1. AMAÇ

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılan iletişim ve operasyon kurallarının oluşturulması amaçlanmıştır.

2. KAPSAM

Bu prosedür, Karamanoğlu Mehmetbey Üniversitesi Bilgi İşlem Daire Başkanlığı bünyesinde yapılan iletişim ve operasyonları kapsar.

3. SORUMLULAR

- Bilgi İşlem Daire Başkanlığı
- Bilişim Kullanıcıları

4. TANIMLAR

Operasyon; İşlem
Administrator; Yönetici
NTP (Network Time Protocol); Ağ zamanlama protokolü
Majör değişiklik; Köklü değişiklik
Minör değişiklik; Çok fazla farklılık yaratmayan değişiklik
back-up; Yedek

5. UYGULAMA

5.1 Operasyonel Prosedürler ve Sorumluluklar

5.1.1 Doküman Haline Getirilmiş Operasyonel Prosedürler

Operasyonel prosedürler, yedekleme, ekipman bakımı, medya ve bilgi işleme, bilgisayar odası, e-posta işleme yönetimi ve güvenlik denetim izleri kontrolü gibi bilgi işlem ve iletişim olanakları ile ilgili sistemsel aktiviteler için hazırlanır.

Operasyonel prosedürlerde görevler ayrılığı ilkesine dikkat edilir.

Operasyonel prosedürler bütün çalışanlara duyurulur ve herkesin erişebildiği ortamlarda tutulur.

Operasyonel prosedürler ve dokümante edilmiş prosedürler resmi doküman olarak görülür ve Bilgi İşlem Yöneticisi tarafından onaylanır.

Bilgi İşlem Yöneticisi; Operasyonel prosedürlerden sorumludur ve bu dokümanların güncel tutulmasını sağlar.

5.2 Operasyonel Değişiklik Yönetimi Prosedürü

5.2.1 Kullanıcı Talebi ve Onayı

Yeni uygulama projeleri veya kapasite artırılması çalışması esnasında bilgi kaynaklarında değişiklik yapma gereksinimi oluşabilir (yeni bir sunucu ve ağ ekipmanlarının kurulması, hafıza artırımı, işletim sistemi güncellemeleri).

Değişiklik gereksiniminde, Kurum talebi üzerinden yapılır. Talep incelenerek, talebin üçüncü parti bir firma veya Kurum tarafından çözülmesine karar verilir. Değişiklik ile ilgili detaylar Kurum Bilgi İşlem Şube Müdürü ile paylaşılarak onay alınır.

Kurum ilgili Bilgi İşlem bölümü çalışanı aşağıdaki kriterlere göre değişikliğin minör ya da majör olduğuna karar verir.

Majör değişiklik: LAN/WAN ekipmanlarındaki ve sunuculardaki kritik donanım değişiklikleri, işletim sistemi değişikleri, veritabanı ve destekleyici uygulamalardaki değişikliklerdir. Kesinti gerektirebilir.

Minör değişiklik: LAN/WAN ekipmanlarındaki, sunucuların ve kişisel bilgisayarlardaki kritik olmayan donanım değişiklikleridir.

Majör ya da minör değişiklikler "Acil Değişiklik" olarak açılabilir. Bu durumlarda Bilgi İşlem Yöneticisinin sözlü ya da yazılı onayı ile bu işlem gerçekleştirilir. Süreç en fazla 1 hafta içerisinde kendi doğal akışı ile sonuçlandırılır, değişiklikle ilgili detay bilgiler ve gerekli onaylar kayıt altına alınır.

İlgili Bilgi İşlem Yöneticisi, yapılacak olan değişikliğin, donanımlarda ve sistemlerde bir değişiklik olup/olmayacağını veya olacaksa da ne gibi değişiklikler getireceğine ilişkin etki analizi yapar ve yapılacak değişikliğin, bu çıkan sonuca göre maliyet değişikleri üzerindeki etkisini analiz eder. Minör bir değişiklik olduğuna kanaat getirirse onaylar, majör bir değişiklik olduğuna karar vermesi durumunda onay için bir üst seviyeye yönlendirir. Bilgi İşlem Yöneticisi, etki analizi ile ilgili raporu, Bilgi Güvenliği Yöneticisinden veya Sistem Ağ Yönetmeninden hazırlanmasını da talep eder.

Değişiklik bütçe limitleri dâhilinde ise Bilgi İşlem Yöneticisi değişikliği onaylar. Değişikliğin bütçe limitlerini aşması durumunda ise değişiklik daha üst düzey bir yönetici onayına sunulur.

