TÜRKİYE KÖMÜR İŞLETMELERİ KURUMU
GENEL MÜDÜRLÜĞÜ
Araştırma Planlama ve Koordinasyon Dairesi
Başkanlığı

Sayı : 83768800-010.06.01-E.401/7648 22.8.2016
Konu : Bilgi Güvenliği Yönetim Sistemi

TAMİM
2016/13

Kurumumuzda uygulanmakta olan **TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi;** güvenliğin sağlanması için, "Ayrıcalıklı Erişim Haklarının Yönetimi", "Ayrıcalıklı Destek Programlarının Kullanımı", "Etkileşimli ve Yeterli Güvenlik Seviyesine Sahip Parolalar Temin Edilmesi" ve "Kötüsel Yazılımlardan Korunma (virüs, worm vb.)" kontrollerinin uygulanması gerektiğini belirtmektedir.

Bu kontroller, kurumsal bilginin korunması ve sürdürülebilir bir bilişim altyapısı için uygulanması gereken kontrollerdir. Bahsi geçen kontroller ile ilgili alınması gerekli tedbirler aşağıda belirtilmiştir.

Kötü amaçlı yazılımlardan (virüs, worm vb.) korunma hususunda;

Bu kontrolün etkin bir şekilde sağlanması ve sürdürülmesi için Kurumumuz bilişim altyapısına dahil olan tüm bilgisayarlara antivirüs yazılımlarının yüklenmesi ve düzenli olarak güncellenmesi gerekmektedir. Bu işlemin otomatik olarak gerçekleştirilmesi ve tüm bilgisayarlarda aynı güncellikte yazılımın kullanılması amacıyla bilgisayarların aktif dizin alanına dahil edilmesi gerekmektedir. Bu nedenle aktif dizin yapısına dahil olmayan bilgisayarlar tespit edilecek ve **gerekli çalışmalar yapılarak tüm bilgisayarlar aktif dizin yapısına dahil edilecektir.** (Aktif dizin yapısına dahil olmayan bilgisayarlar Kurumun kontrolü dışında çalışıyor ve dışarıdan gelebilecek saldırılar için zayıf nokta teşkil ediyor demektir.)

Etkileşimli ve yeterli güvenlik seviyesine sahip parolalar temin edilmesi hususunda;

Kurum ağına sızma yapılsa bile kullanıcı makinelerinin ve sistemlerin ele geçirilmesini engellemenin en basit ama en etkili yöntemi **kuvvetli parola belirlemektir**. Kurumdaki tüm bilgisayarlarda Bilgi Güvenliği Yönetim Sistemi, Parola Politikasında belirtilen standartlara göre parola belirlenmesinin sağlanması için bilgisayarların aktif dizin yapısına dahil edilmesi ve belirlenen parola politikasına göre kullanıcı kurallarında güncelleme yapılması gerekmektedir. **Bu nedenle öncelikle aktif dizin yapısında olmayan bilgisayarlar tespit edilecek, eksik olanlar aktif dizin yapısına dahil edilecek ve parola politikası yaygınlaştırma çalışması gerçekleştirilecektir.**

Ayrıcalıklı Erişim Haklarının Yönetimi ve Ayrıcalıklı Destek Programlarının kullanımı hususunda;

Ayrıcalıklı erişim hakları hem sistemlere erişim hem de kullanıcıların kendi bilgisayarlarında local admin yetkisine sahip olduğu anlamına gelmektedir. Sistemlerin yönetimi ve bilişim sistemlerinin devamlılığı için yetkili ve yetkin personel erişim hakkı verilmesi kaçınılmazdır. Ancak local admin yetkisi bir ihtiyaç değil aksine Kurumu ve kurumsal bilgiyi risk altına alan bir uygulamadır. **Gerçekten ihtiyaç duyulmadıkça hiçbir kullanıcıya local admin yetkisi**

Hipodrom Cad. No: 12 06330 - Yenimahalle / ANKARA
Telefon Nu. : 540 10 00 Belgegeçer Nu. : 384 16 35 P.K.: 64 Ulus / ANKARA
e-posta: ustaes@tki.gov.tr internet adresi: http://www.tki.gov.tr
Bilgi İçin
Esat USTA
Mühendis

verilmemelidir. Aksi takdirde kullanıcılar, Kurum tarafından alınan ve yaygınlaştırılan antivirüs yazılımını devre dışı bırakabilir, bilgisayarlarına istedikleri uygulamayı yükleyebilir (bunlar cyriptolocker vb. zararlı yazılımlarda olabilir), Kurum tarafından uygulanan politikaları devre dışı bırakabilir, sisteme yeni kullanıcı ekleyebilir, network ayarlarını değiştirebilir ve zararlı yazılımın Kurumun tüm bilişim altyapısına bulaşmasına yol açabilir. Bu nedenle Kurum bilişim altyapısında local admin yetkisi verilmiş kullanıcılar tespit edilecek, gereksiz olan yetkiler tespit edilerek kaldırılacak ve ayrıcalıklı erişim hakkı verilen kullanıcılardan da "yetki talep formu" alınacaktır.

Kurum bünyesinde acil durumlarda veya kritik ortamlarda akşamları ve hafta sonları "**Kurum internet**" ağının "**zorunlu kullanıcılar**" haricinde kullanımının önüne geçilerek bu kuralın dikkatli bir şekilde uygulanması sağlanacaktır.

Bilişim sistemlerine erişimlerde; bilişim hizmeti satın alınan firma personelinin ve Kurum çalışanlarının yetkilendirilmesi ve emeklilik, istifa, işten çıkarılma, açığa alınma gibi nedenler ile ücretsiz izin, askerlik, doğum izni gibi uzun süreli işe ara vermelerde gerek firma personelinin gerekse Kurum çalışanlarının sisteme erişim yetkilerinin **gecikme olmaksızın** dondurulması veya kaldırılması süreçleri net bir şekilde belirlenip uygulanabilmesi için ilgili birimler öncelikle Bilgi İşlem Müdürlüğüne bilgi verecek ve yetkisiz erişimlerin önüne geçilecektir.

Herhangi bir nedenle görevinden ayrılan personelin kullanmış olduğu bilişim ürünlerini teslim etmeden ayrılışına izin verilmeyecektir. İlgili birimler teslim aldıkları bilişim ürünlerini Bilgi İşlem Müdürlüğüne **gecikme olmaksızın göndereceklerdir.** İlgili birim tarafından bilgisayara ihtiyaç duyulması halinde Bilgi İşlem Müdürlüğünce yeni kişi adına yeniden yapılandırılıp teslim edilecektir.

Kurumsal bilgi işlem güvenliğimiz için yukarıda belirtilen tedbirlerin alınması ve sürekliliğinin sağlanması hususunda;

Bilginizi, keyfiyetin tüm personelinize duyurulması ile gereğince işlem yapılmasını rica ederim.

e-imza
Mustafa AKTAŞ
Genel Müdür

Dağıtım:
Daire Başkanlıkları ve Müesseseler

Hipodrom Cad. No: 12 06330 - Yenimahalle / ANKARA
Telefon Nu. : 540 10 00 Belgegeçer Nu. : 384 16 35 P.K.: 64 Ulus / ANKARA
e-posta: ustaes@tki.gov.tr internet adresi: http://www.tki.gov.tr
Bilgi İçin
Esat USTA
Mühendis