

Doküman Kodu: BGYS-0003

BGYS - VARLIK ENVANTERİ OLUŞTURMA VE SINIFLANDIRMA KILAVUZU

SÜRÜM 1.00

20.03.2008

Hazırlayan: Fatih KOÇ

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Arařtırma Enstitüsü (UEKAE)'nin misyonu, "bilgi güvenliđi, haberleřme ve ileri elektronik alanlarında Türkiye'nin teknolojik bađımsızlıđını sađlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliđi, haberleřme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulařılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuvarlarında temel ve uygulamalı arařtırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sađlanmaktadır.

Bu doküman, BGYS (Bilgi Güvenliđi Yönetim Sistemi) kurmak isteyen kurumlar için yardımcı kaynak olarak hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

Bu dokümanda anlatılanlar tamamen tavsiye niteliğindedir. UEKAE, yapılan uygulamalardan doğabilecek zararlardan sorumlu değildir. Bu doküman UEKAE'nin izni olmadan deđiřtirilemez.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeđi geçen Ađ Güvenliđi personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Ali DİNÇKAN'a, Burak BAYOĐLU'na ve Bilge KARABACAK'a teşekkürü borç biliriz.

İÇİNDEKİLER

1. GİRİŞ	5
1.1 Amaç ve Kapsam.....	5
1.2 Hedeflenen Kitle.....	5
1.3 Kısaltmalar.....	5
1.4 Tanımlar.....	6
2. VARLIK ENVANTERİ OLUŞTURMA	8
3. SINIFLANDIRMA.....	12
3.1 Varlık Değerleme / Derecelendirme	14
3.2 Varlık Sınıflandırma	14
4. VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI	15
5. BİLGİ ETİKETLEME VE İŞLEME	15
6. SONUÇ	16
KAYNAKÇA	17

1. GİRİŞ

Bilginin etkin bir şekilde korunması, risk analizi çalışmasının sağlıklı bir şekilde yapılabilmesi için bilgi varlıklarını da içeren tüm varlıkların envanterinin çıkarılması ve sınıflandırılması gereklidir. Varlık envanterinin doğru bir şekilde hazırlanması varlıkların önem ve değeri hususunda bir fikir verecektir. Envanter hazırlanması ardından Bilgi Güvenliği Yönetim Sistemi kuran, işleten bir organizasyonda varlık envanterinin sorumlusunun ve envanterin bulunduğu yerin belirlenmesi gereklidir.

1.1 Amaç ve Kapsam

Bu doküman, bir kurumda kurulması planlanan Bilgi Güvenliği Yönetim Sistemi kapsamında yapılacak tüm çalışmaların temelinde yer alan varlıkların envanterinin oluşturulmasına ve varlıkların sınıflandırılmasına kılavuzluk etmek amacıyla hazırlanmıştır.

Bilgi Güvenliği Yönetim Sistemi kurulumu sırasında ilk adımlardan biri olan Varlık envanterinin oluşturulması 2. bölümde ele alınmıştır. Varlık envanteri oluşturulması başlığında envantere olması beklenen varlık bilgilerine değinilmiş, örnek bir varlık envanter tablosu hazırlanmıştır. Varlık sınıflandırması 3. bölümde ele alınmıştır. Varlık sınıflandırması başlığında varlıkların değerlerinin belirlenmesinde kılavuzluk edecek bilgiler sunulmuş, açıklamalar yapılmıştır. Varlık sınıflandırmasının ardından hangi sınıftaki varlığın hangi ortamlarda bulunabileceği, bu varlığın nerelerde saklanabileceği ve bu bilgilerin hangi şartlarda ve ne şekilde kimlerle paylaşılacağı hususlarına 4. bölümde değinilmiştir. Son olarak sınıflandırması yapılmış varlıkların etiketlenmesi ile ilgili hususlara 5. bölümde değinilmiştir.

1.2 Hedeflenen Kitle

Bu doküman, Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulması planlanan veya BGYS işletilen bir kurumda BGYS sorumlusu veya envanter sorumlusu tarafından bir kılavuz olarak kullanılabilir.

