ODTÜ Yerleşke Ağında
Bilişim Servisleri İşletim İlkeleri

1. Amaç

Bu belge, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler (ODTÜ bünyesinde faaliyet gösteren akademik ve idari tüzel kişilikler) tarafından verilen bilişim servislerinin işletim ilkelerini belirlemek amacıyla hazırlanmıştır.

2. Kısaltma ve Tanımlar

BİDB : Bilgi İşlem Daire Başkanlığı

DNS : Domain Name System / Alan Adı Sistemi

TCP/IP : Transmission Control Protocol / Internet Protokol.

IP adresi : Internet Protokol adresi. ODTÜ yerleşke alan ağına bağlı her bilgisayar 144.122.X.X formatındaki IP adresi. ODTÜ yerleşke alan ağında iletişim IP ile sağlanır.

MAC adresi : Media Access Control. Bilgisayarın ağ erişim kartı üzerinde bulunan ve üretici firma tarafından belirlenen karta özel tanımlama bilgisi.

DHCP : Dynamic Host Configuration Protocol. Ağa bağlı bilgisayarların IP ve diğer gerekli bilgileri bir sunucudan alarak ağa erişmelerini sağlayan protokol.

Kapı (port) : İşletim sistemi ve yazılımların kendi içinde ve diğer bilgisayarlarda çalışan işletim sistemi ve yazılımlarla ağ üzerinde iletişim kurabilmesi için tanımlanan sanal çıkış yollarıdır.

Yama (patch) : İşletim sistemi ve yazılımlarda tespit edilen problemlerin giderilmesi ya da mevcut özelliklere yenilerinin eklenebilmesi için üreticiler tarafından geliştirilen yazılımlar.

Sunucu sistem : Sunucu bilgisayar üzerinde çalışan işletim sistemi ve yazılımlar.

Güvenlik tehditleri : Ağa bağlı bilgisayarların güvenlik açıklarından yararlanarak yayılan, bilgilere izinsiz erişim sağlayarak kişisel/kurumsal bilgi güvenliğini ve ağ erişimini tehdit eden yöntemler (virüs, truva atı vb.).

Servis : Son kullanıcılara yönelik bilişim servisleri (örneğin e-posta servisi, Web

servisi vb.)

Bilgisayar Koordinatörü:. Bilişim altyapısı ile ilgili konularda birimlerin BİDB ile iletişimini sağlayan, birimlerin bilişim altyapısından sorumlu kişi(ler).

Servis Sorumlusu : Birimde sunucu sistemin işletiminden sorumlu personel.

Veri Trafiği : Yerleşke alan ağı üzerinde akan veri.

3. Kapsam

Bu belge, ODTÜ yerleşkesinde yerleşke alan ağına bağlı bilgisayarlarda sunucu olarak çalışan sistemlerin kurulumu ve güvenliğinin sağlanması (güvenlik ayarları) ile ilgili bilgileri ve ilkeleri içermektedir. Kurulum ve ayarların bu belgede belirtilenlere göre yapılması, yerleşke alan ağının sağlıklı işletilebilmesi ve ağa bağlı bilgisayarlar üzerindeki kurumsal/kişisel bilgilerin güvenliğinin sağlanabilmesi açısından önem taşımaktadır. Birimler, verdikleri servislerde Bilişim Kaynakları Kullanım Politikaları belgesinde (http://bilisim-etigi.metu.edu.tr/)http://bilisim-etigi.odtu.edu.tr/ belirtilen ilkelere uymakla yükümlüdür.

4. Politika

1. Birimler kendi bünyelerinde bilişim servisleri sunmaya karar vermeden önce, BİDB tarafından merkezi olarak sunulan olanakları değerlendirmeli (http://www.bidb.odtu.edu.tr), öncelikli olarak BİDB tarafından sunulan servislerin kullanılması tercih edilmelidir.

