TÜRKİYE'DE YAZILIM/DONANIM GÜVENLİĞİ DEĞERLENDİRME ÇALIŞMALARI

Mehmet KARA
TÜBİTAK-UEKAE
mkara@uekae.tubitak.gov.tr

ABSTRACT

Information system software and hardware are used widespread in our life and these products include vulnerabilities. Unconscious system users and attackers can use these vulnerabilities. As a result of attacks information systems' confidentiality, integrity or availability are to be danger. Information system products' security process have been carried out since 1970's. Many national standards and guidelines (like ITSEC, TCSEC etc.) were used European countries and United States. So today producer try to design more secure and reliable information systems software and hardware prevent to information system attacks. In this article we study evaluation of the security products according to ISO IEC 15408 standards by the independent security laboratories in the world and Turkey. In addition to development and properties of ISO IEC 15408 standard we take up information system hardware and software products security evaluation in Turkey.

Key words: common criteria, network security, security testing, international standard

1. GİRİŞ

Bilgi sistemleri üzerindeki güvenlik çalışmalarına ilk olarak 1970'li yılların başında başlanmış ve yıllar içerisinde kapsamı ve derinliği genişletilerek sürdürülmüştür. Yazılım/Donanım ve sistem güvenliği değerlendirmesi konusundaki ilk çalışmalar, Orange Book olarak da bilinen TCSEC (Trusted Computer System Evaluation Criteria) standardının 1983 yılında Amerika Birleşik Devletleri Savunma Bakanlığı (USA Department of Defense) tarafından yayınlanması ile başlamıştır [1]. 1985 yılında, TCSEC güncellenmiştir. 1980'li yıllarda Avrupa'da; İngiltere, Almanya, Fransa ve Hollanda kendi güvenlik test metodolojilerini oluşturmuşlardır. Daha sonra Avrupa Komisyonu değerlendirme standartları aradaki farkları ortadan kaldırmak, bir yerde yapılan değerlendirmenin her yerde geçerli olmasını sağlayabilmek için bu ülkeler bir araya gelerek 1991 yılında ITSEC (Information Technology Security Evaluation Criteria) standardını oluşturmuşlardır [2]. Kanada' da CTCPEC (Canadian Trusted Computer Product Evaluation Criteria) standardı ITSEC ve TCSEC'den faydalanarak 1993 yılında milli değerlendirme standardını yayınlanmıştır. Aynı yılda ABD'de FC (Federal Criteria for Information Technology Security) sürüm 1.0 ITSEC konseptlerinden faydalanılarak yayınlanmıştır.

Güvenlik standartlarının ya da kılavuzlarının kullanılmasının temel sebebi, bu alanda üretilen yazılım/donanımların ya da sistemlerin, bağımsız laboratuarlar tarafından belirli kurallar çerçevesinde test ve değerlendirmesini sağlamaktır. Bu test ve değerlendirmenin temel amacı, iddia edilen güvenlik fonksiyonlarının cihaz üzerinde eksiksiz ve karşılıklı destekleyici olarak gerçekleştirildiğini kontrol etmek ve iddia edilen garanti seviyesinin sağlanıp sağlanmadığını belirlemektir. Bu yüzden de dünyanın değişik ülkelerinde değişik güvenlik değerlendirme standartları kullanılmıştır.

