Kritik Altyapıların Siber Güvenliğinin Sağlanmasında Üçlü Boyut Yaklaşımı

İnan Semiz, Kerim Göztepe, Recep Kılıç

***Özet*—Kritik altyapılar ülkeler için hayati öneme sahip sistemlerdir. Bu sistemlerin önemi arttıkça korunmasına yönelik çaba da bir o kadar artmaktadır. Sistemlerin gün geçtikçe karmaşıklaşması, altyapısında bilgi sistemlerinin yoğun kullanılması ve her geçen gün artan siber tehditler bu noktadaki güvenlik çalışmalarını arttırmıştır. Yapılan çalışmalar kritik altyapıların siber güvenliğinin sağlanmasında temel üç boyutu ön plana çıkarmıştır. Bunlar; kurumların sistemlerinin teknik altyapısını ilgilendiren teknik boyut, kritik altyapıların yönetimini ilgilendiren kurumsal boyut, ve siber güvenliğin sağlanmasında önemli bir konu olan ulusal ve uluslararası işbirliği boyutudur.**

***Anahtar Kelimeler*—Supervisor Control and Data Acqusition Systems (SCADA) Kritik Altyapı, Siber Güvenlik**

***Abstract*—Critical infrastructure systems are of vital importance for the countries. As the importance of these systems increasing the protection effort is also increasing. Today the complexity of the systems and the intensive use of information systems cause growing cyber threats for security efforts. Ensuring the security of critical infrastructure, cyber studies have highlighted the main three dimensions. These are technical infrastructure of institutions and systems, institutional dimension that concerns the management of critical infrastructures, and cyber security which is an important issue in maintaining the size of the national and international co-operation.**

***Index Terms*—SCADA, Critical infrastructure, Cyber security**

I. GİRİŞ

KRİTİK altyapılar insanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve herhangi bir aksama, yok edilme veya bu fonksiyonları sürdürmede yetersiz kalma sonucunda belirgin etki gösterecek varlık, sistem veya ilgili parçaları [1] olarak tanımlanabilir. Sağlık, enerji, su, ulaşım, bilgi ve iletişim, finans, gıda, kamu düzeni ve güvenlik, nükleer biyolojik kimyasal ve radyoaktif madde endüstrileri gibi çok değişik alanlar ülkeler tarafından kritik altyapılar olarak kabul edilmektedir [2].

Teknolojinin baş döndürücü bir hızla gelişmesi coğrafi olarak birbirinden ayrı sistem altyapılarının birbirine entegrasyonuna imkan sağlamıştır. SCADA sistemleri [2,3] olarak da adlandırılan, entegrasyonun temelini oluşturan bu kontrol yapıları teknolojinin gelişimi ile paralel olarak mimari yapısı itibariyle;

- birinci nesil monolitik,
- ikinci nesil dağıtık (distributed)
- ve üçüncü nesil ağ tabanlı (networked) olarak üç nesile ayrılabilir [4].

İlk geliştirilen SCADA sistemlerinde hem üreticiye özel protokoller kullandığı hem de diğer ağlarla bağlanmadığı için daha çok fonksiyonellik ön plana çıkmıştır [5]. Bu nedenle çok fazla güvenlik özelliği eklenmemiştir [6]. Fakat süreç içerisinde SCADA sistemleri için standart protokollerin [7] yaygınlaşması sistemlerin internet ya da kapalı bilgisayar ağları üzerinden kontrol edilmesi güvenlik risklerini de artırmaya başlamıştır. Bu riskler SCADA sisteminin internete bağlılık düzeyine göre artmaktadır[8,9]. Geniş alan ağına bağlı kontrol sistemlerinin üçüncü nesilde yoğun biçimde kullanılması sistemlerin yönetiminde büyük kolaylıklar sağlarken dış tehditlere karşı da hassasiyeti aynı oranda arttırmıştır. Son dönemde siber saldırıların öncelikli hedefi haline gelen bu sistemlerin güvenliğine yönelik ülkelerin ulusal ve uluslararası çalışmaları yoğunlaşmıştır [10,11]. Ancak her ne kadar bu konuda birçok çalışma yapılmış olsa da ortak bir yöntem ortaya konamamıştır.

