Farklı Güvenlik Seviyesindeki Ağların Bağlanması İçin Bütüncül Bir Model

M. Kara

***Özet*—Kurumsal bilgilerin bilgisayar ağları üzerinde işlenmeye, iletilmeye ve saklanmaya başlaması ile birlikte kurumlar arası veri paylaşımı da büyük önem kazanmıştır. Gizlilik seviyesi olmayan bilgiler, bilinen güvenlik teknolojileri ile paylaşılmasına karşın farklı güvenlik seviyesindeki ağların birbiri ile veri paylaşımı için bu güvenlik önlemleri yeterli olmamaktadır. Farklı güvenlik seviyesindeki ağ bağlantılarını bazı özel durumlar çerçevesinde ele alan ve özel ihtiyaçlara cevap birkaç ürün dışında konuyu hem yönetimsel hem teknik olarak ele alan bütüncül bir bakış açısına sahip yaklaşımlar bulunmamaktadır. Bu makalede farklı güvenlik seviyesinden ağların birbirine bağlanması bütüncül bakış açısı ile ele alınmış ve genel bir model sunulmuştur.**

Abstract- all information of Organizations are processed on computer networks. This is increase importance of information sharing. Unclassified information can be shared with traditional security solution at internet but traditional security solutions is not secure for data sharing between different security level networks. There are a few special technical solutions connecting different security level networks but none of them is not provide general solution which is include technical and managing concepts. In this paper, a totalitarian model is presented for different security level network connection.

***Anahtar Kelimeler*—Farklı Güvenlik Seviyesine Sahip Ağlar, Bilgi Değişim Geçidi, Diyot, Air Gap, Gizlilik Seviyesi, Güvenlik Önlemleri**

I. GİRİŞ

Günümüzde kurumlara ait veriler hızla kağıt ortamından sayısal ortama taşınmaktadır. Bu da bilgilerin kolay bir şekilde erişilebilir, işlenebilir, saklanabilir ve iletilebilir olmasına imkan vermektedir. Bilgilerin sayısal ortama taşınmış olması, kurumun kendi bilgilerine hızlı erişimi sağlaması yanında diğer kurumlarla da güvenli bir biçimde paylaşılması ihtiyacını doğurmaktadır. Örneğin, Nüfus Vatandaşlık İşlerindeki (NVİ) bazı kişisel bilgilere, Adalet Bakanlığı, Sosyal Güvenlik Kurumu gibi kurumların ihtiyacı olabilmektedir. Suçlulara ve suçlara ait bilgilerin Jandarma Genel Komutanlığı ve Emniyet Genel Müdürlüğü (EGM) tarafından paylaşılması gerekebilmektedir. E-Devlet uygulamaları ile bu paylaşım ihtiyaçları her geçen gün artmaktadır.

Hali hazırda TUBİTAK BİLGEM'de yürütülen Kelepçe projesi kapsamında kurumları veri paylaşım analizi ihtiyaçları ve uygulamaları ele alınmıştır. Bu çalışmada kurumlar arasında bilgi paylaşımının çoğunlukla kağıt, sabit disk, taşınabilir bellek veya CD/DVD gibi çevrim dışı (offline) saklama ortamlarında veya resmi yazılarla ilettiği görülmektedir. Bu çevrim dışı veri iletim yönetimi ile veriler ilgili kuruma zamanında ulaşamamakta ve hızlı bir şekilde işlenememektedir. Bazı uygulamalarda kurumlar arasına kiralık hat çekilerek veya internet üzerinde sistemlere/uygulamalara sınırlı haklar verilerek yapılmaktadır. Bu paylaşımları kapsamlı olarak ele alan yasalar, yönetmelikler bulunmamaktadır.

Veri paylaşım ihtiyacı, gizli veya gizli olmayan bilginin paylaşılarak bilginin ekonomiye kazandırılması düşüncesiyle ortaya atılmıştır. Bu yaklaşımda kamuda toplanan verilerin farklı kurumlar tarafından değerlendirilerek yeni ve topluma faydalı sonuçlar elde edilmesi hedeflenmiştir. Bu paylaşım verilerin ve uygulamaları doğası gereği beraberinde çeşitli kısıtlama ihtiyaçlarını da gündeme getirmektedir. Kısıtlar bilginin mahremiyeti, ticari sırların ve özel hayatın korunması, devletin güvenliği, fikri mülkiyet gibi kavramlar ekseninde gelişmiş, bu çerçevede özellikle hukuk alanında yeni düzenlemeler ihdas edilmiş ve önleyici bir taktikle olası zararların önüne geçecek yapılar kurulmuştur. Kamu sektörü bilgisinin yeniden kullanımı konusu, hukuki düzenlemelerle de iç içe geçmiş olup, bu kapsamda ülkeler yasal düzenlemeler yapmaktadır[1] . Literatürde ve uygulamalarda daha çok tasnif dışı, hizmete özel ve özel verilerin paylaşıldığı görülmektedir. Ülkemizde de kamu kurumlarının birbirleri arasında tasnif dışı, hizmete özel, özel ve gizli bilgileri paylaşma ihtiyacı bulunmaktadır.

