# Siber Güvenlik Konusunda Kurumsal Farkındalık ve Entegre Çözüm Altyapısı

İbrahim Dinçer

***Özet*—Siber Güvenlik Saldırılarının çeşit ve miktarının artmasına karşın, kurum ve kuruluşların gündeminde uygun güvenlik politikalarının belirlenmesi, güvenlik yamalarının zamanında yapılması, güvenlik uzmanı istihdamı gibi konular hala önemli bir sorun olarak yer işgal etmektedir. Bu sorunların çözülmesinin sonrasında da yoğun siber saldırılar karşısında daha etkin önlemler alabilmek için bilişim alt yapısının on-line dinlenerek, elde edilen verilerden olayları analiz edip, çözüm yolarının belirleneceği bir otomasyon alt yapısının tesis edilmesine ihtiyaç bulunmaktadır. Bu alt yapının güvene dayalı işbirliği esaslı bir portal yapısı içinde de işbirliği ile desteklenmesi durumunda etkinliği arttırılmış olacaktır.**

***Anahtar Kelimeler*—Siber Güvenlik, Tümleşik Siber Güvenlik İzleme Sistemi, Siber Güvenlik Analisti, Durumsal Farkındalık**

**Abstract—Despite increased number of cyber-attacks, security policy issues, security patch management, allocation of security analyst for organizations are still live challenges. Even all those issues have been resolved effective hassling for cyber-attacks is only possible via on line cyber defense analysis infrastructure. Having the result of analysis in hand, the precautions for future attacks will be employed and will be shared with trusted shareholders.**

***Index Terms*—Cyber Security, Integrated Cyber Security Monitoring System, Cyber Security Analyst, Situation Awareness**

## I. GİRİŞ

SON dönemlerde kurum ve şirketlerin hizmetlerini internet üzerinden sunmalarına bağlı olarak, internet kullanımında da bir artış gözlenmektedir. İnternet kullanımındaki bu artış da; son yıllarda siber saldırıların da sayısı ve niteliklerinde bir atışa sebep olmaktadır. Bu bağlamda siber güvenlik olarak adlandırılan, bilgi uzayı (siber ortam) güvenliği; hem ulusal güvenliğimiz hem de ticaret ve rekabet gücümüz açısından büyük önem taşımaktadır. Bu kadar hassas ve önemli konuda bakanlar kurulu 20 Ekim 2012 tarihinde ve 28447 Resmi Gazetede yayımlanan "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonu " konusunda bir karar alarak yürürlüğe koymuştur. Kurum ve şirketlerin güvenlik konusundaki genel yaklaşımı ise önceden riskleri analiz edip, değerlendiren ve önleyici tedbirler alan bir yapıyı tesis ederek proaktif olmak yerine; bir olay sonrası sorunu çözmeye yönelik reaktif olmaktadır. Çoğu zaman güvenlik konusunda ayrı bir insan kaynağı bile ayrılmaz; Bilgi Teknolojileri (BT) alt yapısının yönetim sorumluluğu verilen kişilerin bu görevi de yerine getirmesi beklenir. Esasen bir kurum ve kuruluşta kesintisiz bilişim hizmeti sunmak, hizmet sunulan kullanıcı sayısı ile doğru orantılı olarak her bir kullanıcıya zaman ayırmak; kullanıcıların sorunları için zaman harcamak demektir. Çoğu kere böyle yoğun bir hizmet için bile yeterli insan kaynağı tahsis edilmezken, üstüne bu kişilere bir de süreklilik isteyen siber güvenlik konusunda bir sorumluluk yüklemek, olası tehlikeleri ve sonuçlarını baştan kabullenmek anlamına gelebilir.

Manuscript received March 01, 2013.
İbrahim Dinçer, BİTES Savunma Havacılık ve Uzay Teknolojileri

## II. MEVCUT DURUM

Günümüzde küçük firmalardan büyük holdinglere kadar birçok kurum/kuruluş BT alt yapısını kendi bünyesinde kurar ve işletir. Bu durum, mali olarak her birimin benzer mali yatırımı yapmasının yanında, sistemin kesintisiz çalışması için uzman insan kaynağının temini ve idamesi; sitem yönetim personelinin yeterli uzmanlık eğitimleri ve sayısı, uzman personelin sıkça sirkülasyonu, sistem yönetim ve güvenlik politikalarının belirlenip uygulanması, işletme ve idame maliyetleri gibi zorlukları da beraberinde getirmektedir.

