nedenlerden ötürü saklanmakta, hatta yasal işlem yapılmakta dahi tereddüt edilebilmektedir. İç saldırıların dış saldırılardan temel farkı, saldırıları gerçekleştiren kişilerin kurumdaki yetkili kullanıcılar olmasıdır. Bu durum dışa karşı uygulanan güvenlik tedbirlerinin faydasız kalmasına sebep olmakta ve zafiyetlerin istismarını kolaylaştırmaktadır. Kurum içi saldırıların tespitinde, tüm sıra dışı olayların titizlikle incelenmesi gerekmektedir. Bu yüzden, öncelikle kurum içi saldırılara karşı hassasiyetlerinin belirlenmesi için risk değerlendirmesi yapılmalı ve bu doğrultuda gerekli önlemler alınmalıdır. Bu çalışmada kurum içi saldırıların genel özellikleri ve geçmişteki saldırılar incelenmiş, en çok kullanılan saldırı yöntemlerinin emaresi olarak değerlendirilen şüpheli hareketlerin tespit edilmesi amacıyla sunucu izleme ve takip sistemi (SİTS) uygulaması geliştirilmiştir. Bu uygulamadan elde edilen bulgular ve istatistiksel veriler sayesinde kurumlar, hem risk düzeyleri hakkında bilgi sahibi olacak hem de kaydedilmiş verileri analiz ederek saldırılara karşı hazırlık düzeylerini ve muhtemel saldırganları tespit etme kabiliyetlerini artıracaklardır.

Server Monitoring Application for Insider Attack Detection and Prevention

Abstract

Although insider attacks have increased rapidly in recent years and cause enormous damages, there are very few academic studies that have investigated this problem and proposed a solution. Many of these attacks are kept private for reasons such as loss of prestige and advantage of competing companies. The main difference between insider attacks and external attacks is that in the former case, attackers are authorized users in the organization. This causes countermeasures against external attacks to be useless and facilitates the exploitation of weaknesses. In the detection of insider attacks, all unusual events need to be scrutinized. Therefore, risk assessment should be done first to determine vulnerabilities against insider attacks and necessary precautions should be taken in this direction. In this study, general insider attack features and past attacks were investigated, and a server monitoring application was developed to detect suspicious activities. Organizations using this system will be informed about their level of risk, and improve their level of preparation and ability to identify potential attackers by analyzing the collected data.

1. GİRİŞ (INTRODUCTION)

Kurumlar çalışma ortamında sürekli olarak dış ve iç tehditlerle karşı karşıya kalmaktadırlar. 1980'lerden beri potansiyel güvenlik problemi olarak tanımlanan kurum içi saldırılarda yasal çalışanlar yetkilerini istismar ederek kuruma kolayca büyük zarar verebilirler. Kurumların neredeyse tümü kritik bilgisayar varlıklarına karşı yapılan iç saldırılarla karşılaşmıştır. Kurum içi saldırılar kısa vadeli finansal kayıpların ötesinde, uzun vadede müşteri ve saygınlık kaybına da sebep olabilmektedir [1]. Ancak, dış saldırılara büyük önem veren pek çok organizasyon, aynı yaklaşımı iç saldırılar için sergilememektedir. İç saldırılar güvenlik sistemlerini etkileyen, baş etmesi en zor ve en ciddi problemlerden birisidir. Çalışanlar

*Mehmet DEMİRCİ, e-mail: mdemirci@gazi.edu.tr

DOI: 10.29109/gujsc.351365

yetkileriyle orantılı olarak kuruma ve sistemlere zarar verme potansiyeline sahiptir, çünkü iç saldırganlara dönüştüklerinde fiziksel (elektronik bina giriş sistemleri) ve teknik (güvenlik duvarı, saldırı tespit sistemi) güvenlik önlemlerini kolayca atlatabilirler. Dahası, iç saldırganlar kurumdaki politikaların, prosedürlerin ve teknolojik açıklıklarının farkındadırlar. Bu sebepler iç saldırıları tahmin etmeyi ve önlemeyi oldukça zor hale getirmektedir [2].

İç tehditler hakkında çoğu zaman kesin bilgilere ulaşmak zordur. Bunun sebepleri arasında;

- Suçla ilgili kesin olmayan tanımlamalar (Saldırgan çoğu zaman yaptığı şeyin suç olmadığını savunur),
- Belirsiz politikalar (izin verilen ve yasaklanan eylemlerin belirsizliği),
- Veri miktarının fazlalığı ve veriyi incelemenin zorluğu,
- Paylaşma isteksizliği (kamu ve diğer kurumlar nezdinde itibar kaybı, kanuni yaptırımlar, çalışanlar üzerinde moralsizlik gibi faktörler nedeniyle),
- Mahremiyet nedeniyle verileri toplama ve paylaşma zorluğu yer almaktadır [3].

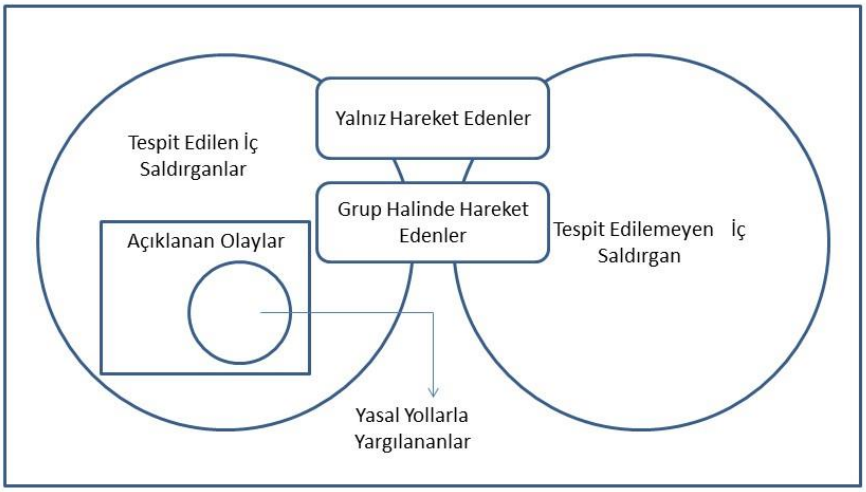
Tüm bu hususlar değerlendirildiğinde iç saldırıların önceden tespiti oldukça güç olmaktadır. Çoğu zaman iç saldırılar tespit edilemeyebilir veya zararları organizasyon tarafından hiç fark edilmeyebilir. Kurum içi saldırganlardan yakalanarak hakkında yasal yollara başvurulanların oranı oldukça azdır (Şekil 1).

Bu çalışmada kurum içi saldırıların tespitini kolaylaştırmak ve potansiyel saldırganları caydırmak amaçlarına yönelik bir yaklaşım ve yazılım geliştirilmiştir. Yaklaşım, çalışanların belirli sistemler üzerindeki hareketlerinin izlenmesi ve şüpheli olanlarla ilgili alarm üretilmesi mantığına dayanmaktadır. İç saldırı emaresi olabilecek hareketlerin belirlenmesi için basına yansımış iç saldırılar ve ilgili akademik literatür incelenerek bu tür saldırıların çeşitli özellikleri ortaya koyulmuştur.

Bu çalışmanın yaptığı katkılar aşağıda belirtilmiştir.

- İç saldırı türleri, iç saldırıların etkileri ve iç saldırılara karşı alınması gereken önlemler hakkında kapsamlı bir inceleme yapılmıştır.
- İç saldırıların tespitine yönelik geliştirilen Sunucu Takip ve İzleme Sistemi (SİTS) yazılımı sunulmuştur.
- Geliştirilen yazılımın farklı iç saldırı senaryolarında, saldırının tespitini sağlamadaki katkısı değerlendirilmiştir.
- Kurum içi saldırılar ile ilgili Türkçe terminolojiye katkı sağlanmıştır.

Kurum içi saldırıların oluşum aşamasında somut delillere ulaşmak zordur. Bu yüzden yapılan bu çalışmada şüpheli hareketler tespit edilmeye çalışılmış, bu hareketlerin saldırıya dönüşmeden önlenmesi veya gerçekleşen bir saldırının en kısa sürede tespit edilmesi amaçlamıştır. Geliştirilen SİTS uygulaması ile kurumların iç saldırılara karşı risk düzeylerini belirleyebilmeleri için istatistiksel verilerin temini ve riski kabul edilebilir seviyeye çekmek için alınan önlemlerin sonuçlarının takibi mümkün olacaktır.



Şekil 1. *İç saldırıların tespit edilme durumları [4] (Detection of insider attacks)*

Makalenin geri kalanı şu şekilde düzenlenmiştir: İkinci bölümde literatürdeki çalışmalar ve sonuçları incelenmiş, üçüncü bölümde ise iç saldırılar tüm yönleriyle ortaya konarak açıklanmıştır. Dördüncü bölümde bu saldırılara karşı geliştirilen SİTS uygulaması tanıtılmış ve saldırılara karşı elde edilen kazanımlar belirtilmiştir. Beşinci bölümde SİTS'in bazı somut saldırı girişimlerinde nasıl çalıştığı açıklanarak etkileri tartışılmış, altıncı bölümde çalışmanın sonuçları ve gelecekteki çalışmalar üzerinde durulmuştur.

2. LİTERATÜR TARAMASI (LITERATURE REVIEW)

İç saldırıların ülkelere verdiği tüm zararlara rağmen yapılan akademik çalışmalar veya bu alanda yapılan yatırımlar yeterli düzeyde değildir. Yapılan çalışmaların çoğu farkındalık oluşturma üzerinedir, ancak özellikle ülkemizde bu konuda yetişmiş personel konusunda sıkıntı yaşanmaktadır. Örneğin Gökmen ve Akgün'ün yaptığı çalışmada öğretmen adaylarının bilişim güvenliği eğitimi verebilmeye yönelik yeterlilik algıları tespit edilmeye çalışılmıştır. Adaylarının çoğunun bilişim güvenliği konularını öğretebilme açısından yeterli olmadıkları, bu konuda bir kurs veya ders almadıkları tespit edilmiştir. Eğitmenlerin dahi bu konuda yetkin olmaması, verilen eğitimin ve öğrencilerde oluşan farkındalık seviyesinin yeterli düzeye ulaşamamasına sebep olmaktadır [5].

