TSE Standard

► 652 ► Mart 2017 ► Ekonomik ve Teknik Dergi ► ISSN:1300-8366

TSE ile Amerikan Makine Mühendisleri Topluluğu (ASME) arasında işbirliği anlaşması imzalandı

BİLGİ GÜVENLİĞİ

Ülkemizde Bilgi Güvenliği Yönetim Sistemi Uygulamaları ve Yasal Şartlar ► Açık Kaynak KodluYazılımlar ve Kamuda Uygulanması ► Banka/Kredi Kartları ve Güvenlik Önlemleri ► Nesnelerin İnterneti (IoT) ve Siber Güvenlik ► Adli Bilişim ve Standardizasyon Bulut Bilişim ve Riskleri ► Sosyal Mühendislik ► Elektronik İmza

TSEKurumsal

ISSN: 1300-8366 ► Yıl: 56 ► Sayı: 652 ► Mart 2017

Sahibi: Türk Standardları Enstitüsü Adına
Sebahittin Korkmaz

Sorumlu Yazı İşleri Müdürü: Doğan Yazar

Yayın Yönetmeni: Abdullah Durmuşoğlu

Editörler: Fatih Işık, Batuhan Batılı

Adres: TSE Basın Yayın Müdürlüğü
Necatibey Cad. No:112 06100 Bakanlıklar / Ankara
☎ 0312 416 66 63
► ✉ mfisik@tse.org.tr

Reklam ve Abone: Adem Dağlı ► ☎ 0312 416 67 47

Grafik Tasarım: Caner Boztaş

Baskı ve Dağıtım: Hamdioğulları İç ve Dış Tic.
Aşağı Öveçler Mh. 1332 Sk. 5/8 Çankaya / Ankara
► ☎ 0312 472 02 18 ► ✉ www.hamdiogullari.com.tr

Yayın Türü: Yerel Süreli

Basım Tarihi: 02.06.2017

Sebahittin Korkmaz
▶ TSE Başkanı

Değerli okuyucular,

Teknoloji, günümüzde öylesine baş döndürücü bir hızla gelişmeye devam etmektedir ki çoğu zaman bu hıza yetişmekte, bu yeniliklere ayak uydurmakta bireysel anlamda zorluk çekebiliyoruz. Teknoloji, özellikle de bilgiye ulaşım şiarıyla anlamlandırılan bilişim teknolojisi, bugün artık gündelik işlerimizin hemen hemen çoğunu yapabildiğimiz pratik bir platform haline gelmiştir.

Türkiye İstatistik Kurumu (TÜİK) tarafından 2016'da yayınlanan raporda Türkiye genelinde internet erişim imkânına sahip hanelerin oranı yüzde 76,3 olarak tespit edilmiştir. Aynı raporda 2016 yılının ilk üç ayında internet kullanan bireylerin yüzde 82,4'ünün sosyal medya üzerinde profil oluşturma, mesaj gönderme veya fotoğraf vb. içerik paylaştığı, bunu yüzde 74,5 ile paylaşım sitelerinden video izleme, yüzde 69,5 ile online haber, gazete ya da dergi okuma, yüzde 65,9 ile sağlıkla ilgili bilgi arama, yüzde 65,5 ile mal ve hizmetler hakkında bilgi arama ve yüzde 63,7 ile internet üzerinden müzik dinlemenin takip ettiği belirtilmiştir.

Dergimizin bu ayki dosya konusu olan 'Bilgi Güvenliği' kapsamına giren kamu hizmetlerinden yararlanma oranı da aynı rapora göre yüzde 61,8; internet üzerinden yapılan alışverişler ise yüzde 34,1 olarak tespit edildi.

Dijital pazarlama ajansı 'We Are Social ile Hootsuite işbirliği ile hazırlanan 'Digital in 2017 Global Overview' araştırmasına göre ise Dünya genelinde web trafiğinin yarısından fazlası artık cep telefonundan geliyor.

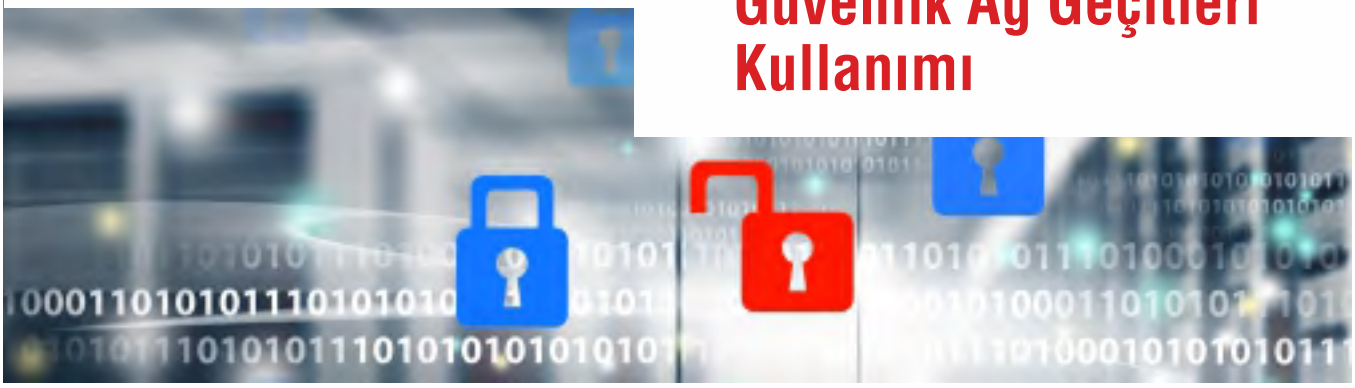
Türk Standardları Enstitüsü (TSE) ülkemizde 'Bilgi Güvenliği' konusunda kamu, özel sektör ve vatandaşlara, yeniliklerle uyumlu ve geniş yelpazede hizmetler vermektedir. Gerek kamunun vatandaşa sunduğu e-hizmetlerdeki güvenlik unsuruna altyapı sağlanması, gerek özel sektöre sistemlerinin kurulmasında sunduğu destek, gerekse de vatandaşlara sunduğu eğitimler Enstitümüzün 'Bilgi Güvenliği' konusuna verdiği önemin birer göstergesidir.

Değerli okuyucular, bu sayımızda 'Bilgi Güvenliği' konusunda hepimizi aydınlatacak oldukça farklı başlıkların yer aldığı kapsamlı bir dosya ile karşınızdayız.

İyi okumalar dileğiyle.

Standard

Ekonomik ve Teknik Dergi



Petrokimyada ilk Risk Yönetimi Sistemi Doğrulama Belgesi Petkim'in oldu

Türkiye'nin tek petrokimya hammadde üreticisi olan Petkim, faaliyet gösterdiği sektörde bir ilke imza atarak Türk Standardları Enstitüsü'nden (TSE) "TS ISO 31000 Risk Yönetimi Sistemi Doğrulama Belgesi" almaya hak kazandı.

