SİBER GÜVENLİK STANDARDLARI VE BELGELENDİRMELERİ

Mariye Umay Akkaya
TSE-Yazılım Test ve Belgelendirme Dairesi Başkan V.
uakkaya@tse.org.tr

ÖZETÇE

Bilginin giderek en değerli varlık haline geldiği çağımızda, tüm dünyada Bilişim Teknolojileri ve Bilgi Güvenliği konularında yapılan çalışmalar her geçen gün artmaktadır.

Günümüzde bilişim teknolojilerinde de standardizasyon, güvenlik, performans ve kalite kontrolleri çok önemli hale gelmiştir. Yazılım ürünlerinin güvenliği, kalitesi, performansı, ürün oluşturulurken izlenen yollar, şifreleme-kriptoloji gibi konular BT ürün ve sistemleri için vazgeçilmez olmakla birlikte, uluslar arası bilişim ve siber güvenlik standartlarına göre bağımsız laboratuvarlarda test edilip, bağımsız belgelendirme kuruluşları tarafından sertifikasyonu ayrıca önem arz etmektedir.

ABSTRACT

In our times where information becomes the most important value, the studies on Information Technologies and Information Security are increasing day by day all around the world.
In our times, standardisation, security, performance and quality controls have become very important in information technologies as well. While security, quality, performance of software products, methods used while creating products, topics such as ciphering, criptology are indispensable for Information Technologies products, testing in independent laboratories based on international information and cyber security standards and certification by independent certification organizations are also very important.

1. GİRİŞ

Bt ürün ve sistemleri için, günümüzdeki Bilişim ve Siber Güvenlik Belgelendirmelerine Örmek Olarak;

2.1 Siber Güvenlik Belgelendirmeleri:

- **TS ISO/IEC 27001: Bilgi Güvenliği Yönetim Sistemi**

- **ORTAK KRİTERLER (Common Criteria)-TSE-CCCS, TSE-OKBS sertifikası:**

TS ISO/IEC 15408 serisi BT ürünlerinin güvenliği için değerlendirme kriterleri

- **KRİPTO MODÜL ve ALGORİTMA BELGELENDİRMESİ: TSE-CMVP ve TSE-CAVP sertifikaları**

- **TS ISO/IEC 19790**: Kripto Modülleri Güvenlik Gereksinimleri
- **TS ISO/IEC 24759:** Kripto Modülleri Test Gereksinimleri

- SAHA GÜVENLİK BELGELENDİRMESİ
TEMEL SEVİYE GÜVENLİK BELGELENDİRMESİ

- Sızma Testi Yapan Personel ve Firmaların Belgelendirmesi "Beyaz Şapkalı Hacker"

2.2 Bilişim Teknolojileri Belgelendirmeleri:

YAZILIM SÜREÇLERİ BELGELENDİRMESİ:

- **TS ISO 15504-SPICE** Yazılım Süreçleri Değerlendirilmesi ve İyileştirmesi
- **TS ISO/IEC 12207** Yazılım Yaşam Döngüsü
- **TS ISO/IEC 15288** Sistem Yaşam Döngüsü

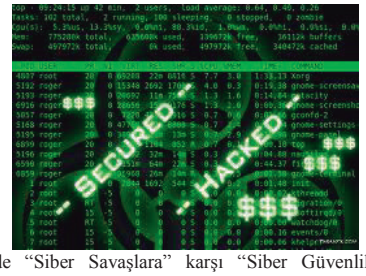
BİLİŞİM TEKNOLOJİSİ- TSE-sertifikası:

- **TS 13298** Elektronik Belge Yönetimi
- **TS ISO/IEC 25051**Yazılım Paketleri Belgelendirmesi
- **TS ISO 9241-151** İnsan-Sistem Etkileşimi-Web Sayfalarının Belgelendirmesi
- **TS ISO/ IEC 40500** Web İçeriği Erişilebilirlik Klavuzu
- IQNET-QWEB BELGELENDİRMESİ

BT ürünlerin ve/veya sistemlerinin tüm bu standartlara uygunluğunun ölçülebilmesi, ve değerlendirilebilmesi ISO/IEC 17025 akreditasyonu olan bağımsız test laboratuvarlarında yapılmaktadır.

3.SİBER SAVAŞLAR, SİBER SAVUNMA VE SİBER GÜVENLİK

Dünyada artık "Siber Saldırı", "Siber Güvenlik", "Siber Ordu", "Siber Terorizm" "Siber Bakan", "Siber Savunma" terimleri sıklıkla kullanılmaktadır. 2010 Kasım ayında ABD`de "Wikileaks" olarak adlandırılan Gizli Diplomatik ve Askeri Belgelerin ifşası, 2007 yılında Rusya-Estonya Siber Savaşı, İran Nükleer Sisteminin Rusya tarafından durdurulması vb. Siber Savaşların dünyadaki örneklerinden sadece birkaçıdır.



