ERZURUM BÜYÜKŞEHİR BELEDİYESİ BİLGİ İŞLEM DAİRE BAŞKANLIĞI

ERİŞİM DENETİMİ PROSEDÜRÜ

(Versiyon 1.0)

2022

Doküman Detayları

Hazırlanma Tarihi	12.12.2022	**Yayın**	Final
Hazırlayan	Olcay Ozan DİKBAŞ – Ersin YILDIZ		
Doküman Numarası	EBB-PR-04		

Revizyon Geçmişi

Revizyon Tarihi	Önceki Revizyon Tarihi	Yapılan Değişikliklerin Özeti
12.12.2022		İlk Yayın

Onay

Onaylayan	İmza	Görevi	Tarih	Versiyon
Zafer AYNALI		Genel Sekreter	12.12.2022	1.0
Murat ALTUNDAĞ		Genel Sekreter Yardımcısı	12.12.2022	1.0
Serkan ÇEKİÇ		Bilgi İşlem Daire Başkanı	12.12.2022	1.0

1. AMAÇ

Bu prosedürün amacı; Erzurum Büyükşehir Belediyesi bünyesinde bulunan bilgi ve bilgi işleme tesislerine yapılacak olan erişimlerin kısıtlanması, sadece yetki verilen kişilerin kontrollü ve kayıt altına alınarak bilgiye erişmesine imkân verecek bir sistemin tesis edilmesidir.

2. KAPSAM

Erzurum Büyükşehir Belediyesi bünyesinde görev yapan tüm personeller için bilgiye erişim kurallarını ve yöntemlerini kapsamaktadır.

3. UYGULAMA

3.1. Erişim Kontrol Politikası

3.1.1. Erzurum Büyükşehir Belediyesi Bilgi Güvenliği Alt Komisyonu tarafından Bilgi Güvenliği Erişim Kontrolü Prosedürü oluşturulmuştur.

3.1.2. Erzurum Büyükşehir Belediyesi, bağlı birimleri ve tesisleri bünyesindeki tüm veri alış verişleri Erzurum Büyükşehir Belediyesi (Belediye Ağı) üzerinden sağlanmaktadır.

3.1.3. Kimin, hangi bilgiye, hangi yetkilerle erişeceği ve erişimin kontrolü için kullanılacak yöntemler için Erişim yetki ve kontrol matrisi oluşturulmuştur.

3.1.4. Herhangi bir gizliliği olmayan, herkesin erişimine açık olan (tasnif dışı gizlilik dereceli) bilgiler için özel bir erişim kontrol tedbiri alınmaz, bu tür bilgiler, kurumumuz internet sitelerinin vatandaşlara açık bölümlerine konulabilir, bina ve tesislerde duyuru panosu vb. ortamlarda yayımlanabilir.

3.1.5. Bilgiye verilen gizlilik derecesine göre uygulanacak erişim kontrol yöntem ve politikası değişir.

3.1.6. Bilgiye kimin hangi yetki ile erişeceği kararı, bizzat bilgi varlıklarının sahipleri tarafından verilir.

3.1.7. Bilgiye erişim talepleri ve ilgili makamlarca bu taleplere yapılan işlemlerin takip edilebilirliğini sağlamak üzere yazılı kurallar oluşturulur.

3.1.8. Erişim izinleri ile ilgili kayıtlar, varsa ilgili mevzuatta belirtilen sürelerce, yoksa varlığın sahibi tarafından belirlenecek süre boyunca saklanır.

3.1.9. Erişim izinleri verilirken, "görevlerin ayrılığı" ve "bilmesi gereken" prensiplerine göre hareket edilir.

3.1.10. "Görevlerin ayrılığı" prensibi uyarınca; kritik iş süreçlerinin gerçekleştirilmesi için birden fazla kullanıcı görevlendirilir. Bilgiye erişim için aşamalı yetkilendirme yapılarak bir kişinin kendi başına tüm bilgi varlıklarına erişimi engellenir. Teknik nedenlerle görev ayrımı yapılamayan süreçlerin (örneğin etki alanı yöneticisi, veri tabanı yöneticisi vb.) kontrolü için ilave tedbirler alınır. Gerekiyorsa idari kontrol mekanizmaları oluşturulur.