2016 Aralık ayı içinde TSE tarafından İzmir ve Ankara bölgesinden toplam beş tetkikçiyle gerçekleştirilen TS ISO 31000 Risk Yönetimi Doğrulama tetkikini başarıyla tamamlayan Petkim, bu belgeyle; risk tanımlama, değerlendirme, analiz etme ve risklerle ilgili aksiyonlar alma konularında sistematik bir yapısı olduğunu tescilledi.

Düzenlenen belge töreninde konuşan TSE Genel Sekreteri Mehmet Bozdemir, petrokimya sektöründe bu belgeyi alan ilk kuruluşun Petkim olduğunu ifade etti.

Bozdemir, "Türkiye'nin en köklü kuruluşlarından Petkim'e bu belgeyi takdim etmekten mutluluk duyuyoruz. Pek çok konuda ilklere imza atan Petkim, petrokimyada bu belgeyi alan ilk kuruluş olma konusunda da öncü bir şirket oldu. 1996 yılında başladığımız belgelendirme çalışmalarını bugün en yüksek seviyeye getirdiğimiz için mutluyuz. Petkim, belge almaya hak kazanan ve tüm sistemi kuran kurumlardan biri oldu. Bu kadar büyük lokasyona yayılmış bir yapıda bu belgeyi almanın yönetimsel süreçler anlamında da çok zor olduğunu belirtmek isterim. Kalite sistemleri günümüzde büyük bir öneme sahip, kalitenin şirketlerin her bir kademesinde küçük de olsa yayılması gerekiyor. Bu anlamda Petkim'in buna çok inandığını ve başardığını söyleyebilirim. Petkim bugün, TSE'nin stratejik bir ortağı konumuna geldi. İşbirliğimizin güçlenerek ve artarak devam edeceğine inanıyorum" diye konuştu.

.

Petkim Genel Müdürü Anar Mammadov ise konuşmasında, Türkiye'de Risk Yönetim Sistemi Doğrulama Belgesi'ne sahip ilk üretici firmalar arasında yer aldıklarını belirterek, "Operasyonel ve finansal anlamda yüksek riskli bir sektörde faaliyet gösteriyoruz. Riskleri azaltmayı ve risk yönetimini şirketimizin her kademesinde etkin şekilde yapılandırmaya büyük önem veriyoruz. Belgeye hak kazanmanın öneminin yanı sıra, şirketimiz bünyesinde risk yönetimini bir kültür haline getiren çalışmalar gerçekleştiriyoruz. Riskleri azaltmada daha iyi noktalara gelmeyi hedefliyoruz. Bu amaçla yürüttüğümüz çalışmalara, çalışanlarımızın gösterdiği katılım ve performanstan da büyük gurur duyuyoruz. Bu vesileyle, TSE'nin işbirliği ve desteğine, emeği geçen tüm Petkim personeline teşekkür etmek isterim" dedi.

Radarlara TSE denetimi

Karayollarında trafik güvenliğinin sağlanması amacıyla mobil ve sabit Hız İhlal Tespit Donanımları (HİTD) ile hız kontrolleri yapılmaktadır. Bu kontrollerde hatalı ölçüm yapılmasının önlenmesi amacıyla Bilim, Sanayi ve Teknoloji Bakanlığının "Hız İhlal Tespit Donanımları Muayene Yönetmeliği" Resmi Gazete'de yayımlandı.

Bu kapsamda hâlihazırda kullanılan ve yeni kullanıma alınacak HİTD'lerin yerinde ve laboratuvarda doğruluğunun tespiti ve muayenesi için uluslararası uygunluk değerlendirme kuruluşu yetkisine sahip olan Türk Standardları Enstitüsü (TSE) yetkilendirildi.

TSE uluslararası kabul edilen referans cihazlar ile sabit HİTD'lerin kontrolünü yerinde, mobil HİTD'lerin kontrolünü ise laboratuvar ortamında yapacak.

Muayene sonucunda doğru ölçüm yapan donanımların kullanımına izin verilecek, hatalı ölçüm yapan donanımlar ise mühürlenerek gerekli işlemlerin yapılması amacıyla ilgili idareye teslim edilecek.

-Periyodik kontroller yapılacak-

Kontroller ilk, periyodik, ani, şikâyet ve stok muayeneleri şeklinde gerçekleştirilecek.

İlk muayene; yeni yapılan veya parçaların birleştirilmesi suretiyle meydana getirilen HİTD'lerin satışa veya kullanılmaya başlanmalarından önce veya ithal edilen HİTD'lerin yurda sokulmaları sırasında veya periyodik, ani, şikâyet ve stok muayeneleri sonunda damgaları iptal olanların tamir ve ayarlanmalarından sonra yapılan muayenedir. İlk muayenenin geçerlilik süresi 1 yıldır.

Periyodik muayene, HİTD'ler için yapılan genel muayene olup geçerlilik süresi 1 yıldır. Bu süre, son muayenenin yapıldığı tarihten itibaren başlar.

Ani muayene, Bakanlık ve il müdürlüklerinin görecekleri lüzum veya ihbar üzerine, HİTD'lerin bulundukları yerlerde habersizce yapılan muayenedir.

Şikâyet muayenesi, HİTD'lerin doğru çalışıp çalışmadığını tespit etmek üzere, kullanıcının veya diğer bir kimsenin yazılı müracaatı üzerine yapılan muayenedir.

Stok muayenesi ise ilk muayene damgasını taşıdıkları halde satılmayıp depo, atölye, imal ve satış yerlerinde veya kullanılmasına ihtiyaç duyulmayarak stok halinde bulundurulan cihazların periyodik muayene süreleri içinde tekrar muayeneye tabi tutulmalarıdır.

Bu maddenin yürürlük tarihinden önce piyasada kullanımda olan HİTD'lerin muayenelerinde tip onay şartı aranmayacak. Ancak söz konusu HİTD'ler için kullanıcısı tarafından hazırlanacak damga planlarının Bilim, Sanayi ve Teknoloji Bakanlığı'na onaylatılması gerekecek.

TSE ile Amerikan Makine Mühendisleri Topluluğu (ASME) arasında işbirliği anlaşması imzalandı

Türk Standardları Enstitüsü (TSE) Başkanı Sebahittin Korkmaz, 14 Şubat 2017 tarihinde New York'ta Amerikan Makine Mühendisleri Topluluğu (ASME) Genel Direktörü Thomas Loughlin ile bir araya geldi.

Ana gündem maddesini nükleer santrallerin oluşturduğu toplantıda ASME'nin çalışma sistematiği ile uygunluk değerlendirme ve standardizasyon faaliyetleri ele alındı. Bu alanlarda detaylı teknik işbirliğinin kısa bir süre içerisinde başlatılması için mutabakata varılan görüşmelerde ayrıca Türk sanayicilerinin bu kuruluşun teknik komitelerinde herhangi bir ücret ödemeksizin üye olarak bulunabileceği teyit edildi.

