NÜKLEER SANTRALLER İÇİN SİBER GÜVENLİK PLANI İÇERİĞİ

Bu doküman, 11/6/2024 tarihli ve 32573 sayılı Resmî Gazete'de yayımlanan Nükleer Tesislerin ve Nükleer Maddelerin Emniyetine İlişkin Yönetmelik kapsamında yetkilendirilen kişi tarafından hazırlanarak Kuruma sunulması gereken Nükleer Santraller İçin Siber Güvenlik Planının içeriğine ilişkin hususları kapsamaktadır.

Temmuz 2024

Sürüm 1

Emniyet ve Güvence Dairesi Başkanlığı

Nükleer Düzenleme Kurum

İÇİNDEKİLER

1. GİRİŞ

Nükleer santrale, siber güvenlik planının dayanağına, amacına ve içeriğine ilişkin genel bilgiler verilir.

Yetkilendirilen kişinin adı, adresi, planı düzenleyen birimin adı ve plan hakkında iletişime geçebilecek kişilere ait telefon ve faks numaraları ile e-posta adresleri de bu bölümde yer alır.

2. TEMEL İLKELER VE POLİTİKALAR

Nükleer santralin emniyet politikasının bir parçası olarak ele alınan siber güvenlik politikası, devletin siber güvenlik politikası ve ilgili düzenleyici gereklerle tutarlı bir şekilde oluşturulur. Bu politikada nükleer santralin üst düzey siber güvenlik hedefleri, siber saldırılara karşı dijital varlıkların korunması, derinliğine savunma ilkelerinin uygulanması, risk tabanlı yaklaşımın benimsenmesi, dereceli yaklaşımın göz önünde bulundurulması ve bilmesi gereken ilkesinin gereken her alanda uygulanması hususlarına dair bilgiler verilir.

Emniyet ve siber güvenlik kültürünün ortak bir paydada sağlandığı ve bu çerçevede siber güvenlik kültürünün nükleer santral yönetimi, çalışanları ve tedarikçiler tarafından benimsenmesine ve geliştirilmesine yönelik politika ve faaliyetler ile bunlara yönelik kullanılacak araçlar ve fiziki imkânlar siber güvenlik politikası kapsamında belirtilir.

3. SİBER GÜVENLİK ORGANİZASYONU

3.1 Siber Güvenlik Organizasyonu Yapısı

Nükleer santralde siber güvenliğe ilişkin birimlerin nükleer santral yönetimi ve diğer ilgili birimlerle olan ilişkisi siber güvenliğe ilişkin sorumlulukları olan ekipler, ekiplerdeki kişiler ile bu kişilerin görev ve sorumlulukları hakkında bilgiler bu bölümde verilir. Siber güvenliğe ilişkin birimlerin içinde yer alan her bir ekibin birbiriyle ilişkisine ve kişiler, ekipler ve birimler arası bilgi akışı ve raporlama mekanizması gibi hususlara ilişkin açıklamalara yer verilir. Tedarikçilerin siber güvenlik organizasyon yapısı içindeki yeri açıklanır. Ayrıntılı organizasyon şeması belirtilir.

3.2 Siber Güvenliğe İlişkin Sorumlulukların Dağılımı

Siber güvenlik alanında faaliyet gösteren birimlerde yer alan pozisyonların ve paydaşların görev, yetki ve sorumluluklarına, birbirleri ve diğer ilgili kurum ve kuruluşlarla iletişim ve etkileşimine dair bilgiler belirtilir. Yetkilendirilen kişi ile yükleniciler ve diğer paydaşlar arasındaki nükleer santralin fiziksel koruma sistemlerinin, kurumsal bilgi sistemlerinin ve enstrümantasyon ve kontrol sistemlerinin siber güvenliğinin sağlanmasına yönelik iş bölümü, protokoller, sözleşmeler ve yazılı düzenlemeler belirtilir. Bir siber olayda nükleer santralde yer alan siber olaylara müdahale ekiplerinin sektörel siber olaylara müdahale ekibi (SOME) ve Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile olan ilişkisi, sorumlulukları ve koordinasyonuna yönelik bilgiler, talimatlar, prosedürler veya diğer yazılı düzenlemeler açıklanır.