Yapılan çalışmaların odaklandığı diğer bir konu da, hassas bilgilere herkesin erişmesini önlemek için kimlik doğrulama sistemlerinin güçlendirilmesidir. Bu konuda Cheon ve diğerlerinin yaptığı çalışmada, veri sızıntılarının önlenmesi için üç aşamalı kimlik doğrulama mekanizması önerilmektedir. Bu öneriye göre, sistem önce çalışanların kimlik bilgilerini sorgulayacaktır. Daha sonra sistem kişinin yasal kullanıcı olup olmadığını doğrulamak için güvenlik kartı, şifreleme anahtarı veya biyolojik özellikleri (iris, yüz, parmak izi) gibi ikincil kimlik doğrulama unsurlarını kontrol edecektir. Çalışmada iki seviyenin de kopyalanma veya taklit edilme imkanı bulunduğu söylenmekte ve biyolojik sinyalleri içeren başka bir kimlik doğrulama yöntemi önerilmektedir. Bu sayede bu özellikler gerçek zamanlı değiştiğinden taklit edilme imkanı bulunmayacaktır. Kullanıcı iki seviyeyi geçtikten sonra üçüncü seviyede hassas bilgilere erişmeye çalıştığında biyometrik sinyaller karşılaştırılacak ve eşleşme sağlandığında bilgilere ulaşabilecektir. Bunun için de çalışmada deriden alınan sinyallerin kullanılması önerilmektedir [6].

İç saldırıların önlenmesine yönelik çalışmalardan bazıları da ağdaki verilerin yetkisiz kişilerin eline geçmemesi için verilerin işaretlenmesi veya şifrelenmesi üzerinedir. Bu konuda Canbay ve Sağıroğlu'nun yaptığı çalışmada veri kaçağının tespiti için kullanılan şifreleme yöntemlerinden bahsedilmiş, probleme ajanlar arasındaki paket transferinin kontrolüyle çözüm bulunmaya çalışılmıştır. Yapılan çalışmada literatürde bulunan sahte nesne ekleme, RSA ile şifreleme, damgalama, dosya parmak izi kontrolü yöntemlerinden bahsedilmiş; damgalama ve RSA yöntemlerinin beraber kullanıldığı bir çözüm önerisi sunulmuştur. Bu yöntemde öncelikle veriye damga bilgisi işlenmekte, ardından RSA algoritmasıyla şifrelenerek bir nevi tuzak veri oluşturulmaktadır. Eğer veri şifrelenmemiş halde bulunursa mevcut damga bilgisini çözen özel anahtar; eğer şifrelenmiş halde bulunursa şifreyi çözen özel anahtar sahibi veri kaçağından sorumlu kişi olarak tespit edilmiştir [7].

Şüpheli hareketlerin tespiti için sınır değerler belirlenerek bunlar aşıldığında takip başlatılması veya veri tabanında kayıtlı izlere rastlandığında alarm üretilmesi esasına dayanan çalışmalar da bulunmaktadır. Kongsgard ve diğerlerinin yaptığı çalışmada iç saldırgan tehdit skoru belirlenmeye çalışılmıştır. Veri sızıntısını önleme sistemlerinden (DLP) elde edilen veriler doğrultusunda ve oluşturulan algoritmalar yardımıyla çalışanlar için tehdit skoru belirlenmiştir. Çalışmada günlük skorlar doğrultusunda durum takvimi oluşturulmuştur. Skorda ani artış, düzensizlik veya olağandışı seviyeler oluştuğunda alarm üretilmesi ve kurumun bu sayede önlem alması hedeflenmiştir. Örneğin bir çalışan hafta sonları erken saatlerde işyerine gelmeye başladığında bu skorda ani bir artış meydana gelecek ve durum araştırılmaya başlanacaktır [8].

Sahte belge ekleme ve balküpü gibi tuzak sistemler kullanmayı öneren çalışmalar da literatürde yer bulmuştur. Kashi ve diğerlerinin yaptığı çalışmada verileri ajanlara dağıtan bir algoritma geliştirilmiştir. Ayrıca dağıtılan bu verilere gerçek gibi gözüken sahte objeler (bir nevi imza) eklenmiştir. Eğer ajanlar bu sahte objelerden bir veya daha çoğunun izlerini tespit ederse alarm vermektedir. Birden çok alarm oluştuğunda yönetici o kullanıcıyı takibe almaktadır [9].

Yapılan tüm bu çalışmalar incelendiğinde iç saldırı yöntemlerinin tümünün tek bir çözüm önerisiyle engellenmesinin mümkün olmadığı görülmektedir. İç saldırganların genellikle yetkili kişiler olması nedeniyle tüm çalışanların bir gün saldırgana dönüşebileceği varsayımıyla hareket edilmeli ve çalışanların sistemler üzerindeki hareketleri mahremiyeti ihlal etmeden izlenmelidir. Oluşan tüm şüpheli durumlar titizlikle incelenmeli ve bu konuda farkındalık oluşturulmalıdır.

3. KURUM İÇİ SALDIRILARIN ÖZELLİKLERİ VE ALINABİLECEK ÖNLEMLER (PROPERTIES OF INSIDER ATTACKS AND PRECAUTIONS)

3.1. İç Saldırgan Çeşitleri (Insider Types)

Kurum çalışanı, kurumun sistemleri ve sistem araçları hakkında bilgi sahibi olan, güvenilir olduğu kabul edilen, kurumun bilgisayarlarına ve ağlarına yasal olarak girmeye yetkili kişilerdir [10]. İç saldırgan; kurumun ağına, sistemine veya verilerine erişmeye halen veya önceden yetkili olan; kurumun bilgi ve bilgi sistemlerinin gizliliğini, bütünlüğünü, erişilebilirliğini bilerek veya bilmeyerek olumsuz etkileyen belli davranışları sergileyen iş ortakları, yüklenici firmalar, şimdiki veya geçmiş çalışanlar olarak tanımlanır [11].

İç saldırgan çeşitleri genel olarak dörde ayrılmaktadır [12]:

- Kurum çalışanları (pure insider)
- Kurum içi ortaklar (yüklenici firma, güvenlikçi, temizlikçi vb.)
- İç bağlantılar (arkadaş, eş, müşteri)
- Dış bağlantılar (eski çalışan, dışarıdan erişim hakkın edinmiş kurum dışı kişi)

Bu kategorilere giren kişilerin her birinin muhtemel hareket tarzları değerlendirilip organizasyonun bilgi güvenliği politikalarına eklenmelidir. Güvenlikçilerin dahi hangi alanlara girebilecekleri, temizlikçilerin nereleri, ne zaman temizleyecekleri, ziyarete gelen aile yakınlarının veya arkadaşların yapmaması gereken hareketler gibi kurallar detaylı bir şekilde belirlenip tüm çalışanlara bildirilmelidir.

3.2. Kötü Niyetli İç Tehdit Kategorileri (Malicious Insider Threat Categories)

Kötü niyetli iç tehdit çeşitlerini yedi başlık altında sıralayabiliriz. Bu tehditlerin ortak özelliği bilerek ve isteyerek mensubu oldukları kuruma zarar vermektir [16].

İç BT Sabotajı: Çalışanlar kendilerini baskı ve stres altında hissettiklerinde, kendilerine zarar geleceğini düşündüklerinde veri tabanları, sistemler, ağ cihazları gibi hedeflere zarar vermeyi seçebilirler. Örneğin ABD'de bir finans sektörü çalışanı yıllık ikramiye hakkındaki anlaşmazlık nedeniyle bir mantık bombası hazırlayarak firmadaki sisteme yüklemiş ve işten ayrıldıktan sonra bu bombayı çalıştırmıştır. Bu saldırı 1300'den fazla sunucuyu etkileyerek toplam 3 milyon dolar civarında kayba yol açmıştır [16].

İç BT Hırsızlığı: Çalışan, yetkilerini kişisel çıkarları için kullanabilir. Bu ihlal, verileri değiştirmek, silmek, bazı durumlarda gizli bilgileri satmak şeklinde olabilir. Bu durum bilgilerin gizliliğini ve bütünlüğünü etkiler. Ekonomik güçlük yaşayan çalışanlar bilgi teknolojileri hırsızlığına daha meyilli olabilmektedir.

Fikri Mülkiyetin Çalınması: Organizasyondaki çalışanlar üretilen değerlere dair fikri mülkiyet hakkının kuruma değil kendilerine ait olduğunu düşünerek çalma yoluna gidebilirler. Bunu yaparken finansal kazanım amacı da gözetebilirler. Bu durumda özellikle organizasyonun sahip olduğu bilgilerin gizliliği tehdit edilir.

Sosyal Mühendislik: Saldırganlar yetkileri olmadığı halde gizli bilgilere ulaşabilmek için oltalama araçları yardımıyla masum çalışanlardan kullanıcı adı ve parolalarını elde ederek saldırı gerçekleştirebilirler. Bu durumda saldırı kurumun yetkili bir çalışanının hesabı üzerinden yapıldığı için iç saldırı olarak değerlendirilir.

İstem Dışı İç Tehdit Olayları: Bazı zararlı davranışlar kazara ortaya çıkar. Kritik bilgileri tutan taşınabilir depolama cihazlarının (disk, flash bellek gibi) kaybedilmesi veya işle ilgili önemli bir telefon konuşmasının kurum dışından biri tarafından duyulması gibi durumlarda herhangi bir saldırı motivasyonu olduğu söylenemez ancak dikkatsizlik veya tedbirsizlikten söz edilebilir.