II. KRİTİK ALTYAPILARIN SAĞLANMASINDA ÜÇLÜ BOYUT YAKLAŞIMI

A. *Çalışmanın Amacı*

Kritik altyapıların siber güvenliğinin sağlanmasında ülkeler ve uluslararası kuruluşlar birçok çalışma gerçekleştirmiş ancak bunlar arasında ortak ve çözüm sağlayan bir yöntem belirlenememiştir. Bu maksatla ortaya konacak bu yaklaşımla ülkelerin kritik altyapılarının siber güvenliğinde kullanabilecekleri temel ve sade bir yöntemin oluşturulması amaçlanmıştır.

B. *Üç Boyut Yaklaşımı*

Kritik altyapıların siber güvenliğinin sağlanmasında üç boyut yaklaşımı teknik boyut, kurumsal boyut, ulusal ve uluslararası işbirliği boyutlarından oluşmaktadır (Şekil 1).

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

Kerim Göztepe, Ph.D. Harp Akademileri Komutanlığı, Kara Harp Akademisi, Harekat Ana Bilim Dalı, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: kerimgoztepe@gmail.com.

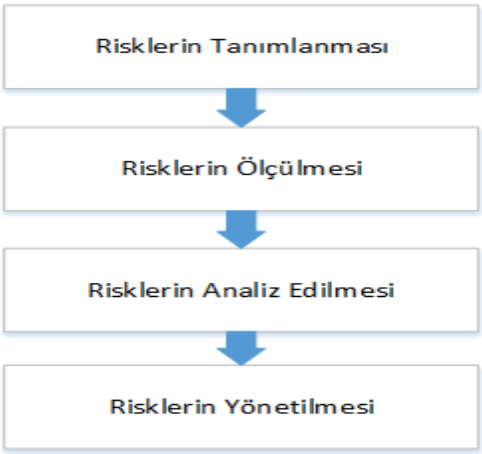
Recep Kılıç, Harp Akademileri Komutanlığı, Kara Harp Akademisi, Yenilevent, 34330, Pbx: +90 212 398-0100, İstanbul-Türkiye, e-mail: rkilic40@gmail.com.

Şekil 1. Üç boyut yaklaşımı

(I) Teknik Boyut

Birinci ve en temel boyut teknik boyuttur. Sistemi oluşturan alt sistemlerin hassasiyetleri aynı zamanda tüm sistemin hassasiyetidir. Bütüncül olarak sistemin güvenliğinin sağlanması ve alt sistemlerin güvenliğinin sağlanmasında sistematik bir yaklaşım önemli bir konudur.

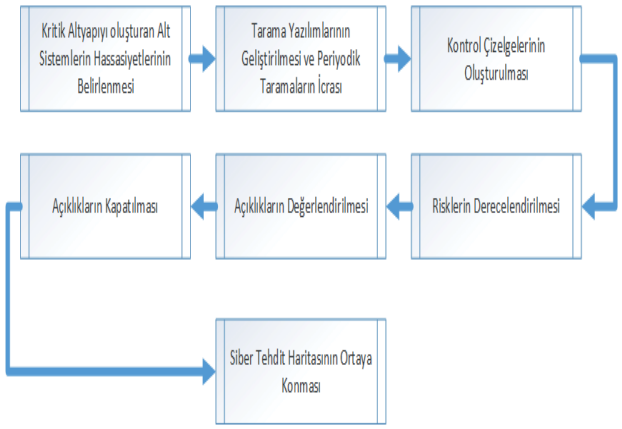
Kritik altyapının yönetilmesini sağlayan sistemin tüm yapısı incelenerek risk yönetimi aşağıdaki basamakları izleyerek uygulanmalı ve sistemlerin risk haritası ortaya çıkarılmalıdır (Şekil 2).



Şekil 2. Risk yönetimi

Teknik boyutta önemle üzerinde durulması gereken bir diğer konu da teknik açıklık yönetimidir. Kısaca, bilgi sistemlerinde var olan teknik açıklıkların tespit edilmesi, açıklıkların değerlendirilip önlemlerin ortaya konması, uygun önlemlerin seçilerek uygulanması ve uygulama sonuçlarının gözlenmesi [3],[12]olarak tanımlanan bu yöntem, kritik bir altyapıdaki temel bilgi güvenliği konularından birisidir ve sürekli işlemesi gereken bir süreçtir. Her ne kadar açıklık yönetimi dendiğinde bazen penetrasyon testlerinin belirli aralıklarla icra edilmesi veya ortaya çıkan açıklıkların kapatılması, bir diğer deyişle yamalanması olarak algılansa da bu yöntemler teknik açıklık yönetiminin sadece bir bölümünü oluşturmaktadır. Kritik altyapıların siber güvenliğinin sağlanmasında teknik açıklık yönetiminin kurumsal olarak belirlenecek bir metodoloji ile işletilmesi büyük önem taşımaktadır. Bu sürecin de en önemli basamağını hassasiyetleri itibariyle korunması gereken sistem veya alt sistemlerin belirlenmesi oluşturmaktadır.