Günümüzde "Siber Savaşlara" karşı "Siber Güvenlik ve Savunma" stratejileri geliştirmemiz ve ülkemizin "Kritik Altyapıları" olan "Bilgi ve iletişim, Enerji, finans, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği, nükleer biyolojik ve kimyasal tesisler" imizi korumak için gereken tedbirleri almamız son derece önemlidir.

İçinde bulunduğumuz "Bilgi ve İletişim" çağında bahsi geçen ve Kritik Altyapılarımız olan "Enerji, finans, sağlık, gıda, su, ulaşım, savunma, kamu güvenliği, nükleer biyolojik ve kimyasal tesisler" artık manual fiziksel yöntemlerle kontrol edilmemekte, bu sistemler "Uygulama Yazılım" larıyla uzaktan kontrol edilmektedir. Bu uzaktan kontrol hız ve performans kazancı sağlarken, malesef kötü niyetli kişi/kurum vb. için de "Siber Saldırı" ortamı haline gelmekte, güvensiz test edilmemiş yazılımlar ve donanımlar yüzünden çok değerli olan "Kritik Altyapılarda" tolere edilemeyecek maddi kayıplar yaşanabilmektedir.

Kritik varlıklar korunamadığı takdirde ülke bilgi güvenliği büyük risk altına girer. Bu da çok daha büyük sorunları beraberinde getirir. Bu kritik varlıklar;

- Enerji
- Savunma
- Finans
- Sağlık
- Gıda
- Su
- Ulaşım
- Bilgi ve iletişim
- Kamu güvenliği
- Nükleer, biyolojik ve kimyasal tesisler

olarak sıralanabilir.

Bahsi geçen ülke kritik altyapılarından herhangi birinde bir sorun çıkması, ülkenin kaosa sürüklenmesine neden olabilecektir. Bu sorun tamamen kaldırılamayacağı gibi, büyük oranda azaltılabilir.

Siber Savunma yöntemlerinden biri de, BT ürün ve sistemlerine Siber Güvenlik standartlarından test ve belgelendirme yapılmasıdır.

3.1 TS ISO/IEC 15408- BT Ürünleri Güvenliği-Ortak Kriterler

Ortak Kriterler, Bilişim teknolojisi ürünleri için geliştirilmiş güvenlik değerlendirme standartları olan ISO/IEC 15408 ve ISO/IEC 18045 standartlarıdır. CTCPEC (Kanada), TCSEC (A.B.D) ve ITSEC (Avrupa) standartlarının "Common Criteria" adı altında birleşmesi ile Ocak 1996'da yayınlanmıştır.

3.1.1 CCRA-Ortak Kriterler Tanıma Anlaşması:

Ortak Kriterler Uluslararası Tanıma anlaşmasıdır. Bu anlaşmayı imzalayan ülkeler, ürün hangi ülkeden sertifika almış olursa olsun o ürünün belirtilen seviyede güvenli olduğunu kabul etmiş sayılırlar.
Ortak Kriterler standardı 2012 itibariyle 26 ülkede geçerliliği bulunan bir standarttır. Bu 26 ülkeden 15'i Certificate Authorising Member (sertifika üretici üye), 11'i ise Certificate Consumer Member (sertifika müşterisi üye) ülkelerdir.
Sertifika Üretici Ülkeler; Türkiye, Almanya, Amerika, İtalya, Fransa, Güney Kore, Japonya, Norveç, İngiltere, Kanada, Avusturalya, İspanya, İsveç, Hollanda, Malezya, Hindistan dır.
Sertifika Müşterisi Ülkeler ise; Avusturya, Çek Cumhuriyeti, Danimarka, Finlandiya, Yunanistan, Macaristan, İsrail, Singapur, Pakistan dır.
Sertifika Üretici Ülke olabilmek için, öncelikle Sertifika Müşterisi Ülke olmak ve gerekli şartları yerine getirdikten sonra başvurunun onaylanması gerekmektedir.