TSE Başkanı Korkmaz'ın ziyareti kapsamında ASME'nin yayımladığı dokümanların daha detaylı takip edilebilmesi amacıyla iki kuruluşun karşılıklı işbirliğini geliştirecek ve tecrübe paylaşımını sağlayacak bir anlaşma metni de imzalandı.

Görüşmelerde ilerleyen süreçte ASME standartlarının adaptasyonu, bu standartların Türk sanayicilerine TSE tarafından temin edilmesi konularında yeni anlaşmaların yapılması ile ilgili mutabakat da sağlandı.

Türkiye'nin standardizasyon yol haritası belirlendi

Türkiye'nin standardizasyon konusunda yol haritasını belirleyen Ulusal Standardizasyon Strateji Belgesi ve Eylem Planı (2017-2020), Yüksek Planlama Kurulunca (YPK) kabul edilerek Resmi Gazete'de yayımlandı.

Bilim, Sanayi ve Teknoloji Bakanlığının koordinasyonunda ilgili tüm paydaşların görüşleri alınmak suretiyle hazırlanan Belge ve Eylem Planı'na göre, Türkiye'nin standardizasyon sistemini daha ileriye taşımak için 4 hedef ve bu hedeflere ulaşmak için gerçekleştirilmesi gereken 21 eylem belirlendi.

Türkiye'nin standardizasyon alanındaki vizyonu, "Tüm paydaşların standart hazırlama sürecine etkin bir şekilde katıldığı, standartları uygulamayı ilke edinmiş, küresel alanda belirleyici ve söz sahibi bir ülke olmak" şeklinde tanımlandı.

Söz konusu vizyon çerçevesinde; standardizasyon altyapısını güçlendirmek, ilgili tüm paydaşların standardizasyon sürecine etkin katılımını sağlamak ve standartların kullanımını yaygınlaştırmak, küresel alanda etkinliği artırmak, yeni teknolojili ürünlere ve iş güvenliğiyle sosyal yaşam kalitesini artırmaya yönelik özgün standartları hazırlamak hedefler olarak belirlendi.

Belgede, anılan hedefler kapsamında gerçekleştirilecek 21 eylem yer aldı. Buna göre, Dördüncü Sanayi Devrimine yönelik Türkiye'nin standardizasyon yol haritası uygulamaya konulacak. Özel sektör, kamu kurumları ve üniversitelerin standart hazırlama süreçlerine katılımları artırılacak. Lise ve üniversitelerin program veya müfredatlarının kapsamına standardizasyona ilişkin derslerin ya da konuların alınması sağlanacak.

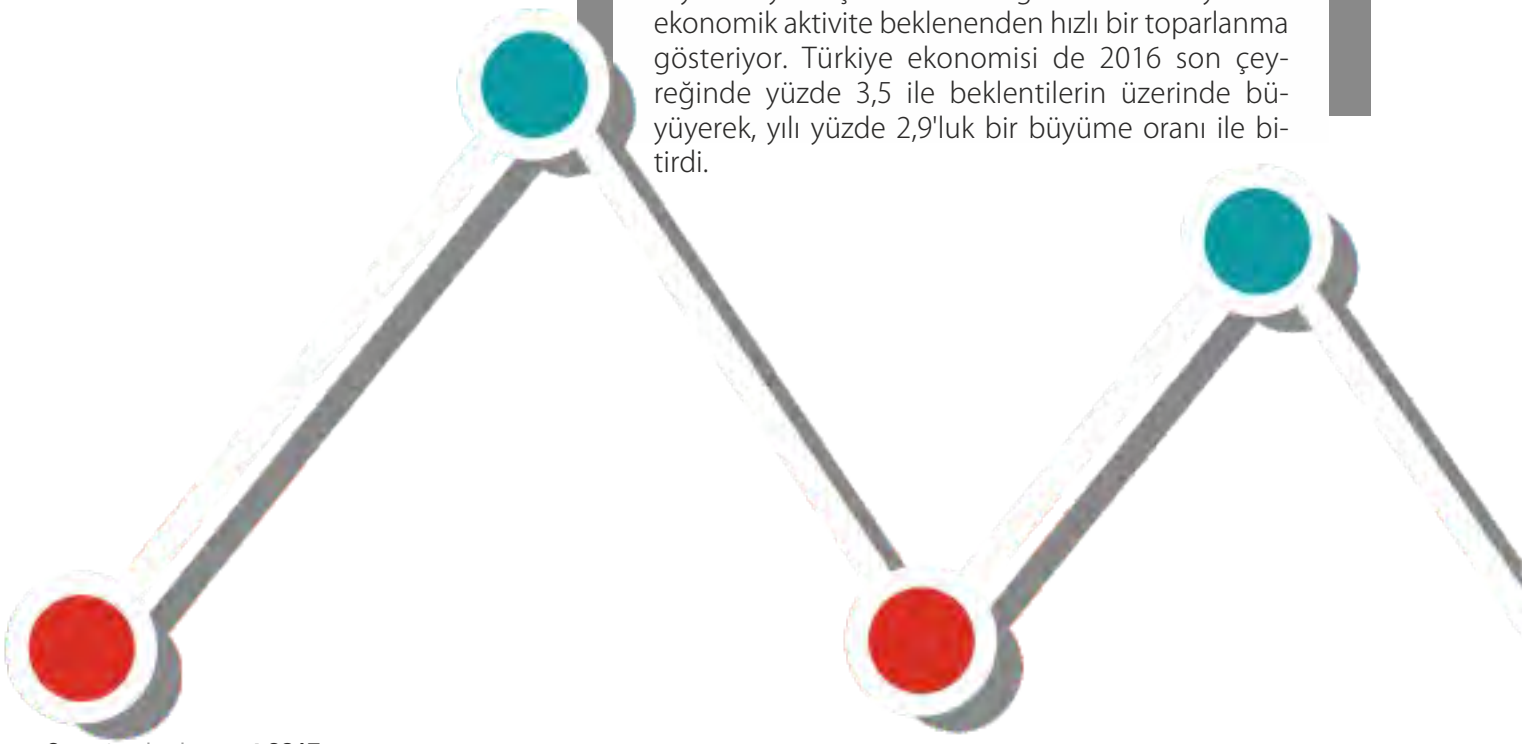
Bunların yanı sıra uluslararası ve bölgesel standart hazırlama kuruluşlarındaki temsil sayısı artırılacak. Yüksek teknolojili yeni ürünlerin standartları hazırlanacak.

Türkiye'nin standardizasyon alanındaki vizyonu, "Tüm paydaşların standart hazırlama sürecine etkin bir şekilde katıldığı, standartları uygulamayı ilke edinmiş, küresel alanda belirleyici ve söz sahibi bir ülke olmak" şeklinde tanımlandı.

