ÇAKMAK 30 YEARS

15 Ağustos 2023

Enerji Sektöründe Güncel Konular #7

Enerji Sektöründe Siber Güvenlik

Bilişim teknolojileri aracılığıyla enerji tesislerinde yürütülen faaliyetler izlenip denetlenebilmekte, arz edilen ve tüketilen enerji miktarlarına ait veriler toplanarak piyasada öngörü oluşturulabilmektedir. Bu nedenle, enerji sistemlerinin fiziki güvenliği yanında bilişim güvenliğinin sağlanması da önem arz etmektedir. Bu yazımızda, enerji sektörü özelinde siber güvenlik konusunu ve Türkiye'de mevcut olan hukuki çerçeveyi inceledik.

1. Enerji Sektöründe Siber Güvenlik Kavramları

Enerji sistemleri günümüzde üretim ve sanayide olduğu kadar bireylerin gündelik yaşantılarının da vazgeçilmez bir parçasını oluşturmaktadır. Diğer birçok sektör ile bütünleşik yapısı dikkate alındığında enerji sistemlerinde meydana gelecek aksamalar toplumsal olarak büyük zararlara yol açabilecek potansiyele sahiptir. Bu sebeple, enerji sektörü, *kritik altyapı* barındıran sektörler arasında kabul edilmektedir. Kritik altyapılar "*işlediği bilginin/verinin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim sistemlerini barındıran altyapıları*" olarak tanımlanmaktadır.[1]

Siber güvenlik ise, genel olarak, siber ortamda yer alan bilgileri istismar etmek, bozmak, değiştirmek, sistemlere erişimi engellemek ya da zarar vermek amacıyla gerçekleştirilen saldırıları önleme veya bunlara karşı savunma, ağların ve altyapının kullanılabilirliğini ve bütünlüğünü ve bunların içerdiği bilgilerin gizliliğini koruma yetisini ifade etmektedir.[2] Buna göre, siber güvenlik tanımı gizlilik, bütünlük ve erişilebilirlik boyutlarını barındırmaktadır. Enerji sistemleri özelinde ise, *gizlilik*; bilgiye yalnızca üretim, iletim, dağıtım şirket personeli ve tüketicilerin ulaşabilmesi; *bütünlük*; gerilim, frekans, elektrik gücü, yük akışı ve faturalandırmaya ilişkin bilgilerin değiştirilmemesi, bozulmaması ve yok edilmemesi; *erişilebilirlik* ise sektörde rol alan aktörlerin belirli bir hiyerarşi içinde bilgiye erişmesi anlamına gelmektedir.[3]

Enerji sektöründe faaliyetlerin bir veya birden fazla merkezden izlenmesini bazen de yönetilmesini sağlayan çeşitli yönetim ve kontrol sistemleri mevcuttur. Endüstriyel kontrol sistemleri olarak anılan bu sistemler, uygulanmakta olan mevzuatta da genel hatlarıyla tanımlanmıştır.[4] Bunlar arasında en sık tercih edilen sistem olarak bilinen Veri Tabanlı Kontrol ve Gözetleme Sistemi ("SCADA") öne çıkmaktadır.[5] Bu sistemlerin

---

1 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), s. 9.

2 Uluslararası Enerji Ajansı tarafından hazırlanan 2021 tarihli "*Enhancing Cyber Resilience in Electricity Systems*" adlı rapor ("UAE Raporu"), s.8. Erişim Tarihi: 9 Ağustos 2023. URL: https://iea.blob.core.windows.net/assets/0ddf8935-be23-4d5f-b798-3aad1f32432f/Enhancing_Cyber_Resilience_in_Electricity_Systems.pdf

3 Aydin, Hakan & Barışkan, Mehmet & Çetinkaya, Ali. (2021). Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi. Güvenlik Bilimleri Dergisi, 10, s. 154-155.