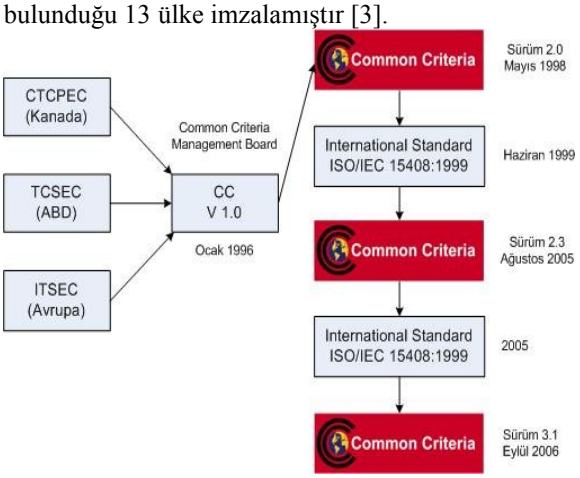
Avrupa Kanada ve Amerika Birleşik Devletleri'nde üretilen yazılım/donanım ve sistemlerin farklı farklı standartlara göre güvenlik değerlendirmelerinin gerçekleştirilmesi, uluslararası satılan ürünlere uygulanmış testlerin diğer ülkelerde anlaşılmamasına, yazılım/donanım ve sistem güvenliği konusundaki çalışmaların farklı ülkeler arasında farklı şekilde geliştirilmeye çalışılması sorunlara sebep olmuştur. Bu sorunların önüne geçilebilmesi için Kanada, Fransa, Almanya, İngiltere, Avustralya, Yeni Zelanda ve Amerika Birleşik Devletleri 1996 yılında bir araya gelerek Ortak Kriterler (Common Criteria) sürüm 1.0 dokümanını yayınlamışlardır. Bu standardın başlıca amacı bilgi sistemlerinde kullanılan yazılım/donanım ve sistemlerin güvenli olarak tasarlanması ve iddia ettikleri garanti seviyesini sağlayıp sağlamadığının belirlemektir. 1998 yılında standardın 2.0 sürümü yayınlanmıştır. 1999 yılında Ortak Kriterler tarafından yayınlanan Ortak Kriterler Standardı sürüm 2.0, ISO (International Organization for Standardization) tarafından ISO/IEC 15408:1999 standardı olarak yayınlanmıştır. Yine aynı yıl Ortak Kriterler tarafından 2.1 sürüm numaralı dokümanı yayınlanmıştır.

2005 yılında Ortak Kriterler Standardı 2.3 sürümü yayınlanmıştır. Aynı doküman ISO tarafından ISO/IEC 15408:2005 standart numarası ile yayınlanmıştır. Ortak Kriterler Standardının

uygulamasını sağlayan CEM (Common Evaluation Methodologie) dokümanı ISO tarafından ISO/IEC 18405:2005 standardı olarak yayınlanmıştır.Şekil 1'de Ortak Kriterlerin tarihsel gelişimi görülmektedir.

2006 yılında Ortak Kriterler'in 3.1 sürümü yayınlanmıştır. Aynı doküman ISO tarafından ISO/IEC 15408 standardı olarak yayınlanması beklenmektedir.

Ortak Kriterler standardı dünyada gün geçtikçe yaygın hale gelmektedir. Hali hazırda dünyada CCRA'yi (Common Criteria Recognition Arrangement) sertifika üreticisi olarak 11 ülke, sertifika tüketicisi olarak Türkiye'nin de aralarında bulunduğu 13 ülke imzalamıştır [3].



Şekil 1 Ortak Kriterlerin gelişimi

2. ORTAK KRİTERLERİN İÇERİĞİ

Ortak Kriterler üç bölümden oluşmaktadır[7].

Bölüm 1, Giriş ve Genel Model, Ortak Kriterlere giriş niteliğindedir. Bu bölüm BT güvenlik değerlendirmelerinin temel konsept ve prensiplerini tanımlar nitelikte olup genel bir değerlendirme modeli sunmaktadır. Bölüm aynı zamanda BT güvenlik hedeflerinin oluşturulması, BT (Bilişim Teknolojileri) güvenlik gereksinimlerinin seçilmesi, tanımlanması ve ürünlerin/sistemlerin üst düzey özelliklerinin yazılması konusunda bilgiler içermektedir. Ayrıca standardın bütün bölümlerinin bütün potansiyel kullanıcılar için nasıl kullanılacağı da bu bölümde tanımlanmaktadır.