2. Birimler, BİDB'nin merkezi olarak sunduğu servislere ek olarak, bu belgede belirtilen genel ilkeler ve servise özel belgelerde yer alan özel ilkeler çerçevesinde servis verebilirler.

3. Birimler, BİDB'nin hazırlayıp duyurduğu servis işletim yönergelerine uygun şekilde servis vermekle yükümlüdür.

4. Birimler, **Bilgisayar Koordinatörlerini** BİDB'ye yazılı olarak bildirmek ve bu bilgiyi güncel tutmakla yükümlüdür. Birimler, verdikleri servislerin ve bu servislerden sorumlu kişilerin (**Servis Sorumlusu**) bilgilerini, Bilgisayar Koordinatörlerine bildirmelidir.

5. Birimler, sunucular üzerinde çalışan işletim sistemlerinde ve sunucu yazılımlarında bilgi güvenliğini sağlamak için gerekli önlemleri almakla yükümlüdür.

6. Birimler, sundukları servislerde ODTÜ Bilişim Kaynakları Kullanım Politikaları belgesinde (http://bilisim-etigi.metu.edu.tr/)http://bilisim-etigi.odtu.edu.tr/ belirtilen ilkelere uygun ve bu ilkelerle çelişmeyecek biçimde, servis standartlarını belirlemek, kullanıcıların uyması gereken kuralları belgelendirmek ve bu kuralları kullanıcılarına duyurmak zorundadır.

7. Birimler, sundukları servislerden kaynaklı veri trafiğinin yerleşke alan ağı üzerindeki veri akışında aksaklık yaratmayacak boyutta tutulması için gerekli önlemleri almakla yükümlüdür.

8. Birimlerde, Servis Sorumlusu'nun bilgisi ve/veya onayı dışında, sunuculara müdahale edilmemeli, sunucuların fiziksel güvenliği sağlanmalıdır.

5. Genel İlkeler

Birimler, sundukları bilişim servislerinde aşağıdaki ilkelere uymakla yükümlüdürler.

1. **Güvenilir işletim sistemleri ve yazılımlar kullanılmalıdır :** Sunucu bilgisayarın işletim sisteminin ve üzerinde çalışan yazılımların, teknik desteği üretici ve sağlayıcıları tarafından verilmeye devam edilen, güvenlik açıkları zamanında duyurulan ve kapatılan, bu nedenle virüs, truva atı vb. güvenlik tehditlerinden göreceli olarak daha az etkilenen bir işletim sistemi olması gereklidir. Bu konuda, açık kaynak kodlu işletim sistemlerinin, kapalı kaynak kodlu işletim sistemlerine göre daha avantajlı olduğu bilinmektedir.

2. **İşletim sistemi ve yazılımlar güncel tutulmalıdır :** Sunucu bilgisayarda kullanılan işletim sistemi ve yazılımlar güncel tutulmalı, duyurusu yapılmış olan yamalar vakit kaybetmeden sisteme uygulanmalıdır (duyuruların izlenebilmesi için, ilgili duyuru listeleri takip edilmelidir).

3. **Erişim güvenliği sağlanmalıdır :** Sunucu bilgisayara güvenlik nedeniyle belirli yerlerden erişimin sağlanmasının gerekli olduğu durumda, erişimin yapılacağı IP adresleri ve/veya kullanıcılar tanımlanmalı ve erişim izni verilmelidir. Bunun yanında, erişim güvenli yollarla yapılmalı (terminal erişimi için telnet yerine ssh, e-posta okuma servisi için imap/pop yerine imaps/pops, dosya transferi için ftp yerine sftp vb.), erişim hakları düzenlenerek kullanıcıların sadece yetkilendirilmiş bilgilere erişimi sağlanmalı ve erişim izni düzenlemesi için güvenlik düzeyini yükselten programlar kullanılmalıdır (güvenlik duvarı, TCP wrapper vb.).