4 Yönetmelik (bu makalede tanımlandığı şekilde) Madde 1'e göre endüstriyel kontrol sistemleri "*enerjinin üretilmesi, enerji sağlayan hammaddelerin işlenip tüketime hazır hale getirilmesi, enerjinin iletim veya dağıtım katmanları aracılığı ile aktarılması gibi süreçlerin izlenmesini, yönetilmesini sağlayan, işletim sistemleri ile çalışan yönetim ve kontrol sistemlerini*" ifade etmektedir.

5 ENISA (European Network and Information Security Agency) tarafından hazırlanan 2011 tarihli "*Protecting Industrial Control Systems*" adlı rapor, s.1. Erişim Tarihi: 11 Ağustos 2023. URL: https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

fonksiyonu, en yalın ifadeyle, gerçek zamanlı verileri toplamak ve işlemek, cihazlarla doğrudan etkileşim kurarak olay kayıtlarını tutmaktır. Günümüzde enerji tesisleri endüstriyel kontrol sistemleri ile donatılmış olup bu sayede veriler kolaylıkla toplanabilmekte ve enerji piyasalarında arz talep dengesi açısından güvenilir tahminlerde bulunulabilmektedir.

2. Siber Güvenliğin Enerji Sektöründeki Önemi

Enerjinin ulaşım, aydınlatma gibi günlük hayatın pek çok alanında daimi bir ihtiyaç olma niteliği dolayısıyla, enerji tesislerinin işlevlerini kesintisiz olarak sürdürmesi büyük önem arz etmektedir. 2022 yılına ilişkin veriler uyarınca, enerji sektörüne karşı şu ana kadar 403 siber saldırının gerçekleştiği ve her bir saldırının ortalama 4.72 milyon dolar zarara yol açtığı tespit edilmiştir.[6]

Siber saldırılar sonucu yaşanan hizmet kesintisi kısa süreli dahi olsa sağlık ve ulaşım gibi pek çok temel hizmetin aksamasına sebep olabilmektedir.[7] Örneğin, 2021 yılında gerçekleşen Colonial Pipeline saldırısında doğal gaz iletim sistemlerinde basınç artışı oluşturularak borular işlevsiz hale getirilmiştir. Bu nedenle devre dışı kalan akaryakıt kara yolu ile transfer edilmiştir.[8] Saldırı neticesinde yerel halk panik halinde benzin stoklamak üzere benzin istasyonlarına hücum etmiş ve bu durum karşısında benzinin fiyatı ülkede son dönemin en yüksek seviyelerine ulaşmıştır.[9]

Siber saldırılar, günlük yaşantının yanı sıra enerji piyasalarının işleyişine de olumsuz etki edebilmektedir. Elektrik piyasasında gün öncesi ve sonrası tahminler yapılmakta, söz konusu tahminlere esas teşkil eden veriler ise santrali donatan bilişim sistemlerinden alınmaktadır. Bu sistemlere yönelik bilgiyi değiştiren veya yok eden saldırılar gerçekleştirildiğinde enerji arz talep dengesi bozulabilecek ve sistemde dengesizlikler oluşturabilecektir. Ayrıca, üretim, iletim ve dağıtım altyapılarının birbiri ile iç içe olması sebebiyle bu altyapılardan birinin zarar görmesi halinde enerji altyapılarının tümü etkilenebilmektedir. Örneğin, 2015 yılında Ukrayna'da bir tedarik şirketine yapılan siber saldırı sonucunda zararlı yazılım aracılığıyla SCADA sistemlerine erişilmiş ve trafo merkezleri güçten kesilmiştir.[10] O gün 3 MWh elektrik arz edilememiş ve yaşanan elektrik kesintisi sonrasında ülke 1 ila 6 saat süreyle karanlığa gömülmüştür. İran'da bulunan bir nükleer santrale düzenlenen Stuxnet saldırısında ise santrifüjlere enerji sağlayan elektrik akım frekanslarında dalgalanmalar meydana getirilerek santrifüjlerin patlamasına yol açılmış ve buna bağlı radyoaktif zararlar meydana gelmiştir.[11]

Tüm bunlardan hareketle, enerji sektöründe siber güvenliğin oynadığı kritik rol nedeniyle, ilgili otoriteler kadar sektörde faaliyet gösteren yatırımcılar tarafından da saldırıların önlenmesi, saldırı anında ve sonrasında gerekli aksiyonların en kısa sürede alınabilmesi için uygun bilişim altyapısının kurulması ve düzenli olarak kontrol edilmesi hayati önem taşımaktadır.

