ERİŞİM KONTROLÜ

Bir kurumda bilgi güvenliğinin sağlanması adına, uygulanması ve uyulması gereken en önemli maddelerden biri olan erişim kontrolü, hangi açıdan bakarsanız mutlaklık içeren maddelerden oluştuğunu görebilirsiniz. Erişim kontrolünü etkin ve efektif olarak uygulamak başta data kaybı olmak üzere birçok konuda daha güvenli bir yapıda olmanızı sağlayacaktır.

1 ERİŞİM KONTROLÜ İÇİN İŞ GEREKSİNİMLERİ

Erişim Kontrolü Politikası

- Erişimle ilgili iş ve güvenlik ihtiyaçları göz önünde bulundurularak erişim denetimi politikası oluşturulmuş ve belgelenmiş olmalıdır.
- Erişim denetimi hem fiziksel, hem işlevsel boyutları ile değerlendirilmiş olmalıdır.
- Erişim denetimi politikası bütün kullanıcılar veya kullanıcı grupları için erişim kurallarını ve haklarını açıkça belirtiyor olmalıdır.
- Kullanıcılara ve servis sağlayıcılarına erişim denetimiyle hangi iş gereksinimlerinin karşılanacağı iyice açıklanmış olmalıdır.
- Politika belgesi şu konuları içermelidir; her bir iş sürecinin güvenlik ihtiyaçları, iş süreçleri ile ilgili tüm bilgiler ve bu bilgilerin yüz yüze olduğu riskler, bilginin yayılması ve yetkilendirme ile ilgili politikalar, bilginin sınıflandırılması, güvenlik seviyeleri ve "gerektiği kadar bilme" prensibi, farklı sistem ve ağlardaki bilginin sınıflandırılması ve erişim denetimine ilişkin politikaların tutarlı olması, bilgiye erişimle ilgili olarak kontratlardan ve yasal yükümlülüklerden kaynaklanan şartların yerine getirilmesi, kurumun yaygın kullanıcı profilleri ile ilgili erişim hakları ve Erişimin talep edilmesi, yetkilendirilmesi ve yönetilmesi görevlerinin birbirinden ayrılması.
- Erişim haklarının "Yasaklanmadıkça her şey serbesttir" değil "İzin verilmedikçe her şey yasaktır" prensibine göre verilmesine dikkat edilmelidir.

2 KULLANICI ERİŞİMİNİN YÖNETİLMESİ

Kullanıcı Kaydı

- Bilgi sistemlerine ve servislerine erişim hakkı vermek için resmi bir kullanıcı kaydı girme ve kullanıcı kaydı silme prosedürü olmalıdır.
- Sistem kayıtları ile ilişkilendirme ve sorumlu tutulabilme açısından kullanıcı kimliklerinin her kullanıcı için farklı olmasına dikkat ediliyor olmalıdır.
- Bilgi sistemini ve servisini kullanabileceğine dair sistem sahibi kullanıcıya yetki vermiş olmalıdır.
- Verilen erişim hakkı kurumsal güvenlik politikasına ve görevler ayrılığı ilkesine uygun olmalıdır.
- Kullanıcılara erişim hakları ile ilgili yazılı belge veriliyor ve kullanıcılardan erişim şartlarını anladıklarına ilişkin imzalı belge alınıyor olmalıdır.
- Görevi değişen veya kuruluştan ayrılan personelin erişim hakları derhal güncellenmelidir.

Ayrıcalık Yönetimi

- Ayrıcalıkların kullanımı sınırlandırılmış ve denetleniyor olmalıdır.
- Ayrıcalıklar "kullanması gereken" prensibine göre ve resmi bir yetkilendirme süreci sonunda verilmelidir.

Kullanıcı Parola Yönetimi

- Kullanıcı parolalarının atanması ya da değiştirilmesi resmi bir prosedür uyarınca yapılmalıdır.
- Kullanıcılara parolalarını saklı tutacaklarına dair bir anlaşma imzalatılmalıdır.

