BOME'lerin Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Kullanımının Etkinleştirilmesi

Melih Durak, İnan Semiz, Selçuk Sönmez

***Özet*—Bilişim teknolojilerinin hızla gelişmesi bu teknolojilerin kritik altyapıların yönetiminde kullanılmasını arttırmıştır. Ancak bu gelişen teknoloji ile yüz yüze kaldığımız siber saldırılar kritik altyapıların korunması sürecinde ülkeleri farklı tedbirler almaya itmiştir. Bu çerçevede Bilgisayar Olaylarına Müdahale Ekipleri (BOME) ulusal seviyede tesis edilmiştir. BOME'lerin güvenlik sürecinde etkin kullanımı saldırıların önlenmesinde büyük önem taşıyacaktır.**

***Anahtar Kelimeler*—Supervisor Control and Data Acqusition Systems (SCADA), Kritik Altyapı, Bilgisayar Olaylarına Müdahale Ekibi (BOME).**

***Abstract*—Fast development of information technologies increase the usage of these technologies in the management of critical infrastructure. However, with the developing technologies we are facing cyber attacks which make countries take differrent precautions for the protection of critical infrastructures. In this regard 'Computer Emergency Response Teams' (CERT) are established in national level. Efficently acting of CERT in cyber security process will play important role in preventing attacks.**

***Index Terms*—Supervisor Control and Data Acqusition Systems (SCADA), Critical Infrastructure, Computer Emergency Response Team (CERT).**

I. GİRİŞ

BİLGİ teknolojilerinin yoğun bir şekilde kullanıldığı kritik altyapılarla ilgili birçok tanımlama yapılmaktadır. Ancak genel olarak bir tanım yapmak gerekirse; yok edilmesi, zayıf bırakılması veya erişilmez kılınması halinde, uzun dönemde, ulusun sosyal ve ekonomik sağlığı üzerinde olumsuz etki bırakacak veya ulusal güvenliği sağlama kabiliyetini etkileyecek fiziksel tesisler, tedarik zincirleri, bilgi teknolojileri ve iletişim ağları [1] olarak tanımlanabilir.

Bütün altyapıların, teknolojik gelişmelerin etkisiyle, birbiriyle bağlantılı ve birbirine bağımlı hale geldiği günümüzde, kamu düzeni, güvenliği ve sağlığı toplumsal refah ve kamu hizmetlerinin sürdürülebilirliği açısından kritik altyapıların korunması hayati önem arz etmektedir. Bir ülkenin kritik altyapısında meydana gelen saldırılar ülkenin diğer kritik altyapılarını da etkileyebilmektedir.

Kritik Altyapılar ülkeden ülkeye farklılık göstermekle birlikte temel olarak Şekil 1.'deki başlıklar altında sıralanabilir [2,3,4].

Şekil 1.Kritik Altyapılar

Kritik altyapıların bilgi teknolojilerinin en önemli özelliği ülkelere coğrafi olarak birbirinden çok uzakta bulunan sistem ve araçları tek bir merkezden daha maliyet etkin bir biçimde kullanmayı sağlamasıdır. Bu kapsamda kullanılan temel sistem dağıtık denetim ve kontrol sistemleri olan SCADA sistemleridir. Bu sistemler en yalın olarak bir merkezden iletim kanalları kullanılarak uzaktaki birimlerin etkinleştirilmesi şeklinde tanımlanabilir. Örnek bir SCADA sistemi Şekil 2.'de gösterilmektedir.

