1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi bünyesinde kullanılan/kullanılabilecek kullanıcı adı ve şifre ile erişim sağlanan sistemlerin güvenliği için güçlü bir şifre oluşturulması, oluşturulan şifrenin korunması ve şifre değiştirme sıklığı hakkında standart oluşturmak.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesinde kullanıcı adı ve hesabı olan (bilgisayar ağına erişen) tüm kullanıcıları kapsamaktadır.

3. SORUMLULAR

- Bilişim Sistemi Kullanıcıları
- Bilgi İşlem Daire Başkanlığı
- Sistem Yönetimi Birimi

4. TANIMLAR

5. UYGULAMA

5.1 Şifreleme Prosedürleri

5.1.1 Kurum Politikaları

Kurumun ihtiyaçları ve politikaları, şifreleme hizmetleri için ele alındığında, şifrelemenin kurumun altyapısında ne zaman ve bazı durumlarda da nerede uygulanacağını tanımlar. Kurum'un şifreleme hizmetlerine yönelik kurum politikaları şu şekildedir:

Bölüm yöneticisinin veya Bilgi İşlem yöneticisinin özel onayı olmadığı müddetçe okunabilir gizli ve çok gizli bilgi e-posta yoluyla gönderilmemelidir.

Her personel, Kurum'un hassas bilgisini içeren tüm taşınabilir cihazların, dizüstü bilgisayarların ve diğer taşınabilir bilgisayarların sabit disklerinin şifrelenmesini (tüm dosyalar) ve cihazlarda önyükleme koruması (bootprotection) bulunmasını sağlamakla sorumludur.

Hassas kurum bilgisini içeren tüm taşınabilir cihazları, dizüstü bilgisayarları ve diğer taşınabilir bilgisayarları kullanan Kurum personeli, eğer cihazlardaki hassas bilgiler şifrelenmemişse, bu cihazları hiçbir koşulda gözetimsiz bırakmamalıdır.

Bilgi İşlem yönetimi, kimlik doğrulama bilgilerinin elektronik herhangi bir ortamda saklanması durumunda şifreler. Bu şekilde, yetkisiz tarafların bu şifreleri ele geçirmeleri durumunda şifreleri kullanamamaları sağlanır.

Eğer şifreler veya Kişisel Kimlik Numaraları (PersonalIdentificationNumbers - PIN) bir bilgisayar sistemi tarafından üretiliyorsa, formül, algoritma ve sürece ait diğer bilgileri içeren

tüm yazılım ve dosyalar ilgili bilgisayar sisteminin desteklediği en sıkı güvenlik önlemleri ile kontrol edilir.

5.1.2 Teknik Politika

Şifreleme hizmetlerine yönelik teknik politikalar, şifrelemenin nasıl yapılması gerektiğini açıklayan uygulama prensibini, teknik kriteri veya bazı durumlarda kurum prosedürlerini tanımlar. Kurum'un şifreleme hizmetleri için kullandığı teknik politikalar şu şekildedir:

Akış Kontrol Sistemleri: Yetkisiz girişleri engellemek için tüm elektronik ticaret sunucuları (ağ, veritabanı, güvenlik sunucuları vs.) özgün dijital sertifika kullanır ve bilginin bu sunuculara ya da bu sunuculardan iletimi için şifreleme kullanılır. Ağ sunucuları, FTP sunucuları ve diğer kamu üyeleriyle iletişimi destekleyen herhangi bir kurum sunucusu için bu yönteme başvurulmayabilir.

Şifre Tasarımı: Kullanıcı şifre veya şifreleme anahtarını ilk kez tanımladığında, bu bilgiler iki kere girilir ve yazılan bilgilerin başkaları tarafından görülmemesi için gizlenir. Girilen bu bilgilerin ikisi de sistem tarafından kabul edilmesi için aynı olmalıdır. Bu kontrol yanlış yazımdan (tuşlama) kaynaklanacak kullanıcı kilitlenmelerine ya da sistemlere erişememeye karşı önlem alır.

Simetrik ve Asimetrik Şifreleme: Kurum simetrik anahtar şifreleme algoritmaları ile birlikte asimetrik anahtar şifreleme algoritmalarını desteklemektedir. Asimetrik anahtar kullanımı durumunda, bir varlığa açık anahtar (publickey) atanması için dijital sertifika kullanılır ve bu sertifikalar RSA veya SHA256 formatındadır.

