T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı

Kritik Bilgi Sistem Altyapıları için Asgari Güvenlik Önlemleri Dokümanı

HAZIRLAYAN

TÜBİTAK

[Bu sayfa boş bırakılmıştır]

İçindekiler Tablosu

Kısaltmalar

DKS	Dağıtık Kontrol Sistemleri
EKS	Endüstriyel Kontrol Sistemleri
IP	İnternet Protokolü
SCADA	Merkezi Denetleme Kontrol ve Veri Toplama (Supervisory Control and Data Acquisition)
VPN	Sanal Özel Ağ

Şekiller

1. Amaç

Bu doküman Siber Güvenlik Kurulu kararı kapsamında bilişim (kritik altyapı) sistemlerinde uygulanması gereken asgari güvenlik önlemlerinin belirlenmesi amacıyla hazırlanmıştır.

2. Kapsam

Bu doküman bünyesinde bilişim sistemi bulunan (kritik altyapı işleten) tüm kurum ve kuruluşları kapsamaktadır.

3. Kritik Altyapı Tanımı ve Kategorileri

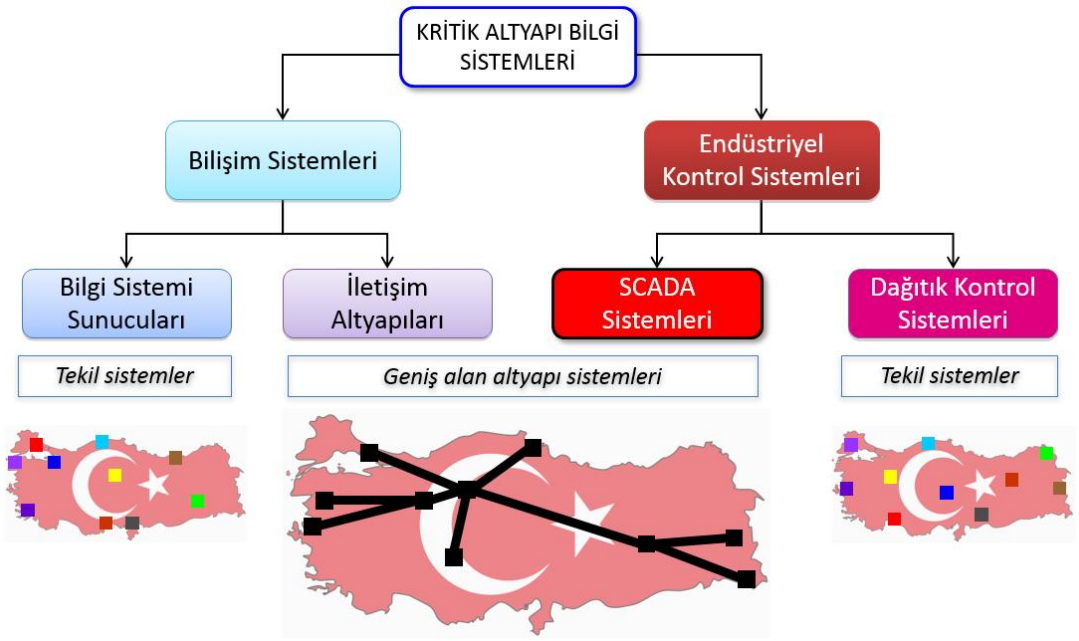
Kritik altyapı, işlediği bilginin gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda, can kaybına, büyük ölçekli ekonomik zarara, ulusal güvenlik açıklarına veya kamu düzeninin bozulmasına yol açabilecek bilişim veya endüstriyel kontrol sistemlerini barındıran sistemlerdir. Kritik altyapılar genel olarak fiziksel varlıklar, insan kaynakları, bilişim sistem ve varlıkları olarak üç katmandan müteşekkildir. Kritik altyapıların bir kısmı sadece bilişim sistemlerinden oluşmaktadır. Bilişim Sistemleri, Bilgi Sistemleri ve İletişim Sistemleri olarak iki kategoriye ayrılabilir.