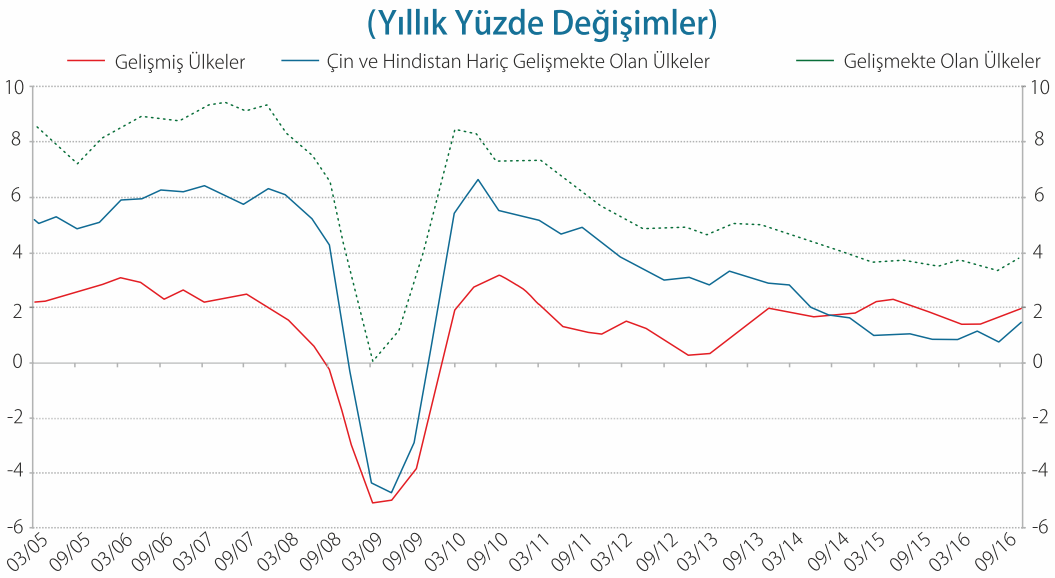
2017 Yılı İlk Çeyreğinde KÜRESEL EKONOMİDE TOPARLANMA SİNYALLERİ

Peyman Yüksel ▶ Ekonomist

Dünya ekonomisinde canlanmaya işaret eden ekonomistler, gelişmekte olan ülkelerin 2017'de yüzde 4,8, önümüzdeki yıl ise yüzde 4,9 büyüyeceğini öngörüyorlar. International Institute of Finance'in aylık hesaplamalarına göre 2010 yılından beri yani uzunca bir aradan sonra, küresel ticarette önemli rol oynayan Güney Kore ve Tayland gibi gelişmekte olan ülkelerde büyüme rakamları olumlu seyretmeye başladı. Euro Bölgesi'nde enflasyon ve ekonomik aktivite beklenenden hızlı bir toparlanma gösteriyor. Türkiye ekonomisi de 2016 son çeyreğinde yüzde 3,5 ile beklentilerin üzerinde büyüyerek, yılı yüzde 2,9'luk bir büyüme oranı ile bitirdi.



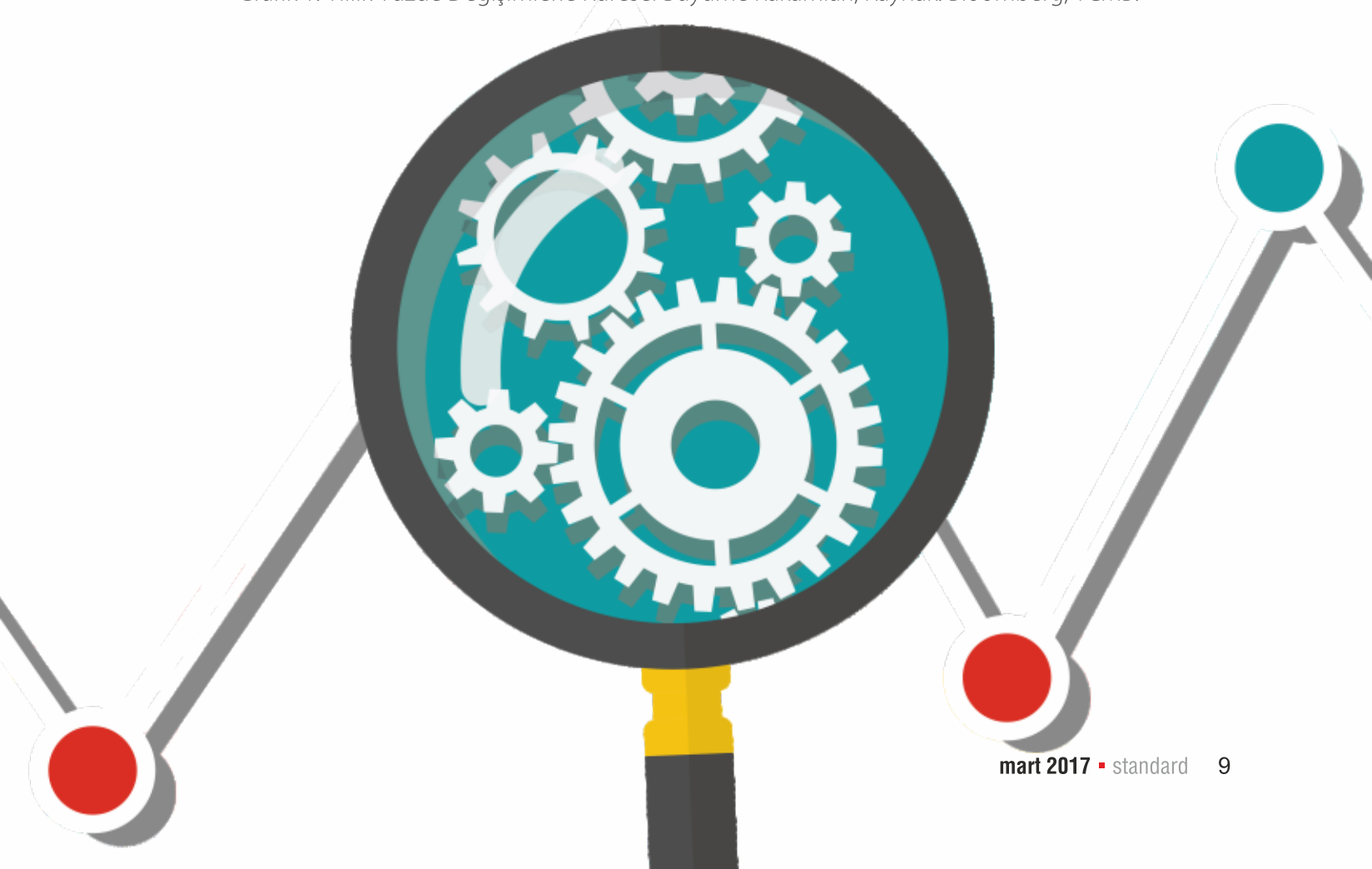
Küresel Büyüme



Gelişmiş Ülkeler: ABD, Euro Bölgesi, Japonya, İngiltere, Kanada, G. Kore, İsviçre, İsveç, Norveç, Danimarka, İsrail
Gelişmekte Olan Ülkeler: Çin, Brezilya, Hindistan, Meksika, Rusya, Türkiye, Polonya, Endonezya, G. Afrika, Arjantin, Tayland, Malezya, Çekya, Kolombiya, Macaristan, Romanya, Filipinler, Ukrayna, Şili, Peru, Fas

Son Veri: 2016 Ç4

Grafik 1: Yıllık Yüzde Değişimlerle Küresel Büyüme Rakamları, Kaynak: Bloomberg, TCMB.