4. **Kullanılmayan servisler kapatılmalıdır :** Sunucu bilgisayar üzerindeki

kullanılmayan gereksiz servisler, olası güvenlik açıkları nedeniyle kapatılmalıdır.

5. **Geri bildirim yapılabilir sunucu yazılımları seçilmelidir :** Sunucu yazılımının seçimi yapılırken, yazılımın kullanıcı sorunlarının iletilebildiği yazışma listelerinin olmasına önem verilmelidir.

6. **Yedekleme politikası belirlenmelidir :** Kullanıcılara ve servise ait bilgilerin tutulduğu disk alanlarının periyodik olarak yedeklenmesi konusunda politika belirlenmeli, kullanıcılar olası riskler konusunda bilgilendirilmelidir.

7. **Kullanıcı yetkilendirme yöntemleri belirlenmelidir :** Kullanıcıların sunucu sistemler üzerinde çalışan servislere erişimlerini sağlayan mekanizmalar (parolalı erişim, IP tabanlı erişim, sertifika tabanlı erişim, akıllı kart erişimi vb.) ve bunlara ilişkin kurallar belirlenmelidir. Merkezi kullanıcı kodları ile yetkilendirme sağlanması gereken servislerde BİDB tarafından belirlenen yetkilendirme yöntemi standardına (LDAPS vb.) uyulmalıdır.

8. **Sunucu yazılımlar, verilecek servise uygun uluslararası standartlarda çalıştırılmalıdır :** Servisler, IANA (Internet Assigned Numbers Authority) TCP/IP kapı (port) numarası tahsislerine uygun olarak 1024 ve altındaki kapılarda çalıştırılmalıdır (http://www.iana.org/assignments/port-numbers).

9. **Kurulum ve işletim dokümanları okunmalı ve belgelendirme yapılmalıdır:** Kurulum ve uyarlama (customization) işleminden önce, yazılımla birlikte gelen tüm dokümanlar okunmalı, kurulum ve uyarlama işlemi belgelendirilmeli ve farklı ortamlarda arşivlenmelidir. Bu çalışma sistemi, olası bir sorunda servislerin hızlı bir biçimde kullanıma hazır hale getirilebilmesi için gereklidir.

10. **Sunucularda kayıt (log) tutulmalı, arşivlenmelidir :** Sunucu bilgisayar üzerinde verilen servislere ilişkin kayıtlar (log) yasal mevzuata uygun şekilde tutulmalı ve arşivlenmelidir.

6. Uygulama ve Yaptırımlar

Birimler servisleri bu belgede belirtilen ilkeler çerçevesinde sunmakla yükümlüdür. Bu ilkelere uyulmadığı durumlarda BİDB, yerleşke ağının sağlıklı işletiminin sağlanabilmesi amacıyla Bilgisayar Koordinatörü'nün ve/veya Servis Sorumlusu'nun uyarılmasından, servis erişiminin haberli ya da güvenlikle ilgili acil durumlarda önceden haber verilmeden, geçici ya da kalıcı olarak kısıtlanmasına kadar koşulların gerektirdiği önlemleri alabilir.

Bu belge yayınlandığı tarihten itibaren geçerlidir. Gerekli görüldüğü durumlarda ODTÜ yetkili makamlarınca, metin üzerinde değişiklik yapılabilir. Bu nedenle kullanıcıların "http://servis-ilkeleri.odtu.edu.tr" adresinde yer alan güncel metinleri takip etmeleri önem taşımaktadır.

EKLER :

Ek-1 : Servise Özel İlkeler

1. E-Posta Servisi İşletim İlkeleri
2. Web Servisi İşletim İlkeleri
3. FTP Servisi İşletim İlkeleri
4. Veri Tabanı Servisi İşletim İlkeleri
5. DNS Servisi İşletim İlkeleri
6. DHCP Servisi İşletim İlkeleri
7. PC Salon İşletim İlkeleri

Ek-2 : Kullanıcı Bilgisayarları İşletim Sistemi Kurulum İlkeleri

Ek-3 : Parola Politikası

E-posta Servisi İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen e-posta servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır.