3. Türkiye'de Enerji Sistemlerinin Siber Güvenliğine İlişkin Hukuki Çerçeve

Her sektörde olduğu gibi enerji sektöründe de artan dijitalleşme siber tehditleri beraberinde getirmekte ve bu doğrultuda devletler siber güvenlik stratejileri oluşturmaktadır. Buna yönelik olarak, Türkiye'de siber güvenlik alanında 1999 yılından itibaren günümüze kadar birçok eylem planı oluşturulmuştur. Güncel olarak ise, 2020/15 Sayılı Cumhurbaşkanlığı Genelgesi[12] uyarınca Ulaştırma ve Altyapı Bakanlığı tarafından hazırlanmış olan 2020-2023 dönemlerini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ("Eylem Planı") uygulanmaktadır.

---

6 "Cyber Attack Statistics to Know in 2023". Erişim Tarihi: 9 Ağustos 2023. URL: https://parachute.cloud/cyber-attack-statistics-data-and-trends/

7 UEA Raporu, s.9.

8 "Colonial Pipeline Ransomware Attack: Everything You Need To Know". Erişim Tarihi: 9 Ağustos 2023. URL: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

9 "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity". Erişim Tarihi: 9 Ağustos 2023. URL: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

10 "2015 Ukraine Power Grid Hack". Erişim Tarihi: 9 Ağustos 2023. URL: https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

11 "Stuxnet (2010)". Erişim Tarihi: 9 Ağustos 2023. URL: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010)

12 29 Aralık 2020 tarihli ve 31349 sayılı Resmi Gazete'de yayımlanmıştır.

Eylem Planı'nda, enerji sektörünün de sayıldığı kritik altyapı sektörlerinin siber güvenliğinin sağlanmasına yönelik ilke ve hedefler belirlenmiş, ilgili kurum ve kuruluşların bu amaç doğrultusunda düzenlemeler ve uygulamaya yönelik çalışmalar yapması gerektiğinden bahsedilmiştir. Eylem Planı'nda belirlenen hedefler arasında kritik altyapıların siber güvenliğinin 7/24 korunması, kritik altyapı sektörlerinde düzenleme ve denetlemeye dayalı siber güvenlik yaklaşımının geliştirilmesi ve siber olaylara müdahale amacıyla proaktif siber savunma anlayışının geliştirilmeye devam edilmesi sayılmaktadır. Bu çerçevede, elektrik, doğal gaz ve petrol piyasalarında siber güvenliğin sağlanmasına yönelik çalışmalar Enerji Piyasası Düzenleme Kurumu ("EPDK") tarafından yürütülmektedir. Haziran ayında yayımlanan Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği[13] ("Yönetmelik") ile yine Temmuz ayında yayımlanmış olan Enerji Sektöründe Kullanılan Endüstriyel Kontrol Sistemleri İçin Güvenlik Analiz ve Test Usul ve Esasları[14] siber güvenlik amacıyla sağlanacak asgari standartları ve kontrol esaslarını düzenlemektedir.

Yönetmelik ile, önceki düzenlemelerden farklı olarak, ana kontrol başlıkları, sektörel kritiklik dereceleri, uygulama ve denetim hususları detaylı olarak ortaya konulmuştur. Bununla birlikte, Yönetmelik uyarınca;

- elektrik piyasasında iletim ve dağıtım lisansı ve geçici kabulü yapılmış ve işletmedeki kurulu gücü 100 MWe ve üzeri lisansa sahip her bir elektrik üretim tesisi sahipleri,

- doğal gaz piyasasında boru hattı ile iletim yapan doğal gaz iletim lisansı sahibi, sevkiyat kontrol merkezi kurmakla yükümlü doğal gaz dağıtım lisansı ve doğal gaz depolama lisansı sahipleri (LNG, yer altı) ve

- petrol piyasasında ham petrol iletim lisansı ile rafinerici lisansı sahipleri

yükümlü kuruluş olarak tayin edilmiştir. Organize Sanayi Bölgesi dağıtım ve üretim lisansı sahipleri ise Yönetmelik kapsamı dışında tutulmuştur.