Bilgisayar ağlarında işlenen, iletilen ve saklanan bilgilerin gizlilik seviyeleri ve koruma önlemleri farklı olmasına karşın, bu ağların birbirleri ile veri paylaşması ve veri aktarması günümüzde bir ihtiyaç haline gelmiştir. Bu ağların güvenlik seviyeleri aynı dahi olsa farklı kurumların verileri olduğu için doğrudan bağlanmaları mümkün olmamaktadır. Veri paylaşımı için kurumlar birbirinden özel ek teknik ve yönetimsel güvenlik önlemleri talep edilebilmektedir. Bu kapsamda bu makalede, farklı ağlar arasında olası bağlantılar ve bunların sağlaması gereken güvenlik önlemleri hem teknik hem yönetimsel olarak bütüncül bir bakış açısı ile ele alınmıştır.

Günümüzde farklı kurumların veri paylaşım ihtiyacının aşağıdaki yapılarda olduğu Kelepçe projesi kapsamında yapılan veri paylaşım ihtiyaç analizi çalışmasında ortaya çıkmıştır.

KAMU ↔ KAMU
KAMU ↔ TÜZEL KİŞİ
KAMU ↔ TSK
KAMU ↔ YABANCI ÜLKE KURUMLARI
TSK ↔ NATO

Bu ağların gizlilik seviyeleri göz önüne alındığında ağlar arasında olabilecek bağlantı türleri Tablo 1'de verilmiştir. Genel uygulamalara bakıldığında günümüz güvenlik teknolojileri ile çok gizli ağlara erişimin verilmemesi yönündedir. Farklı güvenlik seviyelerine sahip ağların bağlantısında yüksek seviyede olan ağın güvenlik gereksinimlerini karşılayacak şekilde yapılandırma gereklidir. Bunun yanında ağların birbirine bağlanmasını sağlayan bilgi değişim ağ geçidi (Information Exchange Gateway- IEG) büyük önem taşımaktadır [2].

		KURUM A				
		Çok Gizli	Gizli	Özel	Hizmete Özel	Tasnif Dışı
KURUM B	Çok Gizli	X	X	X	X	X
	Gizli	X	√	√	√	√
	Özel	X	√	√	√	√
	Hizmete Özel	X	√	√	√	√
	Tasnif Dışı	X	√	√	√	√

Tablo 1 Farklı güvenlik seviyesindeki ağlar arası iletişimde güvenlik gereksinimleri

Farklı güvenlik seviyesindeki ağlar arasındaki bilgi paylaşımı, bütüncül bakışa açısı ile olmalıdır. Bu makale bu bakış açısını koruyacak şekilde tasarlanmıştır.

Bölüm 2'de literatür taraması ele alınmıştır.
Bölüm 3'de bu konuda geliştirilen teknolojiler tanıtılmıştır.
Bölüm 4'de farklı güvenlik seviyesindeki ağların bütüncül bakış açısını ele alınması için yapılması gerekenler ele alınmıştır.
Bölüm 5'de sonuç ve öneriler verilmiştir.

II. LİTERATÜR TARAMASI (NP)

A. *Bilimsel Makaleler ve Standartlar*

Bu konularda yayınlana ve öncelikli makaleler konularında bilgi verilecek.

Gelecek askeri operasyonların etkin ve efektif yapılabilmesi için veri paylaşımı çok önemlidir. Network Enabled Capability (NEC) olarak adlandırılan bu sistemlerle NATO, NATO üyesi ve partner ülkeler arasında bilgi paylaşımı tanımlanmaktadır. Bu tür karmaşık sistemler aslında veri paylaşımı oldukça zordur. Boonstra ve arkadaşları bu tür sistemler arasında veri paylaşımını ağ güvenlik unsurlarını çok küçük güvenlik parçalarına bölünerek her bir noktada sadece gerekli güvenlik unsurlarını içeren bir donanım/yazılım kullanılmasını içeren bir model sunulmuşlardır [3,4,5].

Farklı kurumlar arasında güvenli veri paylaşımı için XML etiketleme ve meta verileri kullanan çözümler geliştirilmiştir[4,6,7]. Bu konuda NATO'da XML kontrolü sağlayan bir koruma profili tanımlanmıştır.

NEXOR firması NATO tarafından güvenli veri haberleşmesinin temini için IEG konsepti, bileşenleri ve amacı konusunda üst seviyeden ele alan referans dokümanını oluşturmuştur [2]. Apiecionek ve arkadaşları Nexor firmasının geliştirdiği IEG'nin yeteneklerine ek olarak Extensible Messaging and Presence Protocol (XMPP), FTP, HTTP gibi birçok protokolü destekleyen çözümü geliştirmişlerdir [8].

Serrano ve arkadaşları genel hatlarıyla NATO ülkeleri ve diğer paydaşlar arasında bilgi paylaşımına yönelik zorluklar irdelemiştir. Böyle bir paylaşım için öncelikli olarak yanıtlanması gereken "Ne paylaşmak isteniyor?", "Hangi durumlarda paylaşım yapılmalı?", "Hangi protokol veya araçlarla yapılabilir?" vb. gibi bazı soruları ele almışlar. NATO için bu tür bir bilgi paylaşımı farklı alanlardaki proje ve organizasyonlardaki girişimler ölçeğinde olup gereksinimlerin sadece bir alt kümesini sağlayan kısmi çözümler önermektedirler. Aynı zamanda NATO bilgi paylaşımı için bir yok haritası çıkarılmıştır. Bunlar her paydaş için farklı cevaplara sahip durumdadır. Paydaşlar arasında bu soruların cevapları hususunda tek bir mutabakata varılması ve ölçeklenebilirlik güç olduğundan bütünsel bir çözüm sağlanmasını kısmen karşılamaktadır [9].