Özellikle güvenlik, birçok kurum/kuruluşta ayrıca bir uzman insan kaynağı istihdam edilmeyen, ihmal edilen ve ancak bir sorun yaşandığında bir süre üzerinde durulan ve olayın sıcaklığı geçtikten sonra da gene eski akışına bırakılan bir konu olarak karşımıza çıkmaktadır. Dünyada günlük 77,000 terabayt verinin [1] dolaştığı yoğun Internet kullanımı dikkate alındığında, her saat binlercesinin geçekleştiği güvenlik ihlallerini tamamen izleme ve kontrol altına almak imkansız hale gelmektedir. Kurumlar ve şirketler her geçen gün artan siber tehlikelerin etkilerini azaltmak üzere, Bilgisayar Acil Müdahale Ekipleri (CERTS) ve Farkındalık Oluşturma (Situation Awareness) arttırıcı Siber Güvenlik Uzmanlığı gibi yapıların oluşturulmasına katkı sağlamaktadır. Siber Güvenlik, bilginin çalınmasını, riske edilmesini veya saldırıya uğramasını önleyici yöntemler olarak tanımlanabilir. Siber strateji kimlik, risk ve vaka yönetimlerini kapsar [2]. Bu görevi yapan kişi veya kişilere de "Siber Güvenlik Savunma Uzmanı" denilmektedir.

Siber Güvenlik Savunma Uzmanları, hızla çeşidi ve miktarı artan siber güvenlik saldırılarına karşı çeşitli yazılım araçları kullanmaktadırlar. Genel olarak güvenlik araçları *Düşük Seviyeli Durum* verisi sağladıklarından, analizlerin

yapılabilmesi için insanın algılamasını kolaylaştırıcı *Yüksek Seviyeli Durum* bilgisine dönüştürmek için çok büyük hacimli bu verilerden ayıklama yapmak gerekir. Bu da Siber Güvenlik Savunma Uzmanının iş yükünün artmasına ve dolayısı ile de performans kaybına sebep olmaktadır. Ayrıca bu tür araçların çoğu da farkındalık yaratma (SA-Situation Awareness) konusunda yeterli değildir. "**Farkındalık Oluşturma**yı" da tanımlamak gerekirse, çevrede olup bitenleri algılama zamanında, anlamlandırma ve yakın geleceğe yansımasını tahmin etme olarak ifade edilebilir.

## III. SORUN ALANLARI

a. Güvenlik Politikaları Açısından Kurumsal Farkındalık ve Kurum Kültürü:

Siber Güvenlik araştırma anket sonuçlarına göre [3], 2010 yılında kurum ve kuruluşların %43'ü kendi kullanıcıları tarafından saldırıya uğramışlar ve bu saldırıların da % 46'sı dışarıdan gelenlere göre daha fazla zarar vermişlerdir. Bu saldırılar da kendi içinde gruplandırılırsa; Yetkisiz kurum verisine erişim %63, Kasıtsız olarak hassas veriye erişim %57, Virüs ve Zararlı kodlar %37, Fikri mülkiyet çalma %32 şeklinde olduğu gözlenebilir. Bu durum açıkça göstermektedir ki kurum/şirket içi tehdit tehlikenin yarısını oluşturmaktadır. Dolayısı öncelikle iç tehdit için çözüm üretmek, tehlikenin yarısını bertaraf etmek demektir. Güvenlik politikalarının kurumsal kültür ve kurumsal farkındalık oluşturacak şekilde benimsetilmeden politikanın sağlıklı ve uzun soluklu olması mümkün değildir. Bunun için üst yönetim zamanında bilgilendirip, problem doğru tanımlanmalı, kullanıcılar mutlaka bilgilendirilmeli, önlemler abartılmadan alınmalı, uygulamaya geçmeden önce kullanıcıdan geri besleme almayı müteakip uygulamaya konulmalıdır. Kullanıcıdan hiçbir şey saklanmamalı ve güvenlik politikaları bir ceza uygulamasına dönüştürülmemelidir. Kurum kültürü oluşturabilmek için de güvenlik politikası belirleyici ve uygulayıcıları mutlaka kurum çalışanları ile sıcak temaslarda bulunmak suretiyle kişisel/ kurumsal beklentilerin nabzını tutmaları gerekir.

b. Siber Güvenlik Uzmanlığı

Genel olarak kurum ve kuruluşlarda güvenlik konuları bir olay vuku bulduğunda gündeme gelir, olayın sıcaklığı geçince işler normal seyrinde devam eder. Bazı kurumlar hariç, güvenlik konusunda ayrı bir personel ayrılmaz; bilişim hizmetlerinin sürdürülmesini sağlayan sistem yönetim personeline personele ek sorumluluk olarak verilir. Dolayısı ile Siber Güvenlik Uzmanlığı gibi bir uzmanlık birçok kurum ve kuruluşta henüz benimsenip istihdam alanı haline dönüşmemiştir.