Öte yandan, Yönetmelik enerji alt sektörlerinde lisans sahibi olan birçok kuruluşu kapsam dâhilinde saymakta ise de, Yönetmelik ile henüz sadece elektrik ve doğal gaz dağıtım sektörleri için modeller belirlenmiştir. Bu sektörler özelinde ilgili modeller çerçevesinde öngörülen yükümlülükler Yönetmelik'in Resmi Gazete'de yayımlandığı tarihte yürürlüğe girmiştir. Bununla beraber, elektrik ve doğal gaz dağıtım lisansı sahipleri dışında kalan lisans sahiplerinin Yönetmelik kapsamındaki yükümlülükleri, bu sektörlere ilişkin model çalışmaları tamamlandıktan ve EPDK tarafından yayımlandıktan sonra uygulama alanı bulacaktır.[15]

Yetkinlik modeli üç temel yetkinlik seviyesinden oluşmaktadır. Yükümlü kuruluşların sahip olması gereken yetkinlik seviyeleri parametreleri EPDK tarafından sektörel kritiklik dereceleri ile tespit edilecek ve belirlenen kritiklik dereceleri yükümlü kuruluşlara tebliğ edilecektir. Kritiklik derecelerine göre ise yükümlü kuruluşların yerine getirmesi gereken ana kontrol başlıkları belirlenecek, yükümlü kuruluşun yine bu başlıklar kapsamında belirlenen tamamlama süresi sonunda altyapısını kontrol başlıkları ile uyumlu hale getirmesi gerekecektir.

Yükümlü kuruluşların yetkinlik modeline uyumluluğu ise üç aşamalı bir denetime tabi olacaktır. Buna göre; ilk aşamada kuruluşun kendi iç kaynaklarıyla kendisini denetlediği "*öz denetim/ fark analizi*" denetimi, ikinci aşamada EPDK'nın belirlediği şartlara uyan firma ve personeller tarafından gerçekleştirilecek olan "*sektörel denetim*" ve nihayet üçüncü aşamada ise EPDK'nın öz kaynakları ile gerçekleştirilecek "*kurum denetimi*" bulunmaktadır.

Yönetmelik tahtında yükümlülüklerin ihlali halinde uygulanacak yaptırımlara ilişkin özel bir hüküm bulunmamaktadır. Bu nedenle, yaptırım türü ve miktarları her bir yükümlü kuruluş için faaliyet gösterdikleri piyasaların ana kanunlarında öngörülen hükümlere göre tayin edilecektir.

---

13 6 Haziran 2023 tarihli ve 32213 sayılı Resmi Gazete'de yayımlanmıştır.

14 16 Temmuz 2023 tarihli ve 32250 sayılı Resmi Gazete'de yayımlanan EPDK'nın 11956 sayılı ve 13 Temmuz 2023 tarihli Kararı ile yürürlüğe girmiştir.

15 EPDK sıkça sorulan sorular: https://www.epdk.gov.tr/Detay/Icerik/3-0-57/sektorel-bilgi-guvenligi.

4. Sonuç

Kritik altyapı olarak enerji sektörü, giderek dijitalleşen enerji sistemleriyle birlikte artan siber güvenlik tehditlerine maruz kalmaktadır. Siber saldırılar sonrası artan farkındalık ile beraber enerji sistemlerinin bilişim güvenliği hususu Türkiye dâhil pek çok ülkenin gündeminde yer edinmiştir. Bu doğrultuda, Türkiye'de elektrik, doğal gaz ve petrol sektörleri özelinde uygulanacak standartlar ve kontroller EPDK tarafından yürütülmektedir. Haziran ayında yayımlanan Yönetmelik, enerji şirketlerine yönelik siber tehditleri tespit etmek, önlemek ve bu tehditlere müdahale etmek üzere kapsamlı bir çerçeve sunmakta ve elektrik, doğal gaz ve petrol piyasalarında faaliyet gösteren lisans sahibi kuruluşlar açısından çeşitli yükümlülükler öngörmektedir. Şirketlerin Yönetmelik'teki yükümlülüklere riayet etmesi sadece işletilen enerji tesisleri için değil tüm ulusal şebeke ve enerji altyapısının entegre olduğu tedarik zinciri ve bireylerin gündelik hayatları açısından büyük önem taşımaktadır.