Bulut Bilişimde İç Tehdit: Kurumda kullanılan bulut sistemlerinin açıkları yüzünden veriler tehdit altına girebilir. Bulut sağlayıcının altyapısına müdahale edilemediği için bu tehdide karşı yapılabilecekler sınırlıdır.

Ulusal Güvenliğe Yönelik İç Tehdit: Casusluk, sabotaj, bilgileri açığa çıkarmak gibi faaliyetleri içerir. Organizasyonun ve ülkenin bilgi güvenliğine en fazla zarar veren; ayrıca saldırganın motivasyonunun ve yeteneğinin üst seviyede olduğu bir tehdit durumudur.

3.3. Kurum İçi Saldırının Unsurları ve Veri Sızdırma Yöntemleri (Elements of Insider Attacks and Data Leakage Methods)

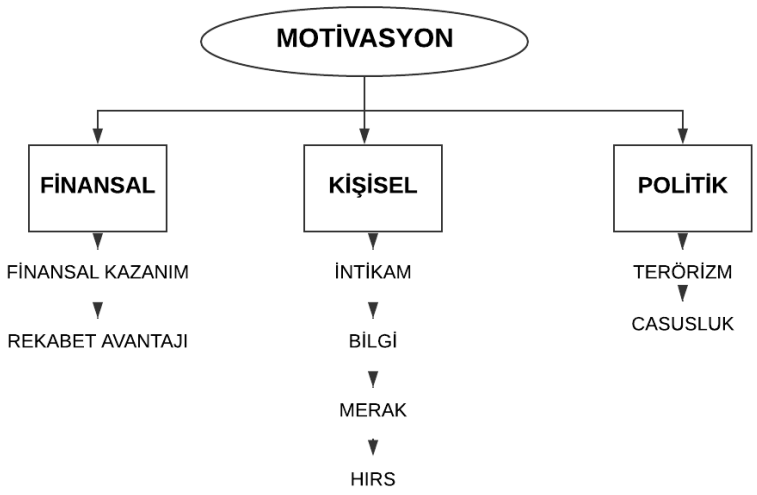
Kurum içi saldırının gerçekleşebilmesi için iç saldırganın sahip olması gereken üç unsur bulunmaktadır [13].

- Motivasyon
- Fırsat
- Yetenek

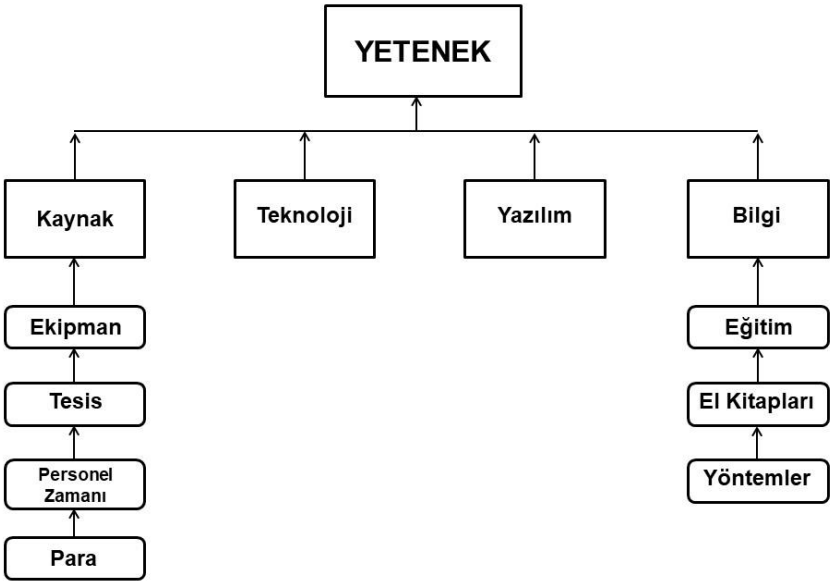
Saldırganların saldırıları gerçekleştirmesinin ardında yatan sebeplere motivasyon denebilir. Motivasyonlar genel olarak finansal, politik, kişisel olarak sınıflandırılabilir [3].

Saldırganın hayatını etkileyen maddi sıkıntılar finansal motivasyon olacaktır. Bilgi karşılığında verilen rüşvet, diğer bir şirkette iş vaadi veya kendisi için maddi rekabet avantajı elde edilmesi finansal motivasyonu somutlaştıran bazı durumlardır. Küresel ekonomik durgunluk, aşırı borçlanma, maddi hevesler iç saldırganların davranışlarını etkileyebilir. Politik motivasyonlar devlete veya kuruma zarar verme, terör yaratma, başka devlet veya şirket adına casusluk yapma gibi amaçları içerir. Kişisel motivasyonlar ise saldırganların şahsi hırsları, bilgi elde etme isteği veya hakkının yendiğini düşünüp intikam alma isteği gibi nedenlerdir [14]. İç saldırganın sahip olabileceği motivasyonlar Şekil 2'de gösterilmiştir.

Gerekli motivasyona sahip olan saldırgan bundan sonra uygun hedef ve fırsat arayışına girer. Bunun için organizasyonun zafiyetlerini analiz eder ve sahip olduğu yetenekleri, yetkileri ve pozisyonu kullanarak ulaşabileceği hedefi belirler. Yetkisi yetersizse, yakalanma ihtimali yüksekse, yaptıklarını gizlemek çok zahmetli ise veya amacına ulaşması zorsa başka hedeflere yönelecektir. Hedef seçiminden sonra sahip olduğu yetenekler yani kaynaklar, teknoloji, yazılım ve bilgi (Şekil 3) saldırının nasıl sonuçlanacağını belirleyecektir.



Şekil 2. *Motivasyon çeşitleri [14] (Types of Motivation)*



Şekil 3. *Yeteneği Oluşturan Unsurlar (Components of Competence)*

İç saldırılarda motivasyon, fırsat ve yeteneğe ek olarak yükseltici veya önleyici unsurlar da bulunabilir. Bir saldırgan için kimsenin şüphesini çekmemesi, güven veren bir karaktere sahip olması, kıdemli sistem yöneticisi olması vs. yükseltici; kurumda güvenlik görevlilerinin ve kameraların olması veya bilgi güvenliği tedbirlerinin alınmış olması ise önleyici unsurlar olacaktır.

Günümüzde veri depolama ve aktarma yollarının çeşitliliği ve ucuzluğu, kurum içinden veri sızdırmayı kolaylaştırmıştır. Veri sızdırmada yöntemler çok çeşitlilik göstermektedir; fakat en sık karşılaşılan üç yöntem bulunmaktadır: İş yerinden e-posta atma, taşınabilir bellek kullanma ve uzaktan ağa bağlanma. CERT'in 2010 yılındaki E-crime araştırmasına göre veri sızdırma suçu işlenirken kullanılan araçlar arasında ilk sırada %44 ile dizüstü bilgisayar, ikinci sırada ise %42 ile flash bellek, iPod gibi taşınabilir cihazlar gelmektedir [12]. Veri sızdırmada kullanılan bazı araçlar Tablo 1'de gösterilmiştir.

Tablo 1. *Veri sızdırma yöntemleri [15] (Data leakage methods)*

Sızdırma Yöntemi	**Açıklama**
E-posta	İç saldırgan veriyi iş yerindeki e-posta hesabını kullanarak sızdırır. E-posta kişisel e-posta hesabına gönderilebilir veya doğrudan rakip firmaya, dış devletlere, organizasyonlara gönderilebilir. Saldırgan e-postanın ek kısmına veya metin kısmına gizli bilgileri açık veya şifreli olarak ekleyebilir.
Taşınabilir Bellek	Yaygın taşınabilir bellek çeşitleri yani USB cihazları, bellek kartları, CD'ler, harici hard diskler gibi araçlar ile veri kopyalanarak kurum dışına çıkartılır.
Yazılı Dokümanlar	İç saldırganlar belgelerin çıktısını veya gizli bilgilerin ekran görüntüsünü alır ve sonra organizasyonun bilgisayarlarından kopyalarını siler.
Uzak Ağ Bağlantısı	İç saldırganlar uzaktan sanal özel ağ (VPN) gibi yollarla ağa bağlanır ve gizli bilgileri indirir.
Dosya Transferi	İç saldırgan işyerinde şirket ağından dosyaları FTP ile veya dosya transferi hizmeti sunan web siteleri vasıtasıyla dışarıya aktarır.
Dizüstü Bilgisayar	İç saldırgan işyerinde şahsi dizüstü bilgisayarına verileri indirerek sızdırır. Örneğin bir programcı şirket için dizüstü bilgisayarında bir uygulama geliştirir ve sonra kasıtlı olarak kaynak kodlarını sızdırır.

3.4. İç Saldırılardaki Muhtemel Hareket Tarzları (Possible Movement Patterns of Insider Attacks)

Yapılan bu çalışmada, iç saldırganın verileri fiziksel veya dijital olarak sızdırmasından önce şüpheli hareketlerini tespit ederek saldırıyı gerçekleştirmesini engellemek amaçlanmaktadır. Ayrıca literatürde

yapılan çalışmaların çok yetersiz olduğu görülmüş; bu kapsamda iç saldırılar ile ilgili kavramlar detaylı bir şekilde açıklanmış ve yabancı kaynaklı terimler Türkçeleştirilmiştir. İç saldırganların kullandığı yöntemleri içeren örnek olaylar analiz edilerek sıklıkla kullanılan iç saldırı yöntemleri doğrultusunda saldırı senaryoları belirlenmiş ve iç saldırganların aşağıda belirtilen hareketlerden birini veya birkaçını yapacağı varsayılmıştır.