c. Siber Güvenlik Uzmanlık Eğitim İhtiyacı

Siber Güvenlik Uzmanlığı henüz tam bir istihdam alanına dönüşemediği; siber saldırı tekniklerinin her geçen gün artmasına bağlı olarak siber güvenlik tehditleri için çözüm yolları ve bilgi birikimi ile eğitim alt yapısı istenilen seviyeye gelememiştir. Her kurum/kuruluş karşılaştığı sorunları kendi iç dinamikleri ile çözmeye çalıştığı ve sertifika eğitimi tarzındaki bazı eğitimlerin yaygınlaşıp, kurumsal hale gelmediği için de bu sorunların büyük bir kısmı hemen her gün farklı yerlerde yaşanmaya devam edecek gibi görünüyor.

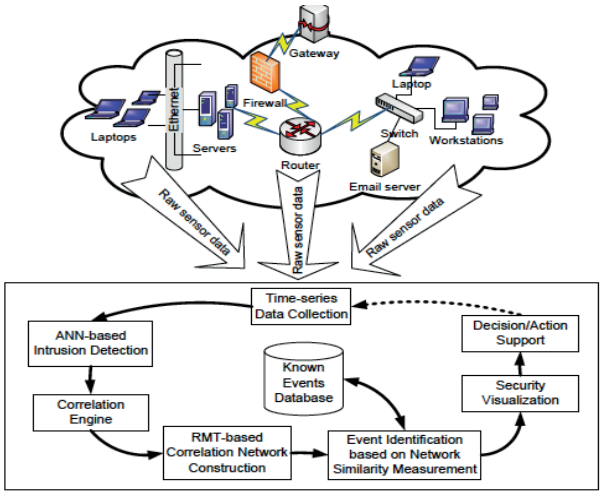
d. Siber Güvenlik Konusunda İşbirliği

Siber Güvenlik saldırısı yaşayan kurum ve kuruluşlar bunları, kendi özeli olarak gördüklerinden ve bir zafiyet algısı içinde başkaları tarafından bilinmesini istemediklerinden, çevre ile paylaşmazlar. Bu da işbirliklerini azaltır ve potansiyel tehditler için bir zafiyet oluşturur. Halbuki en azından benzer iş kollarındaki kurum ve kuruluşlar kontrollü erişimle bir portal yapısı ile bu tür bilgileri ve çıkarılan dersleri paylaşmış olsalar, hem kurumsal kazanımlar artar hem de potansiyel tehlikelere karşı önceden önlem alma imkanı olabilir.

## IV. SİBER GÜVENLİKTE ÇÖZÜM ÖNERİLERİ

Siber Güvenlik konusunda, kurum ve kuruluşlarda hizmet sunan bilişim alt yapısı için (yazılım/donanım) güncel güvenlik yamalarının zamanında yapılması, virüs koruma gibi koruma yazılım araçlarının kurulması; kurumsal farkındalığı arttırıcı on-line ve off-line eğitimlerin düzenli olarak verilmesi, kullanıcılarca benimsenmiş uygulanabilir güvenlik politikalarının hayata geçirilmesi gibi önlemler yeterli olmayabilir.

Farkındalık Oluşturma konusunda sorumluluğu olan, Siber Güvenlik Uzmanlarının günlük iş yoğunluğu nedeniyle bu işi bir otomasyon yardımıyla yapmaları halinde sonuçların olumlu olması söz konusudur. Bu durumda ilk akla gelen, kurum ve kuruluşun büyüklüğüne göre kendi bünyesinde veya bulut bilişim hizmeti gibi hizmet alımı söz konusu ise hizmet sağlayıcı seviyesinde bir "Entegre Siber Güvenlik İzleme Sistemi" [4] şeklinde bir yapının kurulması, siber güvenlik analizlerinin hızla yapılmasını sağlayarak, alınacak önlemleri etkinleştirmektir. Muhtemel bir **E**ntegre **S**iber **G**üvenlik **İ**zleme **S**istemini (**ESGİS**) kavramsal tasarımı aşağıdaki şemada gösterilmiştir. Şekildeki ağ yapısı içinde yer alan Sensörler, sunucu, kişisel bilgisayar, ağ cihazı ve Router'lara takılan yazılım/donanım unsurlarıdır ve zaman içinde rastlanan olaylara ait verileri toplarlar. Bu toplanan veriler, *Düşük Seviyeli Durum verisidir* ancak Farkındalık Oluşturmada kritik bir öneme sahiptir. Sensörlerden toplanan bu durum verisi ön uç veri merkezine gönderilir. Burada saldırı tespit edici Yapay Sinir Ağı (ANN- Artificial Neural Network) esasına [5] göre çalışarak bir karar verir. Daha sonra "**Korelasyon Motoru**", *Düşük Seviyeli Durum verisinden,* olay gösterge korelasyon matrisini oluşturur.