Bir diğer önemli basamak da sistem altyapılarının sürekli olarak taranmasıdır. Teknik açıklık yönetimi aynı zamanda risk yönetimi süreci ile paralel işletilmelidir [8],[12]. Açılıklardan ortaya çıkan risklerin derecelendirilmesi gerekmektedir. Tespit edilen açıklıklar mutlaka yönetim tarafından değerlendirilmeli ve doğrulanmalıdır. Son olarak da açıklıkların ortadan kaldırılması için gerekli yöntemler uygulanmalıdır. Teknik açıklık yönetimi ile kuruma kazandırılması gereken en önemli çıktı da güncel siber tehdit haritasıdır. Bu sayede ihtiyaç duyulan koruma sistemlerinin geliştirilmesi ve gerektiğinde satın alınması sağlanacaktır. Aşağıda teknik açıklık yönetiminin sistematik ve sade biçimde akış diyagramı yer almaktadır (Şekil 3).



Şekil 3. Teknik açıklık yönetimi

Teknik boyutun önemli bir diğer basamağı da sisteme müdahil olan yönetici ve kullanıcıların erişiminin kontrol altında bulundurulmasıdır. Kritik altyapıların yönetiminde grid bir yapı olmalı ve hiçbir zaman bilgi sadece tek noktadan ve kişiden akmamalıdır. Sistemin kontrol edilmesi ile personele güven ayrı konulardır dolayısıyla kontrol güvene mani değildir ve aynı zamanda herkes sisteme ait bilmesi gerektiği kadar bilgiye ulaşmalıdır. Ağ denetimi de bu kapsamda gerek yerel ağlarda gerekse de geniş alan ağında uygulanması gereken bir yöntemdir.

Çoğu zaman gözden kaçan ve etkin uygulanmayan teknik boyutun bir diğer basamağı da ağ topolojilerinin ve sistem konfigürasyon yönetiminin sağlıklı yapılması hususudur. Sisteme giren altyapıların ve yazılımların sürümlerinin sistem envanterine dahil edilmesi veya çıkarılması konfigürasyon yönetiminin en basit tanımıdır.

Kritik altyapıların yönetiminde kullanılan SCADA sistemlerin güvenliğinin sağlanmasında yukarıda ifade edilen teknik boyutun basamaklarının yanında sistemlere kazandırılan bir diğer güvenlik tedbiri de sistemlerin kendini koruma yazılım ve sistemleridir. Bunları sıralarsak [13,14]; güvenlik duvarı (firewall), antivirüs yazılımları, saldırı tespit sistemi (intrusion detection system), alarm zayıflık tarama yazılımları, ağ dinleme ve yönetim yazılımları, kütükleme (log) yazılımları ve yedekleme araçlarıdır. Teknik Açıklık yönetimi ile ortaya çıkacak siber tehdit haritasına göre sahip olunan bu yazılım ve sistemler güncellenmelidir.

(II) Kurumsal Boyut

Kritik Altyapıların kurumsal olarak yönetimi güvenliğin bir diğer boyutudur. Kritik altyapıların yönetiminde kurumsal olarak en önemli basamak kurumun siber güvenlik politikasına sahip olmasıdır. Bu kapsamda kurum olarak siber farkındalığın tüm personel tarafından kanıksanması, kullanıcı, uzman ve yönetici olmak üzere her seviyede eğitimin personele verilmesi gereklidir. Teknik boyuttaki tedbirlerin uygulama kriterlerini içeren, bilginin erişimini, korunmasını ve değişimini belirli kriterlere bağlayan konular yazılı olarak kurum içinde personele bildirilmelidir.

Kritik altyapıların yönetimi siber tehditler haritasına uygun olarak kendi kurumsal yapısı bünyesinde uygun savunma teşkilatı kurmalı, bu yapı ile ulusal ve uluslararası kuruluşlarla gerekli koordinelerde bulunmalıdır.

