1. AMAÇ

Bu politika, Karamanoğlu Mehmetbey Üniversitesinin imzalamış olduğu "Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) Kullanım Politikası Sözleşmesi" kapsamında, Üniversitemizde bilgisayar ağı ve internet kullanan herkesin uyması gereken ilke ve kuralları tanımlamak üzere hazırlanmıştır.

2. KAPSAM

Bu politika, Karamanoğlu Mehmetbey Üniversitesinin Bilgi İşlem Daire Başkanlığı hizmetlerinden (ağ bağlantısı, internet çıkışı, bilgisayar tahsisi vb.) faydalanan tüm akademik ve idari personel ile birlikte tüm öğrenci ve hizmetlerden yararlananları kapsamaktadır.

3. SORUMLULAR

- Bilişim sistemi kullanıcıları
- Bilgi İşlem Daire Başkanlığı ve Birimleri

4. TANIMLAR

Firewall: Güvenlik duvarı, güvenlik duvarı yazılımı
BGYS: Bilgi Güvenliği Yönetim Sistemi
Router: Yönlendirici
Switch: Dağıtıcı

5. UYGULAMA

Üniversite ağı yalnızca iş amaçlı kullanılır. Üniversite yönetimi gerek gördüğü zaman ağ üzerinde kullanıcıların gerçekleştirdiği işlemlerin ve bu işlemlerin içerdiği bilgilerin incelenmesi hakkını BGYS kapsamında saklı tutar. Üniversite, ağ güvenliğini sağlamak için ağ güvenlik sistemleri ile ilgili prosedürleri uygular. Üniversite tüm kamu verisini, ilgili uygulama sistemlerini ve işletim sistemi yazılımlarını yetkisiz veya yasadışı erişime karşı korumak için yeterli seviyede ağ güvenliği kaynağını (Firewall, IPS/IDS vs.) sağlar.

5.1 Ağ Erişimi

Üniversite ağ ve ağ kaynaklarına erişim yetkisi, personelin görev ve sorumluluklarını yerine getirebilmesi için “gerektiği kadar” yetkiye sahip olması ilkesine göre verilir ve erişim verilmeden önce ilgili yöneticilerden onay alınır. Her bir iş fonksiyonu ve görevi için gerekli olan ağ ve ağ hizmetleri önceden belirlenir ve dokümante edilir.

Kullanıcıların ağ üzerinden bağlantı yetkileri firewall erişim-kontrol listeleri vasıtasıyla kısıtlanır. İş tanımlarının gerektirdiğinden daha fazla ağ hizmeti erişimine, ancak Bilgi İşlem Daire Başkanlığından onay alındığı ve ağ hizmeti şirketin genel güvenlik ilkelerine uygun olduğu takdirde izin verilir.

Sistem yöneticileri (Administrators) işletim sistemini, ağ erişimine izin vermeden önce her bir kullanıcının kimliğini doğrulayacak şekilde yapılandırır. Yapılandırma işlemi sonrası, sistem yöneticisi ilgili işlemi Bilgi İşlem Daire Başkanına rapor olarak sunar.

Uzaktan erişim ancak sınırlı olarak sağlanır ve uzaktan erişime ilgili Şube Müdürünün ve Bilgi İşlem Daire Başkanının onayı alındıktan sonra izin verilir.

Router ve firewall gibi kritik cihazlara erişim yetkisi yalnızca şirket Bilgi İşlem ağına bağlı terminallere verilir. Cihazlar yalnızca yetki onaylı terminallerden yönetilirler.

Kontrol ve konfigürasyon için kullanılan bağlantı noktalarına (port) fiziksel ve mantıksal erişim, sistem yöneticisi tarafından sınırlandırılır ve bilgi güvenliği yöneticisi tarafından kontrol edilir.

Ağ ve ağ hizmetlerini içeriden ya da dışarıdan yapılan tüm erişimler yasal düzenleme gereği kayıt altına alınır. Bu kayıtlar düzenli olarak gözden geçirilir ve yetkisiz bir şekilde ağ hizmetlerinin kullanılmaması ya da ağ hizmetlerine yetkisiz personelin erişmemesi sağlanır. Bilgi Güvenliği yöneticisi, sistem ve ağ yöneticisi ile birlikte düzenli olarak hazırladığı bu kayıtları periyodik olarak hafta da bir Bilgi İşlem Daire Başkanına sunar.