BİDB, ODTÜ'deki kişisel ve kurumsal kullanıcılar için merkezi e-posta servisi sağlamaktadır. E-posta servisinden merkezi olarak yararlanmak yerine kullanıcılarına daha fazla disk alanı sunmak isteyen ya da kendi alan adları ile e-posta servisi vermek isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak, BİDB tarafından sunulan merkezi e-posta servisine alternatif e-posta servisi sunmak isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir.

1. **SPAM'e karşı önlem alınmalıdır :** E-posta sunucusunun SPAM kaynağı olarak kullanılması engellenmelidir. Sunucunun SPAM aracı olarak kullanılmasını ve sunucu üzerinden yetkisiz e-posta gönderilmesini önlemek amacıyla, sunucu altyapısında gerekli düzenlemeler yapılmalı, e-posta sunucusu "open relay" olarak kullandırılmamalıdır. Bunun yanında, e-posta sunucusuna gelen SPAM mesajların engellenebilmesi amacıyla kullanılan SPAM filtreleme yazılımlarının SPAM olmayan mesajları da elemesi engellenmeli, filtreleyici yazılımların konfigürasyonları bu çerçevede düzenlenmelidir.

2. **E-posta yolu ile yayılan virüsler engellenmelidir :** E-posta yolu ile yayılan virüslerin engellenebilmesi amacıyla virüs filtreleme yazılımları kullanılmalı ve güncel tutulmalıdır. Bu yazılımlar ile hem sunucudan dışarıya giden hem sunucuya gelen virüslü e-postalar filtrelenmelidir.

Web Servisleri İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen web servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır.

Web servisinden merkezi olarak yararlanmak yerine yerel ağları üzerinde kendi imkanları dahilinde web servisi sunmak isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak, BİDB tarafından sunulan merkezi web servisine alternatif web servisi sunmak isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir:

1. **Güvenilir programlama dili derleyicileri ve yorumlayıcıları seçilmelidir:** Web sunucuları üzerinde, programlama dili derleyicileri ve yorumlayıcılarının, görece daha az güvenlik açığı bulunanları seçilmelidir. Kullanılan derleyici ve yorumlayıcıların kararlı en son sürümünün kullanılması, olası güvenlik açıklarının takip edilmesi ve herhangi bir açık belirlendiği takdirde, gerekli önlemlerin derhal alınıp düzeltme yapılması büyük önem taşımaktadır.

2. **Güvenilir web sunucu yazılımları seçilmelidir :** Web sunucu yazılımları olarak görece daha az güvenlik açığı bulunan yazılımlar seçilmelidir. Kullanılan web sunucu yazılımlarının kararlı en son sürümünün kullanılması, olası güvenlik açıklarının takip edilmesi ve herhangi bir açık belirlendiği takdirde, gerekli önlemlerin alınıp düzeltme yapılması büyük önem taşımaktadır.

FTP Servisi İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen FTP servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır

BİDB, ODTÜ'deki kişisel ve kurumsal kullanıcılar için iki tür merkezi FTP servisi sağlamaktadır.

1. **Anonim FTP servisi (ftp.metu.edu.tr) :** Anonim FTP servisi tüm Internet dünyasına açık olup kullanıcıların ihtiyacı olabilecek masaüstü uygulamaları ve bazı popüler FTP sitelerinin yansılarını barındırmaktadır.

2. **Lisanslı yazılımlar FTP servisi (ftp.cc.metu.edu.tr) :** Lisanslı yazılım FTP servisi sadece yerleşke içinde bulunan personele açık olup yerleşke lisanslı yazılımlara bu servis üzerinden erişilebilmektedir.