1.3 Kısaltmalar

BGYS : Bilgi Güvenliği Yönetim Sistemi

UEKAE : Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü

1.4 Tanımlar

Varlık: Bir işletme için değeri olan ve bu nedenle uygun olarak korunması gereken tüm unsurlardır. İnsan, bilgi, yazılım, donanım, bina, iş araç ve gereçleri gibi işletme için bir değer ifade eden tüm unsurlar varlık olarak değerlendirilmelidir. Örneklerde verilen varlıklar içerisinde en soyut olanı bilgidir. Bilgi bir organizasyonda her yerde bulunabilir. Donanımlar ve yazılımlar bilgiyi işler, donanımlarda ve medyalarda (CD, USB depolama üniteleri) depolanır, dokümanlarda yazılı olarak bulunur. Kurum çalışanlarının zihinlerinde, konuşmalarında bulunur.

Varlık kavramı için örnekler:

- a) Bilgi varlıkları: Kurumun tüm bilgi sistemlerinde, çalışanlarında, kütüphanelerinde tutulan ve kurumun iş süreçlerinde değişik formlarda işlenen veridir;
- b) Yazılım varlıkları: Uygulama yazılımları, sistem yazılımları, geliştirme araçları;
- c) Fiziksel varlıklar: Bilgisayar bileşenleri (işlemciler, ekranlar, diz üstü bilgisayarlar, modemler), manyetik ortamlar (kayıt cihazları ve diskler), diğer teknik araçlar (güç kaynakları, havalandırma üniteleri), mobilya, yerleşim düzeni;
- d) Servisler (Hizmetler): Bilgi işleme ve haberleşme servisleri (web servisi, e-ticaret servisi, ftp servisi), genel faydalar; örneğin ısınma, ışıklandırma, elektrik, havalandırma.
- e) İnsan: Kurum çalışanları da kurum varlığı olarak düşünülmelidir.

Gizlilik: Bilginin içeriğinin görüntülenmesinin, sadece bilgiyi/veriyi görüntülemeye izin verilen kişilerin erişimi ile kısıtlanmasıdır. (Ör: Şifreli e-posta gönderimi ile e-postanın ele geçmesi halinde dahi yetkisiz kişilerin e-postaları okuması engellenebilir)

Bütünlük: Bilginin yetkisiz veya yanlışlıkla değiştirilmesinin, silinmesinin veya eklemeler çıkarmalar yapılmasının tespit edilebilmesi ve tespit edilebilirliğin garanti altına alınmasıdır. (Ör: Veri tabanında saklanan verilerin özet bilgileri ile birlikte saklanması, dijital imza)

Erişilebilirlik/Kullanılabilirlik: Varlığın ihtiyaç duyulduğu her an kullanıma hazır olmasıdır. Diğer bir ifade ile, sistemlerin sürekli hizmet verebilir halde bulunması ve sistemlerdeki bilginin kaybolmaması ve sürekli erişilebilir olmasıdır. (Ör: Sunucuların güç hattı dalgalanmalarından ve güç kesintilerinden etkilenmemesi için kesintisiz güç kaynağı ve şasilerinde yedekli güç kaynağı kullanımı). Bu dokümanda “**Erişilebilirlik**” olarak kullanılacaktır.

Varlık Sahibi: Varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir. Sahip kelimesi Türkçe de *mülkiyet* anlamını içinde barındırmaktadır. BGYS Varlık yönetimindeki sahip kavramı daha çok *sorumluluk* anlamında kullanılmaktadır. Varlık değerinin belirlenmesi, varlığa yönelik risk tanımlamalarının yapılması varlık sahibinin görevleri arasındadır. (Ör: Kurum finansal bilgilerinin sahibi kurumun finans bölüm müdürüdür)

Varlık Emanetçisi: Varlığın sahibi olmamasına rağmen, varlığın sağlıklı bir şekilde sürekliliğinin idamesini sağlayan rolündeki kişi veya kişilerdir. Birçok durumda varlık sahibi ile farklı kişi olabilir. (Ör: Kurum finansal bilgilerinin sahibi finans bölümü müdürü iken emanetçisi ilgili veri tabanı yöneticisidir)