Bu raporda, gizlilik seviyesi yüksek olan savunma, istihbarat ve milli güvenlik kurumlarının ağları ile gizli olmayan kamu ağlarının gerçek zamanlı iş birliği için birbirleri arasındaki etkili ve güvenli veri paylaşımına yönelik gerekli olan güncel ihtiyaçlardan bahsedilmektedir. Aynı zamanda Ezenia InfoWorkSpace (IWS) sisteminin temel yeteneklerine ve MLS (Multi Level Security) ile olan ilişkilerine değinilmektedir [10].

Dean arkadaşları yüksek ve düşük güvenlikli bölgeler arasındaki iki yönlü, güvenli bilgi transferi sağlayan air–gap dışındaki alternatif tekniklerden bahsedilmiştir. Bu teknikler format kontrolü, ağ güvenlik seviyesi kontrolü ve kullanıcı onayı gibi teknolojileri içermektedir. Birleşik Krallık Savunma Bakanlığı sorumluluğunda yürütülen araştırmalarda, QinetiQ firması çift yönlü ve güvenli haberleşme için çeşitli teknolojiler üzerinde çalışmaktadır [11]. James ve arkadaşları bulut üzerinden gizlilik seviyesi olan verilerin güvenli olarak paylaşılması ele alınmaktadır [12].

Asseco Poland tarafından gizlilik dereceleri değişen sivil ve askeri kurumlara arasındaki güvenli haberleşmeyenin sağlanması için Multi Level Security System sistemleri

tasarlamıştır. Bu yapı SOA (Service Oriented Architecture) mimarisi doğrultusunda tasarlanmıştır **Error! Reference source not found.**.

Harris ve arkadaşları, halk sağlığı konusunda devlet kurumları, finans kurumları, üniversiteler ya da hastaneler arası güvenli veri paylaşım standartlarını ele almıştır. Makalede veri paylaşımı için etkili bir organizasyon gerekliliği vurgulanmıştır. Ayrıca güvenli veri paylaşım teknikleri ve esnek mimari hakkında belli standartlara dayanarak yapılan yaklaşımlar ele alınmıştır **Error! Reference source not found.**.

Chen ve arkadaşları Çin'in kamu ve endüstriye ait geniş ağlarının birbirine bağlanması ihtiyacının giderilmesi için güvenlik koruması ve ağ sınır kontrol sisteminin tasarlanması üzerinde durulmuştur. Güvenlik koruması ve ağ sınır kontrol sistemleri, yazılımsal ve donanımsal araçlar ile beraber güvenlik standartları ve politikalarını da kapsamaktadır [15].

B. Ülke ve organizasyonların Genel Yaklaşımları

AGB, Norveç, Japonya, Çin, Avrupa Birliği ülkeleri kamuya ait verileri etkin bir şekilde paylaşılması bu paylaşımdan kamunun ve ülkenin fayda sağlaması için yasal düzenlemeler ve paylaşım standartları oluşturmaktadır. Türkiye'de bilişim sistemlerinin yaygın kullanılmaya başlaması ile birlikte bu ihtiyaç artmıştır. Bu ihtiyacı karşılamak için kurumlar kendi yönetmeliklerini çıkarmakta ileri doğru kapsamlı düzenlemeler ve standartların ortaya konulması beklenmektedir.

ABD, kamu sektörü bilgisinin paylaşılması ve tekrar kullanılması yoluyla değer üretiminin öncüsü olarak kabul edilmektedir. Uygulanan açık erişim politikası ve vergi sisteminin sağlıklı işlemesi ile ABD'de kamu sektörü bilgisinin kullanımından büyük fayda sağlamaktadır. Kamu sektörü bilgisini kullanarak katma değer üreten şirketlerin elde ettikleri gelirlerinden dolayı devlete ödedikleri vergiler kamunun bu bilgileri satması durumunda elde edeceği gelirden fazladır. Kamu sektörü bilgisini katma değerli ürüne dönüştüren özel sektör, devlete daha fazla vergi vermekte, istihdamda artışa neden olmakta, dolayısıyla gelirler artarken istihdama, ulusal ve küresel ölçekte rekabet edebilirliğe ve kalkınmaya katkı sağlanmaktadır [1].

Avrupa Birliği üyesi ülkeler arasında topluma ait açık bilginin paylaşımı için 2003/98/AT sayılı Direktifi oluşturulmuştur. 2008 yılına kadar AB ülkelerinin bazıları, kanun şeklinde yeni düzenlemeler bazıları da mevcut kanunlarda tadilat yaparak direktife uyum sağlamışlardır. 26 Haziran 2013 2003/98/AT tarihinde doküman yeniden güncellenmiştir [17]. Avrupa Birliği'nin siber güvenlik programlarından sorumlu olan Avrupa Ağ ve Bilgi Güvenliği Ajansı (ENISA) da birbirine bağlı ağların güvenliği konusunda çalışmalar yürütmektedir[18].