Merkezi FTP servisinden yararlanmak yerine yerel ağları üzerinde kendi imkanları dahilinde FTP servisi sunmak isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak, BİDB tarafından sunulan merkezi FTP servisine alternatif FTP servisi sunmak isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir.

1. **Uygun transfer modu kullanılmalıdır :** Olası güvenlik tehditlerini engelleyebilmek amacıyla aktif iletim modu yerine pasif iletim modu (passive transfer mode) kullanılmalıdır.

2. **Erişim haklarının kısıtlanması :** FTP servisine erişen kullanıcıların, dosyaların sunulduğu dizin dışına erişim hakkı kısıtlanmalıdır.

3. **Anonim olmayan FTP servisleri :** Lisanslı yazılım bulunduran, anonim olmaması gereken FTP servislerinde, kullanıcı yetkilendirmesinin şifre/parola ikilisi ile yapılması, yazılım dağıtımının lisans anlaşmaları çerçevesinde yapılmasının sağlanması gerekmektedir. Veri transfer protokolü olarak standart FTP yerine SFTP veya FTPS kullanılması önerilmektedir.

Veri Tabanı Servisi İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen veri tabanı servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır

Yerel ağları üzerinde kendi imkanları dahilinde veri tabanı servisi sunmak isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak, veri tabanı servisi sunmak isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir.

1. **Kullanıcı erişimleri düzenlenmelidir :** Veri tabanına erişim hakkı, Servis Sorumlusu tarafından sadece veri tabanına erişmesi gereken kullanıcılara verilmeli, yetkisiz kullanıcıların veri tabanına erişimi engellenmelidir.

2. **Kullanıcılar yetki düzeylerine göre sınıflandırılmalıdır :** Her veri tabanı kullanıcısına gereksinim duyduğu işlemleri yapmasını sağlayacak en alt düzeyde erişim hakkı verilmelidir. Aynı sunucu sistem üzerinde çalışan farklı veritabanları için farklı kullanıcı ve yönetici grupları oluşturulmalıdır. Örneğin, sadece okuma hakkı olması gereken kullanıcıya sadece okuma hakkı verilmeli, yazma ve değiştirme hakkı verilmemeli; X veri tabanında üst düzeyde yetki sahibi olan kullanıcılar, eğer gerekmiyorsa Y veri tabanında aynı yetkilere sahip olmamalıdır.

3. **Veri tabanı yönetim sisteminde öntanımlı kullanıcılar kapatılmalıdır :** Veri tabanı kurulumu sırasında üretici firma tarafından tanımlanan parolasız ya da zayıf parolalı ön tanımlı kullanıcıların devre dışı bırakılması gerekmektedir.

4. **Veritabanlarında veri boyutu kotası tanımlanmalıdır :** Öngörülenin üzerinde disk alanı kullanımını önlemek ve olası servis aksamalarını önlemek amacıyla veritabanlarında kota uygulaması kullanılmalıdır.

5. **Veri tabanına erişecek web tabanlı uygulamalarda erişim denetimi yapılmalıdır** : Veri tabanına erişim hakkı verilen web tabanlı uygulamaların erişiminin IP, kullanıcı kodu ve parola bilgilerinin doğruluğu kontrol edilerek sağlanmalı, erişim kayıtları tutulmalıdır.

6. **Veri/şifre güvenliği için, veri tabanı erişimlerinin farklı sunucular üzerinde olması durumunda iletişim güvenli kanallardan yapılmalıdır :**

Veri/şifre güvenliği için, veri tabanı erişimlerinin farklı sunucular üzerinde olması durumunda ilgili makinalara erişim SSH ile sağlanmalı ve veri tabanı işlemleri için "SSL-tunelling" yapılmalıdır.

DNS Servisi İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen DNS servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır

BİDB, merkezi DNS servisi sağlamaktadır. Bu nedenle, birimlerde DNS servisi sunulmasına gerek bulunmamaktadır. Bununla birlikte yerel ağları üzerinde kendi imkanları dahilinde DNS servisi sunmak isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak, BİDB tarafından sunulan merkezi DNS servisine ek olarak yerel DNS servisi sunmak isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir.