3.1.11. **"**Bilmesi gereken" prensibi uyarınca; sistemde bulunan süreçler ve kullanıcılara, sistem kaynaklarına erişirken, kendilerine atanmış görevlerini gerçekleştirmelerine yetecek kadar yetki verilir.

3.1.12. Kullanıcıların kimliklerinin doğrulanması için asgari teknik önlem olarak, parola kullanımı zorunlu tutulur. Yapılacak risk değerlendirmesine göre daha kritik sistemler için farklı kimlik doğrulama yöntemleri (token, akıllı kart, tek kullanımlık parola, parmak izi/retina/avuç içi tarama vb.) kullanılabilir.

3.1.13. Bilgi varlıklarına yapılan erişimler için iz kayıtları oluşturulur.

3.1.14. Erzurum Büyükşehir Belediyesi (Belediye Ağı) dışındaki ağlar güvensiz ağ olarak kabul edilir. Yetkisiz erişimler de dâhil olmak üzere iç ağı dış tehditlerden korumak için sınır güvenlik sistemleri (güvenlik duvarı vb.) tesis edilir.

3.1.15. Kullanıcı ve sunucuların bulunduğu ağlar, güvenlik duvarları ve/veya ağ cihazları erişim kontrol listeleri vasıtasıyla ayrılır. VTYS(Veri Tabanı Yönetim Sistemleri) sunucularının bulunduğu ağ kesimlerine, normal kullanıcı erişimleri engellenir.

3.1.16. Erzurum Büyükşehir Belediyesi politikaları gereği güvenlik duvarı üzerinde Deep SSL Inspection özelliği açılır ve internet erişimi sağlayacak tüm kullanıcı bilgisayarlarında ilgili güvenlik sertifikaları Güvenilir Kök Sertifikalarına eklenir.

3.1.17. Personelin internet erişimleri için LDAP authentication kullanılır ve internete erişimlerde doğrulama ekranı (captive portal) gelmelidir. Bu doğrulama ekranında kullanıcı adı ve şifre olarak kurumsal e-posta adresi (@erzurum.bel.tr) kullanıcı adı ve parolaları kullanılır. Doğrulama yapmayan kullanıcı internete erişemez.

3.1.18. Dış birimlerdeki ve kırsaldaki sunuculara ya da cihazlara kurum içinden/dışından erişimler (Uzak Masaüstü vb.) SSLVPN aracılığıyla

olacaktır. SSLVPN hesaplarının oluşturulması için erişim talebini yapacak firma personeli Kurumsal Gizlilik Sözleşmesi Formunu doldurarak sözleşme yaptığı idareye resmi yazı ile talepte bulunacaktır. Bilgi İşlem Daire Başkanlığı network sorumlusu gerekli takibi yaparak resmi yazı sonrası VPN hesaplarını oluşturacaktır.

3.1.19. Sorumluluğu sözleşme ile sabit olan ve sunuculara erişmesi gereken kullanıcılardan (Firma personeli veya hizmet alımı) gizlilik sözleşmesi alınarak SSLVPN kullanıcı tanımları yapılmalıdır. Gizlilik sözleşmesi olmayan kullanıcılara erişim yetkisi kesinlikle verilmemektedir.

3.2. Kullanıcı Erişimlerinin Yönetimi

3.2.1. Kullanıcı erişimlerinin yönetimi, sistem ve hizmetlere yetkisiz olarak yapılacak erişimleri engellemek ve sadece yetkili kullanıcıların erişimlerini temin etmek için yapılır.

3.2.2. Başta kişisel verilerin işlendiği bilgi sistemleri olmak üzere erişim kontrolüne tabi tutulacak tüm sistem ve hizmetler için "kullanıcı erişim yönetimi esasları" belirlenir. Belirlenen esaslar, ilgili tüm taraflara (muhtemel kullanıcılara) resmen duyurulur.

