# VERGİ DAİRESİ OTOMASYON PROJESİ'NİN (VEDOP) BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

**A. Altuğ YAVAŞ**[1]

[1]VEDOP Bilgi Güvenliği Yöneticisi, Cybersoft

T.C. Maliye Bakanlığı, Gelirler Genel Müdürlüğü Bilgi İşlem Merkezi 3. Kat

Ziraat Mahallesi Yeni Etlik Caddesi No:16 Etlik Ankara

[1]e-posta: altug.yavas@cs.com.tr

*Anahtar Sözcükler: Bilgi Güvenliği Yönetim Sistemi, VEDOP, E-Devlet*

## ABSTRACT

*VEDOP (Tax Office Automation Project) VEDOP was started as a pilot project in 1995 aiming the complete automation of tax offices. Second phase of VEDOP, covering an e-filing system for tax returns, a data warehouse and the spreading of automation all over Turkey. Both phases' financial portrait is up to 138 million USD. Cybersoft has assigned more than 5,000 man.months to VEDOP and 3,000 man.months to VEDOP-2. Thus, VEDOP is the largest software implementation in Turkish Public IT Sector. The motivation of VEDOP and VEDOP-2 is to implement the new IT technologies in tax automation of Turkey in order to enhance the tax collection, increase the service quality presented to tax payers, integrate Ministry of Finance with other institutions and organizations and supply necessary information to decision-makers for developing successful tax policies and audit strategies.*

## 1. GİRİŞ

Bu bildiride, Vergi Daireleri Otomasyonu Projesi'nde (VEDOP) kurulan Bilgi Güvenliği Yönetim Sistemi hakkında bilgi verilmiştir. İkinci bölümde projenin geçmişinden bahsedilmiş, üçüncü bölümde projenin çalışma ortamı için kurulmuş olan bilgi işlem altyapısı ve uygulamaların çalışma şekli anlatılmış, dördüncü bölümde kurulan bilgi güvenliği yönetim sistemi açıklanmıştır. Son bölüm sonuç bölümüdür.

## 2. PROJENİN TARİHÇESİ VE İŞ AMAÇLARI

VEDOP, 1995 yılında, vergi dairelerinin otomasyona geçirilmesi amacıyla bir pilot proje olarak başlatılmıştır. Pilot projenin başarılı olmasından sonra 1998'de, VEDOP-1 projesi başlamış ve iki yıl içerisinde 22 ildeki 155 vergi dairesinin otomasyonu gerçekleştirilerek proje tamamlanmıştır. 2004 yılında projenin ikinci aşaması olan VEDOP-2 projesi başlatılmıştır. Bu proje halen devam etmektedir.

VEDOP projesinin iş amaçları ve kısa açıklamaları şöyle sıralanabilir:

- **E-Beyanname:** Vergi beyannamelerinin İnternet üzerinden alınması
- **E-VDO (Vergi Daireleri Otomasyonu):** Mevcut Vergi Dairesi uygulamalarının web tabanlı ve n-katmanlı mimariye uyarlanması
- **Elektronik Banka Tahsilat İşleme Sistemi (EBTİS):** Bankalar tarafından toplanan vergi ödemelerine ait bilgilerin elektronik ortamda GGM'ye aktarılması
- **Vergi Denetmenleri Otomasyonu Sistemi (VEDOS):** Vergi denetmenlerinin, denetim bilgilerini bulundukları konumdan bağımsız bir şekilde GGM'ye aktarması
- **Çağrı Merkezi:** Vergi dairelerindeki kullanıcıların yararlanabileceği bir Çağrı Merkezi'nin kurulması
- **Veri Ambarı:** Kayıt dışı ekonominin kayıt altına alınması ve vergi tabanının yaygınlaştırılması
- **EMKAS (Elektronik Muhasebe Kayıt Arşiv Sistemi):** Bakanlıkça belirlenen mükelleflere ait defter ve belgelerin elektronik ortamda alınarak arşivlenmesi ve analiz edilmesi

Projenin iki aşamasının toplam maliyeti yaklaşık 173 milyon YTL'dir. Cybersoft [1] VEDOP-1 için 5000 adam.ay, VEDOP-2 için 3000 adam.ay iş gücü harcamıştır. Bu haliyle VEDOP, Türkiye'de gerçekleşmiş en büyük kamu projesidir.