5.2.2 Test ve Uygulanma

Sistem yöneticileri ve ağ yöneticileri teknoloji varlıklarının kurulum ve testlerini yapar. Sistem yöneticileri ve ağ yöneticileri değişikliklerin testlerinin planlarını hazırlar. Bilgi kaynakları üzerindeki değişikliklerin testi, Kurumun operasyonlarıyla bağıntılı olmayan ayrı bir test ortamında yapılır. Değişiklik yapılan sistemlerin teknik özelliklerinden dolayı testler ayrı bir test ortamında gerçekleştirilemeyecekse, gerçekleştirilen testlerin operasyonlara etkisini en az seviyeye indirgemek için bir değerlendirme yapılır. Sistem üzerinde işlemler geçici olarak başka sistemler üzerinden işlenir veya testler esnasında

beklenmeyen bir durum oluşması halinde operasyonların en az etkileneceği zamanlarda gerçekleştirilir. Testler başarı ile sonuçlandıktan ve bu sonuçlar kayıt altına alınıp ilgili kişi tarafından onaylandıktan sonra değişiklikler canlı ortamda uygulanır.

Bu aşamada, Bilgi İşlem bölümünde görev yapan Bilgi Güvenliği Yöneticisi son kullanıcı dokümanlarını (kullanım kitapçıkları, sistem dokümanları vb.) ve asgari güvenlik standartlarının karşılandığını kontrol eder.

5.2.3 Dokümantasyon

Canlı sistemlerde yapılan değişikliklerin uygulanması için aşağıdaki dokümanlar oluşturulur:

- Kullanıcı Talebi (Açıklama / Gerekçe)
- Etki Analizi
- Harcanacak Çaba (Adam/Gün)
- Maliyet Analizi
- Öncelik Verme
- Alternatifler
- Test Ortamındaki Test Sonuçları
- Her Aşamada Alınan Onaylar
- Geri Dönüş Planı (eğer gerçekleştirilecek değişiklik özel bir geri dönüş prosedürü gerektiriyorsa)

Canlı ortamlarda değiştirilecek unsurların yedekleri (back-up) değişiklik öncesinde alınır.

Verilerin bütünlüğü, doğruluğu ve değişiklik kontrol sürecinin doğru olarak tamamlanması için Bilgi İşlem yöneticisi, varlık üzerinde yapılacak olan değişiklikten etkilenen bir süreç var ise bu iş sürecinin sahiplerine konu hakkında bilgi verir ve etki analiz raporunu kendileri ile paylaşır, bu süreç, ilgili ilgili iş süreç sahipleri tarafından onaylanır. Sistem yöneticisi ve altyapı yöneticisi değişikliği bu gibi durumlarda Bilgi Güvenliği Yöneticisi'nin onayına sunar, Eğer değişiklik, firewall, merkez router, merkez switch, Merkez IPS vb gibi Ana Kontrol Merkezi üzerindeki donanımlar ya da yazılımlar üzerinde yapılacaksa Bilgi İşlem yöneticisi onayı alınır.

5.3 Görevler Ayrılığı

Görev ve sorumluluk alanları, kasıtlı ya da kasıtsız değişiklik yapılmaması veya organizasyon varlıklarının yanlış / kötü amaçlı kullanılmaması için birbirinden ayrılır.

Bilgi İşlem Müdürlüğü ve diğer bölümler görevler ayrılığı ilkesinin uygulanması için koordineli olarak çalışırlar.

Görevler ayrıştırıldıktan sonra sistemlere erişim, canlı veri kütüphanelerine erişim, canlı sistem programlarına erişim, programlama dokümanlarına erişim, işletim sistemi seviyesindeki erişimler kısıtlanır.

Görevlerin ayrıştırılmasının zor olduğu durumlarda, yetkinlikli kullanıcıların aktiviteleri izlenir, denetim iz parametreleri kontrol edilir.

5.4 Test ve Operasyon Faaliyetlerinin Ayrıştırılması

Bkz. Bilişim Sistemi Alım, Geliştirme ve Bakım Prosedürleri.

5.5 3. Parti Sağlayıcı Yönetimi

Bkz. Tedarikçi Yönetimi Prosedürleri.

5.6 Ağ Güvenliği Yönetimi

Bkz. Ağ Güvenliği.

5.7 Ortam Yönetimi & Güvenlik Prosedürleri

Kasetlerin, disklerin, taşınabilir bellek, CD, DVD ve yazılı dokümanların dağıtımında aşağıdaki prosedürlere uyulur.