2. VARLIK ENVANTERİ OLUŞTURMA

Bir organizasyonda varlıkların belirlenmesi ve varlıklara değer atanması, risk analizi süreci için temel bir adımdır. Varlıklara değer atanmasının yapılabilmesi için bir envantere ihtiyaç vardır. Bir çok organizasyonda envanter denince ilk akla gelen bir çeşit “zimmet listesi”dir. BGYS ilk defa kurulmaya çalışılırken başlangıç noktası olarak bu “zimmet listesi” kullanılabilir. Özellikle fiziksel ve yazılımsal varlıklar için zimmet listesi faydalı olacaktır. Ancak zimmet listesi BGYS için gerekli ve yeterli detaya sahip olmayabilir. Zimmet listesi, BGYS için çok önemli olan bilgi varlıklarının tespitinde yetersiz kalabilir.

Organizasyon içinde bir “varlık yönetim kılavuzu” veya “varlık envanteri yönetim kılavuzu” hazırlanmasında fayda vardır. Bu kılavuzda özellikle envantere yeni bir varlığın eklenmesi, envanterden varlık çıkarılması ve envanter sorumlusu net olarak belirtilmesi gerekir.

BGYS için varlık envanteri hazırlanırken öncelikle, tüm varlıkların kapsandığından emin olmak için gruplandırma yapmak varlıkların tanımlanması işini kolaylaştıracaktır. Bilgi varlıkları, yazılımsal varlıklar, fiziksel varlıklar, servisler vb. bir gruplandırma yapılabilir.

Bilgi güvenliği açısından bir donanımın bütünlüğünden söz etmek çok zordur. Bu sebeple asıl korunması ve yönetilmesi gereken bilgi veya süreçleri değerlendirmek, ardından bu bilgi ve süreçleri sağlayan veya barındıran donanım ve yazılımı güvenlik açısından incelemek ve sınıflandırmak daha kolay olacaktır. Diğer varlıklar düşünüldüğünde (yazılım, donanım, fiziksel varlıklar ve insan) bilgi ve süreçler en soyut kavramlardır ve güvenliğin üç temel ögesi (gizlik, bütünlük, erişilebilirlik) için derecelendirmenin kolaylıkla yapılabileceği varlık gruplarıdır.

Oluşturulacak varlık envanteri için öncelikle bilgi varlıkları belirlenmelidir. İlgili bilgi varlığını taşıyan, saklayan ortamların (yazılım, donanım gibi) ilgili bilgi varlığının hemen ardından envantere işlenmesinde envanterin okunabilirliği ve düzenli olması açısından faydası büyüktür.

Ardından süreç varlıkları belirlenmelidir. Organizasyondan organizasyona değişmekle birlikte, bir organizasyonda birçok süreçten söz etmek mümkündür. Fakat bu süreçlerin tamamı BGYS kapsamında değerlendirilemeyebilir. Özellikle ele geçirilmemesi, değiştirilmemesi gerekli bilgiler içeren süreçler veya sürekliliği organizasyonun iş hedefleri ve itibarı için önemli olan süreçler BGYS kapsamında değerlendirilebilir (örneğin web servisi, personel özlük bilgileri).

Varlık envanteri birden fazla tabloda tutulabileceği gibi tek bir tabloda da tutulabilir. Şayet organizasyon içindeki varlık sayısı çok yüksek mertebelerde ise varlıklar yazılım, donanım, bilgi, süreç gibi ayrı ayrı envanterlerde tutulmasında fayda vardır. Tek bir envanter halinde tutulmak istenirse, varlıkları envantere mantıksal gruplar halinde işlemek tüm varlıkların kapsandığından emin olunmasını sağlayacaktır. Örneğin; “web servisi” değerlendiriliyorsa bu servis ile ilgili olarak gerekli varlıklar ardı ardına envantere işlenmelidir. Örneğin web servisi, “web sunucusu yazılımı –X yazılımı–” ile “web sunucusu donanımı –Y donanımı–” üzerinde çalışmakta ve sistem yöneticisi tarafından idamesi sağlanmaktadır).