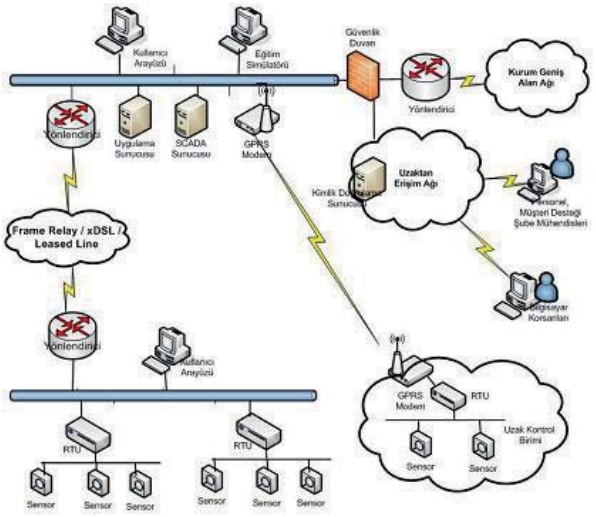
Bir SCADA sistemi,

- Kontrol edilen (makine, tezgâh ya da ardışık işlemlerden oluşan bir sistem),
- Kontrol eden (mikrodenetleyiciler, PLC ya da bilgisayar kumandalı sürücüler),
- SCADA yazılımı (merkezî bir bilgisayara yüklenmiş),
- Ağ elemanları (çoklu sistemler için) olarak özetlenebilir [6].

Melih Durak, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: melihdurak@gmail.com.

İnan Semiz, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: inansemiz@gmail.com.

Selçuk Sönmez, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: selcoksonmez@gmail.com.



Şekil 2. SCADA Sistemi Konfigürasyonu [5].

II. LİTERATÜR TARAMASI

BOME'ler ise bilgisayar ve şebeke güvenliğini izleyen ve siber saldırı mağdurlarına olaylara müdahale hizmeti sunan teknik birimlerdir. BOME'ler, açıklıklara ve tehditlere ilişkin uyarılar ve bilgisayar ve şebeke güvenliğini geliştirmeye yönelik bilgiler yayımlar; farkındalık oluşturma, güvenlik danışmanlığı gibi hizmetleri ve teknolojiyi izleme, güvenlik araçları geliştirme gibi proaktif hizmetlerin yanısıra, siber saldırılara karşı koyma ve bunların yol açtığı zararın azaltılması gibi reaktif hizmetler de sunarlar [7].

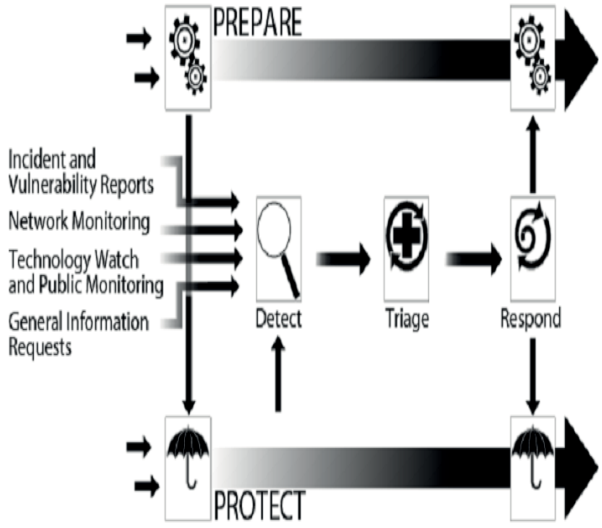
BOME'lerin görev ve sorumlulukları bakacak olursak en yeni tehditlere ilişkin güncel bilgiler sunmak ve ihtiyaç duyan paydaşlara siber saldırılarla mücadele konusunda teknik destek sağlamaktır. BOME'ler tarafından sunulan hizmetler Tablo 1'de gösterilmiştir.

TABLO 1
BOMELER TARAFINDAN SUNULAN HİZMETLER [8].

Reaktif Hizmetler	Proaktif Hizmetler	Güvenlik Kalite Yönetimi Hizmetleri
• Uyarma • Saldırılara müdehale • Saldırı Analizi • Açıklıklara müdehale • Açıklık analizi	• Bilgilendirme • Teknolojiyi İzleme • Güvenlik denetimi ve değerlendirme • Güvenlik yönetimi • Güvenlik araçları geliştirme • Saldırı tespit hizmetleri	• Risk Analizi • İş sürekliliği ve felaket kurtarma • Güvenlik danışmanlığı • Farkındalık oluşturma • Eğitim verme • Ürün değerlendirme veya belgelendirme

Literatürdeki bilgisayar olaylarına müdahale süreçlerine incelediğimizde genel olarak birbirine benzer süreçler ele alınmıştır.

