BİLİŞİM TEKNOLOJİLERİ VE STANDARDİZASYON

İnan ÖZKAN
Türk Standardları Enstitüsü, Ankara
inanozkan@gmail.com

ÖZET

Bilişim teknolojilerindeki değişimin hızı her geçen gün artmaktadır. Değişime ayak uydurabilmek ve yeni nesil teknolojiler ile konuşur halde kalabilmek için elimizdeki en büyük koz standartlardır. Standartlar iş yapış yöntemlerimizden, ürettiğimiz ürüne, şirket personelinin yetkinliklerinden dokümantasyon yapımıza kadar her alana dokunmakta ve dokunduğu alanları geleceğe hazırlamaktadır. Ülkemizde de her alanda olduğu gibi bilişim alanında da standardizasyon ihtiyacı her geçen gün daha fazla hissedilmekte ve talep edilmektedir. İhtiyaçlara cevap verebilmek adına bilişim teknolojileri alanında ürün, sistem, personel ve test anlamında ulusal ve uluslararası standartlar ülkemizde de takip edilmekte ve yaygınlaştırma çalışmaları titizlikle yürütülmektedir. Çalışma içerisinde ülkemizde son yıllarda kamu kurum ve kuruluşları tarafından talep edilerek mevzuatın parçası haline gelmiş olan standartlar ile yaşanılan sorunlara çözüm önerisi getiren standardizasyon faaliyetleri ele alınacaktır. Standardizasyon faaliyetleri içerisinde Beyaz Şapkalı Hacker, Ortak Kriterler, SPICE, Bilgi Güvenliği Yönetimi gibi hizmetlerin ön planı çıktığı görülmekle birlikte hemen hemen ihtiyaç olan her alan için çözüm getiren bir standardın ele alındığı ve gerekli uygunluk değerlendirme faaliyetleri için altyapının hazırlanmış olduğu görülmüştür.

Anahtar Kelimeler
Bilişim Teknolojileri; Standardizasyon; Ortak Kriterler; SPICE.

ABSTRACT

The speed of change in information technologies is increasing day by day. Standard is the biggest trump card to be able to keep up with changing trends and stay in touch with the next generation of technology. The standards touch in every field from our methods of doing business, to the product we produce, from the competencies of company personnel to the production of documentation and prepare us for the future. As is the case in every field in our country, the need for standardization in the field of information technology is felt more and more every day. In order to be able to respond to needs, national and international standards in terms of products, systems, personnel and testing are followed and dissemination efforts are carried out meticulously in our country. In this study, the standardization activities which are proposed by the public institutions and organizations in recent years in our country and which have proposed the solution to the problems with the standards which have become part of the legislation will be discussed. While it seems that the standardization activities such as White Hat Hacker, Common Criteria, SPICE, Information Security Management have come into prominence, it has been seen that there is a standard that provides solution for almost every field is dealt with and infrastructure for necessary conformity assessment activities is prepared.

Keywords
Information Technologies; Standardization; Common Criteria; SPICE.

GİRİŞ

Standart kelimesinin zihinlerde ilk yaptığı çağrışım tekilliktir. Standartlar, tek ve biri yani olması gerekeni ilgilendiği konu için ortaya koymaya çalışırlar. Ancak standart kelimesi için dahi kısa bir araştırma ile birçok farklı tanım elde edebiliriz. İlk kaynak olarak Türk Dil Kurumu standart kelimesini sıfat olarak [1] "belli bir tipe göre yapılmış veya ayrılmış", "belirli ölçülere, yasaya, kullanıma uygun olan" ve "örnek veya temel olarak alınabilen" şeklinde 3 farklı şekilde tanımlarken Türk Standardları Enstitüsü (TSE)[2] "imalatta, anlayışta, ölçme ve deneyde örnekliktir" şeklinde tanımlamaktadır. Örnek verdiğimiz tanımları araştırmayı derinleştirerek çoğaltabilir hatta bizlerde kendi tanımımızı ortaya koyabiliriz. Bu durumda "insanlık için tekliğin ve birliğin sembolü olan standardın nasıl olurda tek bir tanımı olmaz?" sorusunu sormak kaçınılmaz hale gelmektedir. Her ne kadar farklı şekillerde tanımlasak dahi tanımlarımızın tamamı aynı hedefe ulaşmak için kullandığımız farklı yollar olarak görülmelidir. Standardizasyon faaliyetleri de bu anlamda standartları temel alarak farklı yollardan aynı hedef ulaşma çabası olarak görülmelidir. Standartlar ile hedeflenen faydalar[3] herkes için güvenlik, güvenilirlik, koruma, birlikte çalışabilirlik, ekonomik getiri ve yeni seçeneklerin ortaya konulabilmesi olarak özetlenebilir. Standartsız bir dünya hayal edildiğinde ürünlerin istenildiği gibi çalışmadığı, kalitesinin beklentileri yakalayamadığı, diğerleri ile uyumu sağlayamadığı, tek bir üretici ile kısıtlı kalınması zorunluluğunun ortaya çıktığı, üreticilerin en basit çözüm için dahi kendi kapasiteleri ile kısıtlı kalması sebebiyle inovasyonun hız kestiği ve daha kötüsü ürünlerin sağlığı ve yaşamı tehdit ettiği görülecektir[4]. Tüm bu olumsuzlukların günlük hayatımızın tüm alanlarında altyapıların temel taşı haline gelmiş olan bilişim teknolojileri ürünlerinde yaşandığını varsaydığımız da yaşanamaz bir ortamla yüz yüze