Bölüm 2, Güvenlik Fonksiyonel Gereksinimleri, değerlendirme hedefinin güvenlik fonksiyonel gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik fonksiyonel bileşenleri kümesi bu bölümde listelenmektedir. Standardın ikinci bölümü fonksiyonel bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır.

Bölüm 3, Güvenlik Garanti Gereksinimleri, değerlendirme hedefinin güvenlik garanti gereksinimlerinin standart bir dille anlatılabilmesini sağlamak için tanımlanmış olan güvenlik garanti bileşenleri kümesi bu bölümde listelenmektedir. Standardın üçüncü bölümü garanti bileşenlerini, ailelerini ve sınıflarını kataloglar halinde tanımlamaktadır.

3. ORTAK KRİTERLERİN YAPI TAŞLARI

A. Güvenlik Fonksiyonel Gereksinimleri

Güvenlik fonksiyonel gereksinimleri sınıflara ayrılmıştır. Sınıflar güvenlik gereksinimlerinin en genel gruplarıdır ve bir sınıfın bütün üyeleri ortak bir konuda odaklanmışlardır. Ortak Kriterlerin ikinci bölümünde 11 tane fonksiyonel sınıf vardır. Bu sınıflar;

- FAU: Security audit (Güvenlik denetimi)
- FCO: Communication (İletişim)
- FCS: Cryptographic support (Kriptografi desteği)
- FDP: User data protection (Kullanıcı verilerinin korunması)
- FIA: Identification and authentication (Tanıma ve kimlik doğrulama)
- FMT: Security management (Güvenlik yönetimi)
- FPR: Privacy (Gizlilik)
- FPT: Protection of the TSF (TSF'nin korunması)
- FRU: Resource utilisation (Kaynak kullanımı)
- FTA: TOE access (TOE erişimi)
- FTP: Trusted path/channels (Güvenilir yollar/kanallar)

Bütün bu sınıflar çeşitli sayılarda aileler içermektedir. Ailelerin içindeki gereksinimler güvenlik amaçlarını paylaşmaktadır fakat bu gereksinimlerin yaptıkları vurgular farklıdır. Örneğin, güvenlik denetimi sınıfı denetlemenin farklı yönleriyle ilgilenen altı aile içermektedir.

Bütün aileler bir veya daha fazla bileşen içermektedir ve bu bileşenler arasında bir hiyerarşi olabilir veya olmayabilir. Örneğin, veri üretimi denetimi birbirleri arasında hiyerarşi olmayan iki bileşen içermektedir, bu bileşenlerden biri denetim kayıtlarının üretimi diğeri de kullanıcılar ile denetlenecek olayların eşleştirilmesi ile ilgilenmektedir.

B. Güvenlik Garanti Gereksinimleri

Güvenlik garanti gereksinimleri sınıflara ayrılmıştır. Sınıflar güvenlik gereksinimlerinin en genel gruplarıdır ve bir sınıfın bütün üyeleri ortak bir konuda odaklanmışlardır. Ortak Kriterlerin üçüncü bölümünde 8 tane garanti sınıfı vardır. Bu sınıflar;

- ACM: Configuration Management (Konfigürasyon yönetimi)
- ADO: Delivery and Operation (Dağıtım ve işletim)
- ADV: Development (Geliştirme)
- AGD: Guidance Documents (Kılavuz dokümanları)
- ALC: Life Cycle Support (Hayat döngüsü desteği)
- ATE: Tests (Testler)
- AVA: Vulnerability Assessment (Açıklık değerlendirmesi)
- AMA: Maintenance of Assurance (Garantinin sürdürülmesi)

İki tane garanti sınıfı da, APE ve ASE sırasıyla Koruma Profilleri ve Güvenlik Hedefleri için garanti gereksinimlerini içermektedir.

Bütün bu sınıflar çeşitli sayılarda aileler içermektedir. Ailelerin içindeki gereksinimler güvenlik amaçlarını paylaşmaktadır fakat bu gereksinimlerin yaptıkları vurgular farklıdır. Örneğin, geliştirme sınıfı tasarım dokümantasyonunun farklı yönleriyle ilgilenen yedi farklı aile içermektedir (Functional Specification, High-Level Design, Low-Level Design, Implementation Representation, TSF Internals, Representation Correspondence, Security Policy Model).