NATO organizasyon yapısı gereği gizlilik bilgiyi birçok seviyede işlemesi ve başka ülke ve kurumlarla paylaşması gerekmektedir. Bunu için de uzun yıllardır veri haberleşmesi için teknik ve yönetimsel çözümler geliştirmeye çalışmaktadır. Hali hazırda gizli ve hizmete özel verilerin paylaşılması için çözümler geliştirmektedir [7, 16].

III. TEKNOLOJİLER VE ÜRÜNLER

İncelenen bilimsel dokümanlar, IEG ürünleri hakkında internetten elde edilen bilgiler ve üreticilerden alınan ürün ve kullanıcı kılavuzlarından edinilen bilgiler doğrultusunda ağlar arası bilgi akışı cihazlarının diyot çözümleri, air gap çözümleri ve akış kontrolü çözümleri olarak sınıflandırılabileceği tespit edilmiştir.

Akış kontrolü çözümleri, literatürde bilinen adıyla Guard, farklı ağlardaki sistemleri haberleşmesini sağlarken içerik analizi yapabilen, uygulama katmanında trafiği yönlendirebilen cihaz veya sistemlerdir. Klasik güvenlik duvarlarına ve yönlendiricilere benzemekle beraber, uygulama katmanında trafiğin içeriğini kontrol ederek etiket, sınıflandırma veya zararlı yazılım kontrolü de yapabilmektedirler. Akış kontrol sistemleri sadece üzerinde uygulanan kural ve politikalara uygun olan trafiğin geçmesine izin vererek yüksek güvenlik derecesine sahip ağları korumaktadır. Bu güvenlik kuralları veya politikaları, zararlı yazılım analizi, etiket kontrolü, yetki kontrolü, dosya tipi kontrolü, sayısal imza kontrolü gibi derinlemesine paket analizlerini içermektedir.

Diyot (Diode), iki ağ arasında donanımsal olarak ters yönde veri akışını engelleyerek, tek yönlü bir bağlantı sağlayan çözümlerdir. Bu çözümler sayesinde güvenli bir ağın, genel amaçlı bir iç ağdan ters yönde veri akışı riski olmayacak şekilde veri çekebilmesi mümkündür. Böylece kullanıcıların güvenli olmayan kaynaklardan güvenli ağa veri transferine izin verilmektedir. Veri kaynağı tarafındaki kullanıcılar bilgiyi dış diyot sunucusuna gönderir. Daha sonra veri diyottan geçerek iç diyot sunucusuna ulaşır.

Diyot cihazı öncesinde, dışarıdan gelen bilginin kaydedilmesi ve sonra diyot üzerinden içeriye gönderilmesi amacıyla ara sunucular kullanılıyorsa, uçlar arasındaki iletişim gecikmeli çevrimiçi şekilde gerçekleşir.

Air Gap (hava boşluğu), güvenli bir bilgisayar ağının fiziksel, elektriksel ve elektromanyetik açıdan diğer güvenli/güvensiz ağlardan izole edilmiş olmasına dayanan bir güvenlik kavramıdır. Normal koşullarda bir bilgisayar ağı ile diğer dış ortamlar arasında hava boşluğundan bahsedilebilmesi için, bu ağa bilgi aktarımının sadece harici bilgi taşıma ortamlarıyla (disket, USB disk vb.) gerçekleştirilebileceği garanti edilmelidir.

IV. AĞ BAĞLANTILARI İÇİN GENEL GEREKSİNİMLER

Literatür incelendiğinde doğrudan farklı güvenli seviyesinde ağların bağlanmasına yönelik bütüncül bakış açısına sahip

model bulunmuyor. Literatür taramasında da görüldüğü gibi genellikle bu bağlantının özel alanlarına (Bilgi değişim Geçitleri, İçerik Kontrolü, vb.) odaklanmış çözümler bulunmaktadır. Bu makalede farklı güvenlik seviyesine sahip ağların bağlanmasında teknik ve yönetimsel tüm konuları ele alan bir model sunulmaktadır. Bu modelin gerektirdiği temel konular bu bölüm altında ele alınmıştır.

A. Ağ Bağlantılarına Yönelik Zafiyetler, Tehditler ve Riskler

Ağ bağlantılarına yönelik zafiyetler, tehditler ve riskler bu bölümde ele alınmasının nedeni modeli uygulayacak sistem yöneticilerinin bu konuda bilgilendirilmelerini sağlamaktır. Ağlar arasında bağlantıya özel sistem riskleri bu bağlantı için tanımlanan tehditlerin gerçekleşme olasılığına bağlı olarak belirlenmelidir. Tehditlerin gerçekleşme olasılıkları, tehdit ortamı, mevcut güvenlik önlemleri, bağlantı modeli, bağlantı ihtiyacı vb. etkenlere bağlı olarak değişecektir. Tehdit altında olan sistem bileşenlerinin/verilerinin değeri de kurumdan kuruma değişmektedir. Risk değerlendirmesi çalışması, her bağlantı senaryosu için planlama safhasında yapılmalıdır. Güvenlik tedbirleri, sadece burada tanımlanan tehditlerden kaynaklanacak risklerin değil, ağlar arası bağlantı öncesinde gerçekleştirilecek olan risk değerlendirme çalışması sonucunda sistemin tümü için belirlenen risklerin en aza indirgenmesini hedeflemelidir.