4. DİJİTAL VARLIK YÖNETİMİ

Nükleer santrallerde yer alan enstrümantasyon ve kontrol sistemleri, kurumsal bilgi sistemleri ve fiziksel koruma sistemlerinin bir parçası olan veya bu sistemlerle ilişkili dijital varlıklara yönelik olarak aşağıda listelenen bilgiler ve bu bilgilerin yer aldığı prosedürler, talimatlar, iç düzenlemeler ve diğer dokümanlar belirtilir:

- Kritik sistemlerin tanımı, belirlenmesine yönelik yöntemler ve bu sistemlerin listesi
- Kritik dijital varlıkların tanımı, belirlenmesine yönelik yöntemler, hangi kritik sistemde yer aldığının bilgisi ve listesi
- Kritik sistemler ile uzaktan bağlantılı olan dijital cihazların belirlenmesine yönelik yöntemler ve listesi

- Kritik sistemlerin ve kritik dijital varlıkların konumları, birbirleriyle olan bağlantıları, diğer dijital sistemlerle olan bağlantıları
- Kritik sistemler ve kritik dijital varlıkların kullanıcı gruplarının yetkilerinin belirlenmesine yönelik yöntemler
- Kritik sistemler ve kritik dijital varlıkların işlevleri
- Kritik dijital varlık ve/veya kritik dijital sistemlerin diğer sistemlere olan harici bağlantılarını tanımlayan veri akışı ve ağ diyagramları
- Aşağıdaki hususları içeren siber güvenlik gerekleri veya şartnameler:
    - Tedarik edilen sistemlerin bütünlüğünün sağlanması için tedarikçilerin uyması gereken bilgi güvenliği gerekleri
    - Kritik dijital varlıkların güvenli yapılandırması, kurulumu ve işletimi
    - Kritik dijital varlıkların güvenlik özellik/işlevlerinin etkili kullanımı ve bakımı
    - Yönetici işlevlerinin yapılandırması ve kullanımıyla ilgili bilinen zafiyetler ve riskler
    - Kullanıcıların erişebildiği güvenlik özellik/işlevleri ve bunların etkili kullanımı

Yukarıda bahsi geçen yapılandırma hususlarına ilişkin yapılandırma yönetim planı ayrıntılarıyla bu konu başlığı altında açıklanır ve varsa ilgili prosedürler, talimatlar, iç düzenlemeler ve diğer dokümanlar sağlanır. Yapılandırma yönetim planında aşağıda belirtilen konulara ilişkin bilgiler belirtilir:

- İlgili görev ve sorumlulukların belirlenmesi
- Konfigürasyon yönetimi süreç ve prosedürlerinin tanımlanması
- Kritik dijital varlıkların yapılandırması ve etkileşimleri
- Sistem geliştirme yaşam döngüsünde hangi kritik dijital varlığın ne zaman yapılandırma yönetimi altına alınacağı
- Kritik dijital varlıkları tanımlamak için araçlar ve bunları korumak için siber güvenlik önlemlerini yönetmek için oluşturulan süreç

Kritik dijital varlıkların sistem sıkılaştırması için oluşturulan süreç ve yöntemler hakkında ayrıntılı bilgiler verilir. Kritik dijital varlıklar ve bu varlıklarla bağlantılı diğer dijital varlıkların güncellemelerine, yamalarına ve bunların uygulanma sürecine ilişkin ayrıntılı açıklamalar bu bölümde belirtilir.

5. SİBER GÜVENLİK MİMARİSİ VE PROSEDÜRLERİ

Dijital varlıkların korunması için uygulanan siber güvenlik kontrollerinin temel alındığı uluslararası standart ve kılavuz gibi esas dokümanlar belirtilir.