Kritik altyapıların bir kısmı hizmet vermek için bilinen bilişim sistemlerini kullanırken diğer bir kısmı ise Endüstriyel Kontrol Sistemleri (EKS) olarak adlandırılan özel bilişim sistemleri tarafından izlenmekte ya da yönetilmektedir. Endüstriyel Kontrol Sistemleri, topolojilerine ve içerdikleri bileşenlere göre SCADA ve DKS olarak ikiye ayrılmaktadır. Bu durumda, bilişim sistemleri açısından, kritik altyapı bilgi sistemlerini dört farklı kategoride ele alınması mümkün olmaktadır (**Şekil *1***-Kritik Altyapı Bilgi Sistemleri).

a. **Bilgi Sistemleri**, bir kuruma ve paydaşlarına hizmet veren bilgisayar sistemleridir.
b. **İletişim Sistemleri**, coğrafi olarak çok geniş bir alana yayılmış bileşenlerden oluşan, pek çok kurum ve kuruluşa iletişim hizmeti sağlayan sistemlerdir.

c. **SCADA Sistemleri**, coğrafi olarak çok geniş bir alana yayılmış bir sistemin bileşenlerini merkezi olarak izlemek ve kontrol etmek için kullanılan sistemlerdir.

ç. **Dağıtık Kontrol Sistemleri**, , belli bir tesis ve konumla sınırlı bir endüstriyel süreci izlemek ve kontrol etmek için, tesisin tümüne yayılmış kontrol bileşenleri bulunan sistemlerdir.



Şekil 1-Kritik Altyapı Bilgi Sistemleri

Şekil 2'de "Kritik Altyapılarda Bilgi Güvenliği Süreci" özet olarak gösterilmiş olup kurumların bu süreçteki adımları tanımlayan detaylı bir prosedür veya mevzuat hazırlaması faydalı olacaktır. Mevzuat kapsamında ise aşağıdaki şekilde yer alan tüm adımlarla ilgili görev tanımlarının ve yetkilendirmenin açıkça yapılması tavsiye edilmektedir.

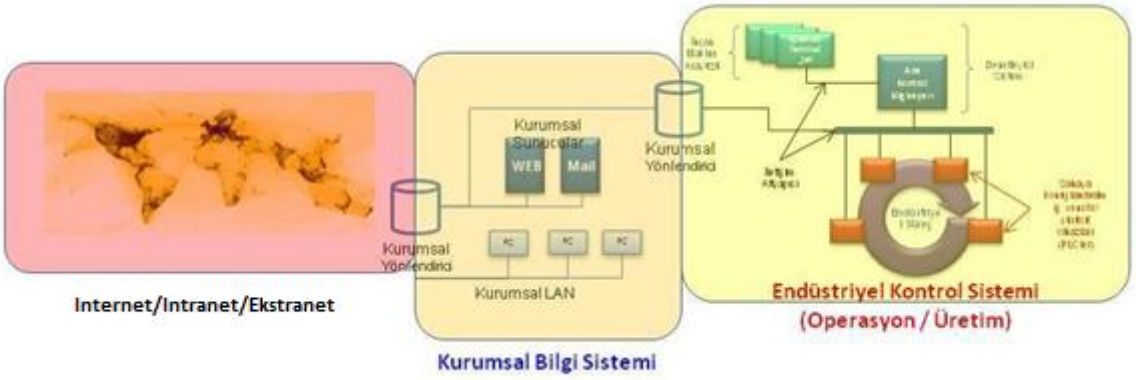
Şekil 2-Kritik Altyapılarda Bilgi Güvenliği Süreci

4. Asgari Güvenlik Önlemleri

Aşağıda yer alan Tablo 1'de kritik altyapı sahibi kurumlar tarafından değerlendirme için kullanılabilecek asgari güvenlik önlemleri yer almaktadır.

Herhangi bir kurum veya kuruluşun kontrolünde bilişim sistemlerinin veya endüstriyel kontrol sistemlerinin bulunması muhtemeldir. Her halükarda kurumun kendi bilgi sistemine sahip olması beklenir. Şekil 3'te Dağıtık Kontrol Sistemi çalıştıran bir kurumun bilişim sistemlerinin genel topolojisi görülmektedir. Farklı kurumlarda Dağıtık Kontrol Sistemi yerine SCADA sisteminin veya kurum dışındaki paydaşlara hizmet veren bilişim sistemlerinin bulunması mümkündür.