Varlık envanteri, olası bir felaket esnasında veya sonrasında, kurtarma veya geriye dönme işlerinde kullanılmak üzere gerekli detayları içermelidir. Varlık tipi, formatı, bulunduğu yer, yedek bilgileri, lisans bilgileri ve ticari bilgileri bulunmalıdır.

Varlık envanterinin aşağıda tanımlanan bilgileri içermesi tavsiye edilir:

Varlık: Tabloda bu bölüme varlığın adı yazılır varlıkların birbirinden ayrılması için gereklidir.

Varlık Grubu: Varlık envanterinin okunabilirliğini arttırmak ve düzenli bir yapıda olmasını sağlamak maksadı ile varlıklar gruplandırılabilir. Mantıksal olarak benzer iş için kullanılan varlıklar bir grupta bulunabileceği gibi (ör: dokümanlar, kılavuzlar, altyapı sistemi, e-posta servisi vb.) iş süreçleri çerçevesinde bir gruplandırma (ör: iş sürekliliği süreci) yapılabilir. Ayrıca varlıklar, mantıksal olarak varlık grupları altında listelenebilirler. Varlık grubu veya varlığın adı yazılır. Ör: Kablosuz ağ sistemi, uygulama ve veri tabanı sistemi.

Kategori: Varlık envanterinde anlaşılabilirliğin artırılması maksadıyla varlıklar ortak kategoriler altında derlenebilirler. Sunucu, yazılım, donanım, medya, doküman, kılavuz, tablo, bilgi, kurum çalışanı vb ortak özelliklere sahip varlıklar bu kategori altında listelenebilir.

Varlık Sahibi: Varlık sahibi, tanımlanan rol ve sorumluluklara paralel olarak belirlenir. (Ör: Muhasebe Bölümü Müdürü)

Emanetçi: Varlığın –varsa– emanetçisini belirtir. (Ör: Ağ Yöneticisi)

Bulunduğu yer: Varlığın bulunduğu fiziksel yeri belirtir.(Ör: Sistem odası)

Gizlilik Değeri: Varlığın yetkisiz kişilerce erişilmesi sonucu doğacak zararı belirtir.

Bütünlük Değeri: Varlığın bütünlüğünün bozulması sonucunda doğacak zararı belirtir.

Erişilebilirlik Değeri: Varlığın erişilebilirlik açısından önemini belirtir.

Gizlilik, bütünlük ve erişilebilirlik değerleri için bir referans tablo örneği Tablo 2’de verilmiştir.

Değer: Gizlilik, bütünlük ve erişilebilirlik değerleri kullanılarak belirlenebilecek bir değerdir.

Varlığın Eklenme Tarihi: Varlığın, varlık listesine eklenme tarihidir. Envanter takibi ve uygun risk analizinin yapılıp yapılmadığını takip etmek için kullanılabilir bir veridir.

Açıklama: Nitel değerlendirmelerle ilgili yardımcı açıklamalar, varlığın kısa tanımını ve gerekli olabileceği düşünülen diğer bilgileri içerir.

Bunların yanında, envanter hazırlanırken her bir varlık için alınmış *güvenlik önlemlerinin* envantere işlenmesi risk analizi için gerekli zaman ve iş gücünü ciddi anlamda azaltacaktır. Karşı kontroller belirlenirken varlık için alınmış güvenlik önlemleri değerlendirilecektir. Donanım varlıkları için *marka, model, seri numarası* bilgileri, yazılımlar için *yazılım tipi, üretici bilgisi, sürüm numarası, lisans bilgileri, yama bilgileri* envantere işlenmesi tavsiye edilen bilgiler arasındadır.

Tablo 1’de bir envanter tablosu örnek olarak verilmiştir.

