Bilgi Güvenliği

Bilgi Güvenliği Yönetim Sürecinde (BGYS) liderliğin en önemli adımı yönetimin beyanıdır.

BGYS;
Kapsamının iyi belirlenmesi,
Süreci için doğru ekibin oluşturulması,
Politikasının oluşturulması,
Hedeflerinin iyi tanımlanması,
Rolleri, sorumlulukları ve yetkileri belirlenmesi,

Bilgi Varlıkları,
Ürün kodları, taşıma koşulları, ürün standartları, satış fiyatları, teslim süresi ve yeri, müşteri irtibat bilgileri, personel bilgileri, finansal raporlar…

Bilgi Formatları,
Sözlü, yazılı, basılı, elektronik ortamda saklamış olabilir.
Sesli ve görsel medya ortamında olabilir.

Bilgi Kimin Sorumluluğundadır?
Bilginin sahibi, kullanan, sistemi yöneten üç kişi bilginin korunmasından sorumludur. (herkes sorumludur)

Bilginin Korunması
Virüs saldırıları, bilgi işlem ekipmanlarının çalınması/kaybolması, kritik sistem arızaları, gizli bilgilerin kaybedilmesi, DoS/DDoS atakları, zararlı yazılımlar…

Bilgi Korunmadığında;
Hizmet kesintisi yaşanabilir, itibar kaybı yaşanabilir, finansal kayıp, iş ve süreç kaybı, kalite kaybı, şirket içi rotasyon hataları, uyumluluk açığı…

Varlık Yönetimi
Varlık listesi oluşturulmalı
Varlık sahipleri tanımlanmalı
Bilgi sınıfları belirlenmeli
Varlık değeri belirlenmeli (Gizlilik-Bütünlük-Erişilebilirlik) (C-I-A)

Varlık Kategorileri

Basılı dokümanlar, elektronik veriler, veri tabanları, paket yazılımlar, kurumsal yazılımlar, fiziksel ve sanal sunucular, iş bilgisayarları, yazılım ve donanımlar, modemler, enerji sistemleri…

Varlık Envanteri Listesi

Departman, varlık adı, lokasyon, kategori, varlık sahibi ve değeri.

Varlık değerlerinin tanımlanması

(1-5)
(Gizlilik, bütünlük, erişilebilirlik puanlaması) -> Puana bağlı varlık değeri

G-B-E (CIA)

Gizlilik: Bilgiye sadece yetkisi olanların erişilebilirliğini sağlamak (Confidentiality). Bilginin yetkisiz kişilerin eline geçmemesidir.

Bütünlük ve Doğruluk: Bilginin kontrol dışı kalarak zarar görmesini ve değiştirilmesini engellemek. Kesin ve eksiksiz sağlanabileceğini göstermek (Integrity). Bilginin yetkisiz kişiler tarafından değiştirilmemesidir.

Erişilebilirlik: Doğru bilginin, gerek duyulan herhangi bir anda yetkisi olan herkes için ulaşılabilir olduğunu göstermek (Availability). Bilginin ilgili ya da yetkili kişilerce ulaşılabilir ve kullanılabilir durumda olmasıdır.

Ör.
İnternet bankacılığına ait hesap bilgimiz bir saldırganın eline geçince gizlilik zarar görmüş olur.
Bir web sayfasının içeriği saldırgan tarafından değiştirildiğinde bütünlük ve doğruluk zarar görmüş olur.
Bir web sayfasına erişim engellendiğinde erişilebilirlik zarar görmüş olur.

Bilgi Sınıflandırması ve Etiketleme

Varlığın sahibi, varlığın doğru şekilde sınıflandırılmasından sorumludur.
(Çok gizli (A), gizli (B), şirkete özel (C), halka açık)
Sadece yönetici
Sadece ilgili departman
Şirket çalışanları
Müşterilere, iş ortaklarına ve halka açık

Varlıkların İadesi

Varlıkların teslimi-iadesi-değişim süreci tanımlanmalı ve bu zimmet işlemi ıslak imzalı olmalıdır.

Bilgi Sistemleri Riski Nedir?

İş süreçlerini olumsuz yönde etkileyecek şekilde otomasyon sisteminin, ağ veya diğer kritik BT kaynaklarının kaybedilmesi potansiyelidir.

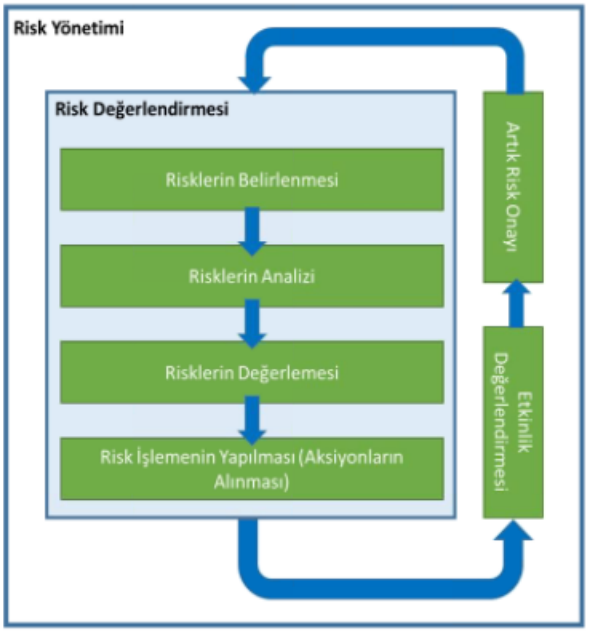
Neden Risk Yönetimi?

