KRİTİK ENERJİ ALTYAPILARININ KORUNMASI VE SİBER GÜVENLİK SEMPOZYUMU SONUÇ BİLDİRGESİ

ELDER ile BGD'nin birlikte düzenlediği Sempozyum, 8 Aralık 2015 tarihinde Bilkent Hotel'de gerçekleştirilmiştir. Sempozyuma ortalama 200 kişi katılım sağlamıştır. Sempozyumun açılışını TEDAŞ Genel Müdürü Mükremin ÇEPNİ, Yenilenebilir Enerji Genel Müdürü Münip KARAKILIÇ, ELDER Genel Sekreteri Uğur YÜKSEL, BGD Yönetim Kurulu Başkanı Ahmet Hamdi ATALAY ve GAZBİR Dernek Müdürü M. Cem ÖNAL tarafından yapılmıştır. Açılış konuşmalarında enerji sektöründe üst yönetimi ve çalışanlarında bilgi güvenliği farkındalığı oluşturulması, milli çözümlerin kullanılması ve dağıtım sektörü özelinde "Siber Güvenlik Stratejisi ve Eylem Planı" oluşturulmasının önemine vurgu yapılmıştır.

Sempozyumda gerçekleştirilen birinci panelde siber güvenlik ile ilgili düzenlemeler ele alınmış ikinci panelde ise kritik altyapıların korunmasına yönelik uygulamalar ve öneriler paylaşılmıştır. Ayrıca Havelsan, Siemens ve Ernst&Young Türkiye tarafından da sunumlar gerçekleştirilmiştir.

Sempozyum bitiminde BGD Denetleme Kurulu Başkanı Mustafa ÜNVER tarafından aşağıda sunulan "Sempozyum Sonuç Bildirgesi" katılımcılarla paylaşılmıştır.

1. Enerji sektörü STK'ları ile başta BGD olmak üzere siber güvenlik konusunda faaliyet gösteren STK'ların işbirliği arttırılmalıdır. Bu kapsamda enerji sektöründe bilgi güvenliği farkındalığın arttırılması, eğitim altyapı ve içeriğinin oluşturulması, sektöre özgü siber güvenlik politika ve stratejilerinin belirlenmesi ve çözüm süreçleri geliştirilmesi gibi ana başlıklarda ortak çalışma grupları oluşturulmalıdır.
2. Siber güvenliğin sağlanmasında en kritik bileşenin insan olduğu tüm katılımcılar tarafından kesin bir dille ifade edilmiştir. Bu tespitten hareketler enerji sektöründe çalışan personele, mutlaka temel bilgi güvenliği eğitimi verilmelidir. Enerji sektörü çalışanları için "Bilgi Güvenliği Eğitimi"nin ELDER tarafından organize edilmesi, eğitimin içeriği ve eğitim verilmesinin BGD tarafından yapılmasının faydalı olacağı değerlendirilmektedir.

3. Sürdürülebilir bir siber mücadele için enerji sektörünün tüm bileşenlerinin siber güvenlik farkındalığını arttıracak etkinlikler düzenlenmeli, çalışanların siber güvenlik farkındalığının dinamik tutulması için zaman zaman bilgi işlem birimlerince hatırlatma mesajları ve dahili tatbikatlar yapılmalıdır.
4. Kritik enerji altyapılarının korunması çalışmalarının tüm enerji sektörünü içine alan bütüncül bir bakış açısıyla ele alınması ve takip edilmesi gerekmektedir. Bunun için ETKB bünyesinde enerji sektöründe çalışan işletmecilerin, ilgili STK'ların ve ilgili kamu kurumlarının temsilcilerinden oluşan "Enerji Sektörü Siber Güvenlik Koordinasyon Kurulu" oluşturulmalı ve bu kurul eliyle siber güvenlik çalışmaları koordine ve takip edilmelidir.
5. Siber saldırıların kritik altyapıları hedef almak suretiyle doğrudan ülkelerin milli güvenliğini tehdit ettiği gerçeğinden hareketle ETKB ya da EPDK tarafından tüm paydaşların katılımıyla enerji sektörüne özel "Kritik Enerji Altyapılarının Korunmasına Yönelik Politika ve Strateji Belgesi ve Eylem Planı" hazırlanmalıdır. Bu çalışmanın kritik altyapı olarak tespit edilen diğer sektörler için de yapılmasının gerektiği belirtilmiştir.
6. Öncelikli olarak dağıtım şirketlerinin siber güvenlik durum tespitinin yapılması gerektiği belirtilmiştir. ELDER ve BGD, 2016 yılında bu konuda bir çalışma yapmayı planlayacaklardır.
7. Kritik enerji altyapılarının korunmasına yönelik çok sayıda standart mevcuttur. Bu standartların tüm yönleriyle incelenmesi ve raporlanması gerektiği değerlendirilmektedir. Bu çalışma sonrası işletmecilerin bilgi güvenliği standartlarına uygun hizmet vermesi yönünde hem belgelendirme hem de denetim çalışmaları yapılmalıdır.
8. Kritik enerji altyapılarının korunması maksadıyla kullanılan donanım ve yazılımların başka güvenlik sorunlarına yol açıp açmadığı ciddi bir endişe olarak karşımıza çıkmaktadır. Bu endişenin bertaraf edilebilmesi için gerek donanım gerek yazılım alanında milli çözümler üretilmesinin şart olduğu düşünülmektedir. EPDK'nın ar-ge desteğinin, milli çözümlerin geliştirilmesi yönünde arttırılarak devam ettirilmesi gerekmektedir.
9. USOM-SOME yapısının henüz bilgilendirmenin ötesine geçmediği belirtilmiştir. SOME'lerin USOM'dan beklentilerini ortaya koyacak bir çalışma yapılmasının yararlı olacağı ifade edilmiştir.
10. Kurumsal SOME'lerin bazı uygulama zorlukları yaşadığından bahisle Kurumsal SOME'lerin katkısıyla Sektörel SOME'lerde fon oluşturulması ve bu fonun Kurumsal SOME'ler için kullanılması yönünde görüş belirtilmiştir.

11. Endüstriyel Kontrol Sistemi (EKS) kullanan kurumlar için EKS-SOME kurulması değerlendirilmelidir.
12. EKS'lerin kurulum aşamasında siber güvenlik ihtiyaçlarının düşünülmesi gerektiği aksi halde hem maliyetin arttığı hem de istenilen seviyede hizmet alınamayabileceği ifade edilmiştir.
13. USOM, yıllık faaliyet raporu yayımlamalıdır.

Kamuoyuna saygıyla duyurulur. 08.12.2015

Sempozyum Yürütme Kurulu