Şekil 3'te beş aşamalı 'Hazırlama, Koruma, Tespit/Tanımlama, Önem derecesine göre ayırma ve müdahale' süreci görülmektedir. Bu temel müdahale süreci olarak literatürde, US-CERT dokümanlarında da belirtilmiştir [9,10].



Şekil 3. Beş Yüksek Seviyeli Olay Yönetim Süreci [9].

Avrupa Birliği'ne baktığımızda bilgisayar olaylarına müdahale süreci Şekil-3'e benzer model aldığı görülmüştür [11].

III. BOME'LERİN KRİTİK ALTYAPILARIN GÜVENLİĞİNİN SAĞLANMASINDA KULLANIMININ ETKİNLEŞTİRİLMESİ

A. *Çalışmanın Amacı*

Kritik altyapılar ülkeler için son derece önemlidir. Dolayısıyla ulusal boyutta siber olaylara müdahale edebilecek yetenekte birimlerin etkin bir biçimde kullanılması siber güvenliğin sağlanmasında en önemli gereksinimlerden bir tanesidir. Bu maksatla bu çalışmada amaç, ulusal boyutta kabul edilmiş kritik altyapıların siber güvenliğinde gerek kritik altyapıyı yöneten kurumların gerekse de BOME'leri yönlendiren kuruluşların etkin bir iletişim içinde siber saldırılara en hızlı biçimde çözüm bulmasına yönelik bir model önerisi sunmaktır.

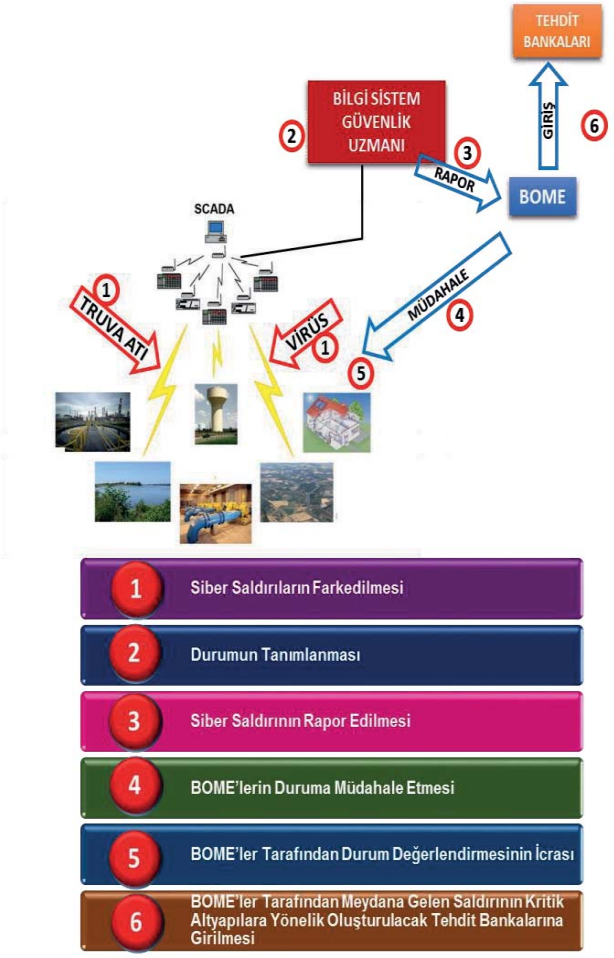
B. *BOME'lerin Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Etkin Kullanım Modeli*

Kritik altyapıların siber güvenliğinin sağlanmasında altı basamaklı model ile siber saldırıların öncelikle fark edilmesi sağlanmış olacak daha sonra da çözüm bulma süreci en kısa sürede tamamlanacaktır. Aşağıdaki Şekil 4.'te süreç adım adım gösterilmektedir.

(I) Siber Saldırıların Fark Edilmesi:

İlk basamak tehdidin farkına varmaktır. Siber saldırı kaynakları ve metotları her geçen gün artmakta ve çeşitlenmektedir. Bu nedenle şüpheci olmak ve sistemde meydana gelen değişimleri iyi gözlemlemek gerekmektedir. Bu maksatla kontrol merkezlerinde vardiya değişimleri büyük önem taşımaktadır.