1. **Zone Transfer özelliği devre dışı bırakılmalıdır :** İkincil DNS sunucusu kullanılmıyor ise, güvenlik açıklarına neden olabileceği için, DNS sunucusunun barındırdığı Alan Adı - IP eşleme bilgilerinin tümünün başka bir istemci bilgisayara topluca iletilmesini sağlayan Zone Transfer özelliği devre dışı bırakılmalıdır.

2. **Dinamik DNS özelliği devre dışı bırakılmalıdır :** Güvenlik açıklarına neden olabileceği için istemci bilgisayarların kendilerini DNS sunucusuna otomatik olarak kaydetmesini sağlayan Dinamik DNS özelliği devre dışı bırakılmalıdır.

3. **Recursive (özyineli) alan adı sorguları engellenmelidir :** Birim dışındaki istemci bilgisayarlardan alınan alan adı sorguları DNS sunucusu tarafından recursive (özyineli) olarak işlenmemeli, bu özellik devre dışı bırakılmalıdır.

4. **Ayrılmış IP aralıklarından gelen sorgular dikkate alınmamalıdır :** Internet dünyasında özel amaçlar için ayrılmış olan IP aralıklarından (10.0.0.0/8, 192.168.0.0/16, 172.16.0.0-172.31.255.255) gelen alan adı sorguları dikkate alınmamalıdır. Bu tür sorgular genel sistem güvenliğini tehdit edici nitelik taşıyabilmektedir.

DHCP Servisi İşletim İlkeleri

Bu belge, ODTÜ merkezi sunucuları dışında, ODTÜ yerleşke alan ağına bağlı sunucu bilgisayarlar üzerinde birimler tarafından verilen DHCP servisi işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır

Birim yerel ağı üzerindeki IP dağıtımlarının, sistem güvenliği ve takip kolaylığı açısından statik olarak yapılması önerilmektedir. Bununla birlikte DHCP servisi kullanan birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak**, IP-MAC-kullanıcı eşleştirmeleri yapılmalı ve eşleştirme kayıtları yasal mevzuata uygun şekilde tutulmalıdır** (DHCP sunucusu üzerinde IP–MAC-kullanıcı eşleştirmeleri tanımlanmalı, bilgisayarların ağa kendisine atanmış olan IP numarası ile erişmesi sağlanmalıdır).

PC Salonu İşletim İlkeleri

Bu belge, BİDB dışında, birimler tarafından sunulan kamusal PC salonlarının işletim ilkelerini, Servis İşletim İlkeleri belgesinde belirlenen politika ve genel ilkelere ek olacak şekilde sunmaktadır

BİDB, sorumluluğunda servise sunulmakta olan PC salonlarının merkezi teknik ve idari işletimini sağlamaktadır. Kendi imkanları dahilinde PC salonu işletmek isteyen birimler, öncelikle gerekli donanım ve yazılım kurulumu konusunda belirlenmiş ilkeleri inceleyip uygulamakla yükümlüdür (Bkz. Servis İşletim İlkeleri -> Genel İlkeler).

Bu ilkelere ek olarak PC salonu işletmek isteyen birimlerin uyması gereken ilkeler aşağıda maddelenmiştir.

1. **PC salon işletim ve kullanım kuralları belirlenmelidir :** Birimler, işlettikleri PC salonlarının işletim ve kullanım kurallarını hazırlamakla yükümlüdürler.