3.2.3. Ayrıcalıklı erişim hakkı talepleri için Ayrıcalıklı Erişim Hakkı Talep Formu düzenlenmiştir.

3.2.4. Ayrıcalıklı erişim hakları mümkün olduğunca kısıtlanmalıdır. Ayrıcalıklı erişim hakları yönetici onayı ile Sistem Yöneticisi tarafından verilmektedir.

3.2.5. Ayrıcalıklı erişim hakkı talebinde bulunacak personeller; kurum bilgi işlem birimine Ayrıcalıklı Erişim Hakkı Talep Formu doldurarak başvuruda bulunurlar. Talepler daha sonra Bilgi İşlem Birimine resmi yazı ile gönderilerek sonuçlandırılır.

3.2.6. Hizmet veya sistemlerin sahiplerince erişim hakları periyodik olarak incelenir. Bilmesi gereken prensibi uyarınca gereksiz olarak verilmiş yetkilerin kaldırılması sağlanır.

3.2.7. İncelemeler tüm kullanıcılar için düzenli aralıklarla ve rutin olarak en az 6 (altı) aylık aralıklarla yapılır.

3.2.8. Bireysel kullanıcı erişim hakları, terfi veya sorumlulukların değiştirilmesi veya görev yeri değişiklikleri sonrasında gözden geçirilir.

3.2.9. Ayrıcalıklı hesapların tahsisi ve kullanımı ile ilgili incelemeler, 3 (üç) ayı aşmayacak şekilde daha sık yapılır.

3.2.10. 90 gün veya daha fazla süre ile kullanılmayan hesaplar devre dışı bırakılır ve erişim izinleri askıya alınır. Bu süre Erzurum Büyükşehir Belediyesi bilgi güvenliği alt komisyonu tarafından değiştirilebilir. Her bir sistem için belirlenecek süreler, kurumların erişim kontrol politikası içinde yazılı olarak kayıt altına alınır.

3.2.11. Ayrıcalıklı erişim hakkı verilen kullanıcı sayısı (etki alanı yöneticisi, veri tabanı yöneticisi vb.) asgari düzeyde tutulur

3.2.12. Sistem ve uygulamaların kontrollerini geçersiz kılma kabiliyetine sahip olabilen destek programlarının kullanımı kısıtlanır ve sıkı bir şekilde kontrol edilir.

3.2.13. Programların kaynak kodları ve ilgili ögelere (tasarımlar, özellikler, doğrulama planları ve geçerleme planları gibi) erişim (yetkisiz işlevsellik girişini ve istenmeyen değişiklikleri önlemenin yanı sıra değerli fikri mülkiyet haklarının gizliliğini sağlamak için) sıkı bir şekilde kontrol edilir.

3.3. İz Kayıtları (Log) Yönetimi

3.3.1. Kurum bünyesindeki kullanıcı faaliyetleri, bilişim sistemlerine yönelik saldırı ya da hatalar, saldırının tespit edildiği anda saldırıya ait detayları gösteren iz kayıtları oluşturulur ve belirli kurallar dâhilinde toplanır.

3.3.2. İz kayıtlarının tutulması ve yönetilmesi (iz kayıtlarının üretilmesi, aktarılması, gözden geçirilmesi, analiz edilmesi ve imha edilmesi gibi süreçler) sadece erişim yetkisi verilen bir birim/kişiler tarafından yapılır. Bu yetkilerin SOME'lere verilmesi uygundur.

3.3.3. Farklı sistemler tarafından üretilen iz kayıtları; güvenlik denetimi sağlamak, iz kayıtlarını daha etkin ve verimli olarak saklamak, yedeklemek ve raporlayabilmek amacıyla merkezi bir sunucuda toplanır.