## 3. BİLGİ İŞLEM ALTYAPISI

VEDOP kapsamında Türkiye çapında bulunan 300 vergi dairesi ve mal müdürlüğündeki 15.000 kullanıcının İnternet'e ve VEDOP uygulamalarına bağlanması sağlanmıştır.

Gelirler Genel Müdürlüğü'nün (GGM) internet bağlantısı toplam 16 Mbit band genişliğine sahiptir. Bu 16 MBit, üç farklı hizmet sağlayıcıdan tahsis edilerek tek bir kaynağa bağımlılık engellenmiştir.

VEDOP ağının kavramsal yapısı Şekil 1'de gösterilmiştir.

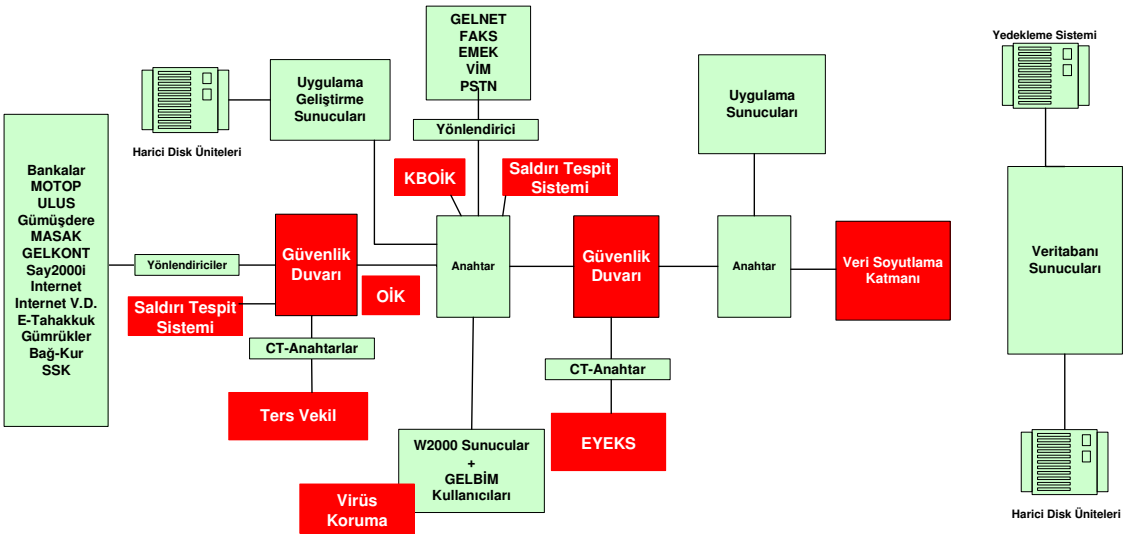
## 4. BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

VEDOP Bilgi Güvenliği Yönetim Sistemi üç temel bakış açısına göre tarif edilecektir:

- İdari yapı

- Teknik altyapı
- İşletim yapısı

Proje süresince gerçekleştirilmek üzere üç "Güvenlik Risk Değerlendirme Faaliyeti" planlanmıştır ve bunlardan ilk ikisi gerçekleştirilmiştir. Bu