Kullanıcı Erişim Haklarının Gözden Geçirilmesi

- Kullanıcı erişim haklarının düzenli aralıklarla kontrol edilmesini sağlayan resmi bir süreç olmalıdır.

3 KULLANICI SORUMLULUKLARI

Parola Kullanımı

- Kullanıcı parolalarının seçilmesi ve kullanılması ile ilgili güvenlik tedbirleri uygulanmalıdır.

- Sistem tarafından geçici olarak verilen parolaların kullanıcı tarafından sisteme ilk girişte değiştirilmesi sağlanmalıdır.
- Kullanıcılar zor kırılacak parolalar seçmeleri konusunda bilinçlendirilmiş olmalıdır.
- Kişisel parolaların hiç kimse ile paylaşılmamasına, yazılı veya elektronik ortamlarda kaydedilmemesine dikkat edilmelidir.
- Kullanıcılar düzenli aralıklarla veya sistem güvenliği ile ilgili bir kuşku oluştuktan sonra parolalarını değiştirmeye zorlanmalıdır.
- Kullanıcılar kişisel işlerinde kullandıkları parolaları kuruluşun iş süreçlerinde kullanmamaları gerektiği konusunda bilinçlendirilmiş olmalılardır.

Gözetimsiz Kullanıcı Ekipmanı

- Atıl cihazlara ait güvenlik gereksinimlerinden, bu cihazları koruma prosedürlerinden ve bu cihazları korumak için üzerlerine düşen sorumluluklardan kullanıcıların ve iş ortaklarının haberleri olmalıdır. (İşi biten kullanıcıların bilgisayarını kapatması ve şifreli ekran koruyucuların kullanılması gibi)

Temiz Masa ve Temiz Ekran Politikası

- Kuruluş kağıt ve taşınabilir elektronik depolama ortamlar ile ilgili olarak temiz masa politikası uygulamalıdır.
- Kuruluş bilgi veya bilgi işlem araçları ile ilgili olarak temiz ekran politikası uyguluyor olmalıdır.
- Hassas bilgileri içeren kağıt ve elektronik depolama ortamlarının kullanılmadığı zaman kilitlenmesi, bilgisayar başından kalkarken personelin oturumunu kapaması veya ancak parola ile açılabilen ekran koruyucu vb. önlemleri devreye sokması, gelen/giden postaya erişim noktalarının ve faks cihazlarının denetlenmesi, fotokopi makinesi, tarayıcı, sayısal fotoğraf makinesi gibi kopyalama teknolojilerinin yetkisiz olarak kullanılmaması ve hassas bilgi içeren dokümanların yazıcı üstünde bırakılmaması konularına özen gösterilmelidir.

4 AĞ ERİŞİM KONTROLÜ

Ağ Hizmetlerinin Kullanılması İle İlgili Politikalar

- Kullanıcıların sadece kullanma yetkisine sahip oldukları ağ servislerine erişebilmesi sağlanmış olmalıdır.
- Ağlar ve ağ servisleri ile ilgili olarak şu konuları düzenleyen politikalar uygulanıyor olmalıdır; kimin hangi ağlara ve ağ servislerine erişebileceğini belirlemek için yetkilendirme prosedürü tanımlanmış olmalıdır, ağ bağlantılarını korumak ve ağ servislerine erişimi engellemek için yönetim denetimleri ve süreçleri belirlenmiş olmalıdır.

Harici Bağlantılar İçin Kullanıcı Kimliği Doğrulaması

- Sisteme dışarıdan yapılacak kullanıcı bağlantıları için kullanıcı kimliği doğrulama mekanizmaları uygulanmalıdır. (Kripto tabanlı teknikler veya klasik "challange- response" mekanizmaları ile çözülebilir. VPN çözümleri de bu teknikleri kullanmaktadır.)