5.7.1 Taşınabilir Ortamların Yönetimi

Eğer taşınabilir ortam içerisinde saklanan bilgi artık ihtiyaç duyulmayacak bir veri ise, geri dönülemeyecek şekilde imha edilir.

Ortamın ya da ortam içerisindeki verinin kaldırılmasında onay gereksinimi var ise, imha öncesinde ve sonrasında denetim kaydı tutulur.

Taşınabilir ortamda veriler sadece iş gereksinimi mevcut ise tutulur.

5.7.2 Taşınabilir Ortamın İmhası

Bkz. Fiziksel Güvenlik Prosedürleri.

5.7.3 Medya ve Bilgi Kullanma Prosedürü

Yönetim ve Bilgi İşlem bölümü, bilgi ve medyanın korunması için fiziksel ortamı sağlamakla sorumludur.

Tüm medyalar (veri ortamları) üreticinin bildirdiği koşullarda saklanır.

Tüm medyalar (veri ortamları) dikkatlice muhafaza edilir, manyetik alanlardan uzak tutulur, aşırı sıcak ya da kirli ortamlarda tutulmazlar.

Yeniden kullanılabilir ortamlardaki verilere tekrar ihtiyaç duyulmayacak ise ortamlar formatlanır.

İlgili bölüm müdürü bu silinme / formatlamayı onaylar.

Ortamların taşınması sırasında aşağıdaki talimatlara uyulur:

Güvenilir bir kurye kullanılır, güvenilir kuryelerinin listesi yönetimce onaylanır. Kuryelere teslimat yapılırken kuryenin kimlik bilgileri ve ilgili kurye Kurumda çalıştığı kontrol edilir.

Ortamın taşınması sırasında medya fiziksel bir zarar almayacak şekilde ve tedarikçi talimatnamelerine göre paketlenir.

Gerekli görüldüğü durumlarda izinsiz değişikliklere karşı özel güvenlik önemleri alınır (kilitli paketleme sistemleri, dijital imza, şifreleme vb.).

5.7.4 Sistem Dokümantasyonun Güvenliği

Sistem dokümanları sistemlerin işleyişi ve yapılandırılması ile ilgili çeşitli bilgiler içerir. Bu sebepten bu bilgilerin açıklanması bilgi işlem kaynaklarında depolanan bilgilerin güvenliğini tehlikeye atar.

Sistem dokümanları belirli standartlarda saklanır. (Bkz. Varlık Sınıflandırma Standartları).

Yazılı ve elektronik ortamda tutulan verilere kimlerin erişiminin olduğu Bilgi Güvenliği Yöneticisi tarafından izlenir. Bu liste sistem yöneticilerinin erişimine açıktır.

Yazılı dokümanlar, anahtarının Bilgi İşlem Şube Müdürü, Bilgi Güvenliği Yöneticisi ve Sistem Yöneticileri'nde bulunduğu kilitli bir ortamda tutulur.

Elektronik ortamdaki dokümanlar dosya paylaşım sistemlerinde tutulmaz. Dosya Paylaşım Sistemlerinde tutuluyorlarsa bu kısma erişim sadece dağıtım listesindeki kişilere açık olur.

Sistem Yöneticileri bu dokümanların kopyalarını Bilgi İşlem Şube Müdürünün onayı olmadan çoğaltamaz ya da kendilerine ait ortamlara alamazlar.

5.8 Bilgi Değişimi

5.8.1 Bilgi Değişimi Politika ve Prosedürü

Bilgi Güvenliği Yöneticisi, tedarikçilerle ne gibi durumlarda bilgi değişiminde bulunulduğunu belirlemek için tedarikçi ilişkilerini gözden geçirir.

Bilgi Güvenliği Yöneticisi Kurumun müşteri ile ne gibi durumlarda bilgi değişiminde bulunduğunu gözden geçirir.

Prosedürler, bilginin tedarikçiye iletimi sırasında kopyalanmasını, yanlış yönlendirilmesini ve değiştirilmesini engelleyici niteliktedir.

Bilginin iletimi sırasında şifreleme teknikleri kullanılabilir. Bu konudaki karar iletilen bilginin varlık değerine istinaden alınır. (Bkz. Şifreleme Sistemleri Politika ve Prosedürleri)

Mesajlar da dâhil olmak üzere bütün bilgilerin imha ve saklama kılavuzları kanun ve regülâsyonlarla uyumludur. (Bkz. Uyum Politika ve Prosedürleri)

Kritik bilgiler fotokopi makineleri, yazıcılar ve faks makineleri gibi yetkisiz personelin erişebildiği yerlerde bırakılmaz.

