

Uygun Güvenlik Çözümüne Yolculuk

Şule Küçükoğlu

Konu:

Farklılık ve rekabet avantajı sağlayan entelektüel varlıklar, organizasyonlar için çok değerlidir. Birçok varlığın kaybedilmesi durumunda bunlar kolaylıkla telafi edilebilirken, organizasyonların yaşam deneyimlerini de yansıtan "bilgi" para karşılığı kolaylıkla yerine konamamaktadır. Bilgiyi korumak, bilginin güvenliğini sağlamak artık zorunludur; eskiden olduğu gibi güvenlik sadece "ek" bir yatırım olarak değerlendirilmemeli ve bir bilgi sistemini, hatta geniş bakış açısıyla bir organizasyon tasarlanırken, bilgi güvenliği de düşünülerek bu konu çözümlerin içine gömülmelidir.

İlgilendiren Sektör ve Şirketler:

- Bilgi ve Ağ güvenliği yönetim sistemi kurmak isteyen tüm şirketler.

1. Giriş

Son 25 yıllık süreçte bilgi işleme, hesap makinesi olma işlevini aşmış, büyük miktarda ham veriyi işleyerek, önemli kararlara girdi oluşturacak yorumlanmış "bilgi" sunan akıllı bir "sistem" haline gelmiştir. Bu akıllı sistemin altyapısı oldukça karmaşıklaşır ve kontrolü güçleşirken, girdileri (veri) ile ürettiği çıktılar da (bilgi) en değerli varlıklar haline gelmiştir. Son 5 yılda, İnternet teknolojisi ile hemen her şeyin elektronikleşmesi ve iletişim ağı üzerinde yer alması kaçınılmaz olmuştur. Bu değişimin gereği, firmaların geleneksel iş yapma tarzı değişmiş, çok kritik ve hayatın bir parçası haline gelen iş uygulamalarına ve verilere erişememe – giderek azalan sürelerde – kabul edilemez olmuştur.

Organizasyon bilgi ve süreçlerine yönelik güvenlik tehditleri artık iş kalitesi ve verimliliğine yönelik tehditler demektir. İşte bu noktada, bir akıllı sistemi kurgularken, bilgi güvenliğini sağlamaya yönelik çözümleri de kontrol listesi içinde bulundurmak, çözümün içine gömmek artık vazgeçilmezdir, hayattır. Çünkü, bilgi güvenliği basitçe, "iş"inizi kesintiye uğratmaksızın devam ettirmenizi garantileyecek önlemleri alma yolculuğudur.

2. Yolculuğa Hazırlık

Güvenlik yolculuğunun ilk adımı, ilgili riskleri ve gereksinimleri doğru saptamaktır. Güvenlik konusunda, en optimum çözümlere karar verilebilmesi, "Nelerin?", "Ne derecede?", "Neye karşı?" ve "Nasıl?" korunması gerektiğinin bilinmesi ile mümkündür.

Bu, "güvenlik değerlendirmesi" sürecidir. Bu süreçte, şu konu başlıkları dikkate alınmalıdır:

2.1. Bilgi Varlıklarının Analizi ve Sınıflandırılması: Bu analiz, nelerin korunması gerektiğini ortaya çıkaracak çalışmadır. En kritik ve önemli varlıklar, bunların kaybı durumunda oluşacak doğrudan ve dolaylı (imaj kaybı vb.) finansal kayıpların büyüklüğü göz önünde tutularak sınıflandırılmalıdır.

2.2. Temel güvenlik hedefleri belirlenmesi: Bilgi güvenliğinin temel kavramları olan "erişilebilirlik", "gizlilik" ve "bütünlük"e ilişkin güvenlik hedefleri belirlenmelidir.

2.3. Risk analizi: Bir sistemin nasıl korunacağına karar vermeden önce, onu hangi tehlikelere karşı korumak gerektiği bilinmelidir. Coğrafyanın karakteristiğinden, teknik hatalara, intikam almak isteyen eski çalışanlardan "hacker"lara kadar tüm riskler göz önünde tutulmalıdır.

Risk analizi metodolojilerinden bazıları (nicel), bir riskin gerçekleşmesi olasılığı ile gerçekleşme durumunda ortaya çıkacak kayıpları gözönünde tutarken, yaygın olan yöntem, yanıtıcı ve sübjektif olan olasılık verileri göz ardı edilerek, sadece kayıpların düşünüldüğü "nitel" yaklaşımdır. Çoğu nitel metodoloji, birbiriyle ilintili birkaç önemli öğeden yararlanır:

Tehditler: Bunlar yolunda gitmeyen ve bir sistemi çalışmaktan alıkoyabilecek her şeydir: Yangın, suiistimal, dikkatsiz çalışanlar vb. Her sistem için, her zaman tehditler vardır.