Ağlarda Cihaz Kimliği Belirleme

- Bağlantının belli bir cihaz kullanılarak yapıldığından emin olmak için otomatik cihaz kimliği belirleme yöntemleri kullanılıyor olmalıdır.

Uzaktan Tanı ve Yapılandırma Portu Koruma

- Yönetim ve yapılandırma portlarına fiziksel ve işlevsel erişimi denetleyen bir güvenlik mekanizması olmalıdır.

Ağlardaki Ayrım

- Bilgi sistemi üstündeki kullanıcı ve servisler gruplara ayrılmış olmalıdır.
- Kurumun ağı dahili ve harici etki alanlarına bölünmüş olmalıdır.
- Etki alanları kurumun erişim kontrol politikası ve erişim ihtiyaçları uyarınca oluşturulmuş olmalıdır.
- Etki alanları sınır güvenliği sistemleri ile korunmalıdır.
- Telsiz ağların diğer ağlardan ayrılması ile ilgili olarak çalışma yapılmış olmalıdır.

Ağ Bağlantı Kontrolü

- Kurum sınırlarının dışına taşan ağlar ve ağ bağlantılarının kullanımı, kurumun erişim kontrol politikası uyarınca kısıtlanmış olmalıdır.
- Elektronik mesaj, tek veya çift yönlü dosya aktarımı, interaktif erişim, bağlantı zamanı ve süresi ile ilgili kısıtlamalar getirilmiş olmalıdır.

Ağ Yönlendirme Kontrolü

- Ağ yönlendirme kontrolleri, bilgisayar bağlantılarının ve bilgi akışının erişim politikasına uygun gerçekleşmesini sağlayacak şekilde tanımlanmış olmalıdır.
- Ağ iletişimi kaynak adres ve hedef adreslere bağlı olarak güvenlik duvarı vb. cihazlar aracılığı ile kontrol ediliyor olmalıdır.

5 İŞLETİM SİSTEMİ ERİŞİM KONTROLÜ

Güvenli Oturum Açma Prosedürleri

- Oturum açma işlemleri yetkisiz erişim olasılığını asgari düzeye indirecek şekilde düzenlenmiş olmalıdır.
- Sistem ve uygulamaya ilişkin olarak yetkisiz kullanıcıya yardımcı olabilecek bilgiler oturuma giriş başarıyla tamamlanana kadar gizlenmelidir.
- Bilgisayarda sadece yetkili personel tarafından erişilebileceğini bildiren uyarı mesajı gösterilmelidir.
- Oturuma giriş sadece tüm girdi verilerinin doğrulanmasından sonra sağlanmalıdır.
- Bir hata durumu varsa sistem verinin hangi kısmının doğru veya yanlış olduğu bilgisini gizlemelidir.
- Sistem tarafından izin verilen başarısız giriş denemelerine sınırlama getirilmiş olmalıdır.
- Oturuma giriş işlemi için zaman sınırı olmalıdır.
- Başarısız giriş denemeleri kaydedilmelidir.
- Ağ üstünden şifrenin açık olarak gönderilmemesi sağlanmalıdır.

Kullanıcı Kimlik Tanımlama ve Doğrulama

- Gerektiğinde sistem kayıtlarının incelenmesi ve bir işlemin sorumlusunun bulunabilmesi açısından her bir kullanıcıya kendine özgü bir kullanıcı kimliği verilmiş olmalıdır.
- Sistem yöneticilerine ait kullanıcı kimlikleri birbirinden faklı olmalıdır.
- Kurum bünyesinde kullanılan kullanıcı tanımlama ve yetkilendirme mekanizmaları iş gereklerine uygun olmalıdır.