Sıra No	Varlık Grubu	Varlık	Kategori	Varlık Sahibi	Varlık Emanetçisi	Gizlilik Değeri	Bütünlük Değeri	Erişilebilirlik Değeri	Değer	Varlığın Eklenme Tarihi	Açıklama
1												
2												
3												

Tablo 1 Örnek bir varlık envanter tablosu

Varlık Değerleri				
Güvenlik Hedefi	DÜŞÜK	ORTA	YÜKSEK	ÇOK YÜKSEK
GİZLİLİK	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu <u>etkilemez /çok az etkiler.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> açığa çıkmaz. Açığa çıkan kritik seviyesi altındaki bilgi kurumu etkiler. Etki <u>orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki <u>orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> açığa çıkar. Açığa çıkan kritik bilgi kurumu etkiler. Etki <u>telafi edilemez ya da uzun vadede telafi edilebilir.</u>
BÜTÜNLÜK	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> kontrol dışı <u>değişmez.</u> Kontrol dışı <u>değişen kritik seviyesi altındaki bilgi kurumu etkilemez / çok az etkiler.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> kontrol dışı <u>değişmez.</u> Kontrol dışı <u>değişen kritik seviyesi altındaki bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> kontrol dışı <u>değişir.</u> Kontrol dışı <u>değişen kritik bilgi kurumu etkiler. Etki orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgi</u> kontrol dışı <u>değişir.</u> Kontrol dışı <u>değişen kritik bilgi kurumu etkiler. Etki telafi edilemez ya da uzun vadede telafi edilebilir.</u>
ERİŞİLEBİLİRLİK/ KULLANILABİLİRLİK	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye</u> erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu <u>etkilemez / çok az etkiler.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye</u> erişilebilir. Erişilebilirliğine zarar gelen kritik seviyesi altındaki bilgi kurumu etkiler. Etki <u>orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye</u> erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki <u>orta vadede telafi edilebilir.</u>	Varlığa bir zarar gelmesi durumunda <u>kritik bilgiye</u> erişilemez. Erişilebilirliğine zarar gelen bilgi kurumu etkiler. Etki <u>telafi edilemez ya da uzun vadede telafi edilebilir.</u>

Tablo 2 Güvenlik hedefi varlık değeri tablosu

3. SINIFLANDIRMA

Organizasyon varlıklarına değer biçilmesi (valuation) risk analizi için temel bir adımdır. Tüm varlıklar belirlendikten sonra ikinci adım olarak, bir varlık için değer atama kriterinin belirlenmesi gerekir. Varlık çeşitleri düşünülecek olursa, değer atama kriteri belirlenmesi organizasyondan organizasyona çok değişiklik göstermektedirler. Kimi varlıkların değeri nicel olarak atanabilirken (rakamsal ifadeler kullanılarak) kimi varlıklar için ise nitel tanımlar kullanılabilir (düşük, çok yüksek gibi).

Nitel derecelendirme için tipik örnek olarak şunlar verilebilir: İhmal Edilebilir, Çok Düşük, Düşük, Orta, Yüksek, Çok Yüksek, Kritik. Kaç derecelendirme seviyesi kullanılacağı organizasyonun güvenlik ihtiyaçlarına bağlıdır. Çok fazla derecelendirme ihtiyacı olan bir organizasyon için 5-7 derecelendirme kullanılabilir iken güvenlik ve derecelendirme ihtiyacı çok fazla olmayan bir organizasyon için 3-4 derecelendirme seviyesi kullanılabilir.

Önemli olan nokta bir varlığa atanacak derecenin kriterinin belli belirsiz ifadeler kullanmadan yazılabilesidir. Yani bir varlık değeri için “düşük” denildiğinde bu tanımın ne anlama geldiği net olarak anlaşılmalıdır.

Bazı varlıklar için, birim maliyet, yenileme maliyeti veya organizasyonda üretilmişe yeniden üretim maliyeti değer atama için kullanılabilir nicel tanımlardır. Genel olarak varlık değerlemesinde nitel tanımlar kullanılmaktadır. Bazı varlıklar için nicel tanımlar (özellikle paraya dayalı tanımlar) kullanılması istendiğinde nicel tanımlarla nitel tanımlar arasında bir eşleşme matrisi kullanılabilir (örneğin değeri 10000 YTL nin altında belirlenmiş varlıklar için “düşük” değeri kullanılması gibi). Organizasyonun ticari ismi ve imajı soyut değer taşıyan varlıkları olarak değerlendirmelidir. Bu tip varlıkların değerinin belirlenmesi çok zordur. Genellikle bu tip varlıkların değeri nitel olarak belirlenir.