2. **PC salonunda kullanılan işletim sistemi ve yazılımların güvenliği sağlanmalıdır :** PC salonundaki bilgisayarlarda kullanılan işletim sistemleri güvenlik açıkları bulunmayacak şekilde yapılandırılmalı, virüs vb. güvenlik tehditlerine karşı gerekli önlemler alınmalı ve gerekli güvenlik güncellemeleri mümkünse otomatik hale getirilmelidir. Otomatik güncellemelerden kaynaklanabilecek sorunlar kullanıcılara bildirilmeli, gerekli görülen durumlarda güncellemeler devre dışı bırakılmalıdır.

3. **PC salonuna giriş/çıkış yapan kullanıcıların kaydı tutulmalıdır :** PC salonunda bulunan bilgisayarlara giriş/çıkış yapan kullanıcıların kaydının (hangi zaman aralığında hangi bilgisayarı kullandığı bilgisinin) birim tarafından (belirlenecek süre içinde geri dönülebilecek şekilde) tutulması gerekmektedir.

4. **PC salonlarında kurulan yazılımların lisans kuralları ihlal edilmemelidir :** PC salonlarındaki bilgisayarlarda kullanılan yazılımların, ilgili yazılımın lisans kuralları çerçevesinde kurulması ve kullanılması sağlanmalıdır.

Kullanıcı Bilgisayarları* İşletim Sistemleri Kurulum İlkeleri

1. Amaç

Bu belge, ODTÜ yerleşkesinde ağ omurgasına bağlı kullanıcı bilgisayarlarına işletim sistemi kurulum ilkelerini belirlemek amacıyla hazırlanmıştır.

2. Kapsam

Bu belge, ODTÜ yerleşkesinde ağ omurgasına bağlı olarak çalışan kullanıcı bilgisayarların işletim sistemlerinin kurulumu ve güvenliğinin sağlanması (güvenlik ayarları) ile ilgili bilgileri ve önerileri içermektedir. Kurulum ve ayarların bu belgede önerilenlere göre yapılması, gerek kişisel ve kurumsal bilgilerin güvenliğinin sağlanması, gerekse yerleşke ağ omurgasının sağlıklı işletilebilmesi açısından önem taşımaktadır. Kullanıcılar, Bilişim Kaynakları Kullanım Politikaları belgesinde (http://bilisim-etigi.metu.edu.tr/) belirtilen ilkelere uymakla yükümlüdür.

3. Politika

1. Kullanıcılar, bilgisayarlarında aşağıdaki ilkelere uymak koşuluyla yerleşke lisansı, kişisel/birim lisansı bulunan ya da serbest yazılım lisansı bulunan (GNU/Linux, FreeBSD vb.) işletim sistemlerini, yazılımları kurabilir ve kullanabilirler.

2. İşletim sistemi kurulumu öncelikli olarak, eğer sağlanıyor ise BİDB Kütüphanesi'nden temin edilen güncel işletim sistemi kurulum medyalarından (CD/DVD ve benzeri) yapılmalıdır. Ancak güvenliğini sağlamak koşulu ile, alternatif işletim sistemi kurulumu yapılabilir.

3. Kullanıcıların, işletim sistemini kurarken ve güvenlik ayarlarını yaparken birim koordinatörlerinden destek almaları önerilir.

4. Genel İlkeler

1. **İşletim sistemi güncel tutulmalıdır :** İşletim sisteminin ve işletim sistemi üzerinde çalışan yazılımların güvenlik tehditlerine karşı korunabilmesi için güncel tutulması gerekmektedir. İşletim sistemi güncellemelerinin otomatik olarak gerçekleştirilebilmesi için gerekli ayarlar yapılmalıdır. Otomatik

* Kişisel masaüstü, dizüstü veya avuç içi bilgisayarlar vb.

güncellemelerden kaynaklanabilecek sorunlar kullanıcılara bildirilmeli, gerekli durumlarda ilgili güncelleme devre dışı bırakılmalıdır.

2. **Güvenli dosya sistemi kullanılmalıdır :** İşletim sistemi kurulumu sırasında sunulan dosya sistemi seçenekleri arasında kullanıcıların erişim haklarının düzenlenmesi vb. imkanların sağlandığı güvenli dosya sistemi seçilmelidir (örneğin FAT32 ya da FAT yerine NTFS ya da EXT2 gibi).