kalacağımız ve bu nedenle bilişim teknolojileri alanında da standartlara ve standardizasyon faaliyetlerine yaşanabilir bir dünya için muhtaç olduğumuz aşikardır.

Bilişim teknolojilerinde standardizasyon faaliyetlerini ihtiyaca göre farklı şekillerde ele alabiliriz. Sınıflandırmayı standardı ortaya konulan olgu yönünden sistem, ürün veya kişi olarak yapabileceğimiz gibi ihtiyaç duyulan özellikler yönünden de kalite ve güvenlik şeklinde yapmakta mümkündür. Bilişim teknolojileri alanında hangi sınıf ve türde olursa olsun standardizasyon ihtiyacını karşılamak ve sorunlara standartlar üzerinden çözüm getirmek adına çalışmalar yapılmaktadır. Çoğunlukla uluslararası çalışmalar takip edilerek kimi zamanda doğrudan sektörden gelen talepler dolayısıyla güncel ve en uygun çözümlerin henüz sorunlar yaşanmadan ülkemize getirilmesi ve standardizasyon altyapısının kurulması sağlanmaktadır. Ülkemizde tüm standardizasyon faaliyetlerinden sorumlu resmi kurum olarak TSE, bilişim teknolojileri alanına da ayrı önem vermektedir. Bilişim teknolojileri standardizasyon faaliyetlerinden sorumlu olacak şekilde TSE bünyesinde çalışmalar oldukça eski yıllara dayanmakla birlikte işler hale getirilen ilk belgelendirme sistemi 2000'li yılların sonlarına doğru kurulmuştur. Değişen ve artan ihtiyaçlar sonrasında TSE bünyesinde Bilişim Teknolojileri Test ve Belgelendirme Dairesi Başkanlığı kurularak standardizasyon faaliyetlerinin etkin ve hızlı şekilde karşılanması amaçlanmıştır. Her ne kadar standardizasyon kurumu tarafından gerekli altyapı kurulmuş ve belgelendirme sistemleri oluşturulmuş olsa da ülkemizdeki standardizasyon farkındalığının eksikliği nedeniyle yaşanan sorunlar gözle görünür hale gelene kadar standartları kullanmakta sektörün büyük bir çekincesi olduğu göz ardı edilemeyecek bir gerçektir. Bu durumda gönüllü bir faaliyet olan standardizasyon çalışmalarına kanun koyucular tarafından mevzuat içerisinde doğrudan atıfta bulunularak sektörün zorunlu olarak standardizasyon faaliyetlerine katılımı sağlanmaktadır.

Bu çalışmada ülkemizde bilişim teknolojileri alanında gerçekleştirilen gönüllü ve zorunlu standardizasyon faaliyetleri ile bu faaliyetlerin konu edindiği bilişim teknolojileri standartları ilgili bilgiler sunulacaktır.