2015 yılında 30 doların altını gören petrol fiyatları nedeniyle üretici birçok ülke ekonomik sıkıntı yaşamıştı. Dünya ekonomik büyümesine en büyük katkıyı sağlayan ülkelerden Çin'de ekonomik daralma yaşanması, petrol satışlarını olumsuz etkilemiş ve bu nedenle Rusya ve Brezilya gibi üretici ülkeler resesyon tehlikesi ile karşılaşmıştı. Grafiğe baktığımızda küresel ekonomide 2010 yılından beri azalan büyüme rakamlarında son aylarda yükselme sinyalleri görüyoruz. Bunlardan en önemlisi; Amerikan Merkez Bankası'nın (FED) mart ayında faizlerde 25 baz puan artışına giderek, faiz aralığını yüzde 0,75-1,00'e yükseltmesi oldu. FED'in faiz artışı kararını, Amerikan ekonomisinin yıllık yüzde 2 büyüyeceğini öngörerek verdiğini düşünebiliriz. Bu konuda dikkat edilmesi gereken hususlar; FED'in faiz artışlarına devam etmesi (2017 yılı için iki kez artış yapabileceğinin sinyallerini verdi), uzun zamandır Amerika tarafından piyasaya sürülen bol miktardaki doların evine dönmesine, Türkiye gibi dış finansman ihtiyacı olan ülkelerin daha pahalı kredi bulmasına neden olacaktır. Krediler pahalandıkça yatırımlar ve dolayısı ile de istihdam azalabilir. Ancak, küresel talepteki ve üretimdeki artışlar, ekonominin canlanmasını sağlayabilir. Zira ABD ekonomisinde istihdam ve üretim rakamlarındaki olumlu gelişmeler, Avrupa Merkez Bankası'nın (AMB) Euro Bölgesi büyüme tahminlerini 2017 için yüzde 1,8, ve 2018 için yüzde 1,7 olarak yukarı yönde revize etmesi, Çin'de ocak ve şubat aylarında sanayi üretiminin beklenenden iyi gelmesi, umutların 2017 yılı için artmasına neden oldu.

Mart ayında dikkat çeken gelişmelerden bazıları:

- Mart ayı sonu itibarıyla İngiltere Brexit sürecini resmen başlattı.

- FAO tarafından uluslararası pazarlarda tahıl, bitkisel yağ, süt ürünleri, et ve şekerden oluşan beş ana gıda maddesinin fiyatları ve ticareti takip edilerek belirlenen Gıda Fiyat Endeksi, 7 aydır aralıksız artarak son İki yılın zirvesine erişti. Yıllık artışın yüzde 17,2'ye ulaşması konusunda Birleşmiş Milletler Gıda ve Tarım Örgütü (FAO) uyarıda bulundu.

- Almanya'nın Baden-Baden kentinde, Maliye Bakanları ve Merkez Bankası Temsilcilerinin katıldığı G20 zirvesi sonuç bildirgesinde; ticaretin katkısını güçlendirmek ve rekabetçi devalüasyona karşı kararlılık, para politikasının tek başına dengeli bir büyümeyi sağlayamadığı, küresel ekonomik iyileşmenin devam ettiği ancak toparlanma için aşağı yönlü risklerin sürdüğü belirtildi.

Kadınların Ekonomiye Katkısı

Birleşmiş Milletler tarafından tanımlanmış "Uluslararası Kadınlar Günü" her yıl 8 Mart'ta kutlanan ve uluslararası bir gündür. 2017 yılı için tema "Değişen Çalışma Yaşamında Kadınlar: 2030 Yılına Kadar Gezegende Yarı Yarıya" olarak belirlendi. Hedefler arasındaki kadın istihdamının artırılması, fırsat eşitliği yaratılması, kadınlara karşı ayrımcılığın sonlandırılması, insan ticareti, cinsel ve diğer sömürü türleri de dahil olmak üzere kamusal ve özel alanlardaki tüm kadın ve kızlara karşı her türlü şiddetin ortadan kaldırılması, erken ve zorla evliliklerin önüne geçilmesi için çalışmalar bulunuyor. Kadınların görünmeyen ve karşılıksız olarak yaptıkları hizmetlerin küresel ölçekte karşılığı 12 trilyon dolara denk geliyor. Dünyada ve ülkemizde kadın çalışanlar erkeklere nazaran yüzde 17 daha az ücret alıyorlar. Kız çocuklarına eğitim fırsatı verilmesi sonucunda çalışma hayatına katılımlarının arttığı görülüyor. Kadın nüfusun iş hayatında daha çok yer alması, ülkelerin ekonomik gelişmişlik seviyesini artırıyor. 2015 yılı ile karşılaştırdığımızda 2016'da ülkemizde sigortalı kadın çalışan sayısının 40 bin azaldığı görülüyor. Bunu önlememiz, yönetimde, mecliste, siyasette, sosyal hayatta kadınlarımıza hak ettikleri saygınlığı vermemiz, kadın işgücünü ekonomiye daha çok yansıtmamız gerekiyor.

Türkiye Ekonomisinde Olumlu Gelişmeler

2017 yılının ilk aylarında Türkiye ekonomisinde olumlu yönde bazı hareketlenmeler olduğu gözlemleniyor. Özellikle Ekim 2016'dan beri ilk defa yükselişe geçen ve beklentilerin üzerinde gelen imalat verileri ve istihdam artışı olumlu karşılandı ve Türkiye ekonomisi 2016 yılının son çeyreğinde yüzde 3,5 büyüme oranını yakaladı. Sanayide yüzde 5'lik artış, tarım sektöründe son aylardaki toparlanma, inşaat sektöründe yükselme ve yüzde 3 büyüyen hizmet sektörü, büyüme rakamlarına olumlu yansıdı. 2016'nın son iki ayı ve 2017''nin ilk iki ayında ihracatta ardı ardına kesintisiz artış yakalandı. Rusya ile sıkın-

tıların yavaş yavaş giderilmesi, petrol fiyatlarındaki artışın petrol üreten ülke ekonomilerini iyileştirmesi, ticareti hareketlendirdi. Buna karşılık dolardaki yükseliş, cari açığın artmasına neden oldu. İthalatımız ocak ayında arttı ancak ihracatımızdan mutlak değer olarak yüksek olduğundan dış ticaret açığında yüzde 10'luk artış yaşandı. Ocak ayında ihracat ve ithalatın böylesine yüksek oranda artması sonucunu doğuran etkenlerin birinin de altın ticaretindeki artış olduğu gözlemlendi. Şubat ayında ise ihracat, geçen senenin aynı ayına göre yüzde 1,9 azalışla 12,1 milyar dolar, ithalat, geçen senenin aynı ayına göre yüzde 1,6 artışla 15,8 milyar dolar, ihracatın ithalatı karşılama oranı yüzde 76,7 ve dış ticaret açığı yüzde15 artışla 3,7 milyar dolar oldu.[1]