5.2 Anahtar Yönetimi

Anahtar yönetimi, şifreleme anahtarları yaşam döngüsüne yönelik Kurum politikalarını ele alır. Gereksinimler şu şekildedir:

Anahtar Üretimi: Tüm simetrik şifreleme anahtarları endüstriyel standartlara göre rastgele seçilir.

Simetrik Anahtar Ömrü: Simetrik şifreleme kullanıldığında, verinin nerede ve nasıl işlendiğine bağlı olarak gerekli politikalar uygulanır. Temel fark verinin beklemede ya da iletimde olmasından ötürüdür. Ayrıca, veri beklemedeyken (örn. saklama ortamında bulunması durumunda) aktif ya da pasif olarak sınıflandırılmaktadır.

Verinin iletimde olması:

Asgari bir standart olarak 128 bit şifreleme kullanılır. Dinamik anahtarlar kullanıldığında, ana anahtarlar iki yılda bir defa değiştirilir. Veri şifreleme anahtarları her oturumda ya da 24 saatte bir değiştirilir.

Verinin beklemede olması:

Aktif veri – sabit disk, diğer bir bilgisayarın erişilebilir saklama ortamı gibi lokal saklama ortamlarında mevcut olan veri;

- Ana anahtarlar en az yılda bir defa değiştirilir.

- Anahtar şifreleme anahtarları, bu anahtarlar ana anahtar (Örn. Kerberos KDC Ana Anahtarı) değilse, üç ayda bir değiştirilir.
- Veri şifreleme anahtarları her yıl en az bir defa değiştirilir.
- Pasif veri – Arşivlenen ve işlenmeye hazır durumda olmayan veri Dinamik anahtarlar kullanıldığında, ana anahtarlar en az iki senede bir değiştirilir.
- Anahtar şifreleme anahtarları, bu anahtarlar ana anahtar (Örn. Kerberos KDC Ana Anahtarı) değilse, yılda en az bir defa değiştirilir.
- Veri şifreleme anahtarları yılda en az bir defa değiştirilir.

5.2.1 Asimetrik Anahtar Yaşam Süresi

Asimetrik şifrelemenin kullanıldığı durumda, bir açık anahtara sahip asimetrik şifrelerin yaşam süreleri yetkili kurumun yayınladığı Sertifika Politikası dokümanı ile belirlenir.

Anahtarın Depolanması: Şifreleme anahtarları bir şifreleme anahtarı depolama biriminde veya kabul edilmiş algoritmalarla şifrelenmiş olarak saklanır; aksi durumlarda şifreler akıllı kart gibi bir akıllı anahtar üzerinde saklanır. Şifreler akıllı kart ya da herhangi bir akıllı anahtar üzerinde tutuluyorsa şifreleme anahtarları bu akıllı anahtarların dışına çıkarılamaz.

Anahtar Arşivleme ve Saklama: Arşivlenen veriye ait anahtarın kendisi de arşivlenir. Şifreleme anahtarları arşivleri korunması için kullanıldığı veri ile birlikte arşivlenemez.

Anahtar İmhası: Şifreleme anahtarları;

Kullanımdan kaldırıldıklarında veya Zarara uğratıldıklarında ve bir anahtar saklama programının bir parçası olmadıkları durumda silinir ya da imha edilir.

5.2.2 Anahtar Sahipliği ve Dağıtımı

Şifreleme anahtarları gizli bilgidir ve bu anahtarlara erişim iş tanımı nedeniyle bu gereksinimde olan kişilerle sınırlandırılır. Şifrelemeyle korunan verinin sahipleri bu veriyi korumak için kullanılan şifreleme anahtar yönetimine dair sorumluluğunu imzalar. Şifreleme anahtarları haberleşme hatları üzerinden aktarılacaksa, şifrelenerek yollanır. Anahtarlar, iletilecek anahtarların şifreleme için kullanıldığı gizli bilginin şifrelenmesinde kullanılan algoritmadan daha güçlü bir algoritmayla şifrelenir.

Anahtarın Zarar Görmesi: Zarar gören şifreleme anahtarları derhal Bilgi Güvenliği Yöneticisi ve korunan verinin bilgi sahibine raporlanır. Ayrıca, anahtar değiştirilir ve/veya ‘Asimetrik Anahtar Yaşam Süresi’ bölümündeki Anahtar İmha prosedürüne göre imha edilir ve yeni bir anahtar üretilir. Yeni anahtar oluşturulur oluşturulmaz, zarar gören anahtarla şifrelenen veri yeni anahtar ile yeniden şifrelenir.

6. İLGİLİ DOKÜMAN

- Şifreleme Politikası
- Ağ Güvenliği Politikası
- Ağ Güvenliği Prosedürü