TS EN ISO/IEC 27001 BİLGİ GÜVENLİĞİ YÖNETİM SİSTEMİ

Bilgi taşıdığı değere nispetle varlık sınıflandırmamız arasında en önde gelmektedir. Bilginin taşıdığı değer nedeniyle onu korumak için elimizden geleni yaparız. Koruma çabasının boşa gitmemesi ve amacına ulaşabilmesi için teknolojik çözümlerle birlikte sağlam bir güvenlik yönetim sisteminin kurulması gerekmektedir. İhtiyaç duyduğumuz etkin bilgi güvenliği sisteminin oluşturulabilmesi için geliştirilen TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi[5] standardı bilgi güvenliğini 7 ana madde ve 14 kontrol başlığı altında ele almaktadır. Ele alınması gereken 14 kontrol başlığı şöyledir:

1. Güvenlik Politikası
2. Bilgi Güvenliği Organizasyonu
3. İnsan Kaynakları Güvenliği
4. Varlık Yönetimi
5. Erişim Kontrolü
6. Kriptografi
7. Fiziksel ve Çevresel Güvenlik
8. Operasyon Güvenliği
9. İletişim Güvenliği
10. Sistem Tedariği, Geliştirme ve Bakımı
11. Tedarikçi İlişkileri
12. Bilgi Güvenliği Vaka Yönetimi
13. Bilgi Güvenliği Açısından İş Sürekliliği Yönetimi
14. Uyum

Akreditasyon kapsamında 27001 standardı bulunan 29 belgelendirme kuruluşu olduğu göz önüne alındığında ülkemizde yaygın olarak kullanılan bilişim teknolojileri standartlarının başında gelmektedir. İlgili alanındaki bazı konularda işletmelere 27001 belge alma zorunluluğu getiren kurumlar şöyledir:

- Enerji Piyasası Düzenleme Kurumu
- Gümrük ve Ticaret Bakanlığı
- Maliye Bakanlığı
- Bilgi Teknolojileri ve İletişim Kurumu
- Sivil Havacılık Genel Müdürlüğü

TS ISO/IEC 15408 ORTAK KRİTERLER

Bilişim teknolojileri ürünlerinin güvenliğine odaklanmış olan standart, Uluslararası Standardizasyon Organizasyonu (ISO) tarafından kabul edilerek yayınlanan bir standart olmakla birlikte bağımsız bir topluluk tarafından geliştirilerek güncellenmektedir[6]. Bağımsız topluluk üyesi olunabilmesi için "Ortak Kriterler Tanıma Anlaşması"na taraf olunması ve tanıma anlaşmasına taraf olacak belgelendirme makamının bulunduğu ülkenin kamu kuruluşu olması gerekmektedir. Her ülkede sadece bir adet belgelendirme makamı tanınmaktadır. Anlaşmaya taraf belgelendirme makamları "üretici üye" ve "tüketici üye" olarak ikiye ayrılmaktadır. Üretici üyeler tarafından verilen belgeler tüm üyeler tarafından kabul edilmekte iken tüketici üyelerin verdikleri belgeler sadece kendi ülkelerinde kabul görmektedir. 17 üretici ve 11 tüketici üyenin taraf olduğu anlaşmada ülkemiz TSE tarafından temsil edilmekte ve üretici üyeler arasında bulunmaktadır.

Standart üç bölüm ve bir metodoloji dokümanından oluşmaktadır:

1. Giriş ve Genel Model (Bölüm 1)
2. Güvenlik Fonksiyel Gereksinimleri (Bölüm 2)
3. Güvenlik Garanti Gereksinimleri (Bölüm 3)
4. Ortak Kriterler Değerlendirme Metodolojisi

Ortak Kriterler standardı içerisinde hedeflenebilecek 7 adet güvenlik seviyesi bulunmaktadır. Güvenlik seviyesi 1'den 7'ye doğru yükseldikçe daha detaylı tasarım dokümantasyonu ve daha derinlemesine güvenlik testleri ihtiyacı ortaya çıkmaktadır. BT ürününün yeterli bir geliştirme ortamında gerçeklenip gerçeklenmediği kontrol edilir, var olan tehditleri analiz edilir, Fonksiyonel ve bağımsız sızma testleri (açıklık analizi çalışması) yapılır ve ürüne uygun garanti seviyesinde belge verilir.