Kurum personeli kritik bilgileri telefonda paylaşırken muhtemel riskleri (konuşmanın dinlenmesi vb.) göz önünde bulundurur.

5.8.2 Bilgi Paylaşımı Anlaşması

Kurum ve 3. Parti tedarikçilerle arasında bir anlaşma imzalar. Bu anlaşmanın sorumluluğu 3. Parti tedarikçiler ile bilgi alışverişi esaslarını gözden geçirmiş olan Bilgi Güvenliği Yöneticisi'nin sorumluluğundadır (Bu anlaşma 3. Parti ile yapılan sözleşmenin bir parçası da olabilir.). Bilgi paylaşımı anlaşması aşağıdaki maddeleri içerir:

Bilgi değişim yönetiminde yönetimin sorumlulukları,

Bilginin gönderildiğine, sevk edildiğine ve ulaştığına dair bildirimlerin bulunduğu bir prosedür,

Bilginin izlenebilirliği, yetkisiz kişilerin eline geçtiğinde okunamamasını garanti altına alacak bir şifreleme sisteminin bulunduğu prosedür, (Bkz. Şifreleme Politika ve Prosedürleri)

Paketleme standartları gibi standartların bulunması;

Gerekli ise emanet anlaşmaları;

Veri kaybı gibi bilgi güvenliği olayların yaşanmasındaki sorumluluklar ve yükümlülükler

Kritik ve hassas verinin sınıflandırılması ve kritiklik derecesine göre taşınması ya da saklanması için bir etiketleme sisteminin kullanılması;

Mülkiyet, veri koruma, telif hakkı, yazılım lisans uyumu vb. hususlar için sorumluluklar.

Örneğin Kurumun test edeceği ya da Kavram Kanıtlama(PoC) işlemleri için yapacağı her çalışmada, çalışmanın sahibi birim ile çalışmayı yapacak firma arasında bilgi paylaşım ya da anlaşması gizlilik sözleşmesi imzalanır.

5.8.3 Fiziksel Ortamların Transferi

Lokasyonlar arası taşınan ortamın korunması için aşağıdaki kural ve prosedürlere uyulur:

Güvenilir taşıma Kurumları ya da kuryeler kullanılır.

Yönetim tarafından kabul edilmiş yetkili kuryeler listesi olur.

Kuryelerin kimlik tespit prosedürleri tanımlanır.

Varlıkların paketlenmesi üretici firmanın kriterlerine göre yapılır ve herhangi fiziksel etkiden korunmasını sağlaması gereklidir. Örneğin, ısı, nem veya elektromanyetik alanlara karşı muhafaza edilir.

Hassas bilginin yetkisiz erişimlerden ve değişikliklerden korunması için çeşitli kontroller konulur, bu kontroller:

- Kilitli taşıyıcılar kullanılır (kutular, çantalar dolaplar)
- Elden teslimat
- Dış müdahaleye karşı kapalı paketleme
- Çok önemli durumlarda teslimatı birden fazla parçaya ayırıp farklı rotalardan sevkiyat yapma.

5.8.4 Elektronik Mesajlaşma

Elektronik ve anlık mesajlaşmalar uygun şekilde korunur. Elektronik mesajlaşma için güvenlik kontrolleri şunlardır:

- Mesajların yetkisiz erişim ve değişiklikten korunması
- Adresin (ulaşacağı noktanın) doğrulanması
- Hizmetlerin güvenilir ve erişilebilir olması
- Yasal mevzuata uygun olunması, örneğin elektronik imza
- Sohbet veya dosya paylaşımı gibi hizmetlerin kullanımından önce Bilgi İşlem yöneticisinden ve talebi yapan kullanıcının birim yöneticisinden onay alınması
- Kamuya açık ağların erişiminde mümkünse 2 seviyeli kimlik kontrolü uygulanması

5.8.5 İşletme Bilişim Sistemleri

- Çeşitli işletme bilgilerinin entegrasyonları ve iş üzerine etkileri göz önüne alınır.
- Yönetim ve muhasebe sistemlerindeki bilinen güvenlik zafiyetleri araştırılır.
- İş ile ilgili haberleşme sistemlerindeki açıklıklar: Örneğin; telefon kayıtlarının kaydedilmesi, telefon hatlarının güvenliği, faksların depolanması ve kayıt altına alınması
- Bilgi paylaşımına politika ve prosedürler aracılığı ile uygun kontroller koyulur.
- Çalışan ve sağlayıcıların kategorilere göre sistemlere ve lokasyonlar erişimleri kısıtlanır.
- Kullanıcı hesap isimleri belirlenir. Örneğin, Kurum çalışanlarının ve sözleşmeli çalışanların tanımlandığı dizinler kullanıcıların yararına olur.
- Sistemler üzerindeki veriler saklanır ve yedeklenir.
- Geri alma / yükleme şartları belirlenir.