Değer oluşturmak ve korumak tüm organizasyon süreçlerinin ayrılmaz bir parçasıdır.
Karar verme sürecinin bir parçasıdır.
Açıkça belirsizliğe değinir.
Sistematik ve iyi yapılandırılmıştır.
Mevcut en iyi bilgiye dayalıdır.
İnsani ve kültürel faktörleri göz önüne alır.
Şeffaf ve kapsayıcıdır.
Dinamik, tekrarlayan ve değiştirmek için duyarlıdır.
Kuruluşta sürekli iyileştirmeyi kolaylaştırır.

Faydaları

Sürdürülebilir karlılık ve büyümenin sağlanması,
Risk kararlarının daha sağlıklı alınması,
Sürprizlere hazırlıklı olunması,
Stratejilerin ve alınan risklerin uyumlu olması,
Fırsatların ve tehditlerin daha iyi tespit edilmesi,
Rekabet gücünün arttırılması,
Etkili kaynak kullanımı,
Yasa ve düzenlemelere uyum,
İtibar ve güvenin korunması,
Kurumsal yönetim kalitesinin sürekliliği,
Şirket değerinin yükselmesi,

RİSK YÖNETİM SÜRECİ



Risk Tespiti / Belirlenmesi

Örn;

İnternetin yedeklenmemesi,
Kritik konumdaki personelin yedeklenmemesi,
Sunuculara yetkisiz erişim olması,
Gizlilik sözleşmelerinin kaybolması,
…

Risk Analizi

Risk belirleme aşamasında tespit edilen risklerin kök nedenlerinin belirlenmesi ve risk değerlendirme sonuçlarının geçerli ve karşılaştırılabilir sonuçlar üretilmesi…

Risk = Süreç / Varlık değeri * Olasılık * Şiddet (gizlilik/bütünlük/erişilebilirlik)

Olasılık

(Çok küçük (1), küçük (2), orta (3), yüksek (4), çok yüksek (5))
Hemen hemen hiç,
Çok az (yılda bir)
Az (yılda birkaç kez)
Sıklıkla (ayda bir)
Çok sıklıkla (her gün, haftada bir)

Risk Etki Derecesi

Çok Hafif, Hafif, Orta, Ciddi, Çok ciddi
Bütünlüğü bozulmaz,
Bütünlük kısmen veya geri dönüşü olacak şekilde bozulur.
KEVK dahilinde bütünlük bozulur.
Bilgi varlıkları kaybolmaya/yetkisiz biçimde değiştirilmeye açık hale gelir.
Bilgi bütünlüğü geri dönülemez şekilde bozulur, yıkıcı olur.

Risk Değerlendirme

68-100 KABUL EDİLEMEZ RİSK (bu risklerle hemen çalışma yapılmalı)
35-67 DİKKATE DEĞER RİSK (risklere mümkün olduğunda çabuk müdahale edilmeli)
1-34 KABUL EDİLEBİLİR RİSK (acil tedbir gerektirmeyebilir)

Risk İşleme Yöntemleri

Riskten Kaçınma, transferi, kabulü.

Risk Analizi Tablosu;

Sıra, süreç, risk, risk sahibi, süreç değeri, olasılık, şiddet, toplam risk.

BGYS Kapsamında Yaklaşım 20 Farklı Politika Bulunmaktadır…

İnternet erişim,
E-Posta Kullanım,
Temiz masa Temiz Ekran,
Şifre,
Mobil Cihaz Kullanım,
Fiziksel Güvenlik,
Uzak Bağlantı,
Kabul edilebilir kullanım Politikası
İzleme Ölçme Analiz Değerlendirme
İç Denetim
Yönetimin Gözden Geçirilmesi
Sürekli İyileştirme

A5	• Güvenlik Politikası
A6	• Bilgi Güvenliği Organizasyonu
A7	• İnsan Kaynakları Güvenliği
A8	• Varlık Yönetimi
A9	• Erişim Kontrolü
A10	• Kriptografi
A11	• Fiziksel ve Çevresel Güvenlik
A12	• İşletim Güvenliği
A13	• Haberleşme Güvenliği
A14	• Sistem Geliştirme ve Bakım
A15	• Tedarikçi Hizmet Sağlama Yönetimi
A16	• Bilgi Güvenliği İhlal Olayı yönetimi
A17	• İş sürekliliği yönetiminin bilgi güvenliği hususları
A18	• Uyum

BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ AMAÇLARI

Varlıkların ve risklerin uygun şekilde yönetilerek

Bilgi güvenliğinin sistematik bir yaklaşım sergileyerek olası ihlal ve kötüye kullanımların önüne geçilmesi

Kazanç
Yasalara uygunluk
Sistematik yönetim
Varlıkların tanımlanması
Risk yönetimi yapılması
İş sürekliliğinin sağlanması,
Fikri mülkiyet haklarının korunması
Müşteri ve tedarikçi güvenliği
İş akışlarının dokümantasyon oluşturulması ve güvence altına alınması

İyi Bir BGYS İçin Kritik Başarı Faktörleri

İşletme hedeflerini yansıtan güvenlik politikaları,
Uygulama yaklaşımında şirket kültürü ve tutarlılık,
Yönetimden görünür destek ve taahhüt,
Varlıkların iyi farkına varılması,
Güvenlik gereklilikleri ve risklerin anlaşılması,
Organizasyon ve taşeronlar dahilinde güvenlik ve politikaların etkin pazarlanması,
Uygun eğitim ve öğrenimin temin edilmesi,
İç denetimler ve geri beslemeleri de içeren bir sürekli ilerleme programı.