- İç saldırıda bulut tabanlı dosya paylaşım programlarının kullanılacağı,
- Saldırının zararlı yazılımlar kullanılarak yapılacağı ve yazılımın arka planda servis uygulaması olarak çalışacağı,
- Saldırganın yetkisi olmayan dosyaları, kontrolün az olduğu mesai dışı saatlerde sızdırmak amacıyla inceleyeceği,
- Saldırganın güncel olmayan bir programda var olan açıklığı istismar ederek kurum bilgisayarlarına zarar vereceği,
- Saldırganın bazı portları kullanarak bilgisayarlara sızma amaçlı uzaktan bağlantı sağlayacağı,
- Saldırganın, sosyal mühendislik ile elde ettiği başka kullanıcının şifresini kullanarak mesai saati dışında oturum açacağı ve yetkisi olmayan dosyaları inceleyeceği ve çalacağı,
- DDoS gibi saldırı denemelerinin yapıldığı zamanlarda sunucuların RAM kaynaklarının tükeneceği ve CPU sıcaklığının aşırı yükselerek sunucu donanımının zarar göreceği,
- Saldırganın sistemlerin açıklıklarını ararken hatalara sebep olacağı, bu hataların tekrarlanacağı ve log kaydı olarak saklanacağı,
- Personelin gereksiz birçok program yükleyeceği ve kontrol edilmediği için sunucuların depolama alanının tükeneceği, sonucunda sunuculara erişilemeyeceği,
- Personelin izin verilmemesine rağmen gereksiz ve keyfi pek çok program yüklemesi nedeniyle sistemlerin yavaşlamasının yanında dış saldırganlar tarafından istismara açık hale geleceği varsayılmıştır.

3.5. Kurum İçi Saldırılara Karşı Risk Değerlendirmesi (Risk Assessment for Insider Attacks)

Kurum için bilgi güvenliğinde önemli kavramlardan biri risk analizidir. Sistemlerin güvenlik seviyesini tespit edip iyileştirebilmek için; var olan risklerin seviyelerini belirleyebilmek ve bunlara karşı tedbirler geliştirebilmek gerekmektedir. Bugüne kadar geliştirilmiş, özellikleri ve uygulama şekilleri farklı pek çok güvenlik çözümü mevcuttur. Bu çözümlerin en üstün olanlarından söz etmek anlamlı değildir çünkü bir çözüm yönteminin etkinliği uygulandığı organizasyonun şartlarına değişebilir. Bu amaçla, organizasyonların kendi ihtiyaçlarını karşılayacak en uygun yöntemi seçebilmelerine yardımcı olacak araçlara ihtiyaç duyulmaktadır [17]. Bu araçlardan en önemlisi risk analizidir. ISO 27001 BGYS standardı, kuruma ait tüm bilgi varlıklarının değerlendirilmesi ve varlıklar üzerindeki tehditler ve açıklıklar belirlenerek risk analizi yapılmasını gerekli kılar [18, 19].

Kurum içi saldırılar konusunda risk değerlendirmesi yaparken kurum dışından gelebilecek saldırılara karşı uygulanan risk analiz yöntemlerini kullanmak zorlaşmaktadır. Kurum içi saldırılarda çoğu zaman var olan açıklık, sonradan tehdide dönüşen öngörülemeyen kişiler tarafından kullanılmakta veya en önemlisi tehdit tarafından açıklık yaratılabilmektedir. Kurum içi saldırılara karşı risk değerlendirmesi yapmak için, uzun dönemde geçerli olacak somut ve doğru verilere ulaşmak oldukça zordur. Bu yüzden risk yönetimi kurum içi saldırılara karşı bir sonuç değil bir süreçtir ve kurumun bilgi güvenliği politikalarının belirlenmesinde önemli rol oynaması gerekmektedir.

Bir kurumda güvenliği sağlamakta kullanılan süreçler ve yöntemlerle ilgili belirsizlik ne kadar fazlaysa risk de o kadar artacaktır. Bu yüzden belirsizlik analiz edilmeli ve en aza indirgenmeye çalışılmalıdır. Risk yönetiminde belirsizliğin iki ana kaynağından söz edilebilir: (1) risk yönetim model veya yöntemlerindeki güven veya kesinlik eksikliği; (2) risk modeli bileşenlerinin (tehdit sıklığı, önlemlerin etkinliği ve sonuçları gibi) doğru değerlerini belirlemedeki bilgi eksikliği ve teknik zorluklar [17].

Bu çalışmada geliştirilen SİTS uygulaması kurum içi saldırılara karşı risk değerlendirmesi yapılabilmesi için belli dönemlere ait istatistiksel veriler sunar. Özellikle belirsiz bir unsur olarak gözüken tehdit değişkeni şüpheli hareketler başlıkları altında tanımlanır ve raporlar kısmı sayesinde ihlal sayıları tehdit faktörünün şiddet ve frekans miktarları hakkında sayısal değerler ortaya çıkarır. Bu sayede kurumun iç saldırılara karşı hassasiyet durumu ortaya çıkarılabilir. Ortaya çıkan sonuçlar doğrultusunda hassas

tarafları hakkında yönetime bilgi sağlanır ve bu doğrultuda gerekli önlemler alınarak risk seviyesi kabul edilebilir düzeylere çekilebilir.

3.6. Kurum İçi Saldırılara Karşı Alınması Gereken Önlemler (Measures Against Insider Attacks)

3.6.1. Yöneticilerin Önleyici Davranış Tarzları (Preventive Behavior by Administrators)

İç saldırganlar kendilerine yandaş bulmak veya çalışanların sahip oldukları bilgileri almak için insanları manipüle etmeye çalışırlar. Yöneticiler çalışanlarla aralarında güven ilişkisi kurarlarsa kullanıldıklarından şüphelenen kişiler bu durumları rahatça yöneticilerle paylaşabilirler. Yöneticiler nezaket, dürüstlük ve açık iletişim ilkelerine uygun hareket etmelidirler. Çalışanlarıyla aralarında geçen konuşmaları onların aleyhine kullanmamaları gerekir [3]. Ek olarak aşağıdaki hususlara dikkat edilmesi iç saldırıların önlenmesinde önemlidir.

- Çalışanların sözlerini küçümsemek, tehditleri göz ardı etmek tehlikelidir.
- Önlem almak için saldırı olmasını beklememek gerekir.
- Çalışanlar arasındaki sorunlar ve çekişmeler büyümeden çözülmelidir.
- Ekonomik durgunluk davranışlarda beklenmedik değişiklikler yapabilir. Bunlar dikkatlice izlenmelidir.
- İç saldırı riskleri ve etkileri paylaşılmalıdır. Bu sayede tecrübeler herkes tarafından bilinecek, aynı hatalar tekrarlanmayacaktır.
- Ayrıntılı bir işten ayrılma prosedürü geliştirilmelidir.
- İç ve dış tehditler arasında dengeli bir yatırım yapılmalıdır [20].

3.6.2. Yönetimin Alması Gereken Güvenlik Tedbirleri (Security Measures to be Taken by Administration)

Kurum içi saldırılara karşı ilgili yönetim birimi tarafından alınması gereken güvenlik önlemleri aşağıda sıralanmıştır: [21-23]

- Politikalar ile kontrolleri net ve düzgün bir şekilde belgelenmeli, sürekli uygulanmalı,
- Periyodik olarak tüm çalışanları kapsayan güvenlik farkındalık eğitimleri yapılmalı,
- İşe alımdan itibaren zararlı veya şüpheli hareketler izlenmeli ve bunlara zamanında müdahale edilmeli,
- Sahip olunan tüm varlıklar bilinmeli,
- Katı şifre ve hesap yönetim politikaları uygulanmalı,
- Eski çalışanların sistemlere erişimi engellenmeli,
- Görevlerin ayrılığı ve en az ayrıcalık ilkesi uygulanmalı,
- Katı giriş kontrolleri uygulanmalı, ayrıcalıklı çalışanlar için izleme politikası oluşturulmalı,
- Tüm hassas bilgiler ve iletişim şifrelenmeli,
- Mobil cihazlar dahil tüm uzaktan bağlantılar izlenmeli ve kontrol altına alınmalı,
- Güvenli yedekleme ve kurtarma prosedürleri uygulanmalı,
- Sosyal medya kullanımı konusunda dikkatli olunmalı,
- Veri sızıntılarına karşı portlar kapatılmalı,
- Resmi bir iç tehdit kriz / acil durum programı geliştirilmeli,
- Çalışanların hareketlerinin izlemek için bir log korelasyon motoru veya güvenlik bilgileri ve olay yönetimi (SIEM) sistemi kullanılmalıdır.