5.9 Halka Açık Bilgiler

İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi kamuya açık bilgilerin hangi mecralardan yayınlanacağını ve neler olduğunu takip eder. Bu açıdan değerlendirilen bilgiler, İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi tarafından yıllık gerçekleştirilen Bilgi Güvenliği Yönlendirme Kurulunda(Güvenlik Kurulu) sunulur.

İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi halka açık bilgilerin bütünlüğünün sağlanması için gerekli kontrollerin koyulması ile sorumludur. İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi dijital sertifika, mesaj onayları gibi bilgi koruma yöntemleri kullanılmasına karar verir.

Herhangi bir bilgi kamuya açılmadan önce bilgi, Sistem Yöneticileri tarafından gözden geçirilir ve operasyon yöneticileri tarafından onaylanır.

Bazı bilgilerin kamuya açılması için sunuculara konması gerekiyorsa, bilgi sunucuya konulduktan sonra sistem yöneticileri bu bilginin doğruluğunu ve geçerliliğini kontrol eder. Bilgiler kamuya açılmadan önce sunucuda var ise, bilgi yayınlanmadan önce kontrol edilir.

Kurum operasyonları için gerekli kritik bilgilere, bu bilgilerin kamuya açılmasından önce ihtiyaç duyulması durumunda üçüncü bir tarafa bilgi doğrulatılır.

Kurum operasyonları için gerekli kritik bilgilerde, bilginin halka doğru ve güvenilir şekilde açıklanabilmesi için bilgi doğrulanma sürecine dâhil edilir.

Bilgi kamuya açıldıktan sonra İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi bu bilginin nasıl göründüğünü kontrol eder.

Bu tür bilgilere yazma ve güncelleme yetkisi sadece yetkili kişilere ve bu kişiler asgari gereksinimleri karşılayacak şekilde verilir. İş Birimi Yöneticisi ve Bilgi Güvenliği Yöneticisi bu dokümanlardaki güncelleme işlerinin denetim izlerini gözden geçirir.

Kuruluşun web sitesinde bulunan kamuya açık metinler Kurumsal iletişim ile koordineli olarak gözden geçirilir ve kalite standartlarına uygunluğu kontrol edilir.

5.10 İzleme

Sistem yetkisiz bilgi işlem faaliyetlerini tespit etmek için izlenir. Operatör denetim kayıtları ve sistem hata kayıtları problemlerin belirlenmesinde kullanılır. Kurumun günlük izleme aktiviteleri kendi iç yönetmeliğine uygundur. Denetim kayıtları toplanır. Denetim kayıtlarının hangi sistemler ve olaylar için oluşturulacağı belirlenir ve bu kayıtlar üzerindeki olaylara yönelik incelemeler gerçekleştirilir.

5.10.1 Denetim Kayıtları

Denetim kaydı tutma mekanizmaları bütün sistemlerde etkindir. Denetim kayıtları aşağıdaki maddeleri içerebilir:

- Kullanıcı ID'leri
- Önemli işlemlerin detayları (sisteme giriş- çıkış tarihi, saati vs.)
- Terminal numaraları, eğer mümkünse lokasyon bilgileri
- Sistem erişimlerindeki başarılı ve başarısız girişimler
- Verilere ve diğer kaynaklara başarılı ve başarısız erişim girişimleri
- Sistem konfigürasyon değişiklikleri
- Yetkilerin kullanımı (yüksek yetkili kullanıcılar; sistem ve/veya uygulama yöneticisi)
- Hizmet programlarının ve uygulamalarının kullanımı
- Erişilen dosyalar ve dosya paylaşım sistemleri
- Ağ adresleri ve protokolleri
- Erişim kontrol sistemi tarafından üretilen alarmlar
- Koruma sistemlerinin aktivasyon ve de-aktivasyon bilgileri (Örn. anti-virüs sistemleri, Saldırı sezme sistemleri)

5.10.2 İzleme Sistemlerinin Kullanımı

Bilgi Güvenliği Yöneticisi, her sistemin ve kullanıcının ne seviyede izleneceğine karar vermek için risk değerlendirmesi yapar.