Kurumsal olarak ulusal ve uluslararası siber güvenlik yapılanmaları ile işbirliği sağlanmalı ve icra edilen siber güvenlik tatbikatlarında kritik altyapı en etkin biçimde test edilmelidir. Teknik boyut ile kurumsal boyutun kesiştiği risk yönetimi, erişim yönetimi, konfigürasyon yönetimi ve teknik açıklık yönetimi gibi süreçlerde yönetim olarak mümkün olan en üst seviyede şeffaf olunmalı ve sistemlerin eksikliklerinin üzerinin kapatılması yerine en ivedi şekilde çözüm için gerekli işlemler yapılmalıdır.

SCADA sistemlerinde yer alan alt sistemlerin üreticilerine yönelik değişiklikler izlenmeli, kullanılan bu altyapının dünyada maruz kaldığı saldırılardan gerekli dersler çıkarılmalıdır. Bazı ülkelerin SCADA sistemlerine saldırı yapılmış ve çok ciddi zararlar verilmiştir. Burada kullanılan sistem altyapısı ile aynı sistemi kullanan altyapının aynı tehditle yüzyüze olduğu aşikardır. Bu durumda üretici firmanın sorgulanması gerektiğinde firma tarafından önleyici ek tedbirler üretmesi beklenmelidir.

(III) Ulusal ve Uluslararası İşbirliği Boyutu

Siber Tehditler saldırı kaynakları ve yöntemleri göz önünde bulundurulduğunda çok farklı ve kapsamlı bir güvenlik anlayışını kurumlar için zorunlu kılmaktadır. Bundan dolayı gerek ulusal gerekse de uluslararası boyutta kurumlar kritik altyapılarının güvenliğini sağlama noktasında her türlü işbirliği yoluna başvurmalıdır.

Ülkeler kritik altyapıların siber güvenliğini sağlama noktasında ulusal boyutta yapmaları gereken ilk adım kritik altyapıları belirlemektir. Kritik altyapıların önem derecesine gore önceliklendirilmesi ve buna uygun yasal çerçevenin çizilmesi gerekmektedir. Dünyada bu konuda çeşitli çalışmalar yapılmıştır. "Kritik Altyapı Belirleme, Önceliklendirme ve Koruma" başlıklı HSPD–7, kritik altyapıların korunması konusundaki ana düzenlemelerden biridir. Bu direktif, kurumlara ve bakanlıklara terörist saldırılardan korunmak için kritik alt yapıları ve önemli kaynakları belirleme ve önceliklendirme yükümlülüğü getirmektedir [15].

Ülke içinde her kurumun kendi sistemlerini siber saldırılara karşı korumak için uyguladıkları politikalar ve metodlar bulunmaktadır. Tüm bu politikaların üstünde bir politika ve kurumlar arası oluşturulacak bir sinerji ile tüm kabiliyetlerin bir havuzda toplanması ulusal olarak atılması gereken bir adımdır. Bu kapsamda kurumların oluşturduğu siber güvenlik teşkilatlarının işbirliği de sağlanmalıdır.

Ulusal sinerjinin oluşturulması sonucunda tüm kritik altyapı ve diğer sistem altyapılarının siber güvenlik tatbikatları ile test edilmesi ve ortaya çıkan açıklıkların ortak elde edilen tecrübelerle yönetilmesi siber tehditlerle mücadele etmede ulusal bazda ülkelere büyük güç katacaktır.

Kritik altyapılarda geniş alan ağının kullanılmaya başlanması nedeniyle bir ülkenin zarar görmesi diğer ülkeleri de etkileyecek ve ülkeler bu konuda birbirine bağımlı olacaktır. Bu nedenle ülkeler ortak bir biçimde kritik altyapıları koruma çabalarını ve prensiplerini, genel kabul gören kılavuzları/standartları, tanımlamaları, kritik altyapı önceliklerini tam olarak belirlemelidir.