Aşağıda açıklanan güvenlik önlemlerinin bir kısmı Endüstriyel Kontrol Sistemlerine, bir kısmı ise bilişim sistemlerine özeldir. Hangi önlemin hangi tip sistem için düşünülmüş olduğu önlemin tanımında açıkça belirtilmiş olmakla birlikte aşağıdaki tabloda da belirtilmiştir (Tablo 1). Tabloda "sistem", yazılım, donanım ve veriyi bir bütün olarak ifade etmektedir.



Şekil 3-DKS çalıştıran bir kurumun bilişim sistemleri topolojisi

Güvenlik Önlemi		Bilişim Sistemi	Endüstriyel Kontrol Sistemi
Sistemlerin yetkisiz erişimden korunması			
	Sistem merkezine fiziksel erişimin yönetilmesi	EVET	EVET
	Sistemlere bilgisayar ağları aracılığı ile erişimin kısıtlanması	HAYIR	EVET
	Taşınabilir saklama ortamlarının kısıtlanması	EVET	EVET
Yetkili personelin sistemlere erişiminin yönetilmesi			
	Sistem yöneticisi ve operatör atama prosedürü	EVET	EVET
	Yetkili personelin kullanıcı kimliklerinin yönetilmesi ve güvenli oturum açma prosedürü	EVET	EVET
	Kayıt yönetimi ve görevler ayrılığı	EVET	EVET
	İşletme prosedürleri, rol ve sorumluluklar	EVET	EVET
Sistem tedarik, geliştirme ve bakımının yönetilmesi			
	Uygulama yazılımlarının güvenliğinin yönetilmesi	EVET	EVET
	Teknik açıklıkların yönetilmesi	EVET	EVET
	Bakım sözleşmesi	EVET	EVET
İş sürekliliği önlemleri			
	Yedek sistem merkezi, prosedür ve testler	EVET	EVET
Bilişim sistemleri güvenliği yöneticisi ve personel istihdamı			
	Güvenlik yöneticisi	EVET	EVET
	Personel sürekliliği	EVET	EVET
	Personel yetiştirilmesi ve eğitimi	EVET	EVET
Dokümantasyon			
	Politika dokümanı	EVET	EVET
	Kayıtların yönetilmesi	EVET	EVET
Bilgi güvenliği olaylarına müdahale			

Tablo 1-Asgari Güvenlik Önlemlerinin Uygulanacağı Sistemler

4.1 Sistemlerin yetkisiz erişimden korunması

4.1.1 Sistem merkezine fiziksel erişimin yönetilmesi

Endüstriyel kontrol sistemlerinin ve bilişim sistemlerinin merkezinde, sunucu vb. kritik altyapı bileşenlerinin yer aldığı sistem merkezleri bulunmaktadır. Bu sistem merkezlerine fiziksel erişim (giriş/çıkış) yetkili personelle sınırlandırılmalı, bu alanlara girişler manyetik kart, parmak izi, yüz tanıma, el geometrisi tanıma ya da retina taramasıyla çalışan biyometrik kontrol sistemleri vb. (kolaylıkla kopyalanması mümkün olmayan) yöntemlerle gerçekleştirilmeli ve kayıt altına alınmalıdır. Kayıtlar kayıt yöneticisi tarafından düzenli aralıklarla gözden geçirilmeli ve gerekli durumlarda yönetime bilgi verilmelidir.

4.1.2 Sistemlere bilgisayar ağları aracılığı ile erişimin kısıtlanması

EKS'nin özellikle İntranet/İntranet/Ekstranet'ten ve zorunlu olmayan durumlarda kurumsal bilgi sisteminden izole edilmesinin sağlanması hedeflenmelidir. İzolasyonun mümkün olmadığı durumlarda EKS'nin İntranet/İntranet/Ekstranet'e veya kurumsal bilgi sistemine bağlanması ile ilgili gereksinim belgelenmeli, sisteme ağ üstünden erişim yapılmasına sadece gereksinime uygun durumlarda izin verilmeli ve bu durumlarda sistemin ağ üstünden gelebilecek saldırılardan korunması için gereken önlemler (sanal özel ağ (VPN-Virtual Private Network) kullanımı, sadece önceden belirlenmiş IP adreslerinden erişime izin verilmesi vb) alınmalıdır.