Geçtiğimiz yıl, 15 Temmuz darbe girişimi yaşanmasına rağmen ülkemize toplam 16,1 milyar dolarlık uluslararası doğrudan yatırımın gelmesi, ekonomide sağlam adımlarda ilerlediğimizi ve yabancıların Türkiye'ye yatırım anlamında güvendiğini gösteriyor. İngiltere'den gelen yatırımların bir önceki yıla göre yüzde 64,3 artarak 961 milyon dolar olduğu gözlemlenirken, Hollanda'dan 956 milyon dolar ve Almanya'dan ise 403 milyon dolarlık sermaye girişi olduğu belirlendi.

Türkiye Ekonomisini Etkileyen Dört Gündem Maddesi

Turizm: Rusya ile yaşanan uçak krizi sonrası turizm sektöründe meydana gelen kayıpların giderilmesi için hükümet yoğun çaba sarf ediyor. 2017 yılının ocak ve şubat aylarında Rusya'dan Antalya'ya gelen turist sayısı 27 bini geçti. Nisan ayından sonra sayının yükselmesi ve 2017 yılı toplamında Antalya'ya 2,5 ila 4 milyon arasında Rus turistin gelmesi bekleniyor. AB ile de ilişkilerin güçlendirilmesi turizm açısından oldukça önem arz ediyor. Çünkü Türkiye, en çok turisti Avrupa'dan alıyor. Hollanda menşeli Booking otel rezervasyon firmasının ülkemizdeki faaliyetleri, vergi mevzuatı yüzünden mart ayında durduruldu. Bu firma ile vergi konusunda anlaşmaya varılıp yeniden işlemlere başlanması, Türk turizm firmaları için oldukça önem taşıyor.

Tarım ve Hayvancılık: Gıda, Tarım ve Hayvancılık Bakanlığı damızlık sığır ve koyun-keçi işletme projelerinde yer alan inşaat yatırımı tutarının yüzde 50'si kadar hibe desteği sağlanacağını Resmî Gazete'de ilan ederek yürürlüğe koydu. Türk ekonomisini etkileyen sektörlerden tarıma da bu yıl özel önem verilmesi gerekiyor. Özellikle Rusya ile yaşanan uçak krizinden bu yana yürürlükte olan yasakların halen kalkmamış olması, çiftçilerimizin 2017 yılını da zor geçirmelerine neden olabilir. Rusya'nın Türkiye'den ithalatı durdurması sonucu domates ihracatı 2016'da 367 milyon dolardan 238 milyon dolara düştü. Miktar olarak da ihracat 543 bin tondan 480 bin tona geriledi. Şimdilik AB'ye ihracatımız olduğu için domates üreticileri büyük bir sıkıntı çekmiyorlar. Ancak 15 Nisan tarihinden itibaren Avrupa'da İspanya, Hollanda ve Belçika üretimi Avrupa piyasasına girdiğinde, Türk üreticilerden alımı durdurabilirler. Buna bağlı olarak da iç piyasada sebze ve meyve fiyatlarında önemli ölçüde düşüş yaşanabilir, iç talep artabilir.

Enflasyon: Mart ayında tüketici fiyatları (TÜFE) yüzde 0,6 olan piyasa beklentisinin üzerinde yüzde 1,02 artış gösterdi ve yıllık enflasyon beklentisi olan yüzde 10,7'nin üzerinde, yüzde 11,29 seviyesinde gerçekleşti. Türk lirasının özellikle dolar karşısındaki değer kaybı, girdi fiyatlarındaki (ücretlerde, faizlerdeki) artış, petrol ve doğalgaz fiyatlarının yükselmesi, gıda fiyatlarının artması enflasyonu yukarı çekiyor. Tarımı destekleyen politikalar enflasyonu düşürebilir.

İşsizlik: 2016 yılında işgücü piyasası 2008'den bu yana en zayıf performansını sergiledi. Türkiye İstatistik Kurumu (TÜİK) verilerine göre işsizlik oranı aralık döneminde yıllık bazda 1,9 puan artarak yüzde 12,7, ocak ayında ise yüzde 13'e ulaştı. Genç nüfusta (15-24 yaş) işsizlik oranı 5,3 puanlık artış ile yüzde 24,5 olurken,15-64 yaş grubunda bu oran 2 puanlık artış ile yüzde 13,3 olarak gerçekleşti. Teknolojiyi yakından takip ederek katma değerli ürünler üretir ve bunları ihraç edebilirsek işsizliğe kalıcı çözümler bulmuş oluruz.

---

[1] *Ekonomi Bakanlığı, Ekonomi Veri Kartları (Cep Kartları), http://bakanrapor.ekonomi.gov.tr/detay.cfm?MID=153*

Mart ayında Türkiye'de:

▪ Ürün İhtisas Borsası alanında faaliyet gösterecek olan Türkiye Ürün Borsası A.Ş. kuruldu. Kuruluş; lisanslı depoculuk sistemi kapsamındaki tarım ürünlerinin fiziki veya elektronik ortamlarda alım satımına aracılık edecek.

▪ Çalışma ve Sosyal Güvenlik Bakanı Mehmet Müezzinoğlu, mart ayının başında 1 milyon 433 bin 290 bin kişiye emekli promosyonu ödemesinin yapıldığını açıkladı. Bakan Müezzinoğlu; mart, nisan ve mayıs aylarında 11 buçuk milyon emeklinin yaklaşık 4 milyar 850 milyonun üzerinde bir promosyonu alacağını belirtti.

▪ JP Morgan, Türkiye'nin 2017 büyüme tahminini yüzde 1,8'den yüzde 2,6'ya çıkarırken Goldman Sachs ise 2017'ye dair büyüme beklentisini yüzde 1,8'den yüzde 2,3'e yükseltti. Ancak, uluslararası kredi derecelendirme kuruluşu Moody's, 17 Mart'ta Türkiye'nin kredi notu görünümünü 'durağan'dan 'negatif'e indirdi.

▪ Şubat ayında beyaz eşyada sıfırlanan Özel Tüketim Vergisi, satışları ikiye katladı. Uygulamanın nisan ayında sona ermesi bekleniyor.

