BİLGİ GÜVENLİĞİ AÇISINDAN HABERLEŞME VE İŞLETİM YÖNETİMİ

Bir kurumda bilgi güvenliğinin tam olarak sağlanmasının adımlarından biri olan haberleşme ve işletme yönetiminde uyulması ve uygulanması gereken kuralların/maddelerin sınıflandırılmış şekilde aşağıda görmekteyiz;

1. İŞLETİM PROSEDÜRLERİ VE SORUMLULUKLAR

Belgelenmiş İşletim Prosedürleri

- İşletim prosedürleri yazılmış olmalı ve süreli güncelleniyor olmalıdır.
- Bilgi işlem ve iletişim ile ilgili sistem açma/kapama, yedekleme, cihazların bakımı, Bilgisayar odasının kullanılması gibi sistem faaliyetleri prosedürlere bağlanmış olmalıdır.
- İşletim prosedürlerine, ihtiyacı olan tüm kullanıcılar erişebiliyor durumda olmalıdır.
- Bu prosedürlere resmi belge muamelesi yapılıyor olmalıdır. (Yapılan tüm değişiklikler için yönetim yetkilendirmesi gerekip gerekmediği tespit edilmelidir.)

Değişim Yönetimi

- Bilgi işlem sistemlerinde yapılan değişiklikler yönetiliyor olmalıdır.
- Asıl sistemler ve uygulama programları sıkı bir değişim kontrolüne tabi tutuluyor olmalıdır.
- Değişikliklerle ilgili planlama ve test yapılıyor olmalıdır.
- Programlarda yapılan değişiklikler için kayıtlar tutuluyor olmalıdır.
- Değişikliklerin, güvenlik dahil olmak üzere potansiyel etkileri değerlendiriliyor olmalıdır.
- Değişiklikler için resmi onay prosedürleri olmalıdır.
- İlgili personele değişiklik detayları bildiriliyor olmalıdır.
- Başarısız değişikliklerin onarılması ve geri alınması ile ilgili sorumlulukları belirleyen prosedürler olmalıdır. (Bilgi işlem sistemlerinde yapılan değişikliklerin yönetilmemesi sonucunda sık sık sistem hatalarının ve güvenlik açıklarının ortaya çıktığı unutulmamalıdır.)

Görevler Ayrılığı

- Bilginin veya bilgi servislerinin kazara ya da kasten yanlış kullanımını veya yetkisiz değiştirilme riskini azaltmak için görevler ve sorumluluklar ayrılmış olmalıdır.
- Bir işin yetkilendirilmesi ile o işin gerçekleştirilmesi farklı kişiler tarafından yapılıyor olmalıdır.

Geliştirme Sistemi, Test Sistemi ve Aktif Sistemlerin Ayrılması

- Geliştirme ve test ortamları esas çalışma ortamından ayrılmış durumda olmalıdır.(Örneğin, geliştirilmekte olan yazılım ile kullanılmakta olan yazılım farklı bilgisayarlarda çalıştırılmalıdır. Gerekli görüldüğü yerde geliştirme ve test ortamları da birbirinden ayrılmalıdır.)

2. ÜÇÜNCÜ TARAFLARDAN ALINAN HİZMETİN YÖNETİLMESİ

Hizmet Alma

- Üçüncü taraftan hizmet alma anlaşmasında belirtilen hizmetlerin tanımının, güvenlik seviyesinin ve denetiminin gerçekleştirilmesini ve sürdürülmesini güvence altına almak için üçüncü taraf gerekli tedbirleri almış olmalıdır.

Üçüncü Taraf Hizmetlerinin Gözden Geçirilmesi

- Üçüncü taraflardan alınan hizmetler, raporlar ve kayıtlar düzenli olarak izleniyor ve gözden geçiriliyor olmalıdır.
- Üçüncü taraflardan alınan yukarıdaki hizmetler, raporlar ve kayıtlar düzenli aralıklarla denetime tabii tutulmalıdır.

Üçüncü Taraf Hizmetlerindeki Değişikliklerin Yönetilmesi

- Bilgi güvenliği politikaları, prosedürleri ve denetimlerinde yapılan bakım ve iyileştirmeleri de içeren hizmet alımı değişiklikleri yönetiliyor olmalıdır.

- Değişiklik yönetimi çerçevesinde işin içindeki süreçlerin kritikliği hesaba katılıyor ve riskler gözden geçiriliyor olmalıdır.