Bütün aileler bir veya daha fazla bileşen içermektedir ve bu bileşenler arasında bir hiyerarşi vardır. Örneğin, fonksiyonel spesifikasyon ailesi birbirleri arasında hiyerarşi olan ve fonksiyonel spesifikasyonun bütünlüğü ve biçimselliği ile ilgilenen dört bileşen içermektedir.

Ortak Kriterler Değerlendirme Garanti Seviyesi (EAL) olarak bilinen yedi adet garanti paketi tanımlamaktadır. Bu yedi garanti seviyesi aşağıdaki gibidir;
EAL1 – fonksiyonel olarak test edilmiş
EAL2 – yapısal olarak test edilmiş
EAL3 – metodolojik olarak test edilmiş ve kontrol edilmiş
EAL4 – metodolojik olarak tasarlanmış, test edilmiş ve incelenmiş
EAL5 – yarı biçimsel olarak tasarlanmış ve test edilmiş
EAL6 – yarı biçimsel olarak doğrulanarak tasarlanmış ve test edilmiş
EAL7 – biçimsel olarak doğrulanarak tasarlanmış ve test edilmiş
Güvenlik Hedefi dokümanı oluşturulurken ürünün güvenlik garanti gereksinimleri belirtilmektedir. Bu gereksinimler belirtilirken garanti seviyelerinden biri seçilmeli ve bu seviyenin gerektirdiği bileşenler listelenmelidir. Ayrıca gerekiyorsa bu bileşenlere üçüncü bölümden ekler yapılabilir veya yeni oluşturulmuş garanti bileşenleri eklenebilir.

Aşağıda bu yedi değerlendirme garanti seviyesi özetlenmektedir. EAL1 giriş düzeyinde bir garanti seviyesidir. Garanti seviyesi artırıldıkça, değerlendirmede detaya inen bileşenler kullanılmaktadır. Fakat herhangi özelleşmiş bir güvenlik yöntemi tanıtılmamaktadır. EAL1 ve EAL3 arasındaki seviyeler genel olarak geliştirilme aşamasında Ortak Kriter değerlendirmesi hesaba katılmadan tasarlanan ürünler için tavsiye edilmektedir.

EAL4 ve üzerindeki garanti seviyelerinden birine uygunluk iddia edebilecek bir ürün, tasarım aşamasından itibaren Ortak Kriterler standardı takip edilerek geliştirilmelidir.

EAL7 düzeyinde hem geliştirici için hem de değerlendirici için maliyet arttıran eylemler bulunduğu için bu seviyenin pratikte gerçeklenmesinin zorlukları bulunmaktadır.

EAL1: Bu seviye ürünün veya sistemin doğru çalıştığına dair güvenin yeterli olduğu ve güvenlik tehditlerinin ciddi olmadığı durumlarda kullanılmaktadır. Bu seviyede yapılan değerlendirmelerde, müşteriye ürün hakkında bağımsız testler ve kılavuz dokümanları hakkında inceleme sonuçları sunulmaktadır.

EAL2: Bu seviyede değerlendirme yapabilmek için ürün geliştirici tasarım bilgilerini ve test sonuçlarını değerlendirme laboratuarına iletmelidir. Ürün geliştiriciden değerlendirme sırasında talep edilecek değerlendirme delilleri fazladan zaman ve maliyet gerektirmemektedir.

EAL2 değerlendirmesi, müşteriler veya ürün geliştiriciler düşük ve orta düzey seviye arasında bir güvenlik gereksinimi duyuyorlar ise ve ürünün geliştirme dokümanlarının tamamına ulaşamıyorlar ise uygulanmaktadır.