Şekil 1. Entegre Siber Güvenlik İzleme Sistemi Kavramsal Tasarımı [4]

Korelasyon matrisi, en son iki olay gösterge çifti arasında ilişki kurar. Daha sonra da RMT (Random Matrix Theory) esasına göre korelasyon ağı oluşturulur. Bir sonraki aşamada ise bilinen olaylar veri tabanı ile benzerlik esasına göre kıyaslama yapılarak olay tipi belirlenir. Bu maksatla SOFM denilen(Self Organizing Featuring Map) Sanal Sinir Ağlarının insan beyninin öğrenme süreçlerini taklit ettiği bir yöntem kullanılmaktadır. SOFM insan beyninde olduğu gibi, eğitildiği ilgili örneklerin ortak özellikleri ile kavrama ve ezberleme yapar.

Burada da iki temel ölçüt uygulanır:

a. Bir olay "Bilinen Olay Veri Tabanındaki"lerden biri ile yüksek benzerliği belirlenebiliyorsa; hassasiyeti gidermek, saldırıyı yok etmek veya etkisini azaltmak için gerekli koruma mekanizması devreye hemen sokulur.
b. Şayet veri tabanında benzer bir olay yoksa "Bilinen Olay Veri Tabanı"na mevcut olay gelecekte dikkate alınmak üzere eklenir.

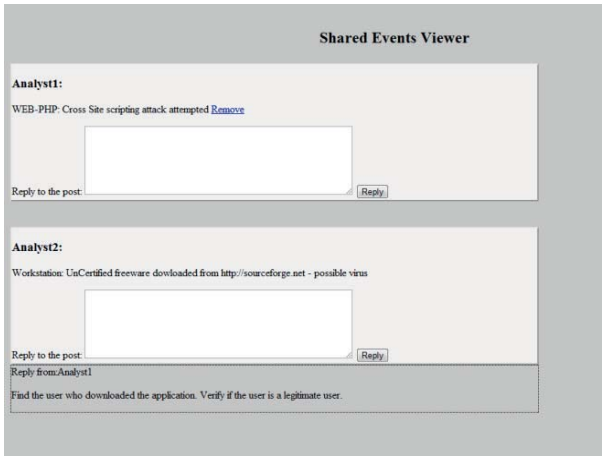
Bu izleme belli bir zaman aralığında devam ettirilir. Zaman içinde veri tabanında daha çok olay biriktikçe, daha doğru olay tanıma ve teşhis yapılabilir hale gelinecektir. Korelasyon ağındaki benzerlikleri ölçmede kullanılan kıyaslama yöntemlerindeki iyileşme, olayların teşhis edilmesini daha sağlıklı hale getirecektir.
Olaylar teşhis edildikten sonra, "**Görselleştirme Motoru**"na gönderilir ve orada ağ konum bilgisi ile birleştirilerek gösterge panosunda yer alır. Burada maksat, güvenlik ihlallerini görselleştirecek bir yapı oluşturmaktır. Bir ağ bölgesinde oluşan olayların sayısı, cereyan eden olayın şiddetini gösterir.

Olay tanıma ve teşhisini kolaylaştırmak için, Bilinen Olay Veri Tabanındaki olay benzeşmesi olmayan durumlarda, belli kurum/kuruluşlar ve servis sağlayıcılar gibi paydaşlar arasında bir portal üzerinden olay paylaşımı yapılarak işbirliğine gidilebilir. Portal üzerinden yapılacak böyle bir işbirliği ile hem Bilinen Olay Veri Tabanı zenginliğini kısa sürede arttırmak hem de saldırı ile ilgili koruma mekanizmalarını bir an önce devreye sokarak saldırıyı yok etmek veya etkisini azaltmak mümkün olabilecektir. Portal için 3 ara yüz [6] oluşturulabilir:

a. Olay Paylaşım Ara Yüzü:
Bu ara yüz vasıtasıyla paydaşlar arasında bilinirliği olmayan olaylar paylaşılır ve olaylarla ilgili yardım almak mümkün olacaktır. Paylaşılan olaylar "Paylaşılmış Olaylar Ara Yüzü" vasıtasıyla diğer paydaşların görmesi sağlanacaktır.