3. SİSTEM PLANLAMA VE KABUL ETME

Kapasite Yönetimi

- Gereken sistem performansını sağlamak için sistem kaynaklarının ne oranda kullanıldığı izleniyor ve ileriye dönük kapasite ihtiyacının projeksiyonu yapılıyor olmalıdır. (Önemli sunumcuların üstündeki sabit disk alanının, RAM ve CPU kullanımlarının izlenmesi gerekir)
- Mevcut aktiviteler ve yeni başlayacak aktiviteler için kapasite ihtiyaçları belirleniyor olmalıdır.
- Tedarik süresi uzun veya fiyatı yüksek ekipmanın alınması ile ilgili planlamalar dikkatle gerçekleştiriliyor olmalıdır.

Sistem Kabulü

- Yeni bilgi sistemleri, yükseltmeler ve yeni versiyonlar için sistem kabul etme kriterleri tespit edilmiş ve belgelenmiş olmalıdır.
- Resmi kabulden önce gerekli testler yapılmalıdır.
- Resmi kabul gerçekleşmeden yeni sistemin kullanılmamasına dikkat edilmelidir.
- Resmi kabulden önce şu hususlara dikkat edilmelidir; mevcut sistemlerle birlikte çalışabilirlik, toplam sistem güvenliği üstündeki etkiler, eğitim ihtiyacı, kullanım kolaylığı (kullanıcı hatalarına meydan vermeme açısından).

4. KÖTÜ NİYETLİ VE MOBİL YAZILIMLARA KARŞI KORUNMA

Kötü Niyetli Yazılımlara Karşı Kontroller

- Kötü niyetli yazılımlara karşı bulma, önleme ve düzeltme tedbirleri alınmış olmalıdır.
- Kullanıcı bilinci oluşturulmuş olmalıdır.
- Güvenlik politikası yetkisiz yazılım kullanmayı yasaklıyor olmalıdır.
- Yabancı ağlardan ve diğer medyadan dosya veya yazılım alınmasına ilişkin risklerden nasıl korunulacağına ilişkin politika hazırlanmış olmalıdır.
- Kritik iş süreçlerini çalıştıran sistemler düzenli olarak taranarak yetkilendirilmemiş yazılım ilaveleri veya dosyaların mevcut olup olmadığı araştırılıyor olmalıdır.
- Kötü niyetli yazılımlara karşı bulma ve önleme fonksiyonlarını yerine getiren programlar kurulmuş ve düzenli olarak güncellemeleri yapılıyor olmalıdır.
- Tarama motorları ve imza dosyaları güncelleniyor olmalıdır.
- Ağ üstünden veya diğer ara yüzlerden masaüstü bilgisayarlara veya sunuculara giren dosyalar, e-posta ekleri ve bağlanılan internet sayfalarının içerikleri kontrol edilmelidir.
- Kötü niyetli yazılımlardan korunma sistemleri, bunlarla ilgili eğitimler, saldırıların rapor edilmesi ve saldırı sonrası tedavi ile ilgili yönetim prosedürleri ve sorumluluklar belirlenmiş olmalıdır.
- Saldırı sonrası iş sürekliliği için plan yapılmış olmalıdır.
- Kötü niyetli yazılımlarla ilgili güncel bilgiler izlenmelidir.

Mobil Yazılımlarla İlgili Kontroller

- Sadece yetkilendirilmiş mobil yazılımlar kullanılıyor olmalıdır.
- Yetkilendirilmemiş mobil yazılımın çalışmasına engel olunmalıdır.
- Yetkilendirilmiş mobil yazılımın güvenlik politikası uyarınca çalışması konfigürasyon aracılığı ile güvence altına alınmalıdır. (Mobil yazılım, bir bilgisayardan diğerine taşınan ve otomatik olarak çalışan yazılımlara denir. Kullanıcının herhangi bir müdahalesi olmadan belli bir görevi yerine getirirler.)

5. YEDEKLEME

Bilgi Yedekleme

- Yedekleme politikası uyarınca bilgi ve yazılımların yedeklenmesi ve yedeklerin test edilmesi düzenli olarak yapılmalıdır.