Ayrıca basit siber saldırıları önleyen ve rapor sunan DDOS Mitigator gibi savunma araçlarının kullanılması bu süreci daha kolay hale getirecektir [12].



Şekil 4. Kritik Altyapıların Siber Güvenliğinde BOME'lerin Kullanım Modeli

(II) Durumun Tanımlanması:

Sistemde meydana gelen aksamanın fark edilmesinden sonraki süreç aksaklığın tanımlanmasıdır. Kritik altyapıların kontrol merkezinde bilgi sistem güvenliğinden sorumlu uzman personelin bulunması tanımlama sürecinde meydana gelen duruma Siber saldırı tanımı konabilmesini sağlayacaktır.

(III) Siber Saldırının Rapor Edilmesi

Eğer meydana gelen aksama ve olay fiziksel ve sistemden kaynaklanmadığı fark edilirse ve bilgi sistem güvenlik personelinin tespiti siber saldırı olabileceği değerlendirilerek bir an önce bu saldırı şüphesinin Ulusal BOME'lere aktarılması gerekecektir. Bu kapsamda Ulusal seviyede belirlenen kritik altyapılar ile BOME'ler arasında bir iletişim altyapısının kurulu olması gerekmektedir.

Bu bildirilerin oluşturulacak olay bildirim formları ile iletilmesi sağlanarak eksik bilgi iletilmesinin önüne geçilecektir.

(IV) BOME'lerin Duruma Müdahale Etmesi:

Sağlanan iletişim kanallarından durumun rapor edilmesi sonucu BOME'ler duruma müdahale eder ve saldırının siber kaynaklı olduğunu tespit ederlerse sorunun çözümüne yönelik aşağıdaki faaliyetleri icra ederler.

- Olay sırasınca olay ile ilgili kanıtların toplanması
- Olay sonrasında kanıtların incelenmesi
- Olay ile ilgili sorumluların belirlenmesi
- Olaya sebep güvenlik problemlerinin (saldırgan tekniği veya açıklık) belirlenmesi [13].

(V) BOME'ler Tarafından Durum Değerlendirmesinin İcrası:

Siber tehditin ortadan kaldırılmasından sonraki aşama bir daha böyle bir saldırının gerçekleşmemesi için alınması gereken tedbirler ve yapılacak işlemlerin değerlendirilmesidir.

Bu süreçte saldırıdan zarar gören kaynakların kurtarılması ve hasarın telafisi yolları araştırılır. Kritik altyapının risk haritası güncellenebilir.

(VI) BOME'ler Tarafından Meydana Gelen Saldırının Kritik Altyapılara Yönelik Oluşturulacak Tehdit Bankalarına Girilmesi

Kritik Altyapılara yönelik saldırıların sınıflandırılması ve daha kolay takibinin ve çözümünün sağlanması maksadıyla meydana gelen saldırılar ve alınan tedbirler oluşturulacak ulusal tehdit bankalarına eklenmelidir. Bu bilgi uluslararası tehdit bankaları ile paylaşılıp diğer ülkelerin tecrübelerinden de istifade edilmelidir. Böylece benzer saldırılarda çözüm bulunması daha kolay olacaktır.

Bu aşamada dünyadaki diğer tehdit bankalarından faydalanılabilir. Örneğin;

- FIRST
- TF-CSIRT
- European Government CERTs [14].

IV. SONUÇ

Bu çalışmada BOME'lerin kritik altyapıların siber güvenliğinin sağlanmasında nasıl kullanılacağı bir model üzerinde gösterilmiştir. Kritik altyapıları yöneten kurumlar tarafından öncelikli olarak yapılması gereken husus sistemin yönetildiği merkezlerde siber farkındalığın yüksek olması ve siber olaylara tanım koyabilecek yetenekte personelin sürekli bulundurulmasının sağlanmasıdır.