Denetim kayıtlarının yönetimini yapan personel bu kayıtların periyodik gözden geçirilme raporunu günlük olarak Bilgi Güvenliği Yöneticisi ve Bilgi İşlem yöneticisi ile paylaşır. Eğer tespit edilen olaylar iş birimlerini etkiliyorsa, bu husus Bilgi Güvenliği Yöneticisi tarafından Bilgi Güvenliği Yöneticisi'ne bildirilir.

Bilgi İşlem Yöneticisi ve Bilgi Güvenliği Yöneticisi bu raporları aylık olarak gözden geçirir. Gözden geçirme esnasında aşağıdaki maddelere dikkat edilir:

- Verilerin değerleri, önemi ve kritikliği.
- Geçmiş deneyimler temel alınarak açıklıkların kontrol edilmesi, filtrelemelerin ve yanlış kullanımların kontrol edilmesi.
- Sistem bağlantılarının kontrol edilmesi.
- Sistemin denetim kaydı tutacak şekilde yapılandırılması.

5.10.3 Denetim İzi Bilgilerinin Korunması

Denetim kaydı dosyaları değiştirilmelere ve silinmelere karşı koruma altında olur.

Denetim kaydı dosyalarına erişim kısıtlanır.

Denetim kaydı dosyalarının tutulacağı saklama ortamları, kayıt işlemlerinde hata oluşma riskini ve daha önceki kayıtların üstüne yazılma riskini en düşük seviyelere çeker.

5.10.4 Denetim Kayıtlarının Yönetimi ve Operasyonu

Sistem yöneticilerinin ve sistem operatörlerinin aktivitelerinin denetim kayıtları tutulur ve bu denetim kayıtları aşağıdakileri içerir:

- Hangi olay ne zaman meydana geldiğinin bilgisi (başarılı ya da başarısız),
- Olay ya da hata ile ilgili bilgileri,
- Hangi kullanıcı hesabı ve sistem yöneticisi ya da operasyon elemanının olduğu,

Sistem yöneticisinin ve sistem operasyon elemanlarının denetim kayıtlarının tutulduğu dosyaya okuma dışında erişim hakkı sadece Bilgi Güvenliği Yöneticisi ve ilgili Bilgi İşlem yöneticisine verilir. Denetim kayıtları periyodik olarak kontrol edilir.

5.10.5 Hata Denetim Kayıtları

Kullanıcılar ya da sistemler tarafından bildirilen hatalar ile ilgili problemlerin bilgileri saklanır.

Sistem yönetimi grubunun sorumlusu hata denetim kayıtlarını gözden geçirir ve bu hataların başarılı bir şekilde sonlandırıldığını kontrol eder.

Eğer hata denetim kaydı tutma özelliği mevcut ise bu özellik etkinleştirilir.

Denetim kaydı tutma işlemi sistemlerin performanslarını etkiler. Bu sebepten, bu mekanizma yeterli bilgiye sahip personeller tarafından etkinleştirilir. Sistemlerde hangi seviyede denetim kaydı tutulacağının kararı performans ile ilgili risk değerlendirmesi yapılarak verilir.

5.10.6 Sistem Saati Senkronizasyonu

Bilgisayarların ve haberleşme cihazlarının gerçek zamanlı çalışma yeteneğine sahip olduğu ortamlarda, saat ayarı kabul görmüş standartlara uygun yapılır (Coordinated Universal Time (UTC) ya da standart yerel saate göre ayarlanır.

Sistem yöneticisi bütün sistemlerin saat ayarlarının eşzamanlı ayarlandığını kontrol eder.

5.11 Bilgi İşlem Varlık Yönetimi

5.11.1 Yazılım Varlıkları

Bilgi Güvenliği Yöneticisi Kurumun sahip olduğu yazılım varlıkları kayıtlarının tümünün detaylı bir listesinin tutulmasını sağlar. Yeni bir yazılım satın alındığında ya da geliştirildiğinde bu envanter güncellenir. Kurumun sahip olduğu bütün yazılım varlıkları için şu bilgiler tutulur:

- Yazılımın adı, geliştiren firma ve sürüm numarası
- Kurulu olduğu donanımın adı ve lokasyonu
- Yükleme için seri numarası
- Yazılımın orijinal kurulum ortamının (CD, Taşınabilir bellek vb.) ve dokümanlarının bulunduğu lokasyon
- Garanti periyodu ve varsa garantinin sonlanma tarihi

Sistem yöneticisi her kullanılan yazılımda lisansların yönetiminden sorumludur. Lisans hakkının kullanılandan az olmamasını kontrol etmek ve lisans sözleşmesinin şartlarına uyulması sistem yöneticilerinin sorumluluğundadır.