4.1.3 Taşınabilir saklama ortamlarının kısıtlanması

EKS'ye taşınabilir saklama ortamlarının bağlanmaması için alınacak önlemler belirlenmelidir. Taşınabilir saklama ortamlarının EKS'ye veya bilişim sistemine bağlanması gerekiyorsa, bu bağlantılarla ilgili gereksinim belgelenmeli, bağlantıya sadece bu gereksinime uygun durumlarda izin verilmeli ve bu durumlarda ortamlardan sisteme kötücül yazılım bulaşmaması için alınacak önlemler belirlenmelidir.

4.2 Yetkili personelin sistemlere erişiminin yönetilmesi

4.2.1 Sistem yöneticisi ve operatör atama prosedürü

EKS'lerde sistem yöneticisi veya operatör olarak, bilişim sistemlerinde ise sistem yöneticisi olarak görev yapacak personelin atanmasını düzenleyecek kurumsal prosedür oluşturulmalıdır. Sistem yöneticisi veya operatör rolü için gerekli yeterlilikler belirlenmelidir. Prosedür kapsamında atama süreci ve süreç boyunca oluşturulacak kayıtlar tanımlanmalıdır. Atanacak personelin güvenlik taraması ile ilgili sonucu belirten kayıt ve atanan personelin yerine getirmekle yükümlü olduğu şartları (kullanıcı adı ve parolasını paylaşmama, sistem üstünde görevlendirildiği işlemler dışında işlem yapmama vb.) kabul ettiğine ilişkin form prosedür kapsamında oluşturulabilecek kayıtlardan birkaçıdır.

4.2.2 Yetkili personelin kullanıcı kimliklerinin yönetilmesi ve güvenli oturum açma prosedürü

EKS'ye erişim yetkisine sahip (sistem yöneticisi, operatör vb.) personelin ve bilişim sistemlerinde sistem yöneticisi olarak görev yapan personelin sisteme erişmek için kullanacağı kullanıcı adları her bir personel için farklı olmalıdır. Yetkili personel, sistem tarafından karmaşık parolalar seçmeye ve parolalarını düzenli aralıklarla değiştirmeye zorlanmalıdır. Yetkili personel, bilişim sistemine erişmeden önce kimliğini kullanıcı kimliği ve parolası ile bilişim sistemine ispatlamalıdır. Bu özellik uygulama yazılımında bulunmuyorsa, geliştirici firma ile görüşülmeli ve güvenli oturum açma işlevi (manyetik kart, biyometrik doğrulama veya her iki yöntem) uygulama yazılımına eklenmelidir.

4.2.3 Kayıt yönetimi ve görevler ayrılığı

EKS'de yetkili personel tarafından yapılan işlemler ve bilişim sistemlerinde sistem yöneticileri tarafından yapılan işlemler kayıt altına alınmalıdır. Sistemler, yetkili personelin yaptıkları işlemlerle ilgili kayıtları silme olasılığını ortadan kaldıracak şekilde yapılandırılmalıdır.

Sistemin Internet'e veya kurum bilişim sistemine bağlı olması durumunda bu ara yüzlerden yapılan işlemlerin de kayıt altına alınması gerekir.

Kayıt yöneticisi rolü tanımlanmalı, kayıtlar kayıt yöneticisi rolüne sahip bir sistem yöneticisi tarafından düzenli aralıklarla gözden geçirilmeli ve gerekli durumlarda yönetime bilgi verilmelidir. Kayıt yöneticisi sistem üstünde herhangi bir işlem yapma hakkına sahip olmamalıdır.