Ürünün güvenlik değerlendirmesinin yapılması ve belgelendirme faaliyetleri birbirinden ayrılmış olup değerlendirme faaliyetleri belgelendirme makamları tarafından lisanslanmış olan laboratuvarlar aracılığı ile yapılmaktadır. Değerlendirme laboratuvarında aranan ön şart TS EN ISO/IEC 17025 Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği için Genel Şartlar standardından akredite olunmasıdır. TSE belgelendirme makamının ikisi yerli olmak üzere beş adet lisanslı laboratuvarı bulunmaktadır[7]. Ayrıca TSE bünyesinde bir adet Ortak Kriterler Değerlendirme Laboratuvarı kurulması çalışmaları sürmekte olup laboratuvarın akreditasyon süreci tamamlanmıştır.

TSE belgelendirme makamı tarafından 50 adet ürüne belge verilmiş durumdadır. Ortak Kriterler ürün güvenliğini hedefleyen ve uluslararası kabul görmüş bir standart olması nedeniyle ülkemiz resmi makamları tarafından gerekli görüldüğü alanlar için zorunlu hale getirilmeye başlanmıştır. Ortak kriterler zorunluluğu olan ürünler;

1. Sağlık Bilgi Yönetim Sistemleri (Sağlık Bakanlığı)
2. Yeni Nesil Ödeme Kaydedici Cihazlar (Gelir İdaresi Başkanlığı)

TS ISO/IEC 15504 YAZILIM SÜREÇ İYİLEŞTİRME OLGUNLUK (SPICE)

SPICE (Software Process Improvement Capability dEtermination) modelinin amacı farklı yazılım süreç değerlendirme model ve yöntemleri için ortak bir ana prensip sağlamaktır[8]. Yazılım satın alma, tedarik, işletim, bakım ve destek için planlama, yönetim, icra, denetim, iyileşme, yeterlilik ve olgunluk düzeyi belirleme standardıdır. Standart içerisinde süreç setleri tanımlanmıştır. Süreç setleri 3 ana sınıf altında incelenmektedir:

1. Temel Süreçler
    a. Satın Alma Süreç Grubu
    b. Tedarik Süreç Grubu
    c. Mühendislik Süreç Grubu
    d. İşletim Süreç Grubu
2. Kurumsal Süreçler
    a. Yönetim Süreç Grubu
    b. Süreç İyileştirme Süreç Grubu
    c. Kaynak ve Altyapı Süreç Grubu
    d. Tekrar Kullanma Süreç Grubu
3. Destek Süreçler
    a. Destek Süreç Grubu

Süreç setleri ile ilişkilendirilen temel pratiklerin yanı sıra genel pratiklerde tanımlanmış olup seviye belirleme kapsamına alınmış olan süreçlere uygulanmaktadır. SPICE standardı içerisinde beş seviye bulunmaktadır. Birinci seviyede temel pratikler değerlendirilirken diğer seviyelerde genel pratikler değerlendirilmektedir.

- Seviye 1 Gerçekleştirilmiş
    - Süreç Performansı
- Seviye 2 Yönetilen
    - Performans Yönetimi
    - İş Ürünü Yönetimi
- Seviye 3 Kurulmuş
    - Süreç Tanımı
    - Süreç Düzenleme
- Seviye 4 Tahmin Edilebilir
    - Süreç Ölçümü
    - Süreç Kontrolü
- Seviye 5 En İyileştirici
    - Süreç Yenileme
    - Süreç Eniyleştirme

SPICE denetimi yapılabilmesi için en az iki kişilik denetim ekibi oluşturulmalıdır. Denetim ekibinde olacak personeller International Assessor Certification Scheme (INTACS) tarafından yetkilendirilmektedir. Yetkinin alınabilmesi için lisanslı kuruluşlardan eğitim alınmalı ve sınavdan başarı sağlanmalıdır. Denetçiler için üç seviye bulunmakta olup denetçi, uzman denetçi ve baş denetçi unvanları bulunmaktadır. Denetim ekibi biri uzman denetçi olmak üzere en az iki denetçiden oluşmalıdır. Ülkemizde akredite olarak SPICE belgesi veren tek kuruluş TSE'dir. TSE tarafından belge verilen 44 kuruluş bulunmaktadır. SPICE belgesinin zorunlu olduğu alan:

1. Sağlık Bilgi Yönetim Sistemleri (Sağlık Bakanlığı)

Ayrıca bir diğer yazılım yaşam döngüsü standardı olan TS ISO/IEC 12207 belgesi yerli malı belgesi almak

isteyen yazılımlar için TOBB Sanayi Müdürlüğü tarafından zorunlu hale getirilmiştir.