ÇAKMAK 30 YEARS

15 August 2023

Current Topics in the Energy Sector #7

Cybersecurity in the Energy Sector

Information technologies enable monitoring and controlling of energy facilities' operations, collecting data on supply and consumption and creating market forecasts. Therefore, it is as important to ensure the information security of energy systems as to ensure their physical security. In this article, we review cybersecurity in the energy sector, and the legal framework in Türkiye.

1. Cybersecurity Concepts in the Energy Sector

Energy systems today constitute an indispensable part of the quotidian life of individuals as well as the production and industrial sectors. Considering its integrated structure with many other sectors, disruptions in energy systems have the potential to cause significant damage to the society. For this reason, the energy sector is recognized among the sectors of *critical infrastructure*. Critical infrastructures are defined as "*infrastructures that host information systems that can cause loss of life, large-scale economic damage, national security vulnerabilities or disruption of public order when the confidentiality, integrity or accessibility of the information/data they process is disrupted*".[1]

Cybersecurity, in general, refers to the ability to prevent or defend against cyber-attacks, aimed at exploiting, disrupting, modifying, preventing access to, or damaging information in cyberspace, and to protect the availability and integrity of networks, infrastructure and the confidentiality of the information contained therein.[2] The cybersecurity definition consists of the aspects of confidentiality, integrity and availability. In the context of energy systems, *confidentiality* refers to ensuring that only generation, transmission, distribution company personnel and consumers have access to information; *integrity* refers to preventing the alteration, corruption and destruction of information on voltage, frequency, electric power, load flow and billing; and *accessibility* refers to ensuring that actors in the sector have access to information within a certain hierarchy.[3]

The energy sector utilizes various management and control systems that enable operations to be monitored, and sometimes managed, from one or more centers. These systems, referred to as industrial control systems, are defined in general terms in the applicable legislation.[4] The Supervisory Control and Data Acquisition

---

1 National Cybersecurity Strategy and Action Plan (2020-2023), p.9.

2 "*Enhancing Cyber Resilience in Electricity Systems*" ("IEA Report") report dated 2021 prepared by the International Energy Agency p.8. Date of Access: 9 August 2023. URL: https://iea.blob.core.windows.net/assets/0ddf8935-be23-4d5f-b798-3aad1f32432f/Enhancing_Cyber_Resilience_in_Electricity_Systems.pdf

3 Aydin, Hakan & Barışkan, Mehmet & Çetinkaya, Ali. (2021). Siber Güvenlik Kapsamında Enerji Sistemleri Güvenliğinin Değerlendirilmesi. Güvenlik Bilimleri Dergisi, 10, p. 154-155.

4 According to Article 1 of the Regulation (as defined in this article), industrial control systems are defined as "*management and control systems operating with operating systems that enable the monitoring and management of processes such as the generation of energy, the processing of raw materials that provide energy and making them ready for consumption, and the transfer of energy through transmission or distribution layers*".

System ("SCADA") is known to be the most frequently utilized system.[5] The function of these systems, in the simplest terms, is to collect and process real-time data, interact directly with devices and keep records of occurrences. Today, most energy facilities are equipped with industrial control systems, enabling data to be easily collected and reliable forecasts to be made in terms of supply and demand balance in energy markets.