EAL3: EAL3 seviyesinde standart, ürün geliştiriciye tasarım sırasında maksimum garanti sağlayabilmesi için yöntemler önermektedir. Geliştiriciler veya müşteriler orta seviyede güvenlik ve bağımsız bir garanti ihtiyacı duydukları

durumlarda bu seviye kullanılmaktadır. EAL3 değerlendirmesi üreticinin test sonuçlarının seçilerek onaylanması ve bilinen açıklıkların üretici tarafından incelendiğinin kanıtlanmasını içeren gri kutu testleri (grey box testing) ile desteklenmektedir. Ayrıca geliştirme ortamı kontrolleri ve ürünün konfigürasyon yönetimi delilleri değerlendirmeler için gerekmektedir.

EAL4: EAL4 seviyesi ticari ürün geliştirme yöntemlerinden maksimum garanti sağlayabilmek için ürün geliştiricilere yöntemler önermektedir. EAL4 var olan ürün geliştirme altyapısını değiştirmeden ulaşılabilecek en yüksek garanti seviyesidir. Ürün geliştiricilerin ve müşterilerin orta seviye ile yüksek seviye arasında bir güvenlik ve bağımsız bir garanti ihtiyacı duyduklarında kullandıkları seviyedir. EAL4 değerlendirmesi ürünün alt düzey tasarımı ve uygulamanın alt kümelerinin analizi ile de desteklenen bir süreçtir. Yapılan testler bağımsız açıklık analizleri ile desteklenir. Geliştirme kontrolleri yaşam döngüsü desteği, tanımlama teknik ve araçları ve otomatik konfigürasyon yönetimi ile güçlendirilir.

EAL5: EAL5 seviyesi, özel güvenlik tekniklerinin orta düzeyde uygulanması ile desteklenen, ticari ürün geliştirme yöntemlerinden maksimum garanti sağlayabilmek için ürün geliştiricilere yöntemler önermektedir. Bu seviyeye aday bir ürün seviyenin gerektirdiği garantiyi sağlayabilecek bir şekilde tasarlanmalı ve geliştirilmelidir. Bu seviye ürün geliştiricileri ve müşteriler yüksek seviyede güvenlik ve bağımsız bir garanti ihtiyacı duyduklarında kullanılmaktadır. EAL5 değerlendirmesi bütün ürün gerçeklemesini içermektedir. Garanti biçimsel bir modelleme, yarı biçimsel bir fonksiyonel spesifikasyon ve üst düzey tasarım ve yarı biçimsel bir eşleştirme ile sağlanmaktadır. Açıklık analizleri kesinlikle yüksek atak potansiyeli olan saldırganlara karşı direnci ölçebilmelidir. Örtülü kanal analizi ve modüler tasarım ayrıca gerekmektedir.

EAL6: EAL6 seviyesi yüksek değerdeki varlıkları korumakta olan ürünler için yüksek garanti seviyesi sağlayan güvenlik teknikleri önermektedir. Bu seviyede ürün geliştirirken dikkat edilmesi gereken nokta ürünün koruyacağı varlıkların değerinin bu seviyede ürün geliştirmenin getireceği maliyeti karşılayacak nitelikte olmasıdır. EAL6 değerlendirmesi tasarımın modüler ve katmanlı bir yaklaşımla ve gerçeklemenin yapısal bir sunumu ile desteklenen bir analizle sağlanmaktadır. Bağımsız açıklık analizleri yüksek atak potansiyeli olan saldırganlara karşı direnci ölçebilmelidir. Örtülü kanal analizi sistematik olarak yapılmalıdır. Geliştirme ortamı ve konfigürasyon yönetimi kontrolleri güçlendirilmelidir.

EAL7: EAL7 seviyesi son derece yüksek risk durumlarında veya korunan varlıkların bu seviyenin getireceği maliyeti karşılayabileceği durumlarda uygulanabilmektedir. EAL7 değerlendirmesinde fonksiyonel spesifikasyonun ve üst düzey tasarımın biçimsel bir sunumu ile biçimsel bir model sunulmaktadır. Ürün geliştiricinin beyaz kutu testlerinin (white box testing) kanıtları ve bu test sonuçlarının bağımsız bir onayı gerekmektedir. Tasarımın karmaşıklığı en düşük değerde olmalıdır.