3.1.2 ORTAK KRİTERLER TARİHÇESİ ve TSE-ORTAK KRİTERLER BELGELENDİRME SİSTEMİ (OKBS)

Türkiye`de Ortak Kriterler programı ilk defa 2001 yılında Genel Kurmay Başkanlığı(TGS) tarafından Türk Silahlı Kuvvetleri için başlatıldı.
Türkiye'nin belgelendirme kuruluşu olarak TSE, 2003 yılında CCRA'ya imzaladığı anlaşma ile "Sertifika Müşterisi" olarak üye olmuştur.
Türkiye`de ilk Kamu Ortak Kriterler Değerlendirme Laboratuvarı 2003'te TUBİTAK UEKAE bünyesinde Ortak Kriterler Test Merkezi(OKTEM) adı altında bağımsız olarak çalışmalarına başladı.
Ortak Kriterler Belgelendirme Sistemi(OKBS) 2005 yılında TSE Ürün Belgelendirme Merkezi altında kuruldu.
TSE, 2008 yılında CCRA'da yapılan düzenleme gereğince "Sertifika Üreten Ülke – Authorizing Country" olmak için başvuruda bulundu.
12-16 Nisan 2010 tarihleri arasında TSE OKBS, CCRA tarafından yapılan Uluslar arası Tetkikten (Shadow Assesment) "Başarı" ile geçti.
17 Kasım 2010 tarihinde Türkiye`nin "Sertifika Üreten Ülke – Authorizing Country" olarak resmi duyurusu yapıldı ve Türkiye bu alandaki 15 ülkeden biri oldu.

3.1.3 ORTAK KRİTERLER STANDARDI

Ortak Kriterler Standardı ürün için; Gizlilik (Confidentiality), Bütünlük (Integrity), Kullanılabilirlik (Availability) kontrollerini;

1.Tasarım sürecini sorgulamak,
2.Teslim & Kurulum sürecini sorgulamak,
3.Tasarım dokümanlarının içerik yeterliliğini sorgulamak,
4.Kaynak kodu sorgulamak,
5.Kılavuz dokümanları sorgulamak,
6.Yaşam Döngüsü Modeli'ni sorgulamak,
7.Geliştirme araçlarını sorgulamak,
8.Geliştirme ortamının güvenliğini sorgulamak,
9.Test dokümanlarını sorgulamak (fonksiyonel, bağımsız ve sızma testleri),suretiyle gerçekleştirir.

- Özetle; Ortak Kriterler, BT ürününün BT ürününün yeterli bir geliştirme ortamında gerçeklenip gerçeklenmediğini kontrol eder, var olan tehditleri analiz eder, Fonksiyonel, Bağımsız ve Sızma testleri (Açıklık Analizi çalışması) yapar ve ürüne uygun garanti seviyesini verir.

3.1.3.1 Garanti Seviyeleri

Ortak Kriterler tanımlanmış, garanti seviyesi gittikçe artan ve Değerlendirme Garanti Seviyesi (EAL) olarak bilinen 7 adet Güvenlik Seviyesi (garanti paketi)sağlamaktadır:

YÜKSEK ATAK POTANSİYELİ, WHITE BOX TEST, YÜKSEK KALİTE

- **EAL7:**
- **EAL6:**
- **EAL5:**
- **EAL4:**
- **EAL3:**
- **EAL2:**
- **EAL1:**

DÜŞÜK ATAK POTANSİYELİ, BLACK BOX TEST, DÜŞÜK KALİTE

3.2 SİBER GÜVENLİK ÖZEL KOMİTESİ

T.C Ulaştırma Denizcilik ve Haberleşme Bakanlığı 2013-2014 Siber Güvenlik Eylem Planı kapsamında, Türk Standardları Enstitüsüne "Sorumlu" olarak verilen ve "Kamu Kurumlarının Kritik BT ürün ve sistemlerinin asgari güvenlik gereksinimlerinin belirlenmesi ve belgelendirmenin yapılması" kapsamındaki Madde 12* yi ve "İlgili" olarak verilen Madde 10**`u gerçekleştirmek üzere, Nisan 2013`de TSE Yönetim Kurulu Kararı ile "Siber Güvenlik Özel Komitesi" kurulmuştur, bu komite kapsamında 27 tane konuda yeni innovasyon ve Arge çalışmalarına başlanmış olup, bunlar "Ulusal Koruma Profili Havuzu Projesi" kapsamında aşağıdaki Tablo 1`deki ürün gruplarında Koruma Profilleri, yeni kriter ve belgelendirmeler oluşturulmuştur:

Siber Güvenlik Eylem Planı Madde 12/a (TSE İlgili) Bilgi sistemlerinin güvenlik testlerini yapan, siber güvenlik konusunda eğitim ve danışmanlık veren, siber güvenlik konusunda belirlenecek diğer alanlarda hizmet sunan gerçek ve tüzel kişilerde bulunması gereken asgari özelliklerin belirlenmesi ve belgelendirme sürecinin tasarlanması-Eylül 2013