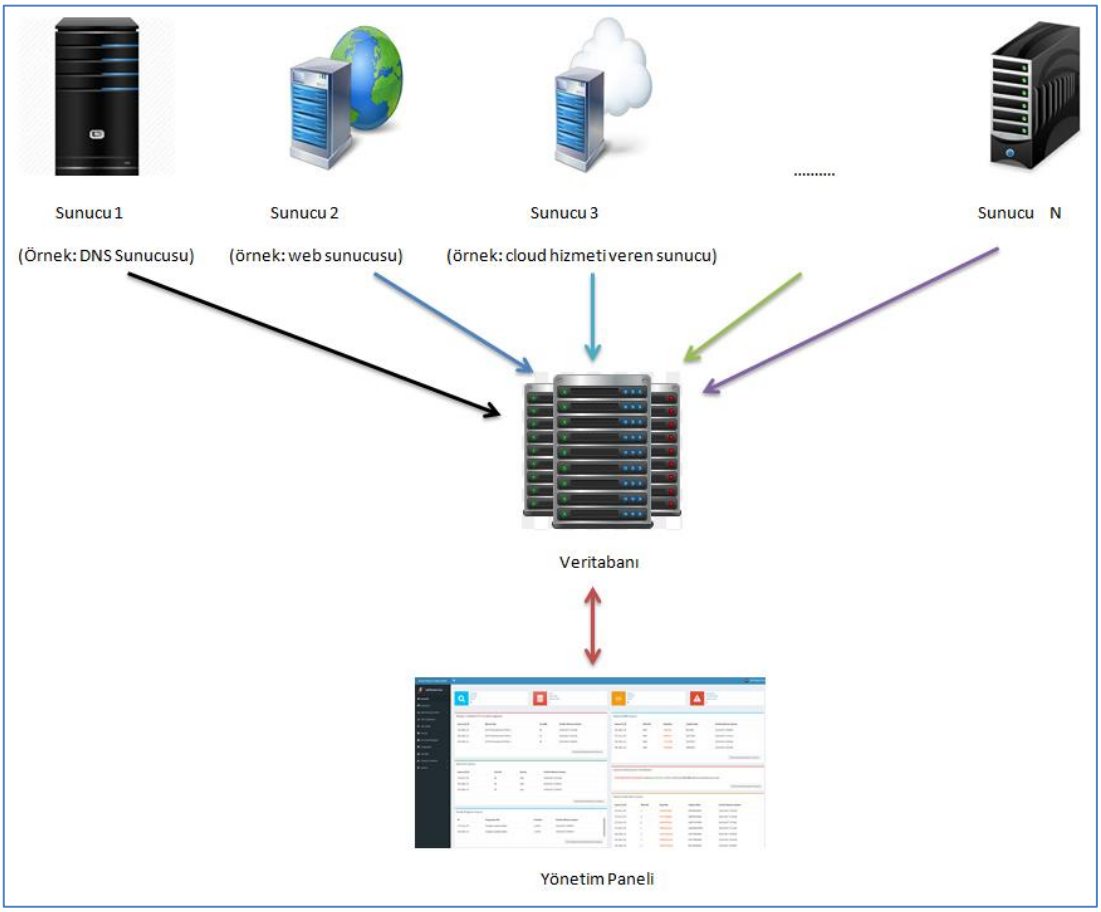
4. SUNUCU İZLEME VE TAKİP SİSTEMİ - SİTS (SERVER MONITORING AND TRACKING SYSTEM)

SİTS uygulaması, organizasyonların bilgi sistemlerinin ve birçok işlevinin sağlıklı çalışması için hayati öneme sahip sunucuların izlenmesi ve belirli kurallara uyan olayların kayıt altına alınması için geliştirilmiştir.

SİTS uygulaması Şekil 4'te görüldüğü gibi üç ana kısımdan oluşmaktadır;

1. Ajan
2. Veri tabanı

3. Yönetim Paneli



Şekil 4. *SİTS uygulamasının çalışma prensibi (Working principle of the application)*

Ajan, belirlenen sunucuların izlenebilmesi için sunuculara kurulan ve belirlenen kurallar çerçevesinde, belirli aralıklarla (bizim uygulamamızda 15 dakikada bir) sistem loglarını ve istenen diğer bilgileri merkezdeki veri tabanına gönderen bir servis uygulamasıdır. SİTS ajanı, Microsoft Visual Studio platformunda C# programlama dili kullanılarak Windows Service uygulaması olarak geliştirilmiştir.

Veri tabanı, sunuculara kurulan ajanlar tarafından gönderilen verilerin tutulduğu veri tabanıdır. SİTS'te veri tabanı yönetim sistemi olarak Microsoft SQL Server kullanılmıştır.

Yönetim paneli, ajandan gelen bilgilerin analiz edilerek, belirlenen kurallar doğrultusunda uyarıların gösterildiği ve istendiğinde logların detaylı bir şekilde incelenebildiği merkezi birimdir. Bu sayede toplu olarak gelen veriler anlamlandırılarak, yöneticinin ihtiyaç duyduğu bilgileri görmesi sağlanır. Yönetim panelinin geliştirilmesinde Microsoft Visual Studio .NET, Microsoft SQL Server ve Asp.NET Framework 4.5.2 kullanılmıştır.

SİTS uygulaması sayesinde, oluşabilecek kullanıcı veya sistem kaynaklı iç tehditlerin önceden tespit edilmesi amaçlanmaktadır. Sunucularda işlemcilerin aşırı ısınması, sistem yoğunluğundan dolayı RAM'in yetersiz kalması, sistemin çalıştığı diskin dolması gibi durumlara karşı alarmlar üretilmekte, böylece sunucu arızası ve sistem kesintisi gibi durumların önüne geçilmesi hedeflenmektedir. Yönetici tarafından belirlenen kapasitelerin altına düşüldüğünde veya işlemciler izin verilen sıcaklıkların üstüne çıktığında ana sayfada uyarı verilmekte, tercihe bağlı olarak yöneticiler e-posta ile uyarılabilmektedir.

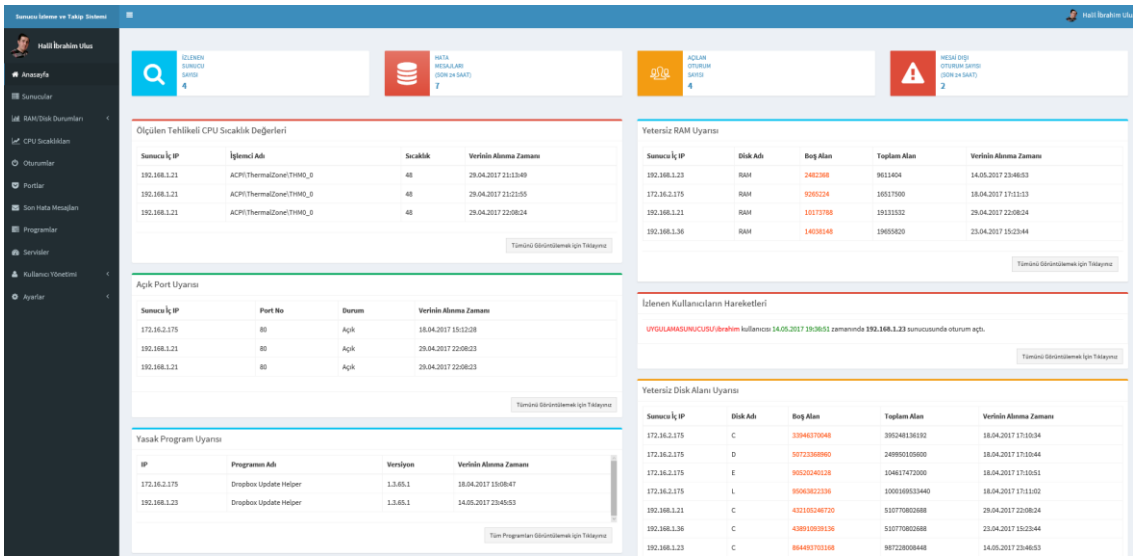
SİTS ajanının merkezdeki veri tabanına sürekli veri göndermeye çalışması fazla kaynak tüketimine sebep olacağından sunucular hakkında istenen bilgiler bir ajan vasıtasıyla 15 dakikada bir gönderilmektedir. Sunuculara kurulan ajan 15 dakika aralıklarla aşağıdaki fonksiyonları çağırmaktadır:

- disableusbports();
- sunucutablosunuguncelle();

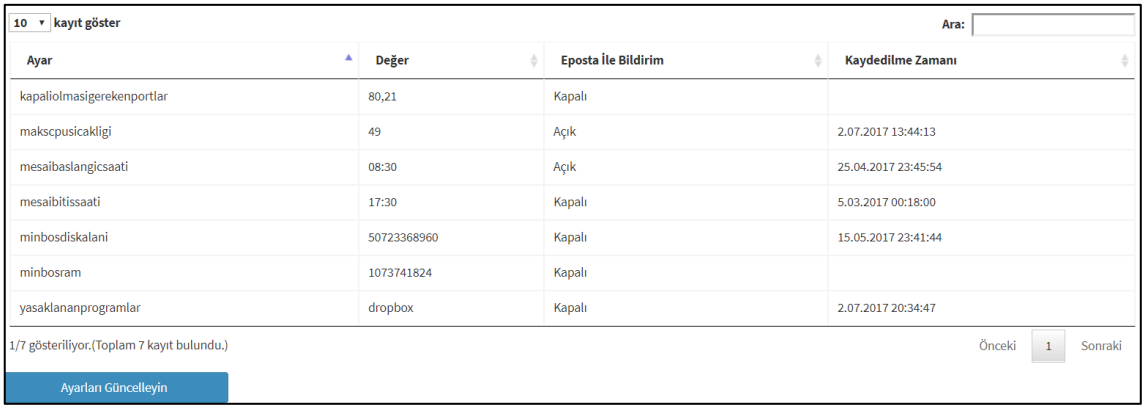
- porttablosunuguncelle();
- bellektablosunuguncelle();
- ServisTablosunuGuncelle();
- programtablosunuguncelle();
- oturumtablosunuguncelle();
- cpusicakligitablosunuguncelle();
- windowslogtablosunuguncelle();

İlk fonksiyondan anlaşılacağı üzere uygulamamız önce eğer açıksa sunucudaki USB portlarını kapatmaktadır. Böylece sunucu odasında bir USB belleğin sunucuya takılması riski ortadan kalkmaktadır. En son olarak gözden kaçan sunucularda oluşan diğer tüm hata ve uyarıların merkezdeki veri tabanına gönderilmesini sağlayan windowslogtablosunuguncelle() fonksiyonu çağrılmaktadır. Bu sayede sistem yöneticisi ilgili hata ve uyarıları inceleyerek hangisinin kritik olduğuna kendisi karar verebilir.

