Types of Information Security Controls

(Bilgi Türleri Güvenlik kontrolleri)

**Özet:**

Bilgi varlıklarının korunabilmesi, kurumların karşılaşabileceği risklerin en aza indirgenmesi ve iş sürekliliğinin sağlanması, Bilgi Güvenliği Yönetim Sistemlerinin kurumlarda üst yönetim desteğiyle hayata geçirilmesiyle mümkün olmaktadır. Bilgi güvenliğinin yüksek seviyede sağlanması ile ilgili olarak literatürdeki mevcut kaynaklar araştırılıp incelendiğinde, kapsamlı ve güncel bir çalışma olmadığı, sunulan çalışmaların yeterli olmadığı, çoğunlukla ticari içerikli veya güvenilir olmayan web sitelerinde yer aldığı ve nasıl korunması gerektiğiyle ilgili kısa bilgilere yer verildiği tespit edilmiştir. Mevcut bilgi güvenliği standartları ile yeni oluşturulmakta olan bilgi güvenliği standartları da bu çerçevede gözden geçirilmiştir.

**Giriş:**

Güvenlik genellikle tehlikeden korunma veya emniyet koşulu olarak tanımlanır. Bilgisayar Güvenliği, özellikle, bir sistemdeki verilerin yetkisiz ifşa, değişiklik veya imhaya karşı korunmasıdır. ve bilgisayar sisteminin yetkisiz kullanımı, değiştirilmesi veya hizmet reddine karşı korunması. Bazı bilgisayar güvenlik kontrolleri üretkenliği engellediğinden, güvenlik tipik olarak Güvenlik ve verimlilik arasında tatmin edici bir denge sağlamak için hangi güvenlik uygulayıcılarının, sistem kullanıcılarının ve sistem operasyonlarının ve idari personelin çalıştığı. Bilgi güvenliği sağlamak için kontroller fiziksel, teknik veya idari olabilir. Bu üç kontrol kategorisi ayrıca önleyici veya dedektif olarak sınıflandırılabilir. Önleyici kontroller istenmeyen olayların ortaya çıkmasından kaçının, dedektif kontroller ise meydana geldikten sonra istenmeyen olayları belirlemeye çalışır. Önleyici kontroller, bilgisayar kaynaklarının serbest kullanımını engeller ve bu nedenle yalnızca kullanıcıların kabul etmeye istekli olduğu dereceye uygulanabilir. Etkili güvenlik bilinci programları, kullanıcıların bu tür denetimlerin bilgisayar sistemlerine güvenmelerini nasıl sağladığını anlamalarına yardımcı olarak önleyici denetimlere karşı tolerans düzeyini artırmaya yardımcı olabilir. Yaygın dedektif denetimleri denetim izlerini, izinsiz giriş tespit yöntemlerini ve sağlama toplamlarını içerir. Diğer üç kontrol türü önleyici ve dedektif kontrolleri destekler. Genellikle caydırıcı, düzeltici ve kurtarma olarak tanımlanırlar. Caydırıcı kontroller, bireyleri bilişim güvenliği politikalarını veya prosedürlerini kasıtlı olarak ihlal etmekten caydırmak için tasarlanmıştır.   
Bunlar genellikle yetkisiz faaliyetler veya potansiyel bir davetsiz misafirin güvenliği ihlal etmemesini (örneğin utançtan ağır cezaya kadar uzanan tehditler gibi) tehdit etmeyi etkilemeyen izinsiz faaliyetler veya sonuç tehditlerini gerçekleştirmeyi zorlaştıran veya istenmeyen hale getiren kısıtlamalar şeklindedir. Düzeltici kontroller ya izinsiz faaliyete izin veren koşulları giderir ya da ihlallerden önce oldukları koşullara geri döner. Düzeltici kontrollerin yürütülmesi, değişikliklere neden olabilir. mevcut fiziksel, teknik ve idari kontroller. Kurtarma denetimleri, kayıp bilgi işlem kaynaklarını veya yeteneklerini geri yükler ve kuruluşun güvenlik ihlallerinden kaynaklanan parasal kayıpları kurtarmasına yardımcı olur. Caydırıcı, düzeltici ve kurtarma kontrolleri ana kategorilerde özel durumlar olarak kabul edilir. fiziksel, teknik ve idari kontroller; açıkça önleyici veya dedektif kategorilerine girmiyorlar. Örneğin, caydırıcılığın bir önleyici biçimi olduğu söylenebilir, çünkü bir davetsiz misafirin geri dönmesine neden olabilir; ancak caydırıcılık aynı zamanda davetsiz misafirin en çok korktuğu şey olan ihlalleri tespit etmeyi de içerir. Diğer yandan, düzeltici kontroller önleyici ya da dedektif değildir, ancak antivirüs yazılımı bir virüsü yok ettiğinde teknik kontrollerle veya yedekleme sırasında idari kontrollerle açıkça bağlantılıdırlar.Prosedürler zarar görmüş bir veritabanını geri yüklemenizi sağlar. Son olarak, kurtarma kontrolleri ne önleyici ne de dedektif değildir, ancak felaket kurtarma veya acil durum planları olarak idari kontrollere dahil edilir. Fiziksel, teknik ve idari kontrollerle çakışan bu sorunlar nedeniyle caydırıcı, düzeltici ve kurtarma kontrolleri bu bölümde daha fazla tartışılmamaktadır. Bunun yerine, üç ana kategorideki önleyici ve dedektif kontroller incelenmiştir.

**Physical Controls(Fiziksel Kontroller)**

Fiziksel güvenlik; kilitlerin, güvenlik görevlilerinin, rozetlerin, alarmların kullanılmasıdır.