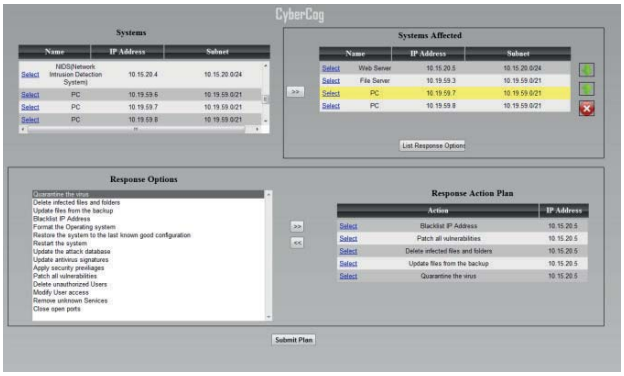

Şekil 2. Olay Paylaşım Ara Yüzü [6]

b. Paylaşılmış Olaylar Ara Yüzü:
Bu akranda diğer paydaşlar tarafından daha önce veri tabanında olmayan paylaşılmış olaylar görüntülenebilecektir. Her bir paydaş kendine göre çözüm önerisi veya hareket tarzını olayı yayımlayan paydaşa gönderebilecektir. Olayın olduğu konumdaki paydaş da bu çözüm önerilerinden bir veya birkaçını seçip uygulayabilecektir.




Şekil 3. Paylaşılmış Olaylar Ara Yüzü [6]

c. Çözüm Seçenekleri Ara Yüzü:
Bu ara yüzde de olayların listesi, etkilenen sistemler ve muhtemel çözüm yolları paydaşlarla paylaşılabilir. Böylece kurumsal olarak daha kısa sürede "Bilinen Olay Veri Tabanı" zenginleşmiş olacaktır.




Şekil 4. Çözüm Seçenekleri Ara Yüzü [6]

## V. SONUÇ VE DEĞERLENDİRME

Siber güvenlik kapsamında her kurum/kuruluş büyüklüğüne göre bir veya birkaç Siber Güvenlik Uzmanı istihdam etmelidir. Buna ilave olarak (yazılım/donanım) güncel güvenlik yamalarının zamanında yapılması, virüs koruma gibi koruma yazılım araçlarının kurulması; kurumsal farkındalığı arttırıcı online ve offline eğitimlerin düzenli olarak verilmesi, kullanıcılarca benimsenmiş uygulanabilir güvenlik politikalarının hayata geçirilmesi en başta yapılması gereken ön koşullar arasında yer almaktadır.

Bütün bu ön koşullar yerine getirildikten sonra da sistemi on-line olarak izleyip, sensörlerden alınan düşük seviyeli durum verisi ile olayları analiz eden; "Bilinen Olay Veri Tabanı"na çözüm seçenekleri ile kaydedebilen **E**ntegre **S**iber **G**üvenlik **İ**zleme **S**istemi (ESGİS)'ne ihtiyaç olacaktır. Bu sistemin etkinliğini arttırmak üzere, olay veri tabanındaki olaylarla eşleşmeyen, güvene dayalı işbirliği esasına dayalı olarak, yeni olayların paydaşlar arasında paylaşılıp, süratle analiz edilmesini sağlayacak bir portal yapısı ile desteklenmesi ile hem olaylara süratle müdahale edilebilir hale gelecek hem de ESGİS'in etkinliği arttırılacaktır.

## KAYNAKLAR

[1] Cisco. (2011). Cisco Visual Networking Index: Forecast and Methodology: 2010 – 2015. [White Paper]. Retrieved from: http://www.cisco.com/en/US/solutions/collateral/ns341/ns525 /ns537/ns705/n s827/white_paper_c11-481360.pdf
[2] http://www.techopedia.com/definition/24747/cybersecurity
[3] 2011 CyberSecurityWatch Survey How Bad Is the Insider Threat?
[4] Visualization of Security Events Using an Efficient Correlation Technique by Qishi Wu, Denise Ferebee, Yunyue Lin, Dipankar Dasgupta
[5] Yapay Sinir ağları,www.ube.ege.edu.tr
[6] CyberCog A Synthetic Task Environment for Measuring Cyber Situation Awareness by Prashanth Rajivan