3.3.4. İz kaydı (log) alınması gereken fiziksel ortam kayıtları; kritik bilişim sistemleri odaları giriş-çıkış kayıtları ve kamera kayıtları ile normal çalışma ortamları giriş-çıkış kayıtları ve kamera kayıtlarından oluşur. Kamera kayıtları 2 (iki) ay, kritik sistem odaları ve çalışma ortamları giriş-çıkış kayıtları 2 (iki) yıl süreyle tutulur.

3.3.5. İz kayıtlarının saklanma süresi belirlenirken yasal zorunluluklar, iz kayıtlarından sağlanacak fayda, saklama maliyeti ve ilgili iz kaydının kritikliği göz önünde bulundurulur. Başka bir yasal zorunluluk yoksa elektronik olarak üretilen tüm iz kayıtları en az 2 (iki) yıl süre ile saklanacak şekilde önlem alınır.

3.3.6. Kritik olaylara ilişkin iz kayıtlarının merkezi sunucuya eş zamanlı olarak (olay oluştuğu zaman) gönderilmesi sağlanır.

3.3.7. Kritik sistemlerde oluşan iz kayıtları eş zamanlı olarak merkezi iz kayıtları sunucusuna aktarılır. Merkezi sunucuya aktarılan kayıtların silinmesi ve değiştirilmesinin engellenmesi için gerekli teknik ve idari tedbirler alınır.

3.3.8. Kayıt üreten ortamların teknolojisine uygun olarak kimlik doğrulama ve yetkilendirme sistemleri hayata geçirilir.

3.3.9. Teknik olarak mümkün olması durumunda, iz kayıtları gizlilik ve hassasiyet seviyelerine göre sınıflandırılarak, ilgili kullanıcıların sadece verilen yetkiler çerçevesinde iz kayıtlarına bakmaları sağlanır.

3.3.10. İz kayıtları periyodik olarak yedeklenir ve yedeklerin uygun şekilde muhafaza edilmesi sağlanır.

3.3.11. Merkezi iz kaydı sunucusu sadece yeni iz kayıtlarının saklanması için fonksiyonlar içerir. Bu sunucuda iz kayıtlarının silinmesi/değiştirilmesi amaçlı erişimlere izin verilmez.

3.3.12. İz kayıtlarının tek yönlü kriptografik özet değerleri (hash) hesaplatılır ve iz kayıtları güvenli ortamlarda saklanır.

3.3.13. Olay sonrası incelenmek üzere güvenilir delillerin elde edilmesi için tutulacak kayıtların asgari niteliklerinin aşağıdaki gibi olması gerekir:

- Fiziksel ortam kayıtları: Çalışma ortamları ve sistem/sunucu odalarına yapılan giriş-çıkışlara ait kamera kayıtları, varsa bunlarla ilgili diğer kayıtlar (kartlı geçiş sistemi, parmak izi okuyucuları vb. sistemler tarafından üretilen iz kayıtları),
- Sanal ortam kayıtları,
- Bilişim sistemleri tarafından üretilen kayıtlar, SBYS'ler,
- Güvenlik duvarları,
- Antivirüs yazılımları,
- Saldırı tespit/önleme sistemleri,
- Yönlendiriciler ve anahtarlama cihazları,

- Sunucular,
- Diğer iş uygulamaları (kritik kurumsal projeler),
- Veri tabanları,
- VPN iz kayıtları.

3.3.14. Tutulması gereken asgari iz kayıtları;

- Kaydı oluşturan sistem,
- Kaydın oluşturulma zamanı (tarih, saat, zaman dilimi),
- Kaydı oluşturan olay,
- Kaydın ilişkili olduğu kişi (IP/Port bilgisi, MAC adresi, işlemi yapan tekil kullanıcı adı veya sistemin adı).

4. YAPTIRIM

Bilgi Güvenliği Politikalarının ve Prosedürlerinin ihlali durumunda, **Bilgi Güvenliği Disiplin Prosedürü** dokümanında belirtilen hususlar ve ilgili maddeleri esas alınarak işlem yapılır.