BOME'lerin ulusal düzeyde kritik altyapı olarak belirlenen kurumlarla gerek idari gerekse de teknik olarak en hızlı iletişim kanallarını tesis etmesi durumun rapor edilmesi sürecini hızlandıracaktır. BOME'lerin uluslararası tecrübelerden de istifade ederek bir tehdit bankası oluşturması ve bunun sürekli güncel tutulmasının sağlanması karşılaşılacak saldırılarda çözüm adına ışık tutacaktır.

BOME'lerin siber olaylara sistematik bir şekilde müdahale etmesi, durumun en erken şekilde tanımlanarak reaktif ve proaktif önlemlerle tedbir getirilmesi ile kritik altyapılarımız korunmuş olacaktır.

KAYNAKLAR

[1] M. Ünver, C. Canbay, B.H. Özkan, Kritik Altyapıların Korunması, Bilgi Teknolojileri ve koordinasyon Dairesi Başkanlığı Ankara,2010, s.4

[2] National Infrastructure Protection Plan, s.19 , http://www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf

[3] Avrupa Komisyonu, "Kritik Altyapıların Korunması için Bir Avrupa Programı,Rapor", http://eurlex.europa.eu/LexUriServ/site/en/com/2005/com2005_0576en01.pdf

[4] Bilgi Güvenliği Politika Konseyi, "Kritik Altyapılar için Bilgi Güvenliği Önlemleri Üzerine Eylem Planı, Karar", s.2, http://www.nisc.go.jp/eng/pdf/actionplan_ci_eng.pdf

[5] D.J. Gaushell, W.R. Block, SCADA communication techniques and standards. Computer Applications in Power, IEEE, 1993, 6.3: s.45-50.

[6] Endüstriyel Otomasyon teknolojileri Scada Sistemleri s.4 http://ytumekatronik.files.wordpress.com/2012/12/scada-sistemleri-1.pdf

[7] S. A. Boyer, SCADA: supervisory control and data acquisition. International Society of Automation, 2009.

[8] M. Ünver, C. Canbay, A.G. Mirzaoğlı, Siber Güvenliğin Sağlanması, Bilgi Teknolojileri ve koordinasyon Dairesi Başkanlığı Ankara,2009, s.41

[9] C. Alberts, A. Dorofee, Georgia Killcrece, R. Ruefle, M. Zajicek, Defining Incident Management Processes for CSIRTs: A Work in Progress,2004, s.25

[10] M. Brown, D. Stikvoort, P. Kossakowski, G. Killcrece ,R. Ruefle, Handbook for Computer Security Incident Response Teams (CSIRTs),2003, s.189

[11] A step-by-step approach on how to o set t up a csırt, European Network and information Security Agency (ENISA), 2006, s.66

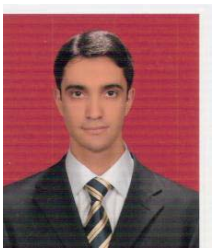
[12] http://www.tubitak.gov.tr/tr/haber/siber-saldirilara-karsi-yerli-savunma-araci-gelistirildi,Erişim Tarihi:12.07. 2013

[13] H. Bahşi, Ulusal Bilgi Sistemleri Güvenlik Programı, TÜBİTAK UEKAE İstanbul,2008.s.11

[14] M.Eriş, Bilgisayar Güvenlik Olayları Müdahale Çalışmaları, TÜBİTAK UEKAE İstanbul,2008,s.33

Melih DURAK lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2007 yılında Beykent Üniversitesinde Uluslararası İlişikiler dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Orta Doğu, ve siber savaş konularına ilgi duymaktadır.

İnan SEMİZ lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Avrupa Birliği, ve siber savaş konularına ilgi duymaktadır.



Selçuk Sönmez lisans eğitimini 2004 yılında Sistem Mühendisliği dalında Kara Harp Okulu'nda tamamlamıştır. Yüksek Lisans Eğitimini 2009 yılında İstanbul Üniversitesi'nde Uluslararası İlişikiler dalında yapmıştır. Hâlihazırda İstanbul'da Kara Harp Akademisi'nde öğrenim görmektedir. Uluslararası ilişkiler, Avrupa Birliği, ve siber savaş konularına ilgi duymaktadır.