Bilgi Güvenliği Yönetim Sisteminde (BGYS) varlığa değer atama kriterleri belirlendikten sonra varlıkların değerlerinin atanması gereklidir. Bilgi varlıkları için güvenliğin üç temel ilkesinin (gizlilik, bütünlük, erişilebilirlik) uygulanması çok büyük bir sorun teşkil etmemektedir. Fakat envantere bulunan bir donanım varlığının gizliliği veya bütünlüğünü değerlendirmek çok daha zor bir eylemdir. Bu zorluğun önüne geçmek maksadıyla varlık değerlendirmesine (derecelendirmesine) bilgi ve süreç varlıklarından başlamakta fayda vardır.

Bilgi varlığı veya süreçler için atanacak güvenlik ilkesi değeri bu bilgi varlığını barındıran donanımı veya servisi sağlayan yazılımı doğrudan etkileyecektir. İlgili bilgi için atanacak değer “Yüksek” olarak belirlenmiş ise bu bilgiyi taşıyan donanım ve oluşturan/işleyen yazılım değeri de bağımlılık derecesine göre belirlenecektir. Örneğin aynı marka ve model iki sunucu web servisinde ve e-posta servisinde kullanılıyor olsun, erişilebilirlik açısından organizasyon için web servisi “Çok Yüksek” e-posta servisi ise “Orta” derecesinde ise bu sunucuların erişilebilirlik derecelerinin aynı olması beklenemez.

Varlığın korunmasını başka bir deyişle güvenliğinin sağlanmasını üç kategori altında inceleyebiliriz.

- Varlığın gizliliğinin korunması
- Varlığın bütünlüğünün korunması
- Varlığın erişilebilirliğinin sağlanması

Varlığın değerini belirlerken bu üç kategori için ayrı ayrı değerlendirmeler yapılmalıdır. Bir varlığın her zaman bu üç özelliği aynı derecede önem arz etmeyebilir. Bir bilginin ele geçirilmesi kimi zaman bütünlüğünün bozulmasından daha önemsiz olabilir (ör: web sayfasından yayımlanan duyurular), kimi durumlarda ise erişilebilirlik gizlilik ve bütünlükten daha önemli hale gelebilir (ör: haberleşme alt yapı varlıklarının sunmuş olduğu servisler). Bu bölümde referans olarak verilecek derecelendirme bilgileri organizasyondan organizasyona değişiklik gerektirebilir.

Her organizasyonda yapılacak derecelendirmede çok fazla derecelendirme seviyesi varsa, bir varlığın derecesinin belirlenmesinde karar verme güçlüğü ortaya çıkabilir veya çok az derecelendirme seviyesi varsa, gerekli ve yeterli derecelendirme sağlanamayabilir. Bu sebeple derecelendirme seviyesinin, organizasyonda karar verme güçlüğü çıkarmayacak kadar az ve gerekli derecelendirmeyi sağlayacak kadar çok olması sağlanmalıdır.

Varlığın sahibi varlığın gizliliğinin, bütünlüğünün, erişilebilirliğinin sağlanmasından birinci derecede sorumlu kişi veya kişilerdir. Varlıkların derecelendirmesinde bir varlığa (gizlilik, bütünlük, erişilebilirlik açısından) değer atamasında birinci derecede sorumluluk ve yetki varlık sahibine aittir. Başka bir deyişle varlığın değerini o varlığın sahibi belirler.

3.1 Varlık Değerleme / Derecelendirme

BGYS kurulum ve idame sürecinde varlıkların değerlerinin belirlenmesi işi çoğu zaman her varlık sahibi tarafından ayrı ayrı gerçekleştirilmemektedir. Varlık derecelendirmesi bir grup veya kurul (BGYS takımı da diyebiliriz) ve varlık sahipleri ile birlikte gerçekleştirilmektedir.

Varlık derecelendirmesi/değerlemesi yapılırken objektifliğin sağlanabilmesi için (derecelendirme sonucunda farklı kişilerin aynı varlığa aynı veya yakın bir dereceyi ataması için) doğru bir metodoloji uygulanması gereklidir. Bu metodoloji organizasyon için varlık sınıflandırma kılavuzuna temel teşkil edecektir.