Açıklar: Açıklar, bir sistemin tehditlere maruz kalmasını ve tehdidin etkili olma olasılığını artıran unsurlardır. Yangın çıkma riski olan bir yerde yanıcı maddelerin bulunması bir açık örneğidir.

Kontroller: Bunlar, açıklara karşı alınması gereken "karşı önlemler"dir:

- Caydırıcı önlemler, kasıtlı tehditlerin oluşmasını önlemeye yöneliktir.
- Önleyici nitelikte olanlar, açıklardan korunma ve bir tehdidin gerçekleşme olasılığı ile etkilerini azaltma amaçlıdır.
- Düzeltici önlemler, gerçekleşmiş bir tehdidin etkilerini azaltır.
- Algılama ve tespiti yönelik önlemler, saldırıları algılayarak önleyici ve düzeltici eylemlerin devreye alınmasını sağlarlar.

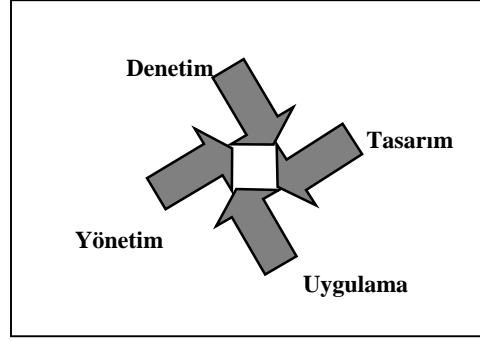
2.4. Etki Analizi: Bir riskin gerçekleşmesinin ardından ortaya çıkacak etkiler ve bedellerin (işe zararlar) anlaşılması çalışmasıdır. Bunlar firmalara göre çok değişken olacağı gibi, riskin türüne göre de değişecektir: firma sırlarının açığa çıkması, finansal verilerin üzerindeki oynamalar, sahte para transferleri vb.

3. Bilgi Güvenliği Bir BT İşi Değildir

Hep adreslendiğinin aksine, bilgi güvenliği sadece bir Bilgi Teknolojisi ya da yine yaygın söylemle Bilgi Sistemleri işi değildir; kurumun her bir çalışanın katkısını ve katılımını gerektirir. Ciddi boyutta bir kurum kültürü değişimi gerektirdiği için, en başta yönetimin onayı, katılımı ve desteği şarttır. BT'nin teknik olarak gerekli olduğunu saptadığı ve uyguladığı teknik güvenlik çözümleri, iş süreçleri ve politikalarla desteklenmemiş ve kurum kültürüne yansıtılmamışsa etkisiz kalacaklardır. Gerekli inanç ve motivasyon yaratılmamışsa, çalışanlar şifrelerini korumakta özensiz, hassas alanlarda gördükleri yabancı kişilere karşı aldırılmaz, kağıt çöpe gerekli imha işlemi yapmadan atacakları bilgilerin değeri konusunda dikkatsiz olabilecekler ve yapılan güvenlik yatırımlarına karşın büyük bir açık oluşturmaya devam edebileceklerdir.

4. Güvenlik Bir Süreçtir

Türkçe sözlükte süreç "Aralarında birlik olan veya belli bir düzen içinde tekrarlanan, ilerleyen, gelişen olay veya hareketler dizisi" olarak açıklanmıştır. Güvenlik de değerlendirme, tasarım, uygulama ve yönetme süreçlerinden oluşan bir yaşam döngüsüdür. Değerlendirme, bulunduğunuz durumun analizidir. Değerlendirme süreci, işinizin devamı için kritik öğeler (fiziksel ve entelektüel varlıklarınız), bu varlıklara yönelik tehditler ve açıklar , tehditleri ortadan kaldırmaya ya da etkilerini azaltmaya yönelik önlemler nelerdir sorularının detaylı yanıtlarını ortaya çıkaracaktır. Bu sonuçlara dayanarak en verimli (mümkün olan en düşük maliyetle, tüm ihtiyaçları karşılayacak) güvenlik çözümü mimarisi tasarımındadır sıra.