4. ORAK KRİTERLERİN TARAFLARI

Bir Ortak Kriterler değerlendirmesinde; Müşteriler, geliştiriciler, sponsorlar, değerlendirme laboratuarları ve sertifikasyon makamı bulunmaktadır. Bunların iletişimi sonucunda bir ürün veya sistem değerlendirilmektedir.

Müşteriler; Ortak Kriterler Standardını, teknik ve prosedürel gereksinimlerini tam olarak ifade edebilmek için kullanılabilmektedir. Müşteriler değerlendirme sonuçlarını, değerlendirilmiş bir ürünün kendi ihtiyaçlarını karşılayıp karşılamadığına karar vermek için kullanabilirler. Aynı zamanda alacakları ürünün ya da sistemin iddia edilen güvenlik özelliklerinin bağımsız bir laboratuar tarafından onaylanmasını sağlamış olurlar. Müşteriler standarda uygun olarak hazırlayabilecekleri Koruma Profilleri (Protection Profile) aracılığıyla BT güvenlik ölçütleri konusunda özel gereksinimleri varsa belirtebilirler.

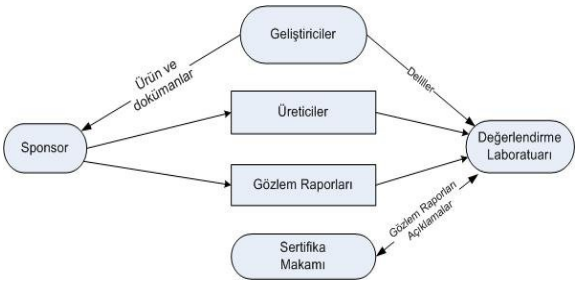
Geliştiriciler, Ortak Kriterlere göre değerlendirecek ürünü hazırlayacak taraftır. Geliştiricilerin, Ortak Kriterler Standardını ve değerlendirme sürecinin nasıl işlediğini bilmesi gerekmektedir. Gereksinimler müşterilerin özel ihtiyaçlarından belirlenebileceği gibi pazardaki ihtiyaçlara göre de bu gereksinimler tespit edebilirler. Ürün geliştiriciler, Koruma Profilinin nasıl oluşturulduğunu ve nasıl kullanılabileceğini incelemelidirler, bu sayede Koruma Profillerine uygunluk sağlayan ve müşterilerin gereksinimleri doğrultusunda ürün geliştirebilirler.

Sponsor, ürünlerin sertifika alması için ürün ve değerlendirme delilleri ile birlikte laboratuara değerlendirme için başvuran taraftır. Sponsor geliştirici olabileceği gibi başka bir firma da olabilir. Bu konuda Ortak Kriterler standardı pratik ve ulaşılabilir kriterler koymaktadır. Geliştiriciler tasarım aşamasından itibaren bu kriterlere uygun davrandıkları takdirde ürün sonlandıktan sonra sertifika almaları kolay olmaktadır. Sponsor, değerlendirme süresince ürün ve dokümantasyonla ilgili Ortak Kriterler laboratuarı ile sürekli haberleşerek değerlendirme sürecinin bir parçası olur.

Değerlendirme laboratuarı, yazılım/donanım ya da sistemin değerlendirmesini yapan taraftır. Yazılım/donanım veya sistem değerlendirme delilleri ile birlikte sponsor tarafında laboratuara sunulur. Laboratuar standarda uygun olarak ürünü veya sistemi değerlendirir ve değerlendirme sonucunu bir rapor ile sertifika makamına bildirir. Laboratuar, değerlendirme sürecinde sponsor ve sertifika makamı ile değerlendirme konusunda gerektikçe haberleşir.