TS 13638 SIZMA TESTİ YAPAN PERSONEL VE FİRMALAR İÇİN ŞARTLAR (BEYAZ ŞAPKALI HACKER)

TS 13638 standardı ulusal standartlarımız arasında olup ülkemizin siber güvenlik alanındaki yetkin personel ihtiyacının karşılanması ve sızma testleri gerçekleştiren kuruluşların bir disiplin altına alınması hedefi ile oluşturulmuştur.

Standart işlevsel olarak hem personel ve sistem belgelendirme hem de sızma testlerinde kullanılabilecek şekilde düzenlenmiştir. Personel belgelendirme ile ilgili olarak 2 alan ve 4 seviye belirlenmiştir. Bunlar:

- Ağ ve Sistem Güvenliği
- Web ve Veritabanı Güvenliği

alanları ile

- Stajyer Sızma Testi Uzmanı
- Kayıtlı Sızma Testi Uzmanı
- Sertifikalı Sızma Testi Uzmanı
- Kıdemli Sızma Testi Uzmanı

seviyeleridir.

Sızma testi uzmanlarının belge alabilmesi için stajyer sızma testi uzmanı seviyesi en alt seviye olarak belirlenmiş ve uygulama gerektirmeyen teorik bilgi ile alınabilmektedir. Ancak diğer üst seviyeler uygulama sınavından da belirli seviyede puan almak, akademik yayın yapmak, açıklık keşfinde bulunmak gibi uzmanlığı gösterebilecek farklı şartlarla donatılmıştır. Sızma testi uzmanı belgelendirmesi için eğitim ve sınavlar düzenlenerek belgelendirme işlemi yapılması faaliyetleri TSE bünyesinde yürütülmektedir.

Sızma testi yapan firmaların belgelendirilebilmesi için öncelikle aynı standarttan belge almış sızma testi uzmanı belgesine sahip uzmanlar bulunması gerekir. Bu kısımda 3 firma seviyesi belirlenmiştir. Bunlar:

- A Seviye Sızma Testi Yapan Firma
- B Seviye Sızma Testi Yapan Firma
- C Seviye Sızma Testi Yapan Firma

C seviye sızma testi yapan firma belgesi bir kişinin çalıştığı firmalarında belgeyi alabilmesi ve sektörde önlerinin kapanmaması için oluşturulmuştur. Ayrıca bazı alanlarda TS EN ISO/IEC 27001 standardı temelli kısmi bilgi güvenliği denetimi yapılmaktadır.

B seviye ve A seviye firmalar içinse stajyer sızma testi belgesine sahip bir personelin bulunması zorunlu tutulmuştur. Böylelikle sızma testi yapan yetişmiş insan kaynağına ulaşılabilmesi hedeflenmiştir. Ayrıca B ve A seviyeleri için firmaların TS EN ISO/IEC 27001 belgesine sahip olunması zorunludur.

TS 13298 ELEKTRONİK BELGE VE ARŞİV YÖNETİM SİSTEMİ

EBYS standardı olarak bilinen TS 13298 standardı kurumlar tarafından kullanılan elektronik belge ve arşiv yönetim sistemlerinin sahip olması gereken özellikleri ortaya koyar. Resmi belgelerin elektronik ortama taşınarak iş ve işlemlerde zaman ve maliyet açısından tasarruf sağlanması bir yana ülke hafızamızı oluşturan belgelerin gelecek kuşaklara mümkün olan en iyi şekilde aktarılması hedefi de standartta yüklenen önemli bir sorumluluktur. Bu nedenle standart referans model olarak yayınlandığı ilk günden beri güncel teknolojik gelişmeler ve ülke ihtiyaçları takip edilerek güncellenmekte ve geliştirilmektedir. 2015 yılında yapılan revizyon ile içerikte geliştirme yapılarak arşiv sisteminin gerekleri tanımlanmış, birlikte çalışabilirlik için elektronik yazışma paketi ve kayıtlı elektronik posta kullanımı zorunlu hale gelmiş ve güvenlik testleri standarda eklenmiştir. Standart aşağıdaki bölümlerden oluşmaktadır:

- Sistem Kriterleri
    - Dosya tasnif planları
    - Saklama Planları
    - Elektronik Belgelerin Kayıt İşlemleri
    - Elektronik Belgelerin Paylaşımı
    - EBYS Kullanım Özellikleri
    - Erişim Kontrolü ve Güvenlik
    - Sistem Tasarımı ve Yönetimi
- Belge Kriterleri
    - Belge Özellikleri
    - Doküman Yönetimi
    - Elektronik Olmayan Sistemlerle Uyumluluk
    - Dijital Görüntüleme Sistemleri
- Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM)
    - Elektronik Arşivleme Sistemi Referans Modeli (ELAS/RM)
    - Arşiv Sisteminin Güvenliği
    - ELAS/RM Uygulama Kılavuzu
    - Arşiv Malzemesinin Tanımlanması
- Üst Veri Yönetimi
    - Üst Veri Elemanları

2015 yılında yapılan önemli bir yenilikte standardın yapısında olmuştur. 2015 yılına kadar sadece ürün

standardı olan TS 13298, Kurum Yeterlilik Sertifikasyonu maddeleri eklenerek belgeli elektronik belge yönetim sistemi kullanan kurumların elektronik belge ve arşiv süreçlerini nasıl yürütmesi gerektiğini ortaya koymuştur. Böylelikle kurumların elektronik belge ve arşiv yönetim süreçleri denetlenebilir hale gelmiştir.

TS 13298 standardı içerisinde test faaliyetleri de önemli bir yer tutmaktadır. Birer madde ile zorunlu hale getirilen testler kendilerini tanımlayan madde sayısından çok daha kritik muhtevaya sahiptir. Standart içerisinde performans, fonksiyonel ve güvenlik testleri yaptırılması istenilmektedir. Testlerin yapılabilmesi için TSE belgelendirme makamı lisanslı laboratuvarlar ile çalışır. Lisanslı laboratuvarlar farklı kapsamlara sahip olmakla birlikte standardın gerektirdiği testlerin tamamını veya belli bir bölümünü yapabilmektedirler. TÜBİTAK YTKDM, TSE BTTM ve özel sektörden bir laboratuvarda da testler yaptırılabilmektedir.

TS 13298 standardına uyumun zorunlu hale getirildiği mevzuat şöyledir:

1. Elektronik Belge ve Arşiv Yönetim Sistemleri (2008/16 sayılı Başbakanlık Genelgesi ile)

DİĞER BİLİŞİM TEKNOLOJİLERİ STANDARTLARI

TSE K 505 Temel Seviye Güvenlik Değerlendirme Kriteri

Ortak kriterler gibi güvenlik standartlarının süreçlerinin uzun ve zahmetli olması nedeniyle hızlı ve temel güvenlik testlerinin yapılmasını hedefleyerek oluşturulmuş bir kriterdir. Belgelendirme faaliyetleri TSE Siber Güvenlik Belgelendirme Müdürlüğü tarafından yapılan kriterin gerektirdiği testler TÜBİTAK OKTEM, TSE BTTM ve özel sektörden bir laboratuvar tarafından yapılabilmektedir.

TS ISO/IEC 25051 Kullanıma Hazır Yazılım Ürünü (RUSP) Kalitesi İçin Gereksinimler ve Test Talimatları

Standart kullanıma hazır yazılım ürünleri için kalite gereksinimlerini ortaya koymaktadır. Temelde üç gereksinimi vardır:

1. Ürün Açıklaması Dokümanı
2. Kullanıcı Kılavuzu Dokümanı
3. Fonksiyonel Testler

Gerekli belgelendirme sistemi TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü tarafından kurulmuş olup testleri yapmaya yetkin 3 lisanslı laboratuvar bulunmaktadır. Bunlar TÜBİTAK YTKDM, TSE BTTM ve özel sektörden bir laboratuvar tarafından yapılabilmektedir.

TS EN ISO 9241-151 Web Kullanıcı Arayüzleri Kılavuzu

Web kullanıcı arayüzü geliştirilmesinde en önemli hedef, arayüzünü, engelli kişilerde dâhil mümkün olan en geniş kullanıcı yelpazesinin erişimine açık hale getirmektir. Kılavuz üst düzey tasarım kararları ve tasarım stratejisi, içerik tasarımı, gezinme, arama ve içerik sunumuna odaklanmaktadır. Belgelendirmesi TSE tarafından yapılabilen standart için ihtiyaç duyulan testler ODTÜ İnsan-Bilgisayar Etkileşimi Araştırma ve Uygulama Laboratuvarı tarafından karşılanmaktadır.