Dünyada ve Türkiye'de ekonomiyi etkileyen gelişmeleri takip etmeye ve çözüm önerilerimize, önümüzdeki günlerde de devam edeceğiz.

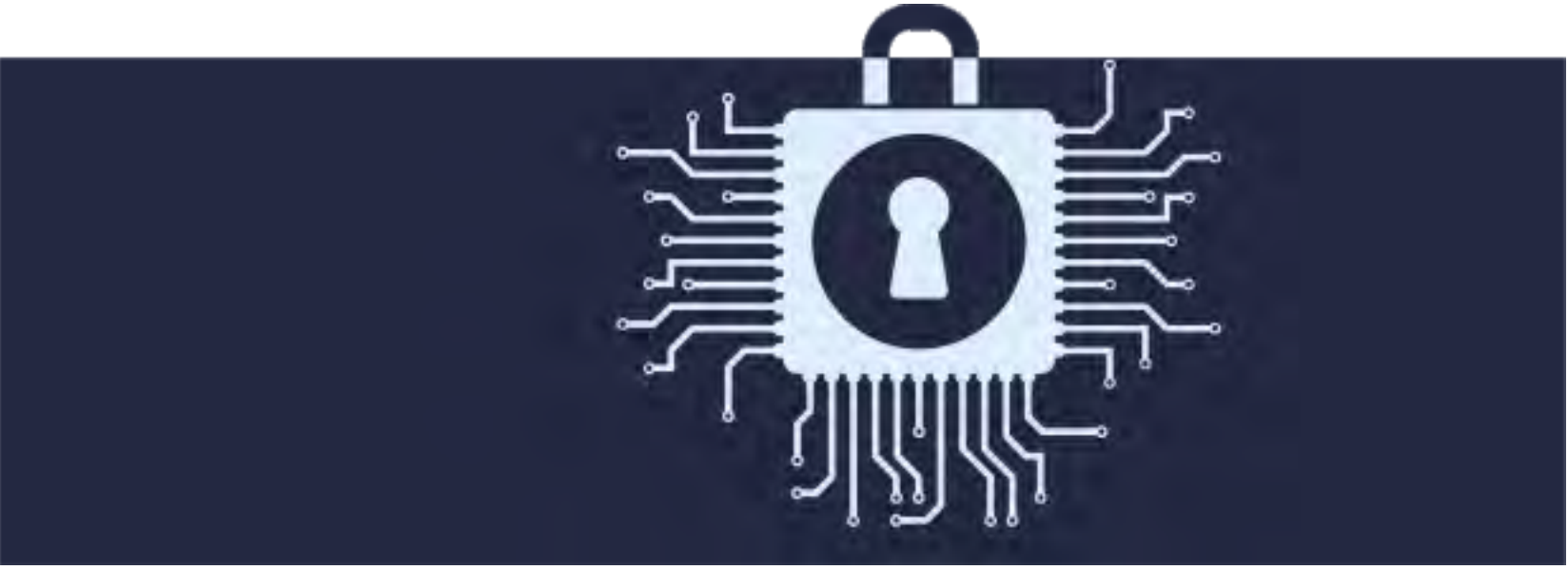
Geçtiğimiz yıl, 15 Temmuz darbe girişimi yaşanmasına rağmen ülkemize toplam 16,1 milyar dolarlık uluslararası doğrudan yatırımın gelmesi, ekonomide sağlam adımlarda ilerlediğimizi ve yabancıların Türkiye'ye yatırım anlamında güvendiğini gösteriyor.

Ülkemizde Bilgi Güvenliği Yönetim Sistemi Uygulamaları ve Yasal Şartlar

Dilek Özeren
Figen Aysun Güngör
TSE Bilşim Teknolojileri
Test ve Belgelendirme Daire Başkanlığı

Bilgi Güvenliği Yönetim Sistemi; bilgi güvenliğini kurmayı, gerçekleştirmeyi, işletmeyi, izlemeyi, gözden geçirmeyi, sürdürmeyi ve iyileştirmeyi temel alan iş riski yaklaşımına dayalı bir yönetim sistemidir. Kuruluşun fiziksel ve elektronik bilgi varlıklarının gizlilik, bütünlük ve erişilebilirliğini korumak için en üstten en alta kadar uygulayacağı iş odaklı yönetim yaklaşımıdır. Ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmakta, bunun neticesinde kurumun itibarı, güvenilirliği, kuruma ait gizli bilgiler, ticari, teknolojik bilgiler, iş sürekliliğini sağlayan bilgi ve süreçler, saldırıya uğrayabilecek değerler olarak ortaya çıkmaktadır. Bilgi güvenliği; iş devamlılığı, kaçınılmaz felaket durumlarında kaybın en aza indirilmesi, kurumların bilgi varlıklarının gizliliğinin, ulaşılabilirliğinin ve bütünlüğünün korunması amaçlarını taşır. Bilgi Güvenliği Yönetim Sistemi sayesinde kurumlar bilgi altyapılarını belirleyip, bu varlıklara yönelik olası tehlikeleri analiz ederek, bu risklerin oluşması durumunda hangi kontrolleri uygulayacaklarına karar verirler.

ISO 27001 standardı, her geçen gün büyümekte olan ISO/IEC 27000 standart serilerinin bir parçası olup, Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından yayınlanmıştır. Aşağıdaki tabloda ISO/IEC 27000 standartları toplu olarak verilmiştir.



TS ISO/IEC 27000:2016 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemleri Genel Bakış ve Sözlük	Bilgi güvenliği konusunda 46 anahtar tanım ve terimi açıklamaktadır.
TS ISO/IEC 27001:2013 Bilgi Teknolojileri Güvenlik Teknikleri Bilgi Güvenliği Yönetimi Sistemleri Şartları	Bilgi Güvenliği Yönetim Sistemi için gerekli olan gereksinimleri içermektedir. Dokümanın ek kısmında da gerekli kontroller ve amaçları listelenmiştir.
TS ISO/IEC 27002:2013 Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetimi Uygulama Prensipleri	27001 EK-A kısmındaki kontrollerini iyi uygulamaları için bir kılavuz görevi gören bu standart, tamamlayıcı açıklamalar içermektedir.
ISO/IEC 27003:2010	Bilgi Teknolojisi – Güvenlik Teknikleri - Bilgi Güvenliği Yönetim Sistemi Uygulama Kılavuzu
ISO/IEC 27004:2016	Bilgi Güvenliği Yönetim Sistemleri İzleme, Ölçüm Analizi ve Değerlendirme Standardı
ISO/IEC 27005:2011	Bilgi Güvenliği Risk Yönetim Standardı
ISO/IEC 27006:2015	Bilgi Güvenliği Yönetim Sistemlerinin Denetim ve Belgelendirilmesi İçin Şartlar
ISO/IEC 27007:2011	Bilgi Güvenliği Yönetim Sistemi Belgelendirme Kılavuzu
ISO/IEC TR 27008:2011	Denetçiler İçin Bilgi Güvenliği Yönetim Sistemi Belgelendirme Kılavuzu
ISO/IEC 27009:2016	Sektöre Özel ISO/IEC 27001 Gereksinimleri