Bilgi İşlem yöneticisi sistemlerin zafiyet değerlendirmesini yaptıktan sonra varlık kayıtlarındaki lisansların gözden geçirilmesini sağlar. Bilgi İşlem yöneticisi, her 3 ayda bir zafiyet değerlendirilmesi ya da iç denetim çalışması kapsamında bütün sunucu ve dizüstü bilgisayarları yetkisiz ve telif haklarını ihlal eden yazılımların kontrol edilmesini sağlar. Bu incelemenin sonucunda tespit edilen aykırılıklar Bilgi Güvenliği Yöneticisi'ne raporlanır ve gerekli disiplin süreci işletilir.

5.11.2 Donanım Varlıkları

Kurumun sahip olduğu donanım varlıklarının detaylı bir listesi donanım varlık envanterinde tutulur. Listenin oluşturulmasından Bilgi İşlem birimi sorumludur. Bütün donanım varlıkları için aşağıdaki bilgiler doldurulur:

- Donanımın türü, seri numarası, üreticisi
- Donanımın nereye kurulduğu bilgisi
- Konfigürasyonu
- Satın alma tarihi
- Garanti periyodu ve garantinin biteceği tarih

Tedarikçi firmaya devredilen bütün sorumluluklar garanti belgesinde yer alır. Garantinin sona ermesinden sonra tedarikçilerle ya da hizmet sağlayıcılarla tedarik anlaşmaları yapılır. Bilgi İşlem Yöneticisi donanım envanterinin periyodik olarak kontrol edilmesinden ve gerektiğinde güncellemelerin talep edilmesinden sorumludur.

5.11.3 Yazılım Varlıkları Yönetimi

Yazılım varlıkları yönetimi Bilgi İşlem bölümünün sorumluluğu altındadır (İşletim Sistemi, 3. Parti uygulamalar, Veritabanı, ağ donanımları vb.)

Bilgi İşlem Yöneticisi yazılım güncellemelerinin başarılı testlerinin ardından yapıldığını garanti altına alır.

Bilgi Güvenliği Yöneticisi ve sistem yöneticileri sertifikaların kayıtlarını yapmak ve gerekli güncelleme bilgilerini almak için üretici firmaların mail listelerine üye olurlar.

Farklı noktalardan gelen uyarılara istinaden yüklenen zafiyet giderici yamalar ve yazılım güncellemeleri, yükleme öncesinde Operasyonel Değişiklik Kontrolü Prosedürlerine göre değerlendirilir, test edilir ve sonrasında gerçekleştirilir.

Yamalar yüklenmeden önce Bilgi Güvenliği Yöneticisi'nin ve Sistem Yöneticisi'nin, yamaların Kurum uygulamalarına etkisini değerlendirmesi gerekir.

Bilgi Güvenliği Yöneticisi, hizmet sağlayıcılar yeni yama gönderdiğinde bütün İşletim Sistemleri'ne bu güncellemenin yüklenmesini sağlar. Bu konuda Bilgi İşlem bölümü, ilgili sistem yöneticileri tarafından yayınlanan yamaların son versiyonu ve sistemlerde bulunan son yama versiyonunu aylık olarak Bilgi Güvenliği Yöneticisi'ne raporlar. Bu iki veri arasında fark olması (yayınlanan yama paketi ve sistemlerde yüklü yama paketi) durumunda bunun nedenleri dokümante edilir.

Kurum içinde geliştirilen (In-house) uygulamalar Uygulama Geliştirme Prosedürüne göre güncellenmelidir.

Veritabanı ve Uygulama: Operasyondan sorumlu personel canlı sistemlerin uygulama ve veri tabanlarını yönetmelidir. Veritabanı ve uygulamalar Asgari Güvenlik Standartları'na göre

yapılandırılır. Veritabanı yöneticileri veritabanlarının istikrarının ve bütünlüğünün sağlanmasından sorumludurlar.

Veritabanları ve uygulamalar tedarikçi tarafından belirlenen / önerilen şekilde yönetilir.