**Şekil 1VEDOP Kavramsal Bilgi İşlem Altyapısı**

## 4.1. İdari Yapı

VEDOP kapsamında işletmeye alınacak uygulamaların mevcut tehditlere karşı güvenliğini sağlamak, yaşanacak güvenlik ile ilgili olan olaylar nedeniyle oluşacak maddi ve manevi kayıpları en aza indirmek, yapılan yatırımların geri dönüşünü en üst seviyeye çıkarmak, temel güvenlik gereksinimleri olan *Gizlilik*, *Bütünlük*, *Elverişlilik* gereksinimlerinin proje kapsamında karşılanmasını garanti etmek ve mevcut tehditlerden kaynaklanan risklerin kabul edilebilir seviyede tutulmasını sağlamak amacıyla proje için bir Bilgi Güvenliği Politikası geliştirilmiştir. Bu Bilgi Güvenliği Politikası'nın geliştirilmesi sırasında projenin gereksinimleri ön planda tutularak TS ISO/IEC 17799 standardından [2] yararlanılmıştır. Politika, 10 konu başlığı, 29 güvenlik amacı ve 111 politika maddesinden oluşmaktadır. Politika, "Nasıl" sorusuna cevap vermekten çok "Ne" sorusuna cevap vermek üzere yazılmıştır.

Bu politikanın sahibi Bilgi Güvenliği Onay Kurulu'dur. Bu kurulun temel görevi politikayı onaylamaktır. Bu kurul, Bilgi Güvenliği Politikası'nın tüm VEDOP kapsamında benimsenmesine ön ayak olur. Kurul, kendisine sunulan raporları değerlendirerek politikada değişiklik yapabilir. bilgi güvenliğinin sağlanması ve sürdürülmesi ile ilgili Bakanlık içerisindeki diğer birimlerin eşgüdümünü sağlamak da bu kurulun sorumluluğundadır. Bu kurul şu üyelerden oluşmaktadır:

- Gelirler Genel Müdürü
- Gelirler Genel Müdür Yardımcısı
- Daire Başkanı (Bilgi İşlem)
- Bilgi Güvenliği Yöneticisi
- Bilgi Güvenliği Uzmanı

faaliyetlerde, Bilgi Güvenliği Politikası ve İşletim Prosedürleri'ndeki hata ve eksiklikler değerlendirilmiş, ayrıca birçok kullanıcı grubu ile yüzyüze görüşmeler yapılarak, bilgi güvenliği politikasının ne kadar gerçek yaşama yansıdığı değerlendirilmiştir. Bu faaliyet Bakanlık ve proje yüklenicileri dışındaki bir BS 7799 Baş Denetçisi tarafından gerçekleştirilmiştir.

Bunun yanında yine proje süresince üç kez gerçekleştirilmek üzere "Zayıflık Taraması ve Sızma Testi Faaliyeti" planlanmıştır. Bu test iki bölümden oluşmaktadır. İlk bölümde farklı işletim sistemlerine sahip olan ve ağın farklı bölümlerinde bulunan toplam 20 sunucu üzerinde zayıflık taraması testleri ile, güncel güvenlik açıklarına karşı bu sunucuların zayıflıkları taranmıştır. İkinci aşamada, bilinmeyen bir kaynaktan VEDOP'un internet üzerindeki giriş noktalarından içeriye yetkisiz sızma gerçekleştirilmeye çalışılmıştır. Her iki testin sonuçları da bir rapor halinde sunulmuştur. Zayıflık Taraması ve Sızma Testi faaliyeti, Bakanlık ve proje yüklenicileri dışındaki bir BS 7799 Baş Denetçisi tarafından gerçekleştirilmiştir.

## 4.2. Teknik Altyapı

Bu bölümde VEDOP'ta alınan teknik güvenlik önlemleri anlatılmıştır. İlk olarak genel güvenlik yapıtaşları açıklanmış daha sonra yazılım uygulaması yardımıyla oluşturulan güvenlik yapısı açıklanmıştır.