2. The Significance of Cybersecurity in the Energy Sector

Energy is among the primary necessities of individuals such as in transportation, lighting and many other areas of daily life. In this respect, it is of great importance that energy facilities continue to function uninterruptedly. According to data for 2022, 403 cyber-attacks have so far taken place against the energy sector, with each attack resulting in an average loss of 4.72 million dollars.[6]

In the event of a cyber-attack, even for a short period of time, many essential services such as health and transportation can be disrupted.[7] For instance, in the Colonial Pipeline attack in 2021, the pipes were rendered dysfunctional by the creation of a pressure surge in natural gas transmission systems, and the disabled fuel had to be transferred by road.[8] As a result of the attack, the local population rushed to gas stations to stock up on gasoline in a panic, and the price of gasoline skyrocketed to the highest level in the country of the recent years.[9]

Cyber-attacks can have a negative impact on daily life as well as on the functioning of energy markets. In the electricity market, the data that constitute the basis for day-ahead and day-after forecasts are obtained from the information systems that power plants are equipped with. When these systems are subjected to attacks that alter or destroy information, the energy supply and demand balance may be disrupted and imbalances may occur in the system. Furthermore, if a damage occurs in one of these components, it can easily affect the others and ultimately, the infrastructure as a whole due to the intertwined nature of the generation, transmission and distribution infrastructures. To give an example, in 2015, as a result of a cyber-attack on a supply company in Ukraine, SCADA systems were accessed through malware and substations were cut off from power. [10] On that day, 3 MWh of electricity could not be supplied and the country was plunged into darkness for 1 to 6 hours after the blackout. In the Stuxnet attack against a nuclear power plant in Iran, fluctuations were caused in the electric current frequencies that provide energy to centrifuges, causing centrifuges to explode and resulting radioactive damage.[11]

In light of these facts, due to the critical role played by cybersecurity in the energy sector, it is of vital importance for the relevant authorities as well as the investors operating in the sector to establish and regularly monitor the appropriate IT infrastructure in order to prevent attacks and to take the necessary actions as soon as possible during and after the attack.

3. Legal Framework for Cybersecurity of Energy Systems in Türkiye

As in every sector, increasing digitalization in the energy sector entails a growing number of cyber threats, which in turn leads states to formulate cybersecurity strategies. In this regard, many action plans have been

---

5 The Report dated 2011 and titled "*Protecting Industrial Control Systems*" prepared by ENISA (European Network and Information Security Agency), p.1. Date of Access: 11 August 2023. URL: https://www.enisa.europa.eu/publications/protecting-industrial-control-systems.-recommendations-for-europe-and-member-states

6 "Cyber Attack Statistics to Know in 2023". Date of Access: 9 August 2023. URL: https://parachute.cloud/cyber-attack-statistics-data-and-trends/

7 IEA Report, p.9.

8 "Colonial Pipeline Ransomware Attack: Everything You Need To Know". E Date of Access: 9 August 2023. URL: https://www.zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

9 "Pipeline Attack Yields Urgent Lessons About U.S. Cybersecurity". Date of Access: 9 August 2023. URL: https://www.nytimes.com/2021/05/14/us/politics/pipeline-hack.html

10 "2015 Ukraine Power Grid Hack." Date of Access: 9 August 2023. URL: https://en.wikipedia.org/wiki/2015_Ukraine_power_grid_hack

11 "Stuxnet (2010)". Date of Access: 9 August 2023. URL: https://cyberlaw.ccdcoe.org/wiki/Stuxnet_(2010)

developed in the field of cybersecurity in Türkiye since 1999. At present, the National Cybersecurity Strategy and Action Plan ("Action Plan") covering the period 2020-2023, prepared by the Ministry of Transport and Infrastructure in accordance with the Presidential Circular No. 2020/15[12], is being implemented.

The Action Plan sets out principles and objectives for ensuring the cyber security of critical infrastructure sectors, also including the energy sector, and calls for the relevant institutions and organizations to work on regulations and implementation towards this end. The objective set in the Action Plan include protecting the cybersecurity of critical infrastructures on a 24/7 basis, developing a cybersecurity approach based on regulation and supervision in critical infrastructure sectors, and continuing to develop a proactive cyber defense approach to respond to cyber incidents. In this regard, the Energy Market Regulatory Authority ("EMRA") is actively engaged in initiatives to enhance the cybersecurity within the electricity, natural gas and petroleum markets. The Regulation on Cybersecurity Competency Model in the Energy Sector[13] (the "Regulation"), published last June, along with the Security Analysis and Testing Procedures and Principles for Industrial Control Systems Used in the Energy Sector[14], published in July, regulate the minimum standards and control principles for cybersecurity.