Bir varlığın gizliliğinin, bütünlüğünün ve erişilebilirliğinin derecelendirilmesi için Tablo 2’de verilen tanımlardan faydalanılabilir. Bu tabloda gizlilik, bütünlük, erişilebilirlik için varlık değeri olarak dört seviye (Düşük, Orta, Yüksek, Çok Yüksek) kullanılmıştır. Bu tablo sadece bir örnek olarak değerlendirilmelidir. Daha önce de belirtildiği gibi, seviyeler ve seviye içerikleri kurumdan kuruma farklılık gösterirler. Varlığın zarar görmesi durumunda bu zararın kuruma etkisi varlığın değerini belirleyen unsurdur.

3.2 Varlık Sınıflandırma

Günümüzde, gerek organizasyon içinde gerekse organizasyonlar arasında bilginin yoğun şekilde aktarılması ve paylaşılması iş gereksinimlerinin karşılanması için kritik önemdedir. Bilginin güvenliği açısından, yoğun şekilde paylaşımı yapılan bilginin uygun şekilde korunması gerekir. Uygulanacak Bilgi Güvenliği Yönetim Sisteminde hangi kullanıcıların hangi bilgiye erişecekleri bilginin sınıflandırma programında belirlenmelidir.

Bilginin sınıflandırılması, etkin bir Bilgi Güvenliği Yönetim Sisteminin kurulması ve geliştirilmesinde önemli bir kavramdır. Bir varlığa verilecek sınıflandırma değeri, varlığın nasıl korunacağına, kimlerin ne ölçüde erişebileceğine, bu varlığın hangi ağda yer alması gerektiği gibi konulara karar verilmesini sağlayacaktır. Bilgi varlıkları belirlenmiş değerlerine, kanuni kısıtlamalara, bilginin hassaslığına ve organizasyon için kritikliğine göre sınıflandırılmalı ve uygun şekilde etiketlenmelidir.

Tutarlı bir sınıflandırma prosedürünün benimsenmesinin faydalarına örnek olarak şunlar sayılabilir;

- Organizasyonun karlılık ve itibarında olası zarar veya hassas bilgi kaybından doğacak menfaat riskini düşürecektir.

- Organizasyonun diğer organizasyonlara ait bilgilerin kaybı ile doğacak iş kayıpları ve mahcubiyet riskini düşürecektir.
- Organizasyona duyulan güveni arttırabilecek ve bilgi açısından hassas işlerin dış kaynaklı yaptırılmasını sağlayabilecektir.
- Risklerin uygun şekilde yönetildiği takdirde organizasyonlar arasında hassas bilgi değişimini kolaylaştıracaktır.

4. VARLIKLARIN KABUL EDİLEBİLİR KULLANIMI

Bilgi varlıklarının, sistem ve süreçlerinin kabul edilebilir kullanımı ile ilgili kurallar organizasyon tarafından dokümanite edilmeli ve uygulamaya konmalıdır. Kabul edilebilir bilgi kullanımı kuralları çerçevesi içerisinde hangi sınıftaki bilgilerin hangi ortamlarda bulunabileceği, bu bilgilerin nerelerde saklanabileceği ve bu bilgilerin hangi şartlarda ve ne şekilde kimlerle paylaşılacağı belirtilmelidir. Bu kurallar birlikte iş yürütülen yüklenici firmalar ve üçüncü parti organizasyonlar için olduğu kadar organizasyon çalışanları için de uygulanmalıdır. Bu kurallar özellikle e-posta ve internet kullanımı, cep telefonu, PDA ve dizüstü bilgisayar ve organizasyonun sınırları ötesine ulaşan bilgi sistem ürünleri için düzenlenmelidir.

5. BİLGİ ETİKETLEME VE İŞLEME

Organizasyonda uygun yönetim seviyesi tarafından gerek elektronik ortamda bulunan bilgilerin gerekse basılı ortamda saklanan bilgilerin etiketlenmesi ile ilgili prosedürler geliştirilmeli ve uygulamaya konmalıdır.