VEDOP'ta kullanılan genel güvenlik yapıtaşları şunlardır:

- **Güvenlik Duvarı:** Değişik noktalara konulmuş üç farklı güvenlik duvarı ile VEDOP'un sınır koruma ihtiyaçları sağlanmaktadır. Bu güvenlik duvarlarından biri ağın internete çıkış noktasında, ikincisi GELBİM ağı ile Vergi Daireleri ağı

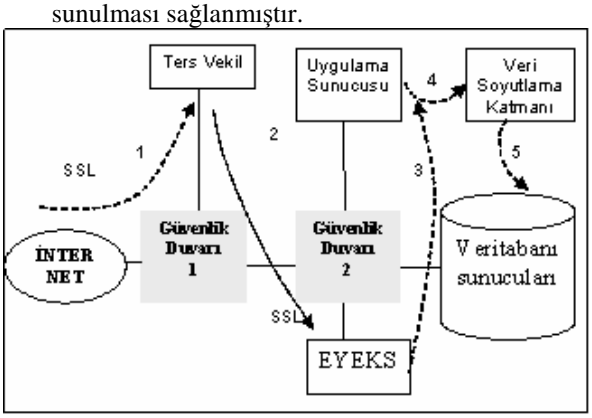
arasına, üçüncüsü de veri bölgesinin girişine konumlandırılmıştır. Güvenlik Duvarları, kendi aralarında kümelenmiştir ve yük paylaşımlı olarak çalışmaktadır. Kullanılan band genişliği, isteğe bağlı olarak ihtiyacı olan uygulamaya öncelikli olarak tahsis edilmektedir. İnternet üzerinden VEDOP uygulamalarına yapılan bağlantılar ve kullanıcıların dışarıya yaptıkları bağlantılar değişik parametrelere bağlı olarak, özellikle vergi beyannamesi son teslimi gibi trafiğin yüksek olduğu günlerinde sürekli izlenmektedir.

- **Kullanıcı Bazlı Oturum İçerik Kontrol Yazılımı (KBOİK):** GGM bünyesindeki tüm kullanıcıların kurumsal e-posta adresi mevcuttur. Bu yazılımla, e-posta sisteminden gelebilecek virüslü e-posta, istenmeyen (spam) e-posta, zincir e-posta gibi saldırılara karşı koruma sağlamaktadır. Ayrıca şüpheli görünen e-postalar, operatör tarafından gözden geçirilmek üzere göz altına alınmaktadır.
- **Oturum İçerik Kontrol Yazılımı (OİK):** Ağ sayfalarına erişimlerde, erişilen sayfaları sınıflandırır ve belirlenmiş sınıflardaki sayfalara erişime izin verilir. Bu şekilde, kötü amaçlı kod barındırabilecek sayfalara ve band genişliğinin etkin kullanımını engelleyecek program indirmelerin önüne geçilmiş olur. Bu yazılımla ayrıca, kullanıcıların uçtan uca dosya paylaşımı ağlarına (Örneğin Kazaa, E-Donkey, i-Mesh gibi) ve anında mesajlaşma sistemlerine (MSN, ICQ, Yahoo Messenger gibi) erişimleri engellenir.
- **Saldırı Tespit Sistemi Yazılımı (STS):** Sistemde, Ağ tabanlı ve konak tabanlı saldırı tespit yazılımları kullanılmaktadır. Bu yazılımlar sayesinde içeriden ve dışarıdan gelebilecek ve güvenlik duvarı tarafından tespit edilemeyecek saldırılara karşı korunma sağlanmış olur.
- **Virüs Koruma Yazılımı**: VEDOP ağına bağlı olan tüm kullanıcı ve hizmet bilgisayarlarında virüs koruma yazılımı kuruludur. Tüm bilgisayarlarda, kullanıcı müdahalesine gerek olmaksızın günde birkaç kez virüs imzaları güncellenmektedir. Virüs koruma sunucusu yedeklenmiştir.