Erişim Kontrolü Politikası'nda tanımlanan hususlar; özel ağ ya da paylaşılan ağlardaki ağ hizmetlerine erişim verilmesi için de geçerlidir.

Ağlar, içerdikleri bilginin kritikliğine göre mantıksal veya fiziksel olarak ayrılır. Ağ mantıksal olarak ayrılmışsa, uygun bölgesel güvenlik cihazları kullanılır. Ağ fiziksel olarak ayrılmışsa, tüm ağ giriş noktalarına fiziksel erişimi korumak için gerekli kontroller bulundurulur.

Tüm ağ donanımı (Router, switch, vs.) ilk şifreleri, yönetici görevine sahip personel tarafından Bilgi İşlem Daire Başkanının onayına istinaden kurulum aşamasında değiştirilir ve bütün bu şifreler özel ve güvenlikli bir yerde saklanır.

Üniversiteye ait bilginin gizliliğini korumak için, şirket ağları kurumla ilgisi olmayan özel ve/veya kişisel bilginin iletimi için kullanılamaz.

Bir uzaktan erişim yazılımıyla doğrudan kişisel bilgisayarlara bağlanmış kişisel haberleşme ekipmanlarının (modem, ISDN kart vb.) kullanımına izin verilmez.

Üçüncü kişilere erişim, bu gereksinimin detaylı bir analizi yapılıp içerdiği riskler değerlendirildikten sonra sağlanır.

5.2 İnternet Hizmeti Yönetimi

İnternet erişimi, iş tanımından ötürü bu erişime gereksinim duyan ve Şube Müdürü tarafından onaylandığı takdirde tüm çalışanlara görevleri kapsamına göre sağlanır.

5.3 Ağ Güvenliği Yönetimi

Tüm ağ donanımları ve haberleşme hatları belirlenir, dokümante edilir ve düzenli olarak güncellenir.

Her seviyede (WAN ve LAN bileşenleri) ağ şemaları oluşturulur ve düzenli olarak fiziksel ve mantıksal topolojiler güncellenir.

Asgari Güvenlik Standartları geliştirilir ve tüm ağ donanımları bu standartlara göre yapılandırılır.

5.4 Veri İletimi

Üniversite ağından üçüncü kişi ağlara veya kamuya açık ağlara iletilen kritik bilgiler şifrelenir. Verinin bütünlüğünün ve gizliliğinin korunması için uygun ve yeterli şifreleme algoritmaları kullanılır.

Şifreleme yazılımına erişim hakkı, ancak gerekli görülen durumlarda Bilgi İşlem Şube Müdürünün ve Bilgi Güvenliği Yöneticisinin onayı alındıktan sonra verilir.

İş ihtiyaçları doğrultusunda gizli bilgi herhangi bir haberleşme ağı üzerinden şifrelenmiş olarak iletilir.

Gerekli görüldüğü durumlarda aktif olarak kullanılmayan gizli bilgiler şifrelenerek saklanır.

Bilgisayarların tamir için dışarıya gönderildiği veya üniversite içi ya da dışında üçüncü kişiler tarafından kullanıldığı ve verinin silinemediği durumlarda, iş ihtiyaçları doğrultusunda verinin yetkisiz ifşasını önlemek için sürücülerdeki tüm veri şifrelenir ya da disk arızası yok ise diski sökülerek tamire gönderilir. Disk arızası olduğu durumda ise, verinin güvenliği açısından diskte kritik bilgilerin olduğu öngörülüyorsa, disk tamir için dışarıya gönderilmeyecek ve yeni disk verilerek kullanıcının varsa yedekleri sistemden dönülerek yeni diske aktarılacaktır, yedekleri yok ise diskin dışarı dan hizmet alınarak içindeki bilgilerin kurtarılması ihtimali varsa diskin gönderileceği tamir servisi ile gizlilik sözleşmesi imzalanması sonrası disk dışarı çıkarılarak gönderilecektir.