B. Ağ Gizlilik Seviyeleri ve Güvenlik Önlemleri

Ağlar arasında paylaşılacak bilginin gizlilik, bütünlük ve erişilebilirlik ihtiyaçlarının bilgi paylaşan kurumlar adına güvence altına alınması amacıyla göz önünde bulundurulması gereken teknik ve yönetimsel güvenlik önlemleri mevcuttur.

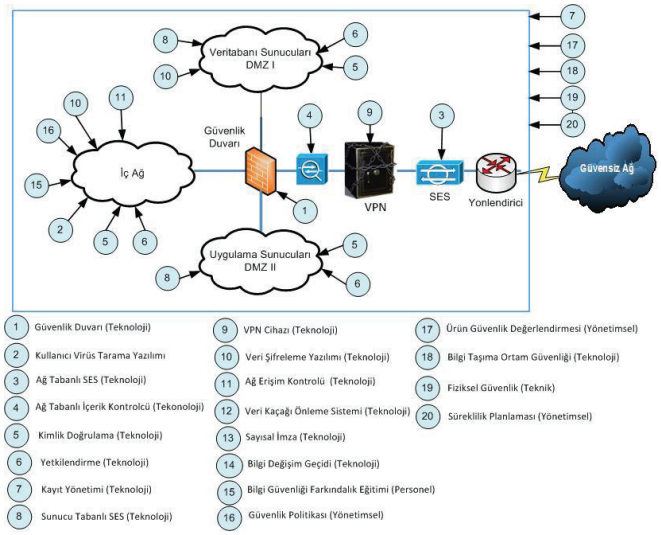
Ağların bütüncül bakış açısı ile güvenliğinin sağlanabilmesi için aşağıdaki güvenlik önlemlerinin alınması gerekmektedir.

- Güvenlik Duvarı
- Zararlı Yazılıma Karşı Koruma
- Saldırı Tespiti ve Önleme
- İçerik Kontrolcüsü
- Yönlendirici
- VPN
- Kimlik Doğrulama
- Erişim Kontrolü
- İnkâr Edememe
- Güvenlik Sıkılaştırmaları
- Denetleme Kayıtları
- Bilgi Değişim Geçidi
- Farkındalık ve Eğitim
- Fiziksel ve Çevresel Güvenlik
- Güvenlik Değerlendirmesi
- Konfigürasyon Yönetimi
- Süreklilik Planlaması
- Acil Durum Müdahale
- Bakım
- Bilgi Taşıma Ortamlarının Korunması
- Personel Güvenliği

Temel olarak gizliliği belirleyen kıstas o ağda bulunan bilginin niteliğidir. Ağda saklanan işlenen, iletilen verinin gizliliği ağın gizliliğini doğrudan etkilemektedir. Bu yüzden farklı güvenlik seviyesindeki ağlarda bulunması gereken güvenlik önlemleri de farklıdır. Farklı güvenlik seviyesindeki ağları birbirine bağlamak isteyen kurumlar risk analizi yaparak her bir güvenlik seviyesi için alınması gereken teknik ve yönetimsel güvenlik önlemlerini belirlemeli bu güvenlik önlemlerini içeren topolojiler oluşturmalıdır.

Askeri ve kamu kurumlarında bilgi Tasnif Dışı, Hizmete özel, Özel, Gizli ve çok Gizli olmak üzere 5 sınıfta ele alınmaktadır [19].

Şekil 1'de Hizmete Özel bir ağın topolojisi ve ağda alınması gereken önlemler bulunmaktadır.



Şekil 1 Hizmete Özel ağın topolojisi

Ağlar arası bağlantı yapacak sistem yöneticilerinin güvenlik önlemlerini kolay ve etkin bir şekilde anlayıp uygulayabilmeleri amacıyla teknik ve donanım/yazılım tabanlı (Güvenlik Duvarı, Saldırı engelleme Sistemi vb) bir gösterim yapılmaya çalışılmıştır. İşletim sistemi gibi birçok güvenlik unsurunu bünyesinde barındırması gereken varlıklar için kimlik doğrulama, yetkilendirme, olay kaydı izleme gibi kavramlar da kullanılmıştır. Bu kavramların ağın gizlilik seviyesine göre varlıklarda da bulunup bulunamayacağı ağ mimarilerinde belirtilmiştir. Ağda güvenliğin sağlanabilmesi için teknik önlemler yanında yönetimsel önlemlerin de alınması gerekmektedir. Ağlarda alınacak yönetimsel önlemler de ayrıca belirtilmiştir.

Bilgi sistemlerinde kademeli güvenlik (Defense in Depth), bilgi güvenliğinin sağlanması amacıyla farklı kademelerde birbirini tamamlayıcı güvenlik önlemlerinin alınmasıdır.