4.2.4 İşletme prosedürleri, rol ve sorumluluklar

EKS'de işlem yapması gereken sistem yöneticisi, operatör vb. roller, bilişim sistemlerinde sistemin yöneticisi rolü ve bu rollerin yerine getirmesi gereken görev ve sorumluluklar tanımlanmalıdır. Sistem üstünde yapılması gereken işlemlerle ilgili prosedürler tanımlanmalı, ilgili personel işlemleri prosedürlere uygun şekilde gerçekleştirmeli, böylece kullanıcı hatalarının en alt düzeye indirilmesi sağlanmalıdır.

Sistem alt bileşenleri (sunucu, veritabanı, ağ cihazı vb.) sınıflandırılması yapılmalı ve bu sınıflandırmalara göre erişim yetkileri düzenlenmeli, sistem yöneticisi yetkileri bu düzenlemelere göre kısıtlanmalı ve her sistem yöneticisi kendi sorumluluğundaki alt sistemlere erişebilmelidir. Sistem yöneticilerinin normal bir kullanıcı hesabı olmalı, günlük cari faaliyetlerde bu hesapları kullanmalı ve sistem yönetim faaliyetlerinde kullanmak üzere ihtiyaç olduğunda kısa süreli olarak ilave bir yetkili kullanıcı hesabı ve parola kullanmalıdır.

4.3 Sistem tedarik, geliştirme ve bakımının yönetilmesi

4.3.1 Uygulama yazılımlarının güvenliğinin yönetilmesi

EKS'lerde ve bilişim sistemlerinde çalışan uygulama yazılımlarından kaynaklanabilecek yetkisiz erişim, kötüye kullanma, hata ve kayıpların asgari düzeye indirilmesi için sağlanması gereken gereksinimler belirlenmelidir. Gereksinimlerin uygulama yazılımları tarafından

sağlandığını güvence altına almak için gözden geçirme ve test prosedürleri oluşturulmalı ve prosedürler uygulanmalıdır.

4.3.2 Teknik açıklıkların yönetilmesi

Kullanılmakta olan EKS'lerde ve bilişim sistemlerinde yer alan ağ elemanları, işletim sistemi, veritabanı vb. sistemlerin bilinen açıklıklardan kaynaklanan risklere maruz kalmaması için gereken önlemler alınmalıdır. Bu konuda öncelikle güncel varlık envanterinin tutulması, ardından üreticilerin ve uzmanlık gruplarının yaptığı yayınların izlenmesi ve son olarak etkin bir yama yönetim sürecinin çalıştırılması gerekmektedir.

4.3.3 Bakım sözleşmesi

EKS'nin ve bilişim sistemlerinin geliştirici ve tedarikçileri ile ilişkiler sözleşme aracılığı ile yönetilmelidir. Sözleşme kapsamında acil durumlarda geliştirici tarafından kuruma verilecek destek, sisteme yapılacak müdahaleler ve olağan bakımlarla ilgili gereksinimler düzenlenmelidir. Tüm bu durumlarda geliştiricinin sağlaması gereken güvenlik şartları kararlaştırılmalı ve sözleşmede belirtilmelidir.

4.4 İş sürekliliği önlemleri

4.4.1 Yedek sistem merkezi, prosedür ve testler

EKS'lerde ve bilişim sistemlerinde sistem merkezinin herhangi bir nedenle devre dışı kalması halinde devreye girebilecek bir yedek sistem merkezinin gerekliliği değerlendirilmeli ve değerlendirme sonucu gerekli altyapı oluşturulmalı veya geliştirilmelidir.

Yedek sistem merkezinin gerekli görüldüğü kritik altyapı sistemlerinde yedek sistem merkezinin devreye girmesi ile ilgili prosedürler oluşturulmalı, bu prosedürler test edilerek işlevsellikleri kanıtlanmalı ve prosedür kapsamında görevlendirilmiş personelin görevlerini benimsemeleri sağlanmalıdır.