Sertifika makamı, değerlendirme laboratuarlarına lisan veren kurumdur. Sertifika makamı değerlendirme sürecini izleyen ve değerlendirme sonucunda da laboratuar tarafından üretilen değerlendirme teknik raporuna göre ürünü sertifikalandıran taraftır.

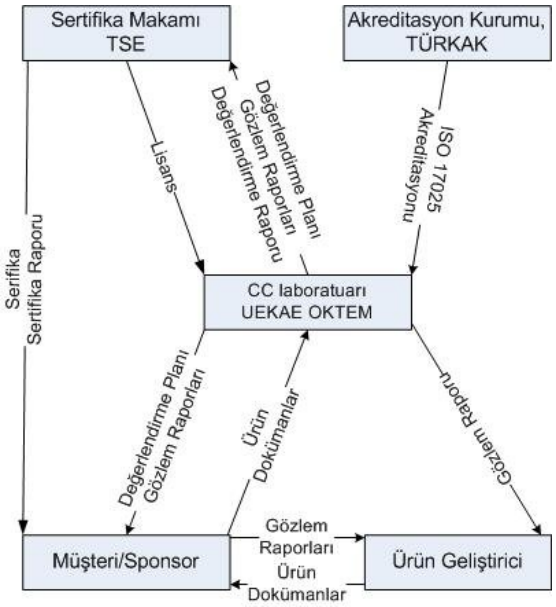
Şekil 2'de Ortak Kriterlerin tarafları görülmektedir.



Şekil 2 Ortak kriterlerin tarafları

4.1 Akreditasyon ve Onay

Ortak Kriterler modeli değerlendirme ve sertifikasyon işlerini ve bu işleri yapacak kurumların rollerini ve sorumluluklarını birbirinden ayırmaktadır. Sertifikalar, ulusal yapılar tarafından lisanslanmış, bağımsız değerlendirme laboratuarlarının değerlendirme teknik raporu baz alınarak verilir. Değerlendirme laboratuarları genelde TS EN ISO/IEC 17025 akreditasyonu almış bağımsız kuruluşlardır. Ortak Kriter değerlendirmeleri yapabilmek için ulusal Ortak Kriterler yapısının Sertifikasyon Kurumu'ndan lisans almaları gerekir. Şekil 3'de Türkiye'deki yapı görülmektedir.



Şekil 3 Ortak Kriterler Türkiye yapısı

Bu yapıda Ortak Kriterler laboratuarı ilk olarak TS EN ISO/IEC 17025 standardına göre bir akreditasyon kurumundan akredite olur. Bu genellikle ülkenin akreditasyon kurumu tarafından yapılır. Bu akreditasyon laboratuarın belirtilen kapsamdaki Ortak Kriterler değerlendirmelerini yapabilecek personeli ve cihazı olduğunu ve laboratuarın TS EN ISO/IEC 17025 standardının gereklerini yerine getirdiğini göstermektedir. Laboratuar bu yapısı ile kendisine değerlendirme için gelen ürünleri değerlendirir ve onlara ait değerlendirme teknik raporu üretir.

Laboratuar akreditasyon işlemlerini tamamladıktan sonra laboratuarın değerlendirdiği ürünlerin sertifikalanabilmesi için, her bir ülke bir tane olan, sertifikasyon makamına başvurur. Sertifikasyon makamı ülkedeki Ortak Kriterler laboratuarlarını denetleyerek onları sertifikalandıran bir kuruluştur. Sertifikalandırma işleminden sonra sertifikasyon makamı değerlendirme süreçlerini yakından izleyerek laboratuarın değerlendirdiği ürünlere sertifika verir.

Bu yapıda ilk olarak OKTEM laboratuarı TÜBİTAK-UEKAE bünyesinde 2001 yılında kurularak Ortak Kriterler konusunda çalışmalarına başlamıştır. Laboratuar 2005 yılında TÜRKAK (Türk Akreditasyon Kurumu) tarafından TS EN ISO/IEC 17025 standardına göre akredite olmuştur. Bu akreditasyon OKTEM laboratuarının Ortak Kriterlerin PP, ST,EAL1, EAL2, EAL3, EAL4 değerlendirmelerin yapabilecek personeli ve cihazı olduğunu ve laboratuarın TS EN ISO/IEC 17025 standardının gereklerini yerine getirdiğini göstermektedir.