Uygulama veritabanları üzerindeki veri sadece iş süreci uygulamaları üzerinden değiştirilir. Verilerin manüel değişimine sadece olağanüstü durumlarda izin verilir. Bu tür değişiklikler uygulamanın iş süreç sahibi tarafından yazılı olarak onaylanır. Buna ek olarak, bu tür değişiklikler Değişiklik Kontrol politikası ve prosedürlerinde belirtildiği şekilde gerçekleştirilir. Veriler değiştirilmeden önce veritabanının tam yedeği alınır.

5.12 Anti – Virüs ve Zararlı Yazılım Prosedürleri

5.12.1 Virüs ve Zararlı Yazılımlardan Korunma Yazılımlarının Kurulması

Bilgi İşlem bölümü anti-virüs yazılımlarının en son sürümlerinin, virüslerin ve zararlı yazılımların bütün giriş noktalarında (Ağ geçitleri, Sunucular, Kişisel Bilgisayarlar vb.) kurulu olduğunu kontrol eder. Bu konuda tespit edilen istisnalar, Bilgi Güvenliği Yöneticisi'ne ve Bilgi İşlem yöneticisine raporlanır.

5.12.2 Virüs Tanımlarının Güncellenmesi

Bu dosyalar, virüs imzalarının verilerini içeren dosyalardır. Anti-virüs güncellemeleri otomatik olarak yapılabileceği gibi manüel olarak da yapılabilir.

Otomatik Güncelleme:

Sistem internete her bağlandığında daha önceden belirlenmiş aralıklarla hizmetin sağlandığı firmaya bağlanıp yeni virüs güncellemesi olup olmadığını kontrol eder.

Eğer yeni bir güncelleme mevcut ise, bu güncellemeyi indirilir ve bir dağıtıcı sunucuya konulur. Bu sunucu üzerinden, İşletim Sistemi'nde bunun için "Job" oluşturarak, bu virüs tanım dosya güncellemelerinin sunuculara ve kişisel bilgisayarlara belirlenen zamanlarda yüklenmesini sağlar. Bu işlem, virüs tanım dosyasının Merkez sunucuya gelmesinden sonraki en yakın zamana ayarlanır. Bu virüs tanım dosyalarının yüklenmesinde çeşitli tedarikçilerin yazılımları kullanılabilir.

Manüel Güncelleme:

Sistem, internete her bağlandığında daha önceden belirlenmiş (scheduled) aralıklarla sağlayıcı firmaya bağlanıp yeni virüs güncellemesi olup olmadığını kontrol eder.

Eğer yeni bir güncelleme mevcut ise, yeni güncelleme hakkında sistem yöneticisini uyarır. Sistem yöneticisi sunucuları ve kişisel bilgisayarların virüs tanım dosyalarını günceller.

5.12.3 Anti-Virüs Yazılım Güncellemeleri

Güncellemeler Anti-virüs yazılımlarının en yeni sürümleridir. Anti-virüs yazılımlarının ve araçlarının yeni versiyonlarının periyodik olarak kontrol edilmesi ve hızlı bir şekilde edinilmesi Bilgi İşlem sistem yöneticilerinin görevidir.

5.12.4 Denetim Kayıtlarının Gözden Geçirilmesi

Bilgi İşlem sistem yöneticileri ve operatörleri, sunucuların ve kişisel bilgisayarların denetim izlerini gözden geçirir ve virüslerle ilgili olayları Bilgi Güvenliği Yöneticisine aylık olarak raporlar.

Bilgi İşlem tarafından ilgili Bilgi Güvenliği Sorumlularına birimlerde kullanılan bilgi sistemleri cihazları üzerinde meydana gelen virüs ve zararlı yazılım aktiviteleri raporlanır. Özellikle kullanıcının Kabul Edilebilir Kullanım Politikasında yazan prensiplere aykırı olarak gerçekleştirdiği olaylar (örn. Anti-Virüs yazılımının çalışmasını engellemek, zararlı yazılımları kasten yüklemek vb.) İş Birimi Yöneticisi ve Bilgi Güvenliği Sorumluları tarafından değerlendirilir ve duruma göre kullanıcıya bilgilendirme yapılır veya disiplin süreci işletilir.

Bilgi İşlem sistem yöneticileri ve operatörleri sunucularda ve kişisel bilgisayarlarda anti-virüs sistemlerinin en son sürümünün yüklü olup olmadığını kontrol eder. Bu konuda görülen eksiklikler Bilgi Güvenliği Yöneticisi ve Bilgi İşlem yöneticisine raporlanır.

6. İLGİLİ DOKÜMAN

- Bilgi Güvenliği Politikası
- İletişim ve Operasyon Yönetimi Politikası.