Yönetim panelinin ana sayfasında önceden tanımlanan kurallar ve oluşturulan korelasyonlar doğrultusunda Şekil 5'te görüldüğü gibi uyarılar gösterilmektedir. Oluşan uyarı mesajları kimi zaman saldırı hazırlığının bir göstergesi olabilir. Çünkü saldırganlar saldırının senaryosunu hazırlarken denemeler yaparlar ve başarısız denemeler hatalara sebep olur. Sorumlular tarafından bu uyarı mesajlarının çok iyi analiz edilmesi gerekir. SİTS yönetim panelinde yönetici tarafından "Ayarlar" kısmında belirlenen kurallardan biri ihlal edildiğinde ana sayfada uyarı oluşturulur (Şekil 6).



Şekil 5. *SİTS yönetim paneli genel görünüm (Management panel overview)*



Şekil 6. *Ayarlar bölümü (Settings section)*

Oluşturulan kurallar yardımıyla saldırı emareleri tespit edilebilmektedir. Kurum içi saldırı olayları incelenerek oluşturulan ve gerçekleşmesi halinde saldırı ihtimaline işaret eden şüpheli hareketler SİTS uygulamasında kural olarak belirlenmiş ve aşağıda sıralanmıştır.

Mesai Saati Dışında Oturum Açma

İç saldırıların birçoğu mesai saatleri dışında olmaktadır. Saldırganlar denetimin daha az olacağını düşündüklerinden yasal olmayan eylemlerini genellikle diğer personel mesaiyi terk ettikten sonra yapmaktadırlar. Mesai saatleri yönetim panelinin ayarlar kısmında belirlenebilmektedir. Bu saatler dışında giriş yapan kişiler ve bunların tüm bilgileri alarmlar kısmında gösterilmektedir. Örneğin, Şekil 7'de görüldüğü üzere kullanıcılar 18:40 ve 19:36'da oturum açmıştır.

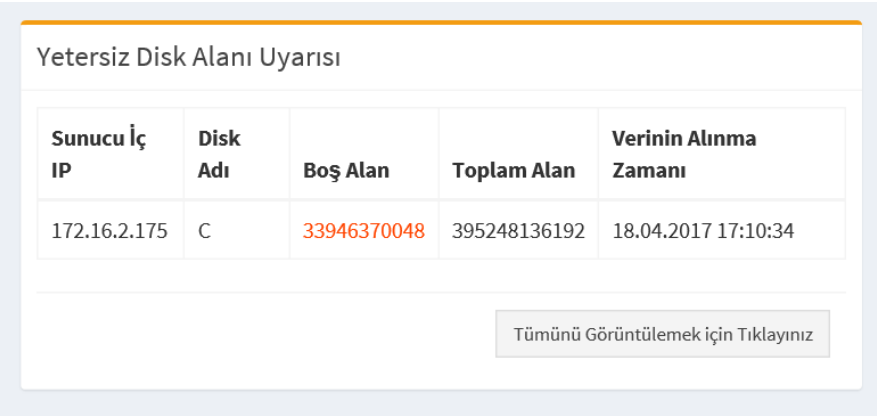
Disk Alanı Yetersizliğinden Sunuculara Ulaşılamaması

Bazen ne kadar basit gözükse de yalnızca disk alanı yetersizliğinden sunuculara erişilememesi, sistemlerin yavaş çalışması, dosya oluşturamama, belgelerde değişiklik yapamama gibi zaman ve maliyet kaybına sebep olabilecek sorunlar oluşabilir. Bu durumda bilgi güvenliğinin erişilebilirlik özelliği ihlal edildiğinden iç saldırıların tehdit kategorisine alınmıştır. Yetersiz disk alanı uyarısı Şekil 8'de gösterilmiştir.

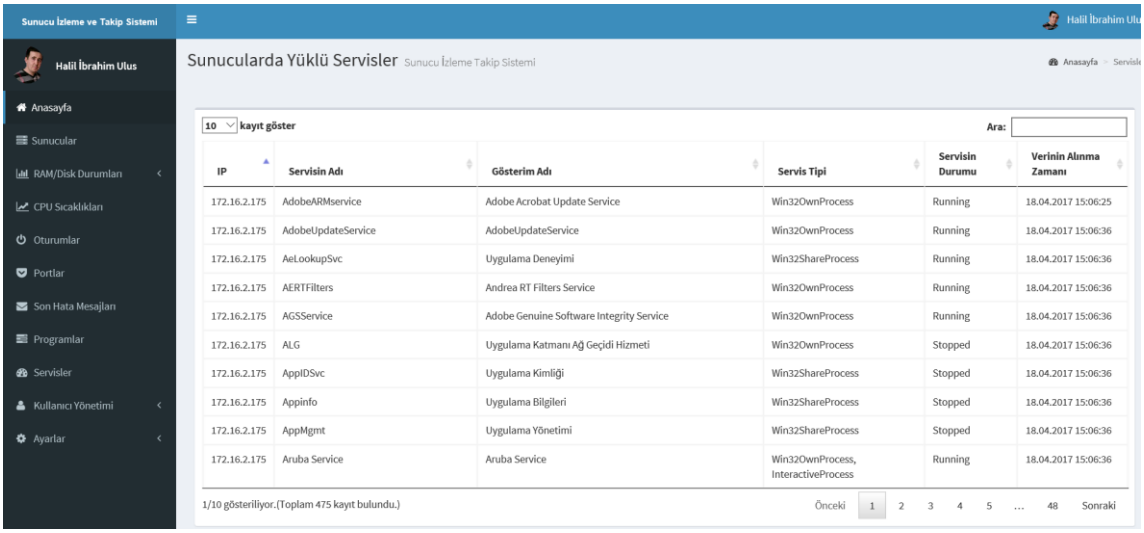
Arkaplanda Sıradışı Servislerin Çalışması

Siber saldırganlar arka kapı zararlı yazılımları, mantık bombaları ve virüsler vasıtasıyla sistemlere erişim sağlarlar ve zarar verirler. Özellikle iç saldırganlar istifa ettiklerinde veya kurum dışından sistem bilgisayarlarına erişmeye çalıştıklarında bu araçlardan faydalanırlar. Bu yazılımlar Windows servisleri olarak arka planda çalıştıkları için bu servislerin analizi ve yabancı servislerin tespiti, saldırıların büyük zararlara yol açmadan önlenmesi açısından önemlidir. Şekil 9'da çalışan servislerin durumu raporlanmaktadır.

Şekil 7. *Mesai saatleri dışında giriş yapan kullanıcı bilgilerinin detaylı gösterilmesi (Detailed information on user logins outside working hours)*



Şekil 8. *Disk alanı yetersizliğinden alarm oluşması (Low disk space alarm)*



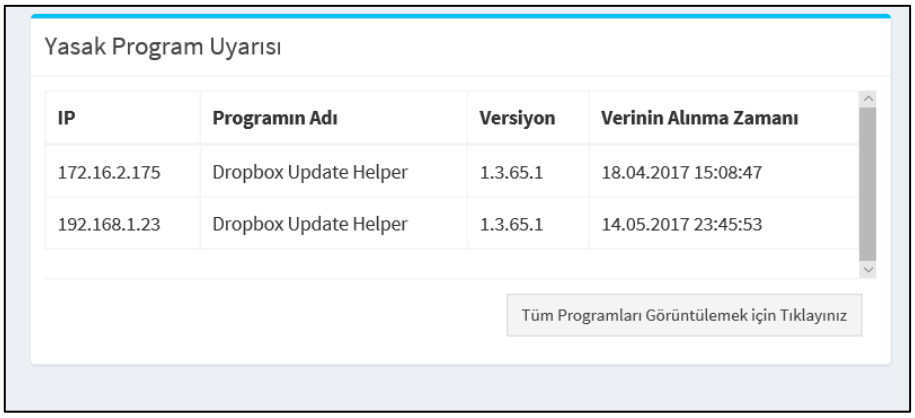
Şekil 9. *Servislerin yönetim panelinde gösterilmesi (Services displayed in the admin panel)*

İstenmeyen Programların Kurulması

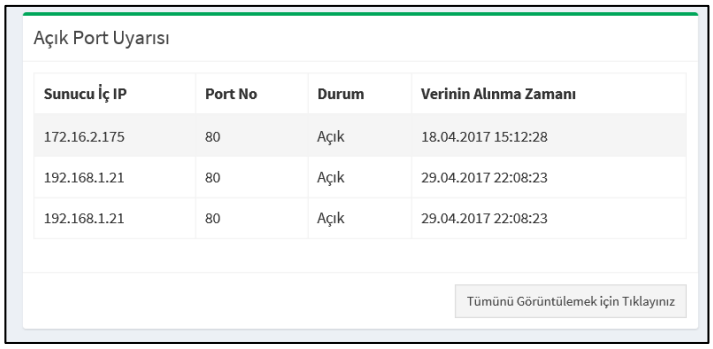
SİTS uygulaması sayesinde sunucuda kurulu sürümleriyle birlikte programları ve son güncellenme zamanlarını da görebilmekteyiz (Şekil 10). Özellikle sıfırıncı gün açıklıkları ve birçok yeni saldırıya karşı programların güncel olması önemlidir. Bunun denetimi SİTS uygulaması sayesinde sürümler kontrol edilerek yapılabilmektedir. Aynı zamanda istenmeyen programların kurularak sistemlere zarar verilmesi, kontrolsüz veri transferi yapılması gibi durumların önüne geçilebilmesi için bu kayıtlar önemlidir.

Kritik Portların Açık Olması:

Bilgi güvenliği politikaları gereği düzenli olarak port taraması yapılmalıdır çünkü siber saldırıların çoğu açık portlar kullanılarak yapılmaktadır. Özellikle 21 (dosya aktarımı), 22 (güvenli veri gönderme), 25 (e-posta gönderme protokolü), 80 (web trafiği yani HTTP), 110 (e-posta indirme protokolü), 443 (TLS/SSL üzerinden HTTP), 445 (Microsoft-DS) portları saldırganlar tarafından sıklıkla kullanılmaktadır. Bu yüzden kullanılmayan portlar kapatılmalıdır. Belirlenen portlar açıldığında SİTS uygulaması tarafından bu durum tehdit olarak algılanmakta ve uyarı verilmektedir. Şekil 11'de belirlenen portun açık olduğu kullanıcılar gösterilmektedir.