- Bir felaket veya sistem hatasından sonra gerekli tüm bilgilerin ve yazılımların kurtarılmasını sağlayacak yedekleme kabiliyeti mevcut olmalıdır.
- Yedeklemenin hangi düzeyde yapılacağı tanımlanmış olmalıdır.
- Yedeklemenin hangi sıklıkla yapılacağı kurumun ihtiyaçları uyarınca ayarlanmış olmalıdır. Onarım (geri dönüş) prosedürleri belgelenmiş olmalıdır.
- Yedek kopyalar kayıt altına alınmış olmalıdır.
- Alınan yedeklerin bir kopyası ana sitede meydana gelebilecek bir felaketten etkilenmeyecek mesafede fiziksel ve çevresel etkenlerden korunarak saklanmalıdır.
- Yedekleme ortamı düzenli olarak test edilmelidir.
- Onarım prosedürleri düzenli olarak kontrol ve test edilmelidir.
- İşletim prosedürlerinde belirtilen zaman dilimlerinde geri dönüş yapıldığı kontrol edilmelidir.
- Ömrünü tamamlayan yedekleme ünitelerinin takibi yapılmalıdır.
- Gizliliğin önem arz ettiği durumlarda yedekler kriptolanarak alınmalıdır.
- Yedekleme ortamının güvenli biçimde imhası için izlenen bir yöntem olmalıdır.

6. AĞ GÜVENLİĞİ YÖNETİMİ

Ağ Kontrolleri

- Ağ yöneticileri, ağlardaki verinin güvenliği ve bağlı bulunan servislere yetkisiz erişimi engellemek için gerekli tedbirleri almış olmalıdır.
- Ağların işletme sorumluluğu mümkün olan yerlerde bilgisayar işletmenlerinden ayrılmış olmalıdır.
- Uzaktan erişim donanımının/ donanımlarının yönetimi için sorumluluklar ve prosedürler belirlenmiş olmalıdır.
- Halka açık ağlardan ve telsiz ağlardan geçen verinin bütünlüğünü ve gizliliği korumak, ağa bağlı sistemleri ve uygulamaları korumak için özel tedbirler alınmış olmalıdır. (VPN, erişim kontrolü ve kriptografik önlemler gibi)
- Ağ servislerini optimize etmek ve bilgi işlem altyapısı ile ilgili kontrollerin koordinasyonunu ve kuruluşun tamamında uygulanmasını sağlamak üzere yönetim faaliyetleri gerçekleştirilmelidir.

Ağ Hizmetleri Güvenliği

- Kurumun içinden sağlanacak veya dışarıdan alınacak ağ hizmetlerinin her birinin yönetilmesi ve güvenliği ile ilgili ihtiyaçlar belirlenmelidir.
- Bu ihtiyaçlar hizmet sağlayıcıları ile yapılan anlaşmalarda yer almalıdır.
- Ağ hizmetleri sağlayıcısının, üstünde anlaşma sağlanan servislerin güvenli olarak verilmesi ve yönetilmesi ile ilgili imkân ve kabiliyetlere sahip olduğu tespit edilmiş olmalıdır.
- Alınan hizmetin kuruluş tarafından izlenmesi ve denetlenmesi konusunda anlaşmaya varılmış olmalıdır.

7. BİLGİ ORTAMI YÖNETİMİ

Taşınabilir Depolama Ortamlarının Yönetimi

- Teyp, disk, disket, kaset, hafıza kartları ve yazılı raporlar gibi sökülebilir bilgisayar ortamlarının yönetilmesi ile ilgili prosedürler olmalıdır.
- Tüm prosedürler ve yetki seviyeleri açıkça tanımlanmış ve belgelenmiş olmalıdır.
- Daha fazla gerekmediği için kurum dışına çıkarılacak yeniden kullanılabilir ortamlar (disket vs.) okunamaz hale getirilmelidir.
- Organizasyondan çıkarılan tüm ortam malzemeleri için yetkilendirme gereklidir ve bu işlemlerin hepsi için resmi kayıtların tutulması gerekir.
- Ortam malzemelerinin güvenliği sağlanmalıdır.
- Taşınabilir hafıza ortamlarını destekleyen ara yüzler gerçekten gerekmedikçe kapalı tutulmalıdır.

Depolama Ortamının İmhası

- Daha fazla kullanılmayacak bilgi ortamı resmi prosedürler uyarınca emniyetli bir biçimde imha ediliyor olmalıdır.
- Emniyetli imhaya tabii tutulacak varlığı belirlemek için prosedür olmalıdır.

- Emniyetli imha işi dışarıdan bir firmaya yaptırılıyorsa gereken güvenlik önlemlerini uygulayan bir firmanın seçilmesine dikkat edilmelidir.
- İmha edilen ortamların kaydı tutulmalıdır.
- Bilginin yetkisiz olarak açıklanmasına veya yanlış kullanımına engel olmak için bilginin yönetilmesi ve saklanması ile ilgili prosedürler oluşturulmuş olmalıdır.