Bu tasarımın uygulanması ve organizasyona entegrasyonu ile iş bitmez. Bundan sonra kesintisiz devam edecek olan ve çözümlerin güncellenerek sağlıklı yaşamasını sağlayacak olan yönetim süreci başlamalıdır. Bu süreç boyunca, gelişen ve yeni ortaya çıkan tehditlerin takip edilip, yeni önlemlerin/kontrollerin devreye girmesi, süreci aksatan öğelerin belirlenmesi ve iyileştirilmesi, gözden kaçan ya da yeni ortaya çıkan açıkların kapatılması gereklidir. Bunun ön koşulu da organize olarak (belli rol ve sorumluluklar atayarak), detaylı iş süreç dokümanları oluşturarak işi şansa bırakmamaktır. Yönetim süreci, belli aralıklarla döngünün ilk süreci olan değerlendirme sürecini işleterek çıktılarını kontrol etmek zorundadır.

Yüzde yüz güvenlik sağlamanın mümkün olmadığı bilinir. Bu döngünün amacı, caydırıcı, önleyici, düzeltici ve algılayıcı kontrollerle riskleri, tehditleri, açıkları ve işimize etkilerini önemli ve kabul edilebilir ölçüde azaltmaktır.

Bireysel olarak yaşamın her anında riskleri analiz edip karşı önlemler geliştirmeye çalışırız. Evimize hırsız girmesi olasılığını tahmin etmeye çalışırız; istatistik verilerden (komşuların anlattıkları, duyduklarımız) yararlanırız, riskleri ve etkilerini değerlendirmek için, koşulları gözden geçirir (zemin katta oturuyoruz ve pencerelerde parmaklık yoktur ya da çelik kapımız yoktur vb.), tehdit gerçekleşirse kayıplarımızı düşünürüz (çokça ziynet eşyası bulunduruyoruz ya da çocuğumuz öğleden sonraları evde yalnız kalmak durumundadır vb.). Bu değerlendirme sonucunda çeşitli caydırıcı (Çelik kapı, pencerelere koruma çözümü, çelik kasa vb.), önleyici (çocuğumuza çok yönlü tembihler ve uygulanacak kurallar - yabancılarla nasıl konuşulacağı, kapı açma kuralları vb.-), algılayıcı (kapı ve pencere alarmı vb.) önlemleri devreye almaya karar veririz. Bu süreç, komşunun başına bir şey gelmesi durumunda, durumun incelenerek göz ardı edilen bir açığın olduğunun fark edilmesi ve bunun için önlem alınması, varolan önlemlerin yeniden gözden geçirilmesi şeklindeki denetim ve iyileştirmelerle devam edecektir.

Aynı kaçınılmazlıkla, işimizin ayakta kalması hedefiyle bilgi varlıkları için risk analizi yapmak ve karşı önlemleri almak, bu süreçleri yaşam döngüsü haline getirmek zorunludur.

Kaliteyi ve standartları yaşam döngüsünün parçası olarak gören firmalar, 1999 yılı sonunda duyurulan ISO 17799 güvenlik standartlarına uyumluluklarını değerlendirmek yoluyla, değerlendirme sürecine daha geniş bir vizyonla ve daha objektif yaklaşmış olacaklardır. ISO 17799 standardı, bir standarttan çok bir "yönetim sistemi" olarak ifade edilen BS 7799'dan türetilmiştir. BS 7799'a göre, diğer iş varlıkları gibi, bilgi de kurum için değerli bir varlıktır ve uygun şekilde korunması gereklidir; bilgi güvenliği teknik bir süreçten çok bir yönetim sürecidir.

ISO 17799, Bilgi Güvenliğini,

- Güvenlik Politikaları
- Güvenlik Organizasyonu
- Varlıkların Sınıflandırılması ve Kontrolü
- Personel Güvenliği
- Fiziksel ve Çevresel güvenlik
- İletişim ve Operasyonel Yönetimde Güvenlik
- Sistem Erişim Kontrolü

- Sistem Geliştirme ve Bakımı
- İş Süreklilik Planları
- Uyumluluk

gibi önemli 10 ana konu başlığı altında geniş bir açıdan ele alır.

Her bir başlık altında, yapılması önerilen işlerin çıktıları olan güvenlik politikaları, süreçler, rol ve sorumluluklar, talimatlar, tanımlar, anlaşmalar, planlar vb. belge haline getirilip, diğer kurum varlıkları gibi uygun şekilde yönetilmeli ve korunmalıdır. Belgeleme, kurum standartlarını ve prensiplerini ödünsüz yaşatabilmek, işi aynı kalite ve verimlilikte devam ettirebilmek açısından en önemli konudur.