Uygulanacak prosedürler aşağıdaki bilgi işleme aktivitelerini kapsamalıdır;

- Bilgiye erişim,
- Kopyalama (elektronik olarak kopyalama, elle kopyalama, okuma ve ezberleme)
- Depolama (elektronik veya basılı olarak)
- İletim (faks, e-posta, basılı olarak iletim, insanlar arası konuşmalar, telefon, cep telefonu vs.)
- Özellikle bilgisayarla ilintili suçlarda kanıt olarak kullanılmak üzere ele alınması, bütünlüğünün korunması ve güvenlik olaylarının kayıt altına alınması
- İhtiyacın sonlanması durumunda yok edilmesi

Organizasyonda bilgiyi işlemekle sorumlu tüm çalışanlar ilgili prosedürü nasıl uygulayacakları hususunda eğitilmelidirler. Elektronik ortamlarda saklanan varlıkların etiketlenmesine / ayırt edilir hale getirilmesine gerekli önem gösterilmelidir. Özellikle bilgi işlem bölümü için, elektronik ortamda tutulan bir bilgi varlığına seçilen sınıflandırmanın uygulanması için gerekli etkin yöntemlerin ve yolların tanımlanması gereklidir.

Uygulanacak prosedürde bilgi sınıflandırma seviyeleri ve her seviye için alınması gereken önlemler tanımlanmalıdır. Bu çerçevede özellikle elektronik ortamlarda bulunan bilgi varlıkları için bilgi işlem çalışanları gerekli önlemleri almalı, ardından varlık, kurum çalışanlarının kullanımına açılmalıdır. Örneğin erişim kontrolü uygulanması gereken bir bilgi varlığına, öncelikle uygulanacak önlemler belirlenip uygulamaya konulmalı, daha sonra varlık yetkili kişilerin kullanımına sunulmalıdır. Aksi takdirde kontrolsüz kopya benzeri zayıflıklarla karşılaşılması muhtemeldir.

Belirlenecek seviyelerde, bir seviyede alınacak önlemler bir alt seviyede alınan önlemlerin tamamını kapsamalıdır. Örneğin G1, G2, G3 seviyeleri belirlenmiş ve uygun etiketleme yöntemleri tanımlanmış olsun. G1 için herhangi bir damga, uyarı erişim kontrolü yok (varlık sahibi onayının yeterli olduğu varsayılmıştır) iken, G2 seviyesindeki bir dokümanın kopyalanması, yazıcıdan çıktısının alınması için kimlik doğrulama uygulanabilir. G3 seviyesindeki bir dokümanın bulunduğu ortama erişim için ayrı bir kimlik doğrulama uygulanabilir. G3 seviyesindeki bir varlığın korunması için alınacak önlemler G2 seviyesindeki bir varlığı korumak için alınacak önlemlerin tamamını kapsamalıdır.

6. SONUÇ

Bu doküman, bir kurumda kurulması planlanan Bilgi Güvenliği Yönetim Sistemi kapsamında yapılacak tüm çalışmaların temelinde yer alan varlıkların envanterinin oluşturulmasına ve varlıkların sınıflandırılmasına kılavuzluk etmesi amacıyla hazırlanmıştır. Bu dokümanda verilen tüm bilgiler tavsiye niteliğindedir. Yapılacak tüm çalışmalar kuruma özgü Bilgi Güvenliği Yönetim Sistemi kapsamı ve programı dahilinde değerlendirilmelidir.

KAYNAKÇA

- [1]. IT Governance “A manager’s Guide to data security and BS 7799/ISO 17799” Alan CALDER, Steve WATKINS 2005
- [2]. ISO/IEC 27002:2005 Information technology -- Security techniques -- Code of practice for information security management
- [3]. ISO/IEC TR 13335-3:1998 Information technology -- Guidelines for the management of IT Security -- Part 3: Techniques for the management of IT Security
- [4]. ISO/IEC TR 13335-1:2004 Information technology -- Security techniques -- Management of information and communications technology security -- Part 1: Concepts and models for information and communications technology security management
- [5]. ISO/IEC Guide 73- 2002 Risk management -- Vocabulary -- Guidelines for use in standards
- [6]. NIST SP 800-30 Risk Management Guide for Information Technology Systems