TS ISO/IEC 19790-24759 Kriptografik Modül Doğrulama

Bilgi teknolojisi sistemlerinde yer alan ve kritik verilerin güvenliğini sağlayan kripto modülleri için güvenlik gereklerini belirleyen bir standarttır. Kripto modüllerinin ISO/IEC 19790 standardına uygunluğunu test etmek için ISO/IEC 24759 standardı test metodolojisi olarak hazırlanmıştır.

SONUÇ

Bilişim teknolojileri alanında üretilen ürün ve yürütülen süreçlerin hem kalite açısından hem de güvenlik açısından ele alınması gerekliliği bulunmaktadır. Süreç kalitesinin yükseltilebilmesi için SPICE, bilgi güvenliğinin sağlanabilmesi için Sızma Testi Firma belgelendirmesi ve 27001 ve elektronik belge ve arşiv süreçlerinin doğru çalıştırılabilmesi için TS 13298 Kurum Yeterlilik Sertifikasyonu standardizasyonun bilişim teknolojileri alanına önerdiği çözümlerdir. Ürün bakımından güvenlik için Ortak Kriterler, Temel Seviye ve Kripto, kalite için 25051 ve 9241 standartları sektöre sunulan çözümlerdir. Ayrıca yetişmiş insan kaynağı ihtiyacı bulunan[9] siber güvenlik alanında çözüm olarak sızma testi uzmanı belgelendirmesi standartlar ile temellendirilerek sunulmuş bulunmaktadır.

TÜBİTAK, TSE ve ODTÜ gibi ülkemizin değerli kurum ve üniversiteleri ile özel sektör tarafından kurulan laboratuvarlar ile desteklenen belgelendirme programları, bilişim sektörünün ihtiyaçlarına cevap verebilecek mekanizmaları oluşturmuş bulunmaktadır. Standardizasyonun faydalarına inanılarak düzenleyici kurumlar tarafından mevzuat içerisinde atıfta bulunularak ilgili belgelendirmeler zorunlu hale getirilmiştir.

Bilişim sektöründe ihtiyaçlara çözüm arayışı sürecinde ilk seçenek olarak standardizasyonun akla gelmesi ancak standardizasyonun faydaları kavrandığında gerçekleşecektir.

KAYNAKÇA

[1]http://www.tdk.gov.tr/index.php?option=com_gts&kelime=STANDART, son erişim tarihi 02.11.2017

[2]https://www.tse.org.tr/tr/icerikdetay/2249/4629/standard-hizmetleri.aspx, son erişim tarihi 02.11.2017

[3]http://www.etsi.org/standards/why-we-need-standards son erişim tarihi 02.11.2017

[4]Importance of Standards, Importance of Standards, Dr. Ntsibane Ntlatlapa, CSIR Meraka Institute

[5]TS EN ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı

[6]https://www.commoncriteriaportal.org/ccra/ son erişim tarihi 02.11.2017

[7]https://bilisim.tse.org.tr/upload/tr/dosya/icerikyonetimi/3299/06102017105941-2.pdf son erişim 02.11.2017

[8]https://bilisim.tse.org.tr/tr/icerikdetay/944/1212/spice-genel-bilgi.aspx son erişim 02.11.2017

[9]http://aa.com.tr/tr/politika/basbakan-yildirim-hedefimiz-siber-guvenligi-milli-guvenlige-entegre-etmek/942904 son erişim 02.11.2017

ÖZGEÇMİŞ

İNAN ÖZKAN

1988 doğumlu. Erciyes Üniversitesi Bilgisiayar Mühendiliği lisans mezunu. Çalışma hayatına Türk Standardları Enstitüsü'nde 2013 yılında TSE Uzman Yardımcısı unvanı ile başladı ve "Uluslararası Sızma Testi Hizmeti Veren Kişi Belgelendirmelerinin İncelenmesi, TSE Belgelendirme Sistemi Ve Ulusal Zayıflık - Exploit Veritabanı Kurulması" adlı tezi ile TSE Uzmanı unvanını aldı. Çalışmalarını bilişim teknolojileri alanında belgelendirme denetimleri ve yazılım test faaliyetleri ile sürdürmektedir.