Güvenlik Politikası: Hedef, bilgi güvenliği konusunda yönetimin bakış açısını, onayını ve desteğini iletmektir. Güvenlik sürecinin, ciddi boyutta bir kültür değişimi gerektirdiği hatırlanırsa, hem birçok önemli konuda organizasyonun kural ve yasalarını yansıtması, hem de yönetimin ciddi yaklaşımını ve kararlılığını yansıtması anlamında güvenlik politika dokümanı vazgeçilmezdir.

Bu doküman, bilgi güvenliğinin tanımını içermeli, hedeflerini ve önemini vurgulamalıdır. Kurumun konuya yaklaşımını yansıtacak şekilde önemli görülen her konuyla ilgili kuralları, prensipleri, standartları ve yasalarla uyumluluk açısından önem taşıyan istekleri içermelidir.

Politika dokümanı tüm çalışanlarla, kurumun uygun göreceği şekilde paylaşılmalı, ulaşılabilir ve anlaşılabilir olmalıdır. Politika dokümanının bir sahibi olmalı ve değişen koşullara göre dokümanın değişim yönetimini sağlamalıdır.

Güvenlik Organizasyonu: Hedef, bilgi güvenliği organizasyonel altyapısının oluşturulması ve yönetilmesidir. Tasarlanan bilgi güvenliği çerçevesinin organizasyon içinde uygulamaya alınması için gerekli rol ve sorumlulukların belirlenmesi, tüm rollerin işbirliği içinde çalışabilmeleri için iş süreçlerinin oluşturulması zorunludur. Bu organizasyon içinde en önemli misyon güvenlik değişim yönetiminin yapılmasıdır. Riskler, iş yapış biçimi, organizasyonel değişimler, bilgi varlıkları, iş ilişkileri, iş ortakları vb. açısından sürekli değişim göz önünde tutularak, güvenlik politikası, organizasyonu ve süreçleri değişim yönetimi yapılmalı ve gerekli düzenleme ile geliştirmeler hayata geçirilmelidir.

Varlıkların Sınıflandırılması ve Kontrolü: Uygun şekilde korunmalarının sağlanması için, organizasyon için önemli görülen tüm bilgi varlıkları belirlenmeli ve sahiplikleri ile sorumlulukları belli kişilere verilmelidir.

Bir varlık envanteri çıkarılarak, tüm varlıklar için organizasyon açısından görece değer ve önem dereceleri ile derecelendirilmeleri risk yönetimi açısından büyük önem taşır. Önemli varlıklar, veritabanları, kullanıcı el kitapları, operasyon ve destek süreçleri, devamlılık planları gibi bilgi varlıkları, sistem ve uygulama yazılımları, geliştirme araçları gibi yazılım varlıkları, bilgisayar donanımı, iletişim donanımı, teyp ve disk gibi manyetik taşıyıcılar gibi fiziksel varlıklar ve bilgisayar ve iletişim servisleri, güç, ısıtma, ışıklandırma, havalandırma gibi servisler olarak sıralanabilir.

Varlık envanter dokümanı oluşturulmalı, varlıkların şu an buldukları yer bilgisi tutulmalı, tüm varlıklar için değer ve önemini yansıtan (gizlilik vb.) bir etiketleme yöntemi düşünülmeli ve bu varlıkların nasıl ele alınacağına ilişkin süreçler belirlenmelidir (örneğin çok gizli bilgilerin kopyalanması, saklanması, elektronik posta ile gönderiminin nasıl olması gerektiğine vb. ilişkin süreç/talimatlar).

Personel Güvenliği: Güvenliğe yönelik insan hatası, hırsızlık, kötüye kullanma risklerini azaltmak amacıyla, tüm çalışanların iş sorumlulukları içinde güvenlikle ilgili maddeler açıkça belirtilmeli, işe alımlarda uygun kontroller yapılmalı ve gizlilik anlaşmaları imzalanmalıdır.

En büyük riskin bilgi ve bilinç eksikliği olduğu düşünülerek, kullanıcıların güvenlik bilincini ve farkındalığını artırmak üzere eğitimler düzenlenmeli, organizasyon güvenlik süreçleri, riskleri, bilgi işleme olanaklarının doğru kullanımı anlatılmalıdır.

Fiziksel ve Çevresel Güvenlik: İş fonksiyonlarına ve bilgi varlıklarına müdahale, yetkisiz erişim ve olası zararların önlenmesi hedeflenerek, fiziksel güvenlik sınırları açıkça belirlenmeli ve bu alanlar kullanım amaçları ile hassasiyet durumlarına göre uygun şekilde korunmalıdır.