Temel siber güvenlik mimarisinin derinliğine savunma ilkesine dayalı olarak tasarlandığı ve dereceli yaklaşıma göre önlemler alındığı açıklanır. Mimaride dereceli yaklaşım esas alınarak oluşturulan ağ topolojisi tasarımı, hangi cihazların hangi ağ seviyesinde konumlandırıldığı, ağ topolojisinde yer alan her bir seviyedeki tüm ve izin verilen portlar, uygulamalar, hizmetler, protokoller, bilgi akışı, filtreleme ve diğer unsurlarla birlikte her bir seviyede uygulanan siber güvenlik önlemleri bu alanda listelenerek ayrıntılı bir şekilde açıklanır.

Nükleer santralin siber güvenlik kontrolleri ve önlemleri ayrıntılı olarak açıklanır ve aşağıda listelenen hususlara ilişkin bilgilere, prosedürlere, talimatlara, iç düzenlemelere ve diğer dokümanlara yer verilir:

- Erişim kontrolü
- Denetim ve hesap verilebilirlik
- Sistem ve iletişim güvenliği
- Tanımlama ve kimlik doğrulama
- Uygulama ve veri güvenliği
- Taşınabilir cihaz ve medya güvenliği
- Sistem sıkılaştırma
- Bakım ve onarım
- Fiziksel koruma

- Konfigürasyon yönetimi
- Süreklilik
- Yedekleme
- Tedarik zinciri
- Sistem izleme ve loglama

Siber güvenlik kontrollerinin her bir sınıflandırmadaki dijital varlığa nasıl uygulandığı listelenir ve hangi parametrelerin tanımlandığı belirtilir. Kontrollere ilişkin doğrulama süreci açıklanır.

6. SİBER GÜVENLİK RİSK VE ZAFİYET YÖNETİMİ

6.1 Siber Güvenlik Risk Yönetimi

Siber güvenlik risk yönetimine ilişkin nükleer santral içi politikalar, hangi standart veya çerçevenin kullanıldığının bilgisi, risk değerlendirmesinin nasıl yapıldığı, varsa değerlendirmenin yaptırıldığı firmanın bilgileri ve akreditasyonu bu bölümde verilir. Siber güvenlik risk yönetiminin nükleer santral yaşam döngüsünün bütün aşamalarında ve yaşam döngüsü boyunca uygulandığına dair bilgiler verilir. Risk yönetimine ilişkin sağlanacak bilgiler iki ayrı risk yönetimi tipini ve alt konularına ilişkin ayrıntıları kapsar:

- Nükleer santral siber güvenlik risk yönetimi
    - Amaç ve kapsam
    - Nükleer santralin tanımlanması
    - Tehditlerin tanımlanması
    - Gereklerin belirlenmesi
    - Doğrulama ve onaylama
- Sistem siber güvenlik risk yönetimi
    - Sistem sınırlarının tanımlanması
    - Dijital varlıkların tanımlanması
    - Sistem siber güvenlik gereksinimleri
    - Doğrulama

Siber güvenlik risk yönetimine ilişkin ek olarak aşağıda listelenen hususlara ilişkin dokümanlar ve ayrıntılı bilgiler sağlanır:

- Tedarik zincirinde yer alan paydaşların analizinin risk yönetimi sürecine dâhil edilmesi
- Sisteme yönelik siber güvenlik risk yönetiminin bir sonucu olarak ortaya çıkan gereklerin karşılanmasına yönelik sorumluluk ve hesap verilebilirliğin sözleşmeye dayalı düzenlemeleri
- Siber güvenlik gereksinimlerinin karşılandığından emin olmak için tedarikçilerin ilgili faaliyetlerinin denetlenmesi
- Siber güvenliğin sağlanması ile ne ölçüde ve etkinlikte sağlandığına yönelik iç denetimler, değerlendirmeler, gözden geçirmeler, tatbikatlar ve testlerin niteliği, bunların kim tarafından nasıl yapıldığı, süreci, metotları, sonuçları ve bunlara ilişkin raporlar, prosedürler, talimatlar, iç düzenlemeler ve diğer dokümanlar

6.2 Siber Güvenlik Zafiyet Yönetimi

Nükleer santralde yer alan kritik dijital varlıkların zafiyet analizlerinin nasıl yapıldığı; hangi yöntemlerin, süreçlerin ve platformların kullanıldığı; ne sıklıkla yapıldığı; raporlamanın nasıl yapıldığı ve analiz sırasında kritik dijital varlıkların işlevlerinin etkilenmemesi için hangi önlemlerin uygulandığı bu bölümde açıklanır.