3. **Kullanıcı hesap parolaları kullanılmalıdır :** İşletim sistemi tek bir kullanıcı tarafından kullanılsa bile işletim sistemine parolasız giriş engellenmeli, kullanıcıların işletim sistemine kullanıcı hesap ve parolaları ile bağlanması sağlanmalıdır. Parolalı erişim, ağa bağlı bilgisayarlardaki verilerin korunması açısından önem taşımaktadır. Kullanıcı hesap parolalarının basit olmaması, rakam, harf ve özel karakterlerden oluşması gerekmektedir (Bkz. http://kullanicikodu.bidb.odtu.edu.tr → Kullanıcı Kodu Şifresi (Parola) Seçiminde Dikkat Edilmesi Gereken Noktalar).

4. **Antivirüs yazılımları kurulmalıdır :** Virüslerin, bilgisayarları etkilemesine karşı alınacak en etkili önlem antivirüs yazılımının kurulması ve güncellenmesidir. Tanımlarına sahip olduğu virüsleri fark edebildiği için antivirüs yazılımının güncellemesini yapmak, yazılımı kurmak kadar önemlidir. ODTÜ yerleşkesinde lisanslı olarak kullanılabilecek antivirüs yazılımları hakkındaki bilgilere ODTÜ Antivirüs web sitesinden (http://antivirus.metu.edu.tr/) ulaşılabilmektedir.

5. **Kullanılması gerekli olmayan servisler kapatılmalıdır :** Güvenlik açıklarının çoğu, işletim sistemi üzerinde denetimsiz şekilde çalışan servislerden ve bu servislerin açmış olduğu kapılardan (portlardan) kaynaklanmaktadır. Bu nedenle, kullanılması gerekli olmayan servislerin kapatılması gerekmektedir.

6. **Depolama ünitesindeki bilgilerin yedeklenmesi :** Depolama ünitesindeki kritik bilgilerin, kullanıcı dosyalarının düzenli olarak yedeklenmesi, kullanıcıların bilgi kaybına uğramasını engelleyecektir. Yedekleme ortamı işletim sisteminin bulunduğu depolama ünitesi üzerinde bulunmamalıdır.

Parola Politikası

Birimler tarafından verilen servislere (sunucu ve kullanıcı bilgisayarlarının işletim sistemleri erişimi, veri tabanı erişimleri, web servisi erişimleri vb.) kullanıcı hesabı ve parola ikilileri ile yapılan yetkilendirmelerde dikkat edilmesi gerekenler aşağıda maddelenmiştir.

1. **Saklanan parolaların güvenliği sağlanmalıdır :** Sunucular üzerinde saklanan parolaların güvenliğinin sağlanması amacıyla gerekli önlemler alınmalıdır (parolaların düz metin olarak saklanmaması, şifrelenmesi için gerekli yapılandırmaların yapılması gibi).

2. **Parolalar zayıflığa karşı kontrol edilmelidir :** Kullanıcı hesabı/parola tanımlaması ya da parola değişikliklerinde zayıf parolaların tanımlanmasına izin verilmemeli, bu amaçla gerekli kurallar belirlenmelidir. Örneğin, parola, 6 karakterden az olmamalı, içinde büyük harf, küçük harf, sayı ve özel karakterden gruplarından en az üçünü içermeli ve sözlükte bulunan kelimeler arasından seçilmemelidir (Bkz. http://kullanicikodu.bidb.odtu.edu.tr → Kullanıcı Kodu Şifresi (Parola) Seçiminde Dikkat Edilmesi Gereken Noktalar).

3. **Parolanın güncelliği sağlanmalıdır :** Servisin kritiklik düzeyine göre parolanın belirli aralıklarla değiştirilmesi sağlanmalıdır.