Compared to the previous regulations, the Regulation sets out the main control headings, sectoral criticality levels, implementation and audit issues in more detail.

According to the Regulation, the responsible entities are:

- in the electricity market, transmission and distribution license holders as well as owners of each operational power plant with an installed capacity of 100MWe or above that has undergone provisional acceptance,
- in the natural gas market, natural gas transmission license holders engaged in pipeline transmission natural gas distribution license holders responsible for establishing a dispatch control center, and natural gas storage license holders (LNG, underground), and
- in the petroleum market, crude oil transmission and refinery license holders.

On the other hand, Organized Industrial Zone distribution and generation license holders are excluded from the scope of the Regulation.

Although many entities holding licenses in various energy subfields fall within the scope of the Regulation, only the control models for the electricity and natural gas distribution have been included under the Regulation while EMRA is currently in the process of developing models for other sectors. The obligations envisaged for these sectors within the framework of the relevant models came into effect on the date of publication of the Regulation in the Official Gazette. However, except for electricity and natural gas distribution license holders, other entities' obligations under the Regulation will come into effect once the model studies for these sectors are finalized and published by EMRA.[15]

The competency model comprises three fundamental competency levels. The parameters for these competency levels, which the responsible entities should meet, shall be determined by EMRA based on the criticality level of each sector, and afterwards EMRA shall notify the criticality levels to these entities. Depending on the criticality levels, main control categories that responsible entities must adhere to shall be determined, and following the targeted completion period stipulated for each heading, responsible entities shall ensure that their infrastructure complies with the requirements set forth under the relevant main control categories.

---

12 Published in the Official Gazette dated 29 December 2020 and numbered 31349.

13 Published in the Official Gazette dated 6 June 2023 and numbered 32213.

14 Entered into force by EMRA's Decision No. 11956 dated 13 July 2023 and published in the Official Gazette dated 16 July 2023 and numbered 32250.

15 EMRA frequently asked questions: https://www.EMRA.gov.tr/Detay/Icerik/3-0-57/sektorel-bilgi-guvenligi

Compliance of responsible entities with the competency model shall undergo a three-stage audit. Accordingly; the first stage involves an "*internal audit/gap analysis*" to be conducted by the responsible entities by using their own resources, followed by a second stage, where a "*sectoral audit*" is to be performed by firms and personnel meeting the conditions determined by EMRA, and finally in the third stage, there is an "*institutional audit*" to be conducted by EMRA's internal resources.

The Regulation does not provide specific provisions with regard to administrative sanctions to be imposed in case of a breach of the obligations. Hence, the type and amount of fines will be determined in accordance with the provisions stipulated in the primary legislations of the energy markets in which they operate.

4. Conclusion

The energy sector, classified as a critical infrastructure, is exposed to growing cybersecurity threats due to the increasing digitalization of energy systems. Following the cyber-attacks, the issue of information security for energy systems has gained prominence on the agendas of many countries, including Türkiye. In this regard, EMRA conducts the standards and controls to be applied in electricity, natural gas and petroleum sectors in Türkiye. The Cybersecurity Competency Model Regulation published in June provides a comprehensive framework for detecting, preventing, and responding to cyber threats and imposes obligations on the license holders in the electricity, natural gas and petroleum markets. Compliance with these obligations in the Regulation is essential not only for the operational energy facilities but also for the entire national grid and the integrated supply chain of energy infrastructure and the daily lives of the individuals.

Selin Erten Yaşar
Kıdemli Avukat/Senior Associate

Başak Köksal Sağnak
Stajyer Avukat/Legal Intern

Çakmak Avukatlık Ortaklığı

www.cakmak.av.tr