Bilgi Depolama ve İşleme Prosedürleri

- Tüm ortamlar gizlilik dereceleri uyarınca etiketleniyor ve yönetiliyor olmalıdır.
- Yetkisiz kişilerin bilgiye erişimine engel olmak için erişim kısıtlaması uygulanmalıdır.
- Bilgiye erişim yetkisi olan kişiler resmi ve güncellenmekte olan bir belgede belirtilmiş olmalıdır.
- Veri girdisinin eksiksiz olduğu, işlemin hatasız tamamlandığı ve çıktı onayından geçtiği kontrol edilmelidir.
- Veri dağıtımının en alt düzeyde tutulması sağlanmalıdır.

Sistem Dokümantasyonu Güvenliği

- İşlemler, prosedürler, veri yapıları, yetkilendirme işlemlerinin uygulama tanımları gibi bir dizi duyarlı bilgiyi içeren sistem dokümantasyonu yetkisiz erişimden korunmalıdır.
- Sistem dokümantasyonu güvenli bir ortamda bulundurulmalıdır.
- Sistem dokümantasyonuna erişim listesi asgari düzeyde tutulmuş olmalıdır.
- Yetkilendirme sistemin sahibi tarafından yapılmış olmalıdır.

8. BİLGİ DEĞİŞ TOKUŞU

Bilgi Değiş Tokuşu İle İlgili Politika ve Prosedürler

- Her türlü iletişim ortamında bilginin güvenliğini sağlamak için resmi bir değiş tokuş politikası veya prosedürü uygulanıyor olmalıdır.
- Elektronik iletişim araçları ile ilgili prosedür ve kontroller şu durumları düzenlemelidir; bilginin kopyalanması, tahribi, içeriğinin veya yolunun değiştirilmesinden korunma. Elektronik iletişim aracılığı ile alınabilecek kötü niyetli yazılımların tespiti ve bertaraf edilmesi. Mesajlara eklenmiş hassas bilgilerin korunması. Elektronik iletişim yöntemlerinin kullanımı ile ilgili rehber ve politikalar. Telsiz veri iletişiminin içerdiği riskler de göz önüne alınarak kullanılması. Bilginin bütünlüğünü ve gizliliğini korumak için kriptografik tekniklerin kullanılması. İş ile ilgili yazışmaların saklanması ve imhası. Fotokopi makinesi, yazıcı ve faks cihazlarında hassas bilgi içeren belgelerin bırakılmaması. Elektronik mesajların harici posta kutularına iletilmemesi için yapılacak düzenlemeler. Personelin telefon konuşmaları sırasında hassas bilgilerin açığa çıkmaması için tedbirli davranması. Cevap verme makinelerine hassas bilgi içeren mesajlar bırakılmaması. Faks cihazlarının kullanılması ile ilgili risklerin personele anlatılması.

Bilgi ve Yazılım Değişim Anlaşmaları

- Kurum ile diğer taraf arasında bilgi ve yazılım değişiminin şartlarını düzenleyen anlaşma yapılmış olmalıdır.
- Bu anlaşmada iş bilgilerinin duyarlılığı ile ilgili güvenlik konularına değinilmiş olmalıdır.
- Nakil halindeki bilgi, yetkisiz erişime, bilinçsiz kötü kullanıma veya değiştirilmelere karşı korunmalıdır.

Nakil Esnasında Bilgi Ortamının Güvenliği

- Güvenilir araç veya kuryeler kullanılmalıdır. Kuryelerin kimliğini kontrol etmek için prosedür geliştirilmiş olmalıdır.
- Nakil esnasında varlığı fiziksel hasardan koruyacak paketleme yapılmalıdır.
- Elektronik olarak taşınan bilgi gerektiği gibi korunuyor olmalıdır.

Elektronik Mesajlaşma

- Mesajlar yetkisiz erişimden korunmalıdır.
- Mesajın doğru adrese gitmesi sağlanmalıdır.
- Elektronik posta hizmetinin sürekliliği ve güvenilirliği yüksek olmalıdır.
- Elektronik imza gibi yasal yükümlülükler olmalıdır.
- Eğer varsa gereği yerine getirilmiş olmalıdır.

- Halka açık sistemler ("Instant Messaging" gibi) kullanılmadan önce yönetimden onay alınmalıdır.

Ofis Bilgi Sistemleri

- Elektronik ofis sistemlerinin birbirine bağlanması ile ilgili olarak burada bulunan bilginin korunması için politika ve prosedürler geliştirilmiş olmalı ve kullanılmalıdır.
- İdari sistemdeki ve muhasebe sistemindeki açıklar dikkate alınmış olmalıdır.
- Bilgi paylaşımının yönetilmesi için politika ve tedbirler mevcut olmalıdır.
- Sistemde gerekli koruma yoksa gizli belgeler ve hassas iş bilgileri sistem dışında tutulmalıdır.