Yetkisiz erişimi önlemek amacıyla, uygun fiziksel giriş kontrolleri konulmalı, ziyaretçilerin hassas alanlara erişimi önlenmeli ya da kontrollü gerçekleştirilmelidir. Hassas bilgi ve bilgi işleme servislerine erişim sadece yetkili personelle sınırlı olmalıdır. Tüm çalışanların açıkça görülebilen kurum kimlik kartı taşımaları sağlanmalıdır. Hassas alanlara erişim kayıtları tutulmalı ve düzenli olarak gözden geçirilmelidir. İçinde personel bulunmadığı zamanlarda hassas alanlar kilitli tutulmalıdır. Yükleme ve dağıtım alanları gibi genele açık olabilecek alanlar mümkünse bilgi işleme alanlarından izole edilmelidir. Tüm fiziksel giriş-çıkış kapılarının kontrol altında tutulması için gerekli çözümler uygulanmalıdır.

İletişim ve Operasyonel Yönetim: Bilgi işleme servislerinin doğru ve güvenli şekilde çalıştırıldığından emin olmak üzere gerekli önlemlerin alınması zorunludur. Bu servislerin operasyon ve yönetimine ilişkin sorumluluklar ve süreçler oluşturulmalı ve uygulamaya alınmalıdır. Farklı sorumlulukların belirgin şekilde ayrılması, kaza ya da kasıt yoluyla yanlış kullanım risklerini azaltmak yönünden çok gereklidir. Yine, geliştirme/test ve operasyon ortamlarının birbirinden ayrılmış olması ve geliştirme ortamından operasyona geçiş için süreçler oluşturulmalıdır. Sistem hatası risklerini azaltmak amacıyla, kapasite planlama ve sistem kabulü süreçleri hazırlanmalıdır. Yeterli kaynaklara ve kapasiteye sahip olunup olunmadığından emin olmak, detaylı planlama ve hazırlık gerektirir. İşin devamı için vazgeçilmez olan bilgi ve yazılımların yedeğinin düzenli ve kontrollü olarak alınması sağlanmalıdır. Operasyon personelinin tüm aktivitelerinin kayıtları tutulmalıdır. Ağ üzerinde dolaşan bilgilerin ve ağ altyapısını oluşturan birimlerin uygun şekilde korunmasının sağlanması için, ağ operasyonu sorumluluğu ile bilgisayar operasyonu sorumlulukları birbirinden ayrılmalı, ağ üzerinde dolaşan bilgilerin güvenliği için gerekli çözümler uygulanmalı, süreçler oluşturulmalı ve gerekli talimatlar politika dokümanına yansıtılmalıdır.

Organizasyonlar arası bilgi ve yazılım değişiminin söz konusu olduğu durumlarda, bilginin kaybolması, değiştirilmesi ve kötüye kullanılmasını engellemek üzere kontrol mekanizmaları devrede olmalı, organizasyonlar arası anlaşmalar imzalanmalı, dolaşım halindeki bilginin korunumu için kural ve standartlar belirlenmelidir.

Erişim Kontrolü: İş ve güvenlik gereklilikleri doğrultusunda, bilgi ve iş servislerine erişim kontrol altında tutulmalıdır. Sadece gerekli olan personele, gerektiği kadar erişim yetkisi sağlanmalı, erişim kontrolü kuralları ve süreçleri belirlenmelidir. Kullanıcı kayıt, kullanıcıya tanınan ayrıcalık özellikleri, kullanıcı şifre yönetimi, erişim haklarının gözden geçirilmesi gibi işlemler için detaylı talimatlar oluşturulmalı, her bir konuya ilişkin isterler/kurallar politika dokümanına yansıtılmış olmalıdır. Kullanıcılar erişim hakları ile bu konuda kendi sorumluluk ve yükümlülükleri hakkında bilgilendirilmiş, bilinçlendirilmiş olmalıdır.

Ağ servislerine yetkisiz erişimler, tüm organizasyonu etkileyecek risklerdir. Kullanıcılara sadece, kendi işlerinin devamı için gerekli olacak doğrudan ağ bağlantısı sağlanmalı, kullanıcı terminalinden bilgisayar servisine kadar tüm ağ servisi kontrol altında olmalıdır. Gerektiğinde iletişim, ayrılmış hatlar üzerinden sağlanabilmeli, belli kullanıcılar için menü ve alt menüler kısıtlanmalı, ayrı mantıksal ağ alanları tanımlamak yoluyla ağ erişimi sınırlandırılabilir, dış bağlantılar için kullanıcı doğrulama çözümleri kullanılmalı ve gerekli durumda bağlantı süresi kısıtlanabilmelidir.