7. SİBER OLAYLARA MÜDAHALE

7.1 Siber Olaylara Müdahale Süreci ve Organizasyonu

Nükleer santralin siber olaylara müdahale politikası ve süreci bu bölümde tanımlanır. Siber olaylara müdahale yönetiminin bütün süreç ve aşamalarında görev alabilecek nükleer santral içinden ve nükleer santral dışından bütün kişiler, ekipler ve paydaşlara ilişkin aşağıdaki hususlara yer verilir:

- Organizasyon yapısı (USOM ve sektörel SOME ile olan koordinasyon ve bağlantılar dâhil)
- Yetkili personel iletişim bilgileri
- Her bir pozisyonun görev ve sorumlulukları
- Her bir pozisyonun yetkinlikleri ve gösterdikleri faaliyetler
- Her bir pozisyonun birbirleriyle etkileşimleri
- Her bir pozisyonun varsa bağlantılı olduğu diğer birimlerle etkileşimleri

7.2 Siber Olaylara Müdahale Planı

Siber olaylara müdahale planına yer verilir. Siber olaylara müdahale planı aşağıda listelenen aşamalara yönelik plan, program, faaliyet, önlem ve yöntemleri içerir:

a) Hazırlık: Hazırlık aşamasındaki müdahale planlama eylemleri (üst yönetim tarafından onaylı) ve bunlarla birlikte siber olaylara müdahale için operasyonel süreçlere rehberlik edecek bir politika, politika ile tutarlı prosedürler ve olay müdahalesi için mevcut varlıkların belirlenmesi yer alır. Siber olaylara müdahalede kullanılacak gerekler ve kriterler açıklanır.

b) Tespit ve Analiz: Tespit ve analiz aşamasında, siber olaylara müdahale ekibi tarafından olayın teknik tanımlamasının nasıl yapıldığı, bilgilerin nasıl toplandığı ve tespiti desteklemek için veri izlemenin nasıl sağlandığı açıklanır. Siber olaylara müdahale ekibinin IT ve OT sistemlerinin işleyişini etkilemeden veya potansiyel adli kanıtları bozmadan olayları analiz etme yolları detaylandırılır. Olayın analizine yönelik olarak aşağıdaki hususlar planda ayrıntılı bir şekilde açıklanır:

- Siber olayın nükleer güvenlik, emniyet ve acil duruma hazırlık ve müdahale üzerindeki potansiyel etkilerinin belirlenmesi ve nükleer santralin güvenli bir duruma getirilmesine yönelik eylemlerin tanımlanması
- Etkin müdahaleyi belirlemek için olayın boyutunun tespit edilmesi
- Bilgi kaybı, nükleer santralde fiziksel hasar ve kamuoyu algısı açısından siber olaydan kaynaklanabilecek potansiyel zararın belirlenmesi
- Bu olayın etkilerinden yararlanarak gelecekte bir saldırı düzenlenmesi olasılığı da dâhil olmak üzere, saldırganın niyeti ve gelecekteki olası tehditler açısından siber olayın niteliğinin belirlenmesi

c) Kontrol Altına Alma, Yok Etme ve Kurtarma: Sonuçları hafifletme eylemleri kapsamında bir siber olayı kontrol altına alma, zararlı yazılımları ortadan kaldırma veya etkilenen sistemlerdeki hataları ya da değiştirilen yapılandırmanın düzeltme ve gerektiğinde telafi edici önlemler kullanarak sistem işlevini ve veri bütünlüğünü kurtarmaya yönelik uygulamalar, prosedürler ve yöntemler açıklanır.