OKTEM laboratuarı, TSE bünyesinde kurulmuş olan Ulusal Sertifika makamından Aralık 2007'de geçici lisans almıştır. Halen sertifikasyon makamı ile lisanslama çalışmaları ve değerlendirmeler sürdürülmektedir.

Sertifikasyon Makamı(TSE) tarafından 2003 yılında kurulmuş ve aynı yıl CCRA'e sertifika müşterisi (Certificate Consuming) olarak üye olunmuştur. TSE, CCRA'e sertifika üretici (Certificate Authorizing) olarak üye olan ülkelerin değerlendirmelerini kabul etmiştir. Halen Türkiye'nin Sertifika üreticisi olma çalışmaları devam etmektedir.[5]

5. SONUÇ ve ÖNERİLER

Bilgisayar sistemlerinde kullanılan yazılım/donanım ya da sistemler üretilirken zayıflıklar ya da daha sonra teknolojik olaylardan dolayı açıklıklar çıkabilmektedir. Bu açıklıklar ve zayıflıklar kullanıcılar tarafından bilerek ya da bilmeden kötüye kullanılabilmektedir. Müşteriler bilgi sistemlerinde kullanacakları ürün ya da sistemlerde bu tür açıklıkların olmamasını istemektedir. Bu açıklıkları engellemenin en etkin yöntemi ise belli standartlara göre ürünün iddia ettiği güvenlik fonksiyonlarının üçüncü taraf bağımsız laboratuarlar tarafından test edilmesi ve değerlendirilmesidir. Bu test ve değerlendirme işlemi dünyadaki birçok ülkede ve Türkiye'de Ortak Kriterler standardı ile sağlanmaktadır.

Türkiye sertifika müşterisi olarak Ortak Kriterlere göre değerlendirilmiş ürünleri kabul etmekle birlikte 2005 yılından beri BT ürünlerini EAL4 seviyesine kadar değerlendirebilmektedir. Özellikle Türkiye'de kurumların kendi sistemleri için ürettikleri ya da ürettirdiklerin yazılım/donanım veya sistemlerin güvenlik özellikleri az sayıda personelle ve sınırlı imkanlarla test edilmektedir. Bu da ciddi güvenlik açıklıklarının ortaya çıkmasına ve sonucunda da maddi ve manevi kayıplara sebep olmaktadır. Olması gereken işleyiş, kurumların kendilerinin ürettiği ya da ürettirdiği BT ürünlerinin güvenlik özelliklerini bağımsız ve yetkin laboratuarlara değerlendirtmesidir. Bu da ancak uluslararası standartlarla ve akredite laboratuarlarla mümkün olabilir.

KAYNAKLAR

[1] http://www.niap-ccevs.org/cc-scheme/cc_docs/
[2] http://www.cesg.gov.uk/site/iacs/index.cfm?menuSelected=1&displayPage=11
[3] http://www.commoncriteriaportal.org/public/expert/index.php?menu=6
[4] http://csrc.nist.gov/publications/nistbul/itl98-11.txt
[5] Mert Üneri, "*Bilgi Güvenliğinde Ortak Kriterler Serifikasyonu*", Bilgi Güvenliği ve Yazılım Kalitesi Sempozyumu, Mart, 2007.
[6] *Information Technology Security Evaluation Criteria (ITSEC)* , June 1991, ISBN 92-826-3004-8, (Genel)
[7] *Common Criteria for Information Technology Security Evaluation Part I, II, III* Verison 3.1 September 2006
[8] *Ortak Kriterler Tanıtımı*, 20 Ağustos 2003, TUBİTAK-UEKAE,