Şekil 10. *Yasaklanan programların kurulu olduğu sunucuların uyarı olarak gösterilmesi (Displaying servers with prohibited programs installed)*



Şekil 11. *Açık olan portların gösterilmesi (Displaying open ports)*

Belirlenen sayının üzerinde şifre denemesi yapılması

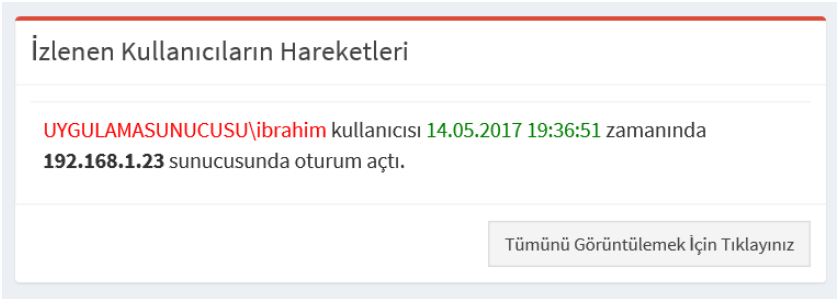
Kurum içi saldırganlar zararlı faaliyetlerini gerçekleştirmek için sistemlere başkasından ele geçirdikleri şifrelerle girerler veya doğru şifreyi bulmak için denemeler yaparlar. Bu yüzden hatalı şifre denemelerinin de takip edilmesi gerekir. Kullanıcı şifresinin belirlenen eşik değerden daha fazla sayıda girilmesi halinde hesap kitlendiğinde uygulamamızın son hata mesajları bölümü kullanılarak bilgi alınabilmektedir.

Şüpheli kullanıcıların takip edilmesi

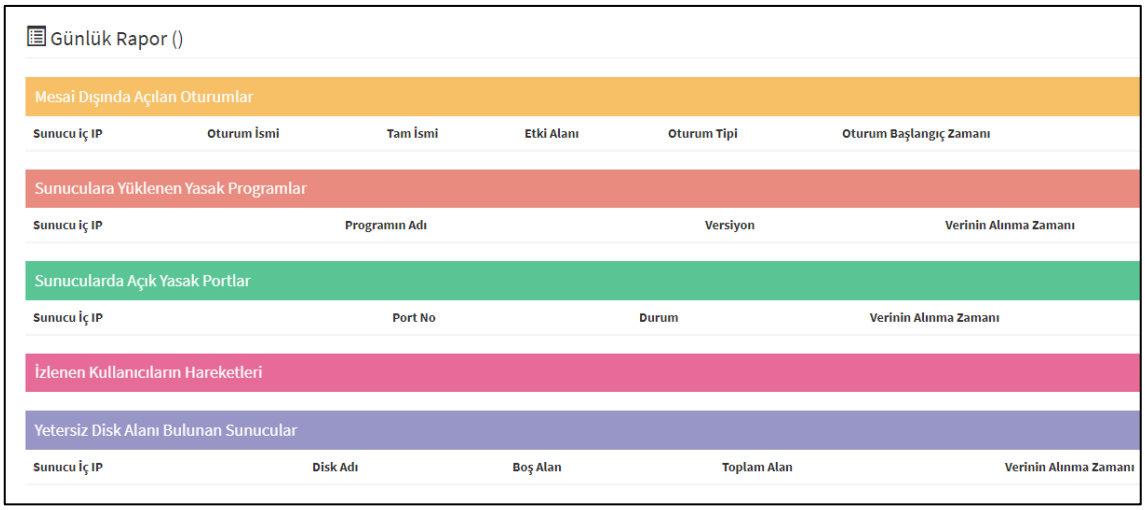
Herhangi bir departmandan veya personelden başka bir kullanıcı ile ilgili şikayet veya muhtemel saldırgan ihbarı gelmesi durumu tehdit olarak değerlendirilir ve şüpheli kullanıcının hareketleri takip edilmeye başlanır. Ayrıca kurumdan ayrılan veya ilişiği kesilen çalışanların eğer saldırı planı varsa, geçmiş olaylar dikkate alındığında saldırıyı çoğunlukla 30 gün içinde gerçekleştirilirler. Bu yüzden bu kişilerin de dikkatle takip edilmesi ve tüm yetkilerinin derhal alınması gerekir. Şekil 12'de daha öncesinde şüpheli olduğu tespit edilen kişinin diğer bir sunucuda oturum açtığı ikazı gösterilmektedir.

Raporlar bölümü

Yönetim panelinin "Raporlar" bölümünde bilgi güvenliği ihlal olayları günlük, haftalık, aylık şekilde istatistiksel olarak Şekil 13'te görüldüğü gibi tek sayfada toplu olarak gösterilmektedir. Ayrıca kullanıcı tarafından istenen tarih girilerek geçmişe dönük kayıtlar da incelenebilmektedir (Şekil 14). Böylece muhtemel deliller saklanmış olmakta ve saldırganın zararlı hareketleri aynı gün icra edilmese de tespit edilebilmektedir.



Şekil 12. *Şüphelenilen kişinin takip edilmesi (Following the suspicious person)*



Şekil 13. *Raporlar bölümünün genel görünümü (Reports section)*

Şekil 14. *Tarih girilerek geçmiş kayıtların incelenmesi (Reviewing past records)*

5. UYGULAMANIN DEĞERLENDİRİLMESİ (EVALUATION OF APPLICATION)

Önceki bölümde bahsedilen tüm senaryolar değerlendirildiğinde geliştirdiğimiz SİTS uygulaması iç saldırganların sıklıkla takip ettiği bazı yöntemlere karşı bir erken uyarı sistemi olacaktır. Böylece zamanında müdahaleyle saldırılar önlenebilecek, saldırı girişiminde bulunanlara yaptırım uygulanabilecek, saldırının engellenemediği durumlarda ise en azından suçlu tespit edilmiş ve belirli kanıtlar toplanmış olacaktır. Aşağıda bazı muhtemel saldırılar ve bunlara karşı SİTS'in etkileri açıklanmıştır. Bu saldırılar SİTS kurulu bilgisayarlar üzerinde denenerek SİTS'in davranışları doğrulanmıştır.

Mesai saati dışında veri sızdırma: İç saldırgan mesai saati dışında sisteme giriş yaparak bazı bilgileri e-posta ile göndermeye çalıştığında, hem mesai saati dışında giriş yaptığı için alarm üretilir ve yöneticiye ikaz e-postası atılır, hem de e-posta portu kapalı olduğu için e-postaya izin verilmez, portun açılması durumunda ise yine alarm üretilir.

Dosya paylaşım programlarını kötüye kullanma: Bilgi sızdırmada kullanılabilecek belli programlar kurulduğunda kurum politikaları gereği sistem ikaz verir. Bazen kullanıcılar keyfi olarak, sebep olacakları zararı bilmeden bazı programları yetkileri olmadığı halde yüklemektedirler. Bu durumlar veri sızıntısının yanında sistemlerin de yavaşlamasına sebep olabilir. SİTS ile böyle durumların da oluşmasının önüne geçilmiş ve kötü niyetli olmayan kullanıcılar uyarılmış olur.

Casus yazılım ile veri sızdırma ve uzaktan kontrol: Bazı durumlarda saldırganların kullandığı yazılımlar kurumda riskli olduğu belirlenmiş programlar listesi içinde yer almayabilir veya kurulum gerektirmeyen özellikte olabilir. Örneğin saldırganlar kendi ürettikleri bir casus yazılımı sunucularda

çalıştırıp bunu istedikleri bilgileri almak veya sistemlere zarar vermek amacıyla kullanabilirler. Her gün rutin olarak SİTS uygulamasını kontrol eden sorumlu kişi farklı bir servis uygulamasının arka planda çalıştığını fark ederek olası bir saldırıyı yakalayabilir. Ayrıca bu uygulama portları kullanarak haberleşmek istediğinde alarmlar üretilir.

Şüpheli kullanıcının bilgi çalma veya sabotaj amaçlı saldırı yapması: İnsan kaynaklarından gelen bir uyarı, bir çalışanın şikayeti veya sistem üzerinde şüpheli davranışlar sergileme sonucunda potansiyel saldırgan olarak etiketlenen bir kullanıcı, SİTS uygulaması ile takip edilebilmektedir. Örneğin şüphelinin kendi bilgisayarı dışında bir makinede oturum açması durumunda kullanıcı adını, oturum açtığı bilgisayarı ve oturum açma zamanını içeren bir uyarı mesajı oluşturulur.

Bunun gibi daha birçok saldırı senaryosunda SİTS uygulaması saldırıyı önleme veya zamanında müdahale etme imkanı vermektedir. Aslında SİTS yönetim paneli olmadan da kullanıcının alarmlarda yer alan türde bilgilere ulaşması mümkündür. Fakat büyük miktardaki kayıtların taranması, tüm gerekli yerlerin tek tek incelenmesi uzun zaman, ileri seviyede teknik bilgi ve iş gücü gerektirecektir. SİTS uygulaması ciddi bir zaman tasarrufu sağlamakta ve önemli verileri önümüze getirerek gözden kaçma riskini azaltmaktadır.

Kurumdaki tüm varlıkların kontrol edilmesi bilgi güvenliği açısından çok önemlidir zira bazen atıl kalmış eski bir sunucu dahi saldırı için kullanılabilir. SİTS uygulaması sayesinde tüm varlıkların kontrolü sağlanabilmekte ve beklenmedik ortamlar üzerinden saldırıya uğrama riski azaltılmaktadır.