VEDOP'da kullanılan uygulama düzeyi güvenlik yapıtaşları şunlardır:

- **Ters Vekil:** Ters vekil, dışarıdan VEDOP üzerindeki uygulamalara bağlanan kullanıcılar ile EYEKS uygulama sunucusu arasında yer alır. Dışarıdan bağlanan kullanıcıların doğrudan EYEKS uygulama sunucusuna erişmesini engeller.
- **Erişim Yetkilendirme ve Kişiselleştirme Sistemi (EYEKS):** EYEKS, tüm uygulamalar için genel bir kullanıcı doğrulama, yetkilendirme ve kişiselleştirme sistemidir. Bu sayede, VEDOP sistemlerini kullanan tüm iç ve dış kullanıcıların yönetimi ve yetki seviyelerinin belirlenmesi doğru ve hızlı bir şekilde tek bir merkezden gerçekleştirilir. Ters Vekil sunucusundan gelen istekler EYEKS tarafından tanıma/kimlik doğrulama/yetkilendirme sürecinden geçirilerek 6 uygulama sunucundan birine iletilir. EYEKS dağıtık oturum yapısını desteklemektedir. Aynı kullanıcıdan gelen farklı istekler, yük dengeleme algoritması tarafından farklı uygulama sunuculara iletilmiş olsa da kullanıcı tek bir oturumda çalışıyormuş gibi davranır. EYEKS'in bazı özellikleri şunlardır:
  - Tek kullanımlık parola tanımlanabilmesi
  - Yardım Masası ve Çağrı Merkezi'nde çalışanların, problemli kullanıcı adına sisteme girebilmeleri
  - Kullanıcı yetkilerinin devredilebilmesi
  - Ayrıntılı işlem kayıtlarının tutulması

- **Veri Soyutlama Katmanı (VSK-DAL**): VEDOP'daki tüm uygulamalar, veritabanı ve veri ambarı sunucularına sadece DAL katmanı aracılığı ile erişebilmektedir. Bu sayede uygulamaların, veri modelindeki değişimlerden etkilenmemesi, farklı veritabanlarına dağılmış verilerin uygulamalara bütünlük içerisinde sunulması sağlanmıştır.




**Şekil 2 Uygulamaların Çalışma Şekli**

Güvenlik açısından bakıldığında uygulamalar şu şekilde çalışır (Şekil 2):

1. İnternet üzerinden ya da vergi dairelerinden gelen istekler 1. Güvenlik Duvarı'ndan geçerek ters vekil sunucusuna gelir. Bu bağlantı SSL tabanlı olarak gerçekleştirilir. Kullanıcının tek muhatabı ters vekil sunucusudur. Bu katmanın arkasındaki işlemler kullanıcıya saydam olarak gerçekleştirilir.
2. Ters vekil sunucusu bu istek için EYEKS ile arasında bir oturum açar. Bu istek 2. Güvenlik Duvarı'ndan geçerek EYEKS'e ulaşır.
3. EYEKS, yetkilendirme işlemi sonucunda isteği uygulama sunucusuna gönderir.
4. Uygulama sunucusu veritabanı sorgusuna ihtiyaç duyduğunda bu sorguyu VSK'na gönderir.
5. VSK, isteği XML biçiminden SQL biçimine çevirerek veritabanına gönderir.

## 4.3. İşletim Yapısı

VEDOP'ta kurulu sistemlerin tüm işletimi ve bakımı, VEDOP Sistem Yönetim Grubu tarafından gerçekleştirilmektedir. Çalışan sistemlerin bir çoğu kesintisiz hizmet verdiklerinden, bu sistemlerin çalışması, operatörler tarafından 7 gün 24 saat denetlenmektedirler.