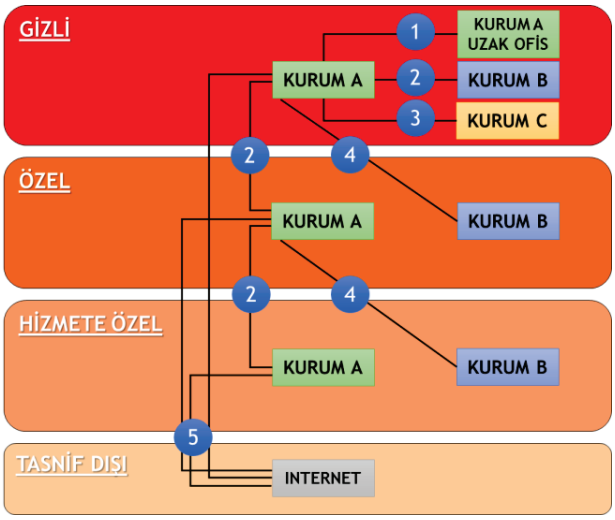
Sistem yaşam döngüsü içerisinde personel, teknoloji ve işletme açısından güvenlik önlemleri alınmalıdır. Farkı gizlilik seviyesindeki ağlar için belirlenen güvenlik önlemleri kademeli güvenlik bakış açısı ile oluşturulmalıdır.

C. Ağlar Arası Bilgi Akışı

Ağlar arası bağlantının güvenli şekilde temini için gizli kanalın varlığı, bilgi sızması, ağ atakları, ağın izlenmesi ve güvenlik etiketlerinin değiştirilmesi gibi güvenlik tehditlerine karşı teknik koruma sağlanması, gerekli politika ve direktiflerin oluşturulması ve uygulanması önemlidir.

Farklı güvenlik seviyelerine sahip ağların bağlantısında yüksek seviyede olan ağın güvenlik gereksinimlerini karşılayacak şekilde yapılandırma gereklidir. Bunun yanında ağların bir birine bağlanmasını sağlayan bilgi değişim geçidi (IEG) büyük önem taşımaktadır.

Şekil 2'de bağlanacakları ağların güvenlik sınıflandırmaları yanında ağların güvenlik ilkelerini, sahiplerini ve yöneticilerini de dikkate alan beş farklı senaryo belirtilmiştir.



Şekil 2 Farklı güvenlik seviyesindeki ağlar arası iletişim senaryoları

Senaryo 1: Aynı güvenlik sınıflandırma seviyesinde ve aynı KURUM etki alanında fakat farklı otoriteler tarafından yönetilen iki etki alanının birbirine bağlanmasını göstermektedir. Örnek olarak aynı kurumun merkez ve uzak ofisinin bağlantısı verilebilir.

Senaryo 2: Aynı güvenlik sınıflandırma seviyesinde fakat farklı güvenlik ilkelerine sahip iki etki alanının birbirine bağlanmasını göstermektedir. Aynı güvenlik seviyelerini kabul eden iki kamu kurumunun bağlantısı buna örnek olarak verilmektedir. Bu senaryonun diğer bir durumu da aynı kurumun farklı güvenlik sınıflandırma seviyesindeki ağlarının bağlanmasıdır.

Senaryo 3: Aynı güvenlik seviyesindeki kamu kurumu ve özel bir kurumun etki alanlarının kurduğu bağlantıyı göstermektedir.

Senaryo 4: Aynı güvenlik sınıflandırma sistemini kabul eden iki farklı kurumun iki farklı seviyedeki ağının bağlantısını ifade eder.

Senaryo 5: Kurum ağının Internet'e veya diğer tasnif dışı sistemlere bağlantısını göstermektedir. Burada farklı seviyelerden tasnif dışına bağlantı söz konusu olduğundan her durum ayrı olarak ele alınmalıdır.

Bu noktada genel olarak daha fazla ihtiyaç duyulduğu belirlenen Senaryo 4 üzerinden sistemin nasıl olması gerektiği yönünde öneriler yer alacaktır.

Yüksek güvenlikli etki alanın bütünlük ve kullanılabilirliği, düşük güvenlikli etki alanından sadece beyaz listeye alınmış mesaj formatına sahip mesajlarının geçmesine izin verilerek sağlanabilir. Bilgi akış sistemi virüs/zararlı yazılım taraması gibi içerik taramalarını dış güvenlik bileşenlerine bırakabilir. Bilgilerin gizliliği ise sadece izin verilen etikete sahip mesajların geçmesine izin verilerek sağlanır.

D. Paylaşılacak Bilgiler ve Müşterek Sınıflandırma

Genel gereksinimler açısından ilk dikkate alınacak husus kurumlar arasında paylaşılacak verilerin belirlenmesidir. Kullanım durumlarına bağlı olarak bilgi paylaşım amacı da ortaya konulmalıdır. Paylaşılacak bilgiler kategorize edilerek listelenmelidir. Sistemlerin gizlilik seviyelerinin müşterek kriterler üzerinden tespiti, alınması gereken önlemlerin standartlaşması açısından önemlidir. Bu şekilde kurumdan kuruma değişen gizlilik seviyesi kriterleri için ortak bir nokta belirlenebilmektedir.

Birçok durumda bilgi otomatik olarak toplanmakta ve belirli durumlarda paylaşılmaktadır. Bu işlemlerin manuel olarak gerçekleştiği durumlar da mevzu bahistir. Dolayısıyla verinin hangi durumda ne şekilde toplandığı net şekilde ifade edilmelidir.