Parola Yönetim Sistemi

- Kurum bünyesinde kullanılan belirli bir parola yönetim sistemi olmalıdır.
- Parola yönetim sistemi şu özelliklere sahip olmalıdır; kullanıcıları bireysel parolaların kullanımına zorluyor olmalıdır, kullanıcıların kendi parolalarını seçmelerine ve değiştirmelerine izin veriyor olmalıdır, kullanıcıyı kuvvetli parola seçmeye zorlamalıdır, kullanıcıyı belli zamanlarda parolasını değiştirmeye zorlamalıdır, sisteme ilk girişte geçici parolayı değiştirmeye zorlamalıdır, eski parolaları hatırlayarak tekrar kullanılmalarına engel olmalıdır, parolalar ağ üstünden gönderilirken ve saklanırken kriptolama gibi yöntemlerle korunuyor olmalıdır.

Yardımcı Sistem Programlarının Kullanımı

- Sistem araçlarının sistem özelliklerini ve uygulama programlarının yetkilerini aşarak ekstra işlemler yapmadığı kontrol ediliyor olmalıdır.

Oturum Zaman Aşımı

- Kullanılmayan oturumlar tanımlı bir süre sonunda kapatılmalıdır.

Bağlantı Süresinin Sınırlandırılması

- Kurum dışından veya halka açık alanlardan yüksek riskli uygulamalara erişim durumunda bağlantı süresi kısıtlanmalıdır.
- Kullanıcı belli aralıklarla kimliğini tekrar doğrulamaya zorlanıyor olmalıdır.

6 UYGULAMA VE BİLGİ ERİŞİM KONTROLÜ

Bilgi Erişimi Kısıtlaması

- Erişim kontrolü politikası uyarınca kullanıcılar ve destek personeli için bilgi sistemleri fonksiyonları ve bilgilerine erişim kısıtlanmış olmalıdır.
- Kullanıcıların bilgiyi yazma, okuma, silme veya çalıştırma hakları düzenlenmelidir.

Duyarlı Sistem Yalıtımı

- Uygulamanın duyarlılığı uygulama sahibi tarafından açıklanmış ve belgelenmiş olmalıdır.
- Duyarlı bilgilerin bulunduğu sistemler diğer sistemlerden izole edilmelidir. (Kendisine ait bilgisayarda çalıştırılması, ayrı ağ bölmesine yerleştirilmesi, ağ kaynaklarının ayrılması, sadece gerekli uygulamalar ile iletişim kurulması vb. İzolasyon fiziksel veya işlevsel olarak gerçekleştirilebilir.)

7 MOBİL BİLGİ İŞLEME VE UZAKTAN ÇALIŞMA

Mobil Bilgi İşleme ve İletişim

- Dizüstü bilgisayar, cep bilgisayarı, cep telefonu, akıllı kartlar vb. mobil bilgi işlem ve iletişim araçlarının kullanılmasından kaynaklanan risklerden korunmak için benimsenmiş bir politika ve uygulanmakta olan güvenlik önlemleri olmalıdır.
- Mobil bilgi işlem politika belgesi fiziksel koruma, erişim denetimi, kriptografik denetimler, yedekleme ve virüs koruması konularını içermelidir.
- Mobil bilgi işlem araçlarının halka açık yerler, toplantı odaları gibi korumasız ortamlarda kullanılması sırasında yetkisiz erişime ve bilginin açığa çıkmasına karşı kriptografik tekniklerin kullanılması gibi önlemler alınıyor olmalıdır.
- Hırsızlığa karşı önlemler alınıyor olmalıdır.
- Hassas bilgi içeren araçların başıboş bırakılmamasına özen gösterilmelidir.

Uzaktan Çalışma

- Uzaktan çalışma faaliyetleri için organizasyonun güvenlik politikasına uygun plan ve prosedürler geliştirilmiş olmalıdır.
- Uzaktan çalışmanın yapılacağı yerde ekipman ve bilginin çalınmasına, bilgiye yetkisiz erişim yapılmasına, kuruluşun dahili sistemlerine uzaktan yetkisiz erişime ve bilgi işlem araçlarının kötüye kullanılmasına engel olmak için uygun önlemler alınmış olmalıdır.