Ve bilgisayarlara, ilgili ekipmanlara (tesisler dahil) ve işleme tesisinin kendisine erişimi kontrol etmeye yönelik benzer. Ek olarak, bilgisayarların, ilgili ekipmanların ve bunların içeriklerinin casusluk, hırsızlık ve tahribat veya kaza, yangın veya doğal afet (örneğin, sel ve depremler) nedeniyle oluşabilecek hasarlardan korunması için önlemler alınması gerekmektedir.

**Önleyici Fiziksel Kontroller**

Yetkili olmayan personelin bilgi işlem olanaklarına girmesini engellemek (yani bilgisayar kaynaklarını barındıran yerler, yardımcı programları, bilgisayar basılı kopyalarını ve girdi veri ortamlarını) önlemek ve doğal afetlere karşı korunmaya yardımcı olmak için önleyici fiziksel kontroller kullanılır. Bu kontrollerin örnekleri arasında şunlar bulunur:

• Dosyaları ve belgeleri yedekleyin

• Çitler

• Güvenlik görevlileri

• Rozet sistemleri

• Çift Kapılı Sistemler

• Kilitler ve anahtarlar

• Yedek güç

• Biyometrik erişim kontrolleri

• Yer seçimi

• İtfaiyeciler

**Dedektif Fiziksel Kontroller**

Dedektif fiziksel kontroller, koruyucu hizmetler personelini, fiziksel güvenlik önlemlerinin ihlal edildiği konusunda uyarmaktadır. Bu kontrollerin örnekleri arasında şunlar bulunur:

• Hareket dedektörleri

• Duman ve yangın dedektörleri

• Kapalı devre televizyon monitörleri

• Sensörler ve alarmlar

**Dedektif Teknik Kontroller**

Dedektif teknik kontroller personeli ihlallere karşı uyarmakta veya önleyici teknik ihlallerine teşebbüs etmektedir. Kontroller. Bunlara örnek olarak, takip eden bölümlerde ele alınan denetim izleri ve izinsiz giriş tespit uzman sistemleri dahildir.

**İdari Kontroller**

İdari veya personel güvenliği, bilgi işlem kaynakları için kabul edilebilir bir koruma düzeyi sağlamak üzere oluşturulan yönetim kısıtlamaları, operasyonel prosedürler, hesap verebilirlik prosedürleri ve tamamlayıcı idari kontrollerden oluşur. Ayrıca, idari kontroller, bilgi işlem kaynaklarına erişimi olan tüm personelin gerekli yetkilere sahip olmasını sağlamak ve uygun güvenlik izinleri.

**Önleyici İdari Kontroller**

Önleyici idari kontroller, kişilerin davranışlarını kontrol etmede personel odaklı tekniklerdir. .Bilgi işlem verilerinin ve programların gizliliğini, bütünlüğünü ve kullanılabilirliğini sağlamak..Önleyici örnekleri idari kontroller şunları içerir:

• Güvenlik bilinci ve teknik eğitim

• Görevlerinin ayrılması

• Çalışanları işe alma ve işten çıkarma prosedürleri

• Güvenlik politikaları ve prosedürleri

• Denetim

• Afet kurtarma, acil durum ve acil durum planları

• Bilgisayar erişimi için kullanıcı kaydı

**Dedektif İdari Kontroller**

Güvenlik politikaları ve prosedürlerine ne kadar iyi uyulduğunu belirlemek için dedektif idari kontroller kullanılır sahtekarlığı saptamak ve kabul edilemez bir güvenlik riski taşıyan kişilerin istihdam edilmesinden kaçınmak. Bu tip kontrolün içeriği:

• Güvenlik incelemeleri ve denetimleri

• Performans değerlendirmeleri

• Gerekli tatiller

• Arkaplan araştırması

**Sonuç:**

Bilgi güvenliği kontrolleri fiziksel, teknik veya idari olarak sınıflandırılabilir. Bunlar ayrıca önleyici ve dedektif kontrollere ayrılmıştır. Sergi 162.1, bu bölümde tartışılan kontrolleri listeler. Kuruluşun gizlilik, bütünlük ve kullanılabilirlik gereksinimlerini belirlemek için kuruluşun güvenlik politikası gözden geçirilmelidir. Kullanıcıların göz önünde bulundurmasını sağlamak için önleyici ve dedektif kontrol önlemleri arasında dikkatli bir denge kurulması gerekmektedir. Güvenlik kontrolleri makul ve kontrollerin verimliliği aşırı derecede engellememesini sağlamak. Belirli bir bilgisayar ortamına en uygun fiziksel, teknik ve idari kontrollerin kombinasyonu, nicel bir risk analizi yapılarak belirlenebilir.   
Bu genellikle pahalı, sıkıcı ve sübjektif bir süreç olduğu için, ancak gerekli bakım standardını karşılama olarak adlandırılan alternatif bir yaklaşım sıklıkla kullanılır. Uygun bakım standardını karşılayan kontroller, benzer koşullar veya ortamlarda çoğu kuruluş tarafından sağduyulu sayılabilecek kontrollerdir. Uygun bakım standardını karşılayan kontroller genellikle makul bir maliyet için hazırdır ve kuruluşun güvenlik politikasını destekler; en azından bireysel hesap verebilirlik, denetlenebilirlik ve görevlerin ayrılmasını sağlayan kontrolleri içerir.

KAYNAKÇA:

Information Security Management Handbook Kitabı

Konu: Types of Information Security Controls

(Bilgi Türleri Güvenlik kontrolleri)