E. Risk Analizi

Veri paylaşımının sınırsız bir şekilde yapılmasının önündeki en büyük engel veriye ve sistemlere yönelik risklerdir. Her bir bağlantı kurulumu kendine özel şartlar altında değerlendirilmeli ve süreç buna göre işletilmelidir. Genel tek bir bağlantı çözümünün bütün durumlar için yeterli olacağı varsayımında bulunmak doğru değildir.

F. Ortak Prosedürler

Bilgi değişimini yöneten kurallar tanımlanmalıdır. Ne zaman ve nasıl paylaşım yapılacağı, bilginin iletim esnasında nasıl korunacağı ve işleneceği belirlenmelidir. Bu şekilde uçlar arasında güven (trust) ilişkisi kurulmalıdır. Bunun için ikili veya çoklu anlaşmalar imzalanmalıdır. Eğer mevcutsa ulusal

bilgi güvenliği makamından görüş talep edilmeli veya yeterli olgunlukta ise bilgi paylaşımı kapsamında kurumlar arası ilişkileri düzenleyen mevzuata başvurulmalıdır. Ayrıca iletişim gereksinimi durumunda bağlantı kurulacak noktaların belirlenmesi gerekmektedir.

G. Standart ve Formatlar

Sürekli veri paylaşım ilişkisinin ve birlikte çalışabilirliğin devam etmesi için veri formatı ve ortak standartlar üzerinde fikir birliği olmalıdır. Uyumsuz standartlar gelecek için verimli paylaşım hususunda sıkıntı oluşturacağı için mümkünse uluslararası veri standartları kullanılmalı değilse iki kurumun anlaştığı veri formatı oluşturulmalıdır. Bu veri formatının uygulama seviyesinde içerik kontrolünün yapılabilmesi önemlidir. Örneğin Bilgisayar Olaylarına Müdahale Ekipleri arasında bilgi paylaşımına yönelik Incident Object Description Exchange Format (IODEF) formatı bu konuda örnek olarak verilebilir.

H. Paylaşım Altyapıları/Sistemleri

Özellikle tasarım aşamasından başlanarak paylaşımın yapılacağı altyapının ve sistemin nasıl olması gerektiği analiz edilmelidir. Bu paylaşımlara için geliştirilmiş sistemler varsa onlar tercih edilmeli yoksa risk analiz sonucunda teknik riskleri minimize edecek bir çözüm geliştirilmelidir. Böyle bir yapıya NATO bünyesinde zararlı yazılım bilgilerini paylaşarak korelasyon kuran ve üye ülkeleri bilgilendiren MISP paylaşım altyapısı örnek olarak verilebilir.

1) İletim Protokolleri

Grafiksel kullanıcı arayüzü bulunabileceği gibi aynı işlevler ve isteğe bağlı geliştirmeler, uygulamanın sunduğu API (Application Programme Interface) vasıtasıyla da gerçekleştirilebilir.

Bütünlük ve gizliliğin temini, bilginin iletiminde zorunluluk olduğu için hangi taşıma protokolünün kullanılması gerektiği belirlenmelidir. İletim protokolü seçimine göre Paylaşım Altyapıları/Sistemleri başlığında belirtilen sistemin özellikleri tanımlanırken iletim protokolleri de göz önüne alınmalıdır. Burada söz konusu protokoller HTTP, XMPP veya SMTP olabilir.

2) Ortak Ağlar

Verinin hangi tipteki ağlar üzerinde (tasnif dışı, hizmete özel, gizli, internet, kiralık hat vb.) iletildiği analiz edilmelidir. Internet veya kurum gizli ağı kullanılmakla birlikte her bir kullanım durumu için hangi ağın kullanılacağı tanımlanmalıdır. Söz konusu ağ Internet olabileceği gibi sadece gizli haberleşmelerin yapılacağı gizli ağ da olabilir.

3) Bağlantı Sistemlerinin Güvenlik Test Politikaları

Bilgi sistemlerinin güvenlik testlerinin nasıl ve hangi aralıklarla yapılacağı tanımlanmalıdır. Örneğin ağlar arası bağlantı amacıyla kullanılan sunucular ve ağ içerisinde ilişki kurdukları diğer bütün sunucu, aktif ağ cihazları ve uygulamalar için güvenlik testleri planlanmalı ve plana uygun şekilde periyodik olarak gerçekleştirilmelidir. Testler uygulama, uygulama platformu, işletim sistemi ve ağ olmak üzere dört seviyede gerçekleştirilebilir.

4) Bağlantı Sistemi Akreditasyonu

Bu doküman göz önünde bulundurularak iki kurumun uzmanlarının ortak kuracağı bir komisyon veya üçüncü bir tarafça sistemin istenilen gereksinimleri karşıladığının tespit edilerek akredite edilmesi gerekmektedir.