Bilgi Güvenliği Politikası'nın hayata geçirilmesi amacıyla bir Bilgi Güvenliği Geliştirme Grubu kurulmuştur. Bu grup, teknik bir yönetim yapısıdır ve Bilgi Güvenliği Politikası'nı uygulamakla yükümlüdür. Bu grup aşağıdaki üyelerden oluşur:

- Bilgi Güvenliği Yöneticisi (Cybersoft)
- Bilgi Güvenliği Uzmanı (SBS)
- Bilgi Güvenliği Uzmanı (Bakanlık)

Bu grup Bilgi Güvenliği Politikası'nın uygulanması dışında, şu görevleri yerine getirmekle yükümlüdür:

- Bilgi Güvenliği Politikası'nda ihtiyaç duyulan değişikliklerin Onay Kurulu'na teklif edilmesi
- Bilgi Güvenliği Politikası'nın hayata geçirilmesini sağlayacak İşletim Prosedürleri'nin yazılması
- Yazılan işletim prosedürlerinin uygulanmasının sağlanması ve karşılaşılan problemlerin çözülmesi
- Bölüm 4.2'de belirtilen ve teknik altyapıyı oluşturan varlıkların sisteme dahil edilmesi, bakımı, problemlerinin giderilmesi, güncellemelerinin ve yamalarının yapılması
- Dış ve iç güvenlik denetimlerinin ("Güvenlik risk değerlendirme" ve "Zayıflık Taraması ve Sızma Testi" faaliyetlerinin) planlanması ve gerçekleştirilmesi
- Dış ve iç güvenlik denetimleri sonucunda ortaya çıkan güvenlik açıklarının kapatılması ve zayıflıkların giderilmesi için öncülük edilmesi
- Onay Kuruluna sunulmak üzere periyodik raporlar oluşturulması. Bu kapsamda hazırlanacak 3 temel rapor belirlenmiştir:
  - Güvenlik Açıkları ve Zayıflıkları Raporu
  - Bilgi Güvenliği İhlalleri Raporu
  - Bilgi Güvenliği İle İlgili Arıza Raporu

Bu grubun bu görevlerini yerine getirmek üzere en az haftada bir kez toplanması öngörülmüştür.

Grup, politikayı destekleyecek şekilde işletim prosedürleri geliştirir. Bu işletim prosedürleri, teknik altyapının, Bilgi Güvenliği Politikası'nı destekleyecek şekilde nasıl kullanılacağını tarif eder. İşletim prosedürleri daha çok "Nasıl" sorusunu cevaplamak üzere geliştirilmiştir. Analoji yapmak gerekirse, Bilgi Güvenliği Politikası Anayasa'ya, işletim prosedürleri de yasalara benzetilebilir. VEDOP'ta 16 işletim prosedürü tanımlanmış ve yazılmıştır. Bu prosedürler, Bilgi Güvenliği Politikası'ndaki maddelerle birebir eşleştirilmiştir. Her prosedür, en az bir Bilgi Güvenliği Politikası maddesinin gereksinimlerini karşılayacak şekilde ve en iyi pratiklerden yararlanılarak oluşturulmuştur. Prosedürler "bir işi en iyi o işi yapacak olan kişi bilir" yaklaşımı ile prosedürde tarif edilen faaliyetleri gerçekleştirecek kişilerle birlikte yazılmıştır.

# 5. SONUÇ

VEDOP'da kurulan Bilgi Güvenliği Yönetimi Sistemi, hem bürokratik yapıya hem de projenin ihtiyaçlarına uygun olarak gerçekleştirilmiştir. Projenin aktif olarak içinde bulunan taraflar olan Maliye Bakanlığı, Cybersoft ve SBS'den temsilcilerin güvenlik faaliyetlerine katılmaları sağlanarak bilgi güvenliği konusunda farkındalığın tüm taraflarda oluşmasına çaba gösterilmiştir. VEDOP'da sahip olunan değerli varlıkların ihtiyacı olan koruma, kurulan Bilgi Güvenliği altyapısının yaşayan bir sistem olması ile sağlanmaktadır.

KAYNAKLAR

[1] http://www.cs.com.tr

[2] Türk Standardı TS ISO/IEC 17799, Bilgi Teknolojisi – Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, Kasım 2002