Sistem Geliştirme ve Bakımı: Geliştirilen bilgi sistemleri iş uygulamalarının, tüm güvenlik isterlerini karşılmasını ve organizasyon güvenlik politikalarını destekleyecek şekilde planlanıp tasarlanmasını garantilemek üzere, güvenlik isterleri tanımlanmalı ve belgelenmelidir. Uygulama sistemi verilerinin kaybını, yetkisiz değişimini ve kötüye kullanımını önlemek üzere, gerekli kontroller uygulama içine yerleştirilmeli, kullanıcı ve işlem kayıt bilgilerinin uygulama tarafından tutulması sağlanmalıdır. Veri girişinde hataya neden olabilecek ya da uygulama güvenlik açığı oluşturabilecek konular düşünülerek kontroller konulmalı, gerekli kodlama yapılmalı ve test edilmelidir. Gerektiğinde mesaj doğrulama teknikleri, kriptografik çözümler uygulanmalıdır.

Program kaynak kodlarının da uygun şekilde korunması esastır. Program kaynak kodları operasyon sistemi üzerinde tutulmamalı, erişim hakları sınırlı olmalı ve uygun şekilde yedeklenmelidir.

İş Devamlılığı Yönetimi: Güvenlik sürecinin en önemli kavramlarından biri iş devamlılığı yönetimidir. Büyük çaplı sistem çökmeleri, arızalar ya da doğal felaketler gibi durumlarda, kritik işlerin devamını sağlayabilmek üzere gerekli önlemler alınmalıdır. Bu konuda önlem ve çözümlere karar vermek üzere, öncelikle iş devamlılık ve etki analizi yapılmalıdır (donanım arızası, sel, yangın gibi durumlarda oluşacak zararların boyutları saptanır vb.). Belirlenen risklerin gerçekleşmesi durumunda, işin belli seviyede devamı için yapılacaklar, sorumluluklar, iletişim bilgileri, operasyon detayları, acil durumu ortadan kaldırmak üzere yapılması gerekenler belirlenerek belgelenmelidir. Yapılan acil durum planları düzenli aralıklarla test edilmeli ve doğrulanmalıdır; test sonuçlarına göre gerektiğinde yeniden düzenlenmelidir.

Uyumluluk: Bilgi sistemleri tasarımı, operasyonu, kullanımı ve yönetimi birtakım kanuni, düzenleyici veya sözleşmeye dayalı yaptırımlara tabi olabilir. Bu başlık altında, bu yaptırımların ve ilgili güvenlik gerekliliklerinin ihlalinin önlenmesi hedeflenmelidir. Örneğin fikri haklara ilişkin yasalarla uyum için ilgili süreçler, kural ve politikalar belirlenmeli ve belgelenmelidir. Yasal gereklilik nedeniyle belirli süreyle saklanması gereken kayıtlar kayıp, imha ve sahtekarlık risklerine karşı uygun şekilde korunmalıdır. Bilgi sistemlerinin organizasyon güvenlik politikaları ve standartlarıyla uyumluluğu, düzenli aralıklarla denetlenmelidir.

Sonuçlar ve Öneriler

Bilgi güvenliği sürecinin ilk adımı olan güvenlik değerlendirmeleri bu konuda ISO standardının önerdiği başlıklar göz önünde tutularak, geniş bir bakış açısıyla gerçekleştirildiğinde, ortaya çıkacak veriler, tüm yolu aydınlatacak bilgilerdir. Bu geniş kapsamlı çalışma, organizasyonun her başlık altında var olan risklerini, tehditlerini, açık ve eksikliklerini gözler önüne serecek ve çok detaylı önlem ve çözüm önerileri sunacaktır. Bu veriler, detaylı olarak çözüm ve önlemleri yaşam döngüsü içine entegre edecek ve yaşatacak anahtarları da elimize verecektir. Bu değerli "bilgi" artık verimli ve uygulanabilir bir güvenlik çözümü tasarlama ve projelendirme aşamasında kullanılabilir.

Referanslar

[1] BSI, 2001. Information technology – Code of practice for information security management BS ISO/IEC 17799:2000 BS 7799-1:2000

[2] Sean Boran, 2001. IT Security Cookbook

[3] Information Systems Audit and Control Assosiation, 2002. CISA Review Manual