V. SONUÇ VE ÖNERİLER

Bilgilerin sayısal ortama taşınmış olması, kurumların ve ülkelerin kendi bilgilerine hızlı erişimi sağlaması yanında diğer kurumlarla ya da ülkelerle güvenli bir biçimde paylaşılması ihtiyacını doğurmaktadır. Özellikle gizli gizlilik dereceli bilgilerin paylaşılması için uzun yıllardır çalışmalar sürdürülmesine karşın somut uygulanabilir teknolojik ve yönetimsel araçlar bulunmamaktadır. Çoğunlukla özel durumlar için özel çözümler önerilmektedir. Fiziksel güvenlik için Air-Gap, Diyot gibi teknolojiler, içerik kontrolü için de akış kontrol sistemleri uygulanmaktadır. Bu teknolojik çözümler yanında güvenli veri paylaşımının sağlanması için risk analizi, ortak prosedürler, standart formatlar, ikili anlaşmalar, paylaşım alt yapıları, iletişim protokolleri gibi hususların göz önüne alınacağı bir bütüncül bir model oluşturulmuştur. Bu modelin kurumlara uygulanmasında o kurumlara özgü verilerin çıkarılması, verilerin standart hale getirilmesi içeriğinin kontrol edilmesi önem arz etmektedir. Sonraki çalışmalarda bu model veri paylaşmak isteyen değişik kurum verilerine uygulanabilir.

KAYNAKLAR

[1] D. Civelek, Ö. Aşık, *"Kamu Sektörü Bilgisinin Paylaşımı ve Yeniden Kullanımı"*, DPT Çalışma Raporu, Şubat 2011
[2] Nexor, *IEG Reference Architecture*, 2013 [Online], Available: http://www.nexor.com/white-papers/nato-ieg-reference-architecture
[3] D. Boonstra, H.A. Schotanus, C.A.A Verkoelen, A.C.M. Smulders; "*A Methodology for the Structured Security Analysis of Interconnections*" The 2011 Military Communications Conference
[4] A. J. Blažič, S. Šaljić; *"Security and Confidentialty in Interconnected Networks" ICDS 2011:* The Fifth International Conference on Digital Society
[5] T. Grance, J. Hash, S. Peck, "*Security Guide for Interconnecting Information Technology Systems",* NIST; 2002
[6] Sander Oudkerk, Ian Bryant, Anders Eggen, Raymond Haakseth*, "A Proposal for an XML Confidentiality Label and Related Binding of Metadata to Data Objects"*, NATO RTO-MP-IST-091; 2009
[7] K. Wrona, S. Oudkerk, G. Hallingstad; *"Designing Medium Assurance XML-Labelling Guards for NATO*" NATO Consultation, Command&Control Agency
[8] L. Apiecionek, M. Romantowski, J. Sliwa "*Safe Exchange of Information for Civil-Military Operations*" Military Communication Institue, Poland; 2011
[9] O. Serrano, P. Lagadec, L. Dandurand, F. Jordan, "*CIS Security Information Sharing Challenges"*; NATO NCIA,2013
[10] Ezenia Inc, "*The Future Evoluation of Multi-Level Security for the Federal Government"*, Ezenia Inc.; 2007

[11] T. Dean, G. Wyatt, *"Information Exchange Between Resillient and High-Threat Networks: Techniques for Threat Mitigation",* QinetiQ; 2004
[12] J. R. James, F. Mabry, *"Seeing the Real World: Sharing Protected Data In Real Time"*, 45th Hawaii International Conference on System Sciences; 2012
[13] Multilevel Security Services European Defence Agency; Asseco Poland; 2011
[14] D. Harris, L. Khan, R.Paul, Bhavani Thuraisingham, "*Standards for secure data sharing across organizations*",Computer Standards & Interfaces archive, Volume 29 Issue 1, January, 2007
[15] B. Chen, B. Jin, X. Zou; "*The Security Protection and Control Systems of Network Boundary*"; The 3rd Research Institute of Ministry of Public Security, China; 2009
[16] NATO, "*Information Assurance Technical and Implementation Directive for the Interconnection of CIS"*, 2008
[17] European Union, "*Directive 2003/98/EC on the re-use of public sector information*", 2013, http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2013:175:0001:0008:EN:PDF
[18] Online Available: http://www.nexor.com/data-diodes
[19] SSM, *"Gizlilik Derecelendirme Kılavuzu" Hazırlama Rehberi*, 2007, [Online], Available, http://www.ssm.gov.tr/anasayfa/kurumsal/Documents/GizlilikDerecelendirmeKilavuzu.pdf

M. Kara, 1993 yılında Yıldız Teknik Üniversitesi Elektronik ve Haberleşme Mühendisliği Bölümünden mezun oldu. 1996 yılında Yüksek Lisansını, 2002 yılında da Doktorasını Kocaeli Üniversitesi Fen Bilimleri Enstitüsü Elektronik ve Haberleşme Anabilim dalında tamamladı. Doktora tezini Bilgisayar Ağlarında Çok Yollu Yönlendirme konusunda yaptı. 1994-2000 yılları arasında Kocaeli Üniversitesi Bilgisayar Mühendisliği bölümünde Araştırma Görevlisi olarak, 2000-2001 yıllarında Armada Bilgisayar AŞ'de Sistem Mühendisi olarak çalıştı. 2001'den beri TÜBİTAK BİLGEM'de çalışmaktadır. Bulanık mantık, siber güvenlik, ağ ve sistem, protokol güvenlik analizi, kritik altyapı güvenliği, güvenli yazılım geliştirme, Ortak Kriterler, sistem, yazılım/donanım güvenlik testleri konularında çalışmaktadır. Ulusal ve uluslararası dergi ve konferanslarda yayınları bulunmaktadır.