Kritik Altyapıların siber güvenliğinde en can alıcı noktalardan bir tanesi de uluslararası işbirliğinin sağlanmasıdır. Siber uzay ülkeler arasındaki sınırları kaldırmıştır. Sınırların ortadan kalktığı bu ortamda birleşme ve işbirliği yapma bir zaruret halini almıştır. Her an ülkelerin en önemli yapılarının zarar görebileceği bu yol ve yöntem üzerinde beraber hareket etmek, güvenlik seviyelerinin ve tecrübelerinin paylaşımına imkan sunan tatbikatları icra etmek bu yapıların güvenliğinin sağlanmasında önem taşıyan uygulamalardan bir tanesidir. Uluslararası işbirliği boyutunda bir diğer önemli aşama da siber saldırılara uluslararası hukuk çerçevesinde uygulanacak yaptırımlardır. Ülkelerin bu aşamada uzlaşıya varması kritik altyapıların güvenliğinin sağlanmasında en önemli adımlardan bir tanesi olacaktır.

III. SONUÇ

Bu çalışma ile kritik altyapıların siber güvenliğinin sağlanmasında ortaya konacak tedbirleri çerçeveleyen idarelerin daha kolay sistemlerini kontrol edebilecekleri bir yapı oluşturulması hedeflenmiştir.

Kritik altyapıların yönetimi ve izlenmesi büyük oranda teknoloji ile bütünleşen SCADA sistemleri ile yapılmaktadır. SCADA sistemlerinin bilgi sistemleri ile bütünleşmesi birçok kolaylık ve esneklik sağlaması yanında ciddi güvenlik risklerini de beraberinde getirmiştir. Bu kapsamda ulusal ve uluslararası boyutta kritik altyapıların güvenliğinin nasıl sağlanacağı sorusu gün geçtikçe önem kazanmaktadır.

Bu konuda Dünya'da birbirinden bağımsız yapılan birçok çalışma biraraya getirildiğinde dikkat çeken en çarpıcı husus çalışmada ortaya konan üç temel boyutun kritik altyapıların güvenliğinin sağlanmasında esas hatlar olduğudur. Ortaya konacak her türlü güvenlik tedbiri ve uygulaması bu üç boyuttan herhangi biri içinde değerlendirilebilecektir. Teknolojik gelişmeler sonunda ortaya çıkan bilişim dünyasında siber tehditlerle mücadele ancak kapsamlı bir yaklaşımla gerçekleşebilir. Üç boyut yaklaşımı bu mücadelede etkin bir şekilde kullanılabilir.

KAYNAKLAR

[1] Avrupa Komisyonu, 702 sayılı "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması,"Konulu Tebliğ, 2004, s. 3.
[2] D.J. Gaushell, W.R. Block, SCADA communication techniques and standards. Computer Applications in Power, IEEE, 1993, 6.3: s.45-50.
[3] S. A. Boyer, SCADA: supervisory control and data acquisition. International Society of Automation, 2009.
[4] R.L Krutz, Securing SCADA systems. John Wiley & Sons, 2005.
[5] J. Pollet, Developing a solid SCADA security strategy. In: Sensors for Industry Conference, 2002. 2nd ISA/IEEE. IEEE, 2002. s. 148-156.
[6] V. M. Igure, S.A. Laughter, R.D. Williams, Security issues in SCADA networks. Computers & Security, 2006, 25.7: s.498-506.
[7] G. Clarke, D. Reynders, E. Wright, Practical modern SCADA protocols. IDC technologies, 2004.
[8] M. Kara, S. Çelikkol, 4. Ağ ve Bilgi Güvenliği Sempozyumu Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği, Kocaeli Üniversitesi, 2011.
[9] C. Nan, I. Eusgeld, W. Kröger, Analyzing vulnerabilities between SCADA system and SUC due to interdependencies. Reliability Engineering & System Safety, 2013, 113: s.76-93.
[10] N. Cai, J. Wang, X. Yu, Scada system security: Complexity, history and new developments. In: Industrial Informatics, 2008. INDIN 2008. 6th IEEE International Conference on. IEEE, 2008. s.569-574.
[11] T. Brown, Security in SCADA systems: How to handle the growing menace to process automation. Computing & Control Engineering Journal, 2005, 16.3: s.42-47.
[12] H. Bahşi, Teknik Açıklık Yönetimi, 2008.
[13] P.A.S. Ralston, J.H. Graham, J.L. Hieb, Cyber security risk assessment for SCADA and DCS networks. ISA transactions, 2007, 46.4: 583-594.
[14] C. P. Pfleeger, S. Pfleeger, Lawrence. Security in computing. Prentice Hall PTR, 2006.
[15] M. Ünver, C. Canbay, B.H. Özkan, Kritik Altyapıların Korunması, Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı Ankara,2010, s.14.