Siber olaylar esnasında tehlikeye giren bileşenler veya sistemler, tekrar çalışır hale getirilinceye kadar işlevlerini yerine getirebilmeleri için alınacak telafi edici önlemler listelenir ve bunların nasıl uygulanacağı açıklanır.

Kurtarma önlemlerinin hangi dijital varlıklar için nasıl kullanılacağına ve tedbirlerin uygulanmasına yönelik sürecin yönetimine ilişkin bilgiler siber olaylara müdahale planı kapsamında belirtilir.

ç) Olay Sonrası Faaliyetler: Siber olaylara müdahale planı, gelecekte benzer türde olayların tekrarlanmasını önleyecek, bunların hızlı bir şekilde tespit edilmesini sağlayacak ve/veya sonuçlarını en aza indirecek önlemlerin uygulanmasına yönelik olay sonrası faaliyetleri açıklar. Siber olay sonrası bulguların nasıl tutulduğuna ve bu bulgulara yönelik hangi düzeltici ve önleyici faaliyetlerin yürütüleceğine ilişkin bilgiler verilir.

d) Raporlama: Bir siber olaya müdahale sırasında USOM, sektörel SOME ve diğer yetkili kurumlara veya kuruluşlara yapılacak olan raporlamaya ilişkin bilgiler, prosedürler, talimatlar, iç düzenlemeler ve diğer dokümanlar bu bölümde sağlanır. Raporlama için kullanılacak format, bilgi akışı ve onay sırası gibi bilgiler verilir. Siber olayın raporlanması ve dış kuruluşlardan gelen bilgi talepleri için varsa irtibat noktası olarak atanan kişinin bilgisi verilir.

8. PERSONEL YÖNETİMİ

8.1 Personelin İşe Alımı ve Yetkinlikler

Nükleer santralde siber güvenliğe yönelik faaliyet gösteren birimlerdeki pozisyonlara yönelik gerekler, personel alımında her bir pozisyon için güvenilirliğin teyidi, işe alım süreci ve süreçte uygulanan testler, işe alımdan sonra yürütülen personel takip çalışmaları ve personelin iş alanlarına veya sahip oldukları sorumluluklara ve bilgi seviyelerine yönelik yapılan testler ve değerlendirmelere dair prosedürlere yer verilir.

8.2 Farkındalık ve Eğitim

Siber güvenliğe yönelik faaliyet gösteren birimlerde görev yapmakta olan personelin çalıştığı alan ve iş tanımının gerektirdiği eğitimlere yönelik programlar ve takvimler, eğitimlerin içeriği ve niteliği, eğitimleri veren kuruluşların bilgileri, bu hususları içeren prosedürlere, talimatlara, iç düzenlemelere ve diğer dokümanlara yer verilir. Hangi iş tanımlarına veya pozisyonlara hangi eğitimlerin ne sıklıkla verildiği ayrıntılarıyla açıklanır. Eğitimlerin etkinliğinin ve personelin eğitimden edindiği kazanımların ölçülmesi için uygulanan değerlendirmeler ve periyotları hakkında bilgiler verilir.

8.3 Yaptırım ve Disiplin

Personelin kendi iş alanının ve sorumluluklarının getirdiği gereklere ve/veya siber güvenlik gereklerine uymaması veya bunlara karşı yönde bir eylem yürütmesi durumunda başlatılacak disiplin ve/veya yaptırım sürecine yönelik bilgiler, prosedürler, talimatlar, iç düzenlemeler ve diğer dokümanlar bu bölümde belirtilir.

9. EKLER

Siber güvenlik planına ilişkin gerekli görülen ekler sunulur.

10. REFERANSLAR

Plan içeriğinde atıf yapılan mevzuat, standart, kılavuz ve talimatlar planda belirtildiği biçim ve sırasıyla sistematik olarak listelenir.