Şifreleme seviyesi verinin sınıflandırmasına göre seçilir.

Dosya transferi yapan yazılımlar ile transfer edilecek bilgi kamuya açık değilse, kullanıcının kullanıcı adı ve şifresi doğrulanır .

5.5 Ağ Değerlendirmesi

Ağ zayıflıkları uzman personel ya da Üniversitenin anlaştığı Teknik Danışman/Şirket tarafından sürekli olarak ölçülür. Belirlenen riskler değerlendirme raporunda dokümante edilir. Düzenli olarak Bilgi Güvenliği Yönlendirme Kurulu'na (Güvenlik Kurulu'na) değerlendirme raporu iletilir. Her yıl üçüncü kişi bağımsız denetleyicilerle ağ değerlendirmesi gerçekleştirilir. Bu şekilde yönetime, müşterilere ve ağ hizmetlerinden yararlanan ilgili taraflara güvence sağlanır.

5.6 Taşınabilir Cihazlarda Saklanan Verilerin Güvenliği

Dizüstü bilgisayar, gibi taşınabilir cihazlar, üniversite bilgilerini üniversite dışına taşıma imkânı sağladıklarından, bilgi sistemleri için önemli açıklar içerebilmektedir. Bu nedenle dizüstü bilgisayar, akıllı cep telefonları, tablet bilgisayar (ör: iPad) gibi taşınabilir cihazların kullanımının getirdiği risklere karşı dikkatli olunması esastır.

Taşınabilir cihazların güvenliğinde, söz konusu cihazların kullanımında aşağıda belirtilen hususlara dikkat edilir:

- Taşınabilir cihaza erişim için mutlaka tahmin edilmesi zor bir PIN ya da parola oluşturulur ve cihazın kullanılmadığı zamanlarda otomatik olarak devreye girmesi sağlanır.

- Kullanıcı, cihaz kaybı yaşanması durumunda, veri kaybına uğranmaması amacıyla taşınabilir cihazın düzenli olarak verilerinin yedeklenmesi işlemini Yardım Masası ile irtibata geçerek sağlar.
- Taşınabilir cihaz üzerinde (varsa) kurulu olan anti virüs programları devre dışı bırakılamayacak şekilde yapılandırılır.
- Taşınabilir cihazlara indirilen (download) uygulamalar ya da dosyalar indirilmeden önce indirilen program/dosya kaynaklarının güvenilirliğinden emin olunur.
- Cihazların çalınma riskine karşı kullanıcıların özellikle halka açık mekanlarda cihazlarını gözetimsiz bırakmamaları ve cihazların fiziksel güvenliğini sağlamaları esastır.
- Kullanıcılar kendilerine tahsis edilen dizüstü bilgisayarları kullanmadıkları durumlarda da güvence altına alır.
- Uçak, otobüs ve benzeri halka açık ulaşım araçlarında taşınabilir cihazlar baş üstü bagajlarına değil koltuk altına konulmalıdır. Taşınabilir cihazlar, havaalanı, tren ya da otobüs terminallerinde güvenlik kontrollerinden geçilirken sürekli olarak izlenir ve göz teması kesilmez.
- Taşınabilir cihazlar intranete uzaktan erişim amacıyla kullanılıyorsa erişim için kullanılan kullanıcı adı ve parola bilgileri bilgisayar üzerinde herhangi bir dosya içinde saklanamaz.
- Taşınabilir cihazlara disk şifreleme için, kullanıcılar bitlocker şifresi koymalıdır.

Taşınabilir cihazların yasa dışı, başkalarını rahatsız edici, prosedür ve rehberlerine/kılavuzlarına aykırı ya da üniversiteye zarar verecek herhangi bir şekilde kullanılmaması esastır. Üniversite, bu cihazları ve bu cihazlarla gerçekleştirilen aktiviteleri izleme, kaydetme ve düzenli olarak denetleme hakkını saklı tutar.

6. İLGİLİ DOKÜMAN

- Ağ Güvenliği Prosedürü
- Şifreleme Politikası
- Şifreleme Prosedürü
- Kabul Edilebilir Kullanım Politikası