Siber Güvenlik Eylem Planı Madde 12/b (TSE Sorumlu): Kamu kurumları tarafından kullanılan ve siber güvenlik açısından kritik öneme sahip bilgi teknolojileri ve bilgi sistemleri ürünlerinin ve bunların sahip olması gereken asgari güvenlik gereksinimlerinin belirlenmesi ve belgelendirmenin yapılması-Ağustos 2014

Siber Güvenlik Eylem Planı Madde 10 (TSE İlgili): Kritik altyapılar için geliştirilen yazılımlar için güvenli yazılım geliştirme temel kurallarının yayımlanması

Tablo-1: Siber Güvenlik Özel Komitesi Çalışma Konuları

1	Güvenli Web Uygulamaları Koruma Profili ve Bankacılık sektörü ve Güvenli E-Ticaret Kriterleri
2	Güvenli EBYS (Elektronik Belge Yönetim Sistemi) Koruma Profili
3	Güvenli CBS (Coğrafi Bilgi Sistemleri) Koruma Profili
4	Temel Seviye Güvenlik Kriterleri Belgelendirmesi
5	Saha Güvenlik Belgelendirmesi
6	E-Kimlik Koruma Profili
7	GEM Koruma Profili
8	Mobile ID Koruma Profili
9	Güvenli IC Koruma Profili
10	Gömülü OS Koruma Profili
11	Yazılım Geliştiricisi ve Testçilerileri için Kriterlerin Belirlenmesi
12	Bulut Bilişimi
13	Sağlık Bilişimi Uygulamaları Koruma Profili
14	SSL kriterleri
15	Penetrasyon Testi yapan firmalar ve personeller için idari ve teknik kriterler
16	Biyometrik Ürünlerin Güvenlik Gereksinimleri ve Test Kriterlerinin hazırlanması
17	IT products Vulnerability Gap Library-Kütüphanesi ve Web sitesinin hazırlanması
18	Mobil Uygulamalar Koruma Profili
19	Web Servisleri Koruma Profili
20	Veri Merkezleri (Sistem Odaları) Belgelendirmesi
21	Savunma Sanayi Ürünleri Test Kriterleri

4. **Akıllı Kartlar Güvenliği Türkiye Konsorsiyumu (Smart Card Security Turkey Consortium, SCS-Turkey):**

TOBB, SABANCI, İTÜ, TÜBİTAK ve TSE olmak üzere 5 ortakla kurulmuş olup, amaç SOGIS-MRA ya girmektir, Japonya` da da benzeri bir konsorsiyum oluşturulmuş olup, Akıllı Kartların güvenliği konusunda 8 adet Koruma Profili hazırlanmaya başlanmıştır.

SCS TURKEY
SMART CARD SECURITY TURKEY CONSORTIUM

5. **TSE KRİPTO BELGELENDİRMESİ- Kripto Modül Doğrulama Programı (CMVP)**

Kripto Algoritma Doğrulama Programı (CAVP)

Kripto Modülleri İçin Güvenlik Gereksinimleri(TS ISO/IEC 19790)

Kripto Modülleri İçin Test Gereksinimleri(TS ISO/IEC 24759)

Güvelik seviyeleri:

- Güvenlik Seviyesi 1
- Güvenlik Seviyesi 2
- Güvenlik Seviyesi
- Güvenlik Seviyesi 4

TSE CRYPTO

Değerlendirmeler 10 ayrı alana göre yapılmaktadır. Bu alanlar;

1) Kriptografik Modül Spesifikasyonu
2) Kriptografik Modül Port ve Arayüzleri
3) Roller, Servisler ve Kimlik Doğrulama
4) Sonlu Durum Modeli
5) Fiziksel Güvenlik
6) Çalışma Ortamı
7) Kriptografik Anahtar Yönetimi
8) Oto Sınama
9) Tasarım Güvencesi
10) Diğer Ataklara Karşı Savunma

SONUÇ

BT ürün ve sistemleri, uluslar arası Bilişim ve Siber Güvenlik Standartlarından bağımsız, akredite laboratuvarlarda test ve bağımsız belgelendirme makamlarından belgelendirilmesi, siber savaşlar karşısında alınan savunma yöntemlerinden biridir.

KAYNAKÇA

[1] http://bilisim.tse.org.tr/
[2] www.commoncriteriaportal.org
[3] 20.06.2013 tarihli Resmi Gazetede yayımlanan "Siber Güvenlik Eylem Planı"
[4] TS ISO/IEC 15408: BT Ürün Güvenliği standardı
[5] TS ISO/IEC 19790 ve 24759: Kripto Modülleri Güvenlik ve Test Gereksinimleri Standartları