Bunun gibi özellikleri sayesinde SİTS uygulaması kurumlarda iç saldırı tespitini kolaylaştıracaktır. Ayrıca saldırganlar takip edildiklerini bildikleri için birçok durumda yakalanma riskini göze almayarak saldırıdan vazgeçeceklerdir ve böylece uygulama caydırıcılık sağlamış olacaktır. Dahası, hatalı davranışlar sergileyenlerin belli aralıklarla uyarılması kullanıcılar üzerinde bir farkındalık oluşturacaktır.

SİTS kural tabanlı bir yazılım olduğu için önceden belirlenen alarm şartlarını sağlayan saldırılar için tam başarıyla alarm oluşturulmakta, mevcut kurallara göre şüpheli kabul edilmeyen hareketler sergileyen yeni bir saldırı için ise alarm üretilmemektedir. Bununla birlikte SİTS uygulamasına yeni alarm ekleme özelliği bulunmaktadır ve gerektiğinde alarmlar güncellenerek yeni saldırı türlerine karşı savunma sağlanabilir.

6. TARTIŞMA VE SONUÇ (DISCUSSION AND CONCLUSION)

Yapılan bu çalışmanın amacı; kurumlar açısından giderek büyük bir tehdit unsuru olarak ortaya çıkmaya başlamış iç saldırılar hakkında bilgi vermek ve çözüm önerisi olarak uygulama düzeyinde geliştirilen SİTS programının bu tehditlere karşı etkinliğini göstermektir. Literatürde bu konuda yapılan araştırma sayısı oldukça azdır ve çalışmalarda genellikle riskleri ortaya koyup bazı öneriler sunma yoluna gidilmekte, teknik düzeyde savunmaya yardımcı çözümler sunulmamaktadır. Ayrıca kurumlar için iç saldırıların büyük zararlar doğurabileceği açık olduğu halde alınan önlemler ve çözüm arayışları yetersiz seviyede kalmaktadır. Bu yüzden yapılan bu çalışma hem akademik literatürün önemli bir eksiğini kapatmakta, hem de kurumlar için örnek çözüm önerisi olarak değerlendirilebilecek bir araç sunmaktadır.

Geliştirilen SİTS uygulaması, iç saldırıların ve saldırganların tespit edilmesi amacıyla sunucuların üzerindeki belli hareketleri izlemek için geliştirilmiş bir araçtır. Bu uygulama sayesinde sunucudaki aktiviteler kontrol altına alınarak, saldırganı bulmayı kolaylaştırıcı verilerden elde edilmiş, özet ve yararlı bilgilere ulaşılabilmektedir. Bu sayede organizasyonların ayrıcalıklı yetkilere sahip sistem yöneticilerinin de izlenmesi ve tehdit oluşturan kötü niyetli çalışanların tespit edilmesi sağlanacaktır. Belirlenen şüpheli hareketlerin tespiti ile SİTS uygulaması iç saldırganların sıklıkla takip ettiği bazı yöntemlere karşı kurum için bir erken uyarı sistemi olacaktır. Kurum içi saldırılara karşı risk değerlendirmesi yapılmak istendiğinde uygulamanın raporlar kısmında yer alan sayısal bulgular kullanılarak daha doğru sonuçlara ulaşılabilecektir.

Gelecekte yapılacak çalışmalarda, kullanıcıların tüm hareketlerinin farklı düzeylerde risk veya şüphe taşıdığı göz önüne alınarak daha hassas bir analiz yapılması planlanmaktadır. Bu kapsamda geçmiş saldırılarda gözlenen hareketlerin gerçekleşme sıklığına ve etkilerine göre şüpheli hareketlere risk puanları verilerek, ayrıca kullanıcının farklı hareketlerinin birbirleriyle ilişkileri incelenerek ve aralarındaki bağ dikkate alınarak belirlenen bir formülasyon ile kullanıcı hareketlerinin saldırıya dönüşme

ihtimali hesaplanabilir. Ayrıca, SİTS'in yakalayamadığı daha karmaşık saldırıların tespit edilmesi için normal kullanıcı profilleri oluşturulup anomali tespiti yapılabilir. Bu geliştirmelerle birlikte sistemin erken uyarı kabiliyetinin daha da artması beklenmektedir.

KAYNAKLAR (REFERENCES)

[1] R. Willison, M. Warkentin, "Beyond Deterrence: An Expanded View of Employee Computer Abuse", MIS Quarterl, 37 (1), 2013, 1-20.

[2] A.M. Munshi, "A Study Of İnsider Threat Behaviour: Developing A Holistic İnsider Threat Model", Ph.D. Thesis, Curtin University, School of Information Systems, Bentley, Western Australia, 2013.

[3] J. Long, J. Wiles, R. Rogers, P. Drake, R.J. Green, G. Kipper, R.T. Blackwood, and A. Schroader, "Techno Security's Guide to Managing Risks for IT Managers, Auditors, and Investigator", Burlington, MA: Elsevier, 2007, 337-383.

[4] S.J. Stolfo, S.M. Bellovin, S. Hershkop, A. Keromytis, S. Sinclair, And S.W. Smith, "Insider Attack and Cyber Security Beyond the Hacker", New York: Springer, 2008, 20-24.

[5] Ö.F. Gökmen, Ö.E. Akgün, "Bilgisayar ve Öğretim Teknolojileri Eğitimi Öğretmen Adaylarının Bilişim Güvenliği Eğitimi Verebilmeye Yönelik Yeterlilik Algılarının İncelenmesi", İlköğretim Online, 14(4), 2015, 1208-1221.

[6] S. Cheon, J. Kang, M. Park, and J. Eom, "The Scheme of 3-Level Authentication Mechanism for Preventing Internal Information Leakage", 2014 Fourth International Conference on Digital Information and Communication Technology and its Applications (DICTAP), Thailand, 2014, 154-157.

[7] Y. Canbay, Ş. Sağıroğlu, "Veri Kaçağı Tespitinde Yeni Bir Yaklaşım", Savunma Bilimleri Dergisi, 15 (1), 2016, 149-177.

[8] K.W. Kongsgard, N.A. Nordbotten, F. Mancini, and P.E. Engelstad, "An Internal/Insider Threat Score for Data Loss Prevention and Detection", IWSPA '17 Proceedings of the 3rd ACM on International Workshop on Security And Privacy Analytics, New York, 2017, 11-16.

[9] S.P. Kashi, N.C.S. Reddy, G.P. Reddy, "A Model For Traitor Detection With Appraising", International Journal of Computer Applications, 93(3), 2014, 1-5.

[10] S.L. Pfleeger, J.B. Predd, J. Hunker, C. Bulford., "Insiders Behaving Badly: Addressing Bad Actors and Their Actions", IEEE Transactions on Information Forensics and Security, 5 (1), 2010, 169-179.

[11] G.J. Silowash, D.M. Cappelli, A. Moore, R.F. Trzeciak, T. Shimeall, and L. Flynn, "Common Sense Guide to Mitigating Insider Threats", 4th Edition; SEI Technical Report CMU/SEI-2012-TR-012, URL: http://www.webcitation.org/query?url=http%3A%2F%2Fresources.sei.cmu.edu%2Fasset_files%2FTechnicalReport%2F2012_005_001_34033.pdf&date=2017-07-09, Erişim Tarihi: 10 Nisan 2017.

[12] K.R. Sarkar, "Assessing Insider Threats To Information Security Using Technical, Behavioural And Organisational Measures", Information Security Technical Report, Elsevier Advanced Technology Publications Oxford, 15(3), 2010, 112-133.

[13] N. Elmrabit, S. Yang, L. Yang, "Insider Threats in Information Security Categories and Approaches", 21st International Conference on Automation and Computing (ICAC), Glasgow, UK, 2015, 1-6.

[14] A. Munshi, P. Dell, H. Armstrong, "Insider Threat Behavior Factors: A comparison of theory with reported incidents", 45th Hawaii International Conference on System Sciences, USA, 2012, 2402-2411.

[15] D. Cappelli, A. Moore, R. Trzeciak, "The CERT® Guide to Insider Threats How to Prevent, Detect, and Respond to Information Technology Crimes (Theft, Sabotage, Fraud)", Massachusetts: Pearson Education, Inc, 2012, 61-98.

[16] M.R. Randazzo, M. Keeney, E. Kowalski, D. Cappelli, and A. Moore, "Insider Threat Study: Illicit Cyber Activity in the Banking and Finance Sector", Carnegie Mellon Software Engineering Institute Technical Report CMU/SEI-2004-TR-021ESC-TR-2004-021, Software Engineering Institute, 2005, 3-23.

[17] F. Aktaş, İ. Soğukpınar, "A New Approach for Choosing Proper Risk Analysis and Management Method in Information Security", Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 3 (1), 2010, 39-46.

[18] E. Şahinaslan, R. Kandemir, A. Kantürk, "Bilgi Güvenliği Risk Yönetim Metodolojileri ve Uygulamaları Üzerine İnceleme", ABGS 2010–Ağ ve Bilgi Güvenliği Sempozyumu, 2010.

[19] B. Karabacak, S. Özkan, "Bilgi Güvenliği Yönetim Sistemi İçin Süreç Tabanlı Risk Analizi", III. Ağ ve Bilgi Güvenliği Sempozyumu, Ankara, 2010.

[20] C. Colwill, "Human factors in information security: The insider threat-Who can you trust these days?", Information Security Technical Report 14, Elsevier, 2009, 186-196.

[21] E. Cole, S. Ring, "Insider Threat Protecting the Enterprise from Sabotage, Spying, and Theft", USA: Syngress Publishing, 2006, 1-96.

[22] T.R. Peltier, "Information Security Fundamentals", USA: CRC Press, 2013, 1-17.

[23] R. Willison, M. Warkentin, "Beyond Deterrence: An Expanded Vıew Of Employee Computer Abuse", MIS Quarterly, 37(1), 2013, 1-20.