9. ELEKTRONİK TİCARET HİZMETLERİ

Elektronik Ticaret

- Halka açık ağlar vasıtası ile taşınan elektronik ticaret bilgileri, hileli kazanç faaliyetleri, anlaşma itilafları ya da bilginin değişikliğe maruz kalması gibi bir dizi ağ şebekesi tehdidine karşı korunuyor olmalıdır.
- Kriptografik önlemler alınmış olmalıdır.(Elektronik ticaret ile ilgili risklerin çoğu kriptografik tedbirlerin uygulanması ile bertaraf edilebilmektedir).
- Ticaret ortakları arasındaki elektronik ticaret düzenlemeleri, iki tarafı bilgilendiren, yetkilendirme detaylarının dâhil olduğu, üzerinde anlaşma sağlanan ticari şartların yazılı olduğu bir belge ile tespit edilmiş olmalıdır.

Çevrimiçi Hizmetler

- Çevrimiçi işlemlerle ilgili bilgi hatalı gönderme, hatalı yönlendirme, mesajın yetkisiz kişiler tarafından ifşa edilmesi, değiştirilmesi, kopyalanması veya tekrar gönderilmesine karşı korunmalıdır.

Halka Açık Bilgi

- Halka açık bilginin bütünlüğü yetkisiz kişilerin değişiklik yapmaması için korunmalıdır.
- Sistem üstünde teknik açıklık testleri yapılıyor olmalıdır.
- Halka açık sisteme konmadan önce bilginin onaylanmasını sağlayan belgelenmiş bir süreç olmalıdır.

10. İZLEME

Olay Kayıtlarının Tutulması

- Erişimi izlemek ve gerektiği takdirde soruşturmalarda kullanmak üzere gerekli sistemlerde kullanıcı faaliyetleri ve güvenlik ile ilgili olay kayıtları tutuluyor ve bu kayıtlar belirli bir süre boyunca saklanıyor olmalıdır.
- Kullanıcı kimlikleri, Oturuma giriş ve çıkış tarihleri ve zamanları, eğer mümkünse terminal kimliği, başarılı ve reddedilmiş sistem erişim denemeleri, sistem konfigürasyonunda yapılan değişiklikler, ayrıcalıkların kullanılması, hangi dosyalara erişimin gerçekleştiği ile ilgili kayıtlar tutuluyor olmalıdır.
- Sistem yöneticilerinin kendi faaliyetlerini silme yetkisine sahip olmaması gerekir.

Sistem Kullanımını İzleme

- Bilgi işlem araçlarının kullanımının izlenmesi ile ilgili prosedürler geliştirilmiş olmalıdır.
- Bu prosedürler uygulanmalıdır.
- Sistem kullanım kayıtları düzenli olarak gözden geçirilmelidir.
- Bilgi işlem araçlarında yapılan işlemlerin hangi düzeyde kaydedileceği risk değerlendirme çalışması sonucunda belirlenmiş olmalıdır.

Kayıt Bilgilerinin Korunması

- Kayıt alma araçları ve kayıt bilgileri yetkisiz erişim ve değiştirmeye karşı korunuyor olmalıdır.

Yönetici ve İşletmen Kayıtlar

- Yönetici ve işletmen faaliyetlerinin kaydı tutulmalıdır.

- Başarılı veya başarısız faaliyetin tarihi ve zamanı, faaliyetle ilgili bilgi (örneğin sistemde oluşan hata ve alınan tedbir), işlemin hangi kullanıcı hesabı üstünde ve hangi yönetici tarafından yapıldığı, hangi süreçlerin etkilendiği kaydediliyor olmalıdır.
- İşletmen kayıtları, düzenli olarak incelenmelidir.

Hata Kayıtlar

- Hatalar rapor edilip düzeltici tedbirler alınıyor olmalıdır.
- Bilgi işlem ya da iletişim sistemleri ile ilgili olarak kullanıcılar tarafından rapor edilen hataların kaydı tutuluyor olmalıdır.
- Hataların tatmin edici bir şekilde giderildiğinden emin olmak için hata kayıtları gözden geçirilmelidir.

Saat Senkronizasyonu

- Sistem bilgisayarları veya diğer bilgi sistemi cihazlarının saatleri standart bir zaman bilgisine göre ayarlanmış olmalıdır.
- Bilgisayar saatlerinin doğru ayarlanmış olması farklı bilgisayarlardan alınmış olay kayıtlarının birlikte incelenebilmesi açısından büyük önem arz etmektedir. Bu iş için NTP protokolü kullanılabilir.