4.5 Bilişim Sistemleri Güvenliği Yöneticisi ve Personel İstihdamı

4.5.1 Güvenlik yöneticisi

EKS'lere ve bilişim sistemlerine yönelik olarak tanımlanan kurumsal yükümlülüklerin yerine getirilmesi konusunda kurumlarda liderlik yapacak ve yönetimle sağlıklı bilgi alışverişini sağlayacak bir rol tanımlanması gerekmektedir. Bu rol "Bilişim Sistemleri Güvenliği Yöneticisi" olarak adlandırılabilir. Güvenlik Yöneticisi rolü için bilgi güvenliği konusunda uzmanlaşmış personel istihdam edilmesinin, kurumda bulunan EKS'nin ve bilişim sistemlerinin kapsamı göz önünde bulundurularak, güvenlik yöneticisinin yardımcılarla desteklenmesinin gerekli olduğu değerlendirilmektedir.

4.5.2 Personel sürekliliği

Özellikle kamu kurumlarında personel sürekliliği bilinen bir problemdir. Kritik altyapı sistemi çalıştıran kurumlarda sistem yöneticilerinin ve güvenlik yöneticisinin kurum adına üstlendikleri ve yönettikleri riskler göz önünde bulundurularak uygun koşullarda istihdam edilmeleri büyük önem arz etmektedir.

4.5.3 Personel yetiştirilmesi ve eğitimi

Kritik altyapı sistemi çalıştıran kurumlarda sistem yöneticisi ve güvenlik yöneticilerinin kurum adına kurum içi/kurumlar arası/yurt içi/yurt dışı eğitimlerine gönderilerek bilgilerinin güncel ve eğitim seviyelerinin yüksek tutulması büyük önem arz etmektedir

4.6 Dokümantasyon

4.6.1 Politika dokümanı

İlgili kurumlar, yukarıda sayılan önlemlerin her biri ile ilgili değerlendirmelerini ve bu önlemleri kurumlarında nasıl uyguladıklarını açıklayan bir politika dokümanı oluşturmalıdır.

4.6.2 Kayıtların yönetilmesi

İlgili kurumlar yukarıda sayılan önlemlerin uygulanması sırasında oluşması beklenen kayıtları oluşturmalı ve saklamalıdır. Kayıtların bir kısmının elektronik ortamda, bir kısmının ise matbu olarak oluşması beklenmektedir. Kayıtlar delil niteliğinde olup, güvenlikleri ile ilgili başlıca gereksinim sadece kurum yöneticisi ve bilişim sistemleri güvenliği yöneticisi tarafından okunabilir ve hiç bir kurum çalışanı tarafından değiştirilemez olmalarıdır. Bu konu ile ilgili teknik detaylar halen farklı bir çalışma grubu tarafından belirlenmektedir.

Politika dokümanı ve kayıtlar hem kurum yönetiminin, hem de kurum dışından gelen denetçilerinin değerlendirmesine açılacak ve güvenlik önlemlerinin etkinliği ile ilgili fikir üretilmesine yardımcı olacaktır.

Kayıtlar hukuki platformlara taşınan bilgi güvenliği olaylarında delil olarak kullanılacaktır.

Dolayısı ile doküman ve kayıtların kurumsal bilişim sistemleri güvenliğinin etkin bir şekilde uygulanmasında önemi büyüktür.

4.7 Bilgi Güvenliği Olaylarına Müdahale

Bilişim sistemlerinin güvenliği ve iş sürekliliği öncelikle teknik bir konu olarak ele alınsa da kasıtlı olarak yapılan yetkisiz işlem ve zarar vermelerin hukuka aykırılık oluşturduğu akıllardan çıkarılmamalıdır. Dolayısı ile sebep olan faillerin ve delillerin tespiti açısından hukuka aykırı durumun yetkili güvenlik güçlerine ivedilikle iletilmesi ve sistem müdahalelerinin koordine ve işbirliği içerisinde yürütülmesi için prosedürler oluşturulmalıdır.

5. Sonuç

Bu dokümanda Türkiye'de bulunan kritik altyapı sistemlerinde uygulanması gereken asgari güvenlik önlemlerinin belirlenmesi hedeflenmiştir. Kritik altyapı kapsamında değerlendirilen

kurumlar ve bakanlıklar tarafından başlangıç aşamasında zemin oluşturmak üzere asgari güvenlik önlemlerinin neler olabileceği de belirtilmiştir.