Tablo: ISO/IEC 27000 Standartları

TS ISO/IEC 27001:2013 standardının kılavuz standardı olan TS ISO/IEC 27002'nin farklı sektörlerde hizmet veren kuruluşlara özel güvenlik önlemlerini içeren kılavuz standartları bulunmaktadır:

- Telekomünikasyon sektörü için; (TS ISO/IEC 27011 Telekomünikasyon kuruluşları için ISO/IEC 27002 standardını temel alan Bilgi Güvenliği Yönetimi Kılavuzu)
- Enerji sektörü için; (ISO/IEC 27019 Enerji sektörü için ISO/IEC 27002 standardını temel alan Bilgi Güvenliği Yönetimi Kılavuzu)
- Sağlık sektörü için; (ISO 27799 Sağlık kuruluşları için ISO/IEC 27002 standardını temel alan Bilgi Güvenliği Yönetim Sistemi Kılavuzu)
- Finans sektörü için; (TS ISO/IEC 27015 Finansal Hizmetler İçin Bilgi Güvenliği Kılavuzu)

Telekomünikasyon, enerji, sağlık, finans sektörlerinde Bilgi Güvenliği Yönetim Sistemleri belgelendirmesi TS ISO/IEC 27001:2013 standardına göre yapılmaktadır. Yukarıda adı geçen standartlar bu sektörlere yönelik kılavuz dokümanlardır.

TS ISO/IEC 27001 Bilgi Güvenliği Standardı Mevcut Yasal Şartlar

Yasal şartlar aşağıda belirtilen yönetmeliklerde açıklanmıştır:

1. Kamu kurum ve kuruşlarının KamuNet ağına dahil olmaları ile ilgili Başbakanlık Genelgesi (2016/28), 3 Aralık 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Genelgeye göre KamuNet (Kamu Sanal Ağı); kamu kurum ve kuruluşları tarafından içerik güvenliği sağlanan veri iletişiminin, kurumlar arası internete kapalı olan daha güvenli sanal bir ağ üzerinden yapılarak siber güvenlik risklerinin minimize edilmesi, mevcut ve kurulacak olan güvenli kapalı devre çözümlere standart sağlanması, ortak uygulamalar için uygun altyapının tesis edilmesi ve oluşturulması, planlanan ortak veri merkezi/merkezlerinin dâhil edilmesi amacıyla oluşturulmuştur. KamuNet Ağı'na Dahil Olmak İçin Asgari Güvenlik Gereksinimlerinden biri olan "Bilgi Güvenliği Yönetim Sistemi (BGYS) kurularak tüm süreçler ile ilgili siber güvenlik politikaları ve prosedürleri oluşturulmalı (ISO 27001 standardına uyumlu hale getirilmeli)," maddesi kamu kurum ve kuruluşlarında bir Bilgi Güvenliği Yönetim Sistemi kurulması gerekliliğini ortaya koymuştur.

2. Elektronik haberleşme şebekesi sağlayan ve altyapısını işleten sermaye şirketlerin/kurumların, BTK tarafından elektronik haberleşme hizmeti sunan ve/veya 20.07.2010 tarihinden itibaren TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alması zorunlu hale getirilmiştir (Elektronik Haberleşme Yönetmeliği'nin ilgili, "İşletmecilerin Yükümlülükleri Elektronik Haberleşme Güvenliğini Sağlama Yükümlülüğü" maddesinde; İşletmeci, TS ISO/IEC 27001 veya TS ISO/IEC 27001 standardına uygunluğu sağlamakla yükümlüdür" denmektedir).

Elektronik haberleşme şebekesi sağlayan ve altyapısını işleten sermaye şirketlerin/kurumların, BTK tarafından elektronik haberleşme hizmeti sunan ve/veya 20.07.2010 tarihinden itibaren TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alması zorunlu hale getirilmiştir.

3. Gümrük İşlerini Kolaylaştırma Yönetmeliği Kapsamında Yetkili Yükümlü Sertifikası (YYS) alacak ithalat ve ihracatçıların ISO/IEC 27001:2013 Belgesi alması zorunluğu; Gümrük ve Ticaret Bakanlığı'na bağlı Risk Yönetimi ve Kontrol Genel Müdürlüğünün Yetkili Yükümlü Sertifikası alacak firmalarda başvurularda arayacağı belgeler arasında ISO/IEC 27001 Belgesi alma zorunluluğu getirilmiştir. 10 Ocak 2013 tarihli "Gümrük İşlemlerini Kolaylaştırma Yönetmeliği" tüm ihracat ve ithalatçıları ilgilendiren maddeler içermektedir. İlgili yönetmeliğin 10. maddesinde yer alan, "Başvuru için aranacak belgeler" kısmında, istenen belgeler arasında, "Avrupa Akreditasyon Birliğinin karşılıklı tanıma anlaşmalarına imza atmış akreditasyon kurumları tarafından akredite edilmiş uygunluk değerlendirme kuruluşlarınca düzenlenecek ve akreditasyon kurumunun markasını taşıyan, güncel ISO 9001 ve TS ISO/IEC 27001 sertifikalarının aslı veya düzenleyen kuruluş tarafından onaylı örneği" yer almıştır.

4. Maliye Bakanlığı Gelir İdaresi Başkanlığı E-fatura Özel Entegratörlük için başvuru yapan firmalara TS ISO/IEC 27001 Belgesi alınması zorunluluğu getirilmiştir (Maliye Bakanlığı Gelir İdaresi Başkanlığı e-Fatura Uygulaması Kılavuzunda; "Özel entegratör bilgi güvenliği için TS ISO IEC 27001 veya ISO 27001 Belgesi'ne sahip olmalıdır" ifadesi yer almıştır).

5. Elektrik Piyasası Düzenleme Kurulu (EPDK) Elektrik Piyasası Lisans Yönetmeliği'ne göre TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi alınması zorunluluğu; Enerji Piyasası Düzenleme Kurumu (EPDK) Lisans Yönetmeliklerinde değişiklik yaparak, TS ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi'ni zorunlu hale getirdi. 26.12.2014 tarihli ve 29217 sayılı Resmi Gazete'de yayımlanan değişikliklerle, lisans sahiplerine 01.03.2016'dan itibaren Türk Akreditasyon Kurumu'ndan (TÜRKAK) akredite bir belgelendirme kuruluşundan ISO/IEC 27001 Belgeli olma zorunluluğu getirilmiştir.

Yasal şartların yanı sıra Bilgi Güvenliği Yönetim Sistemi özellikle kurumsallaşmaya çalışan kurumlar için yönetim sistemlerinin en önemli ve en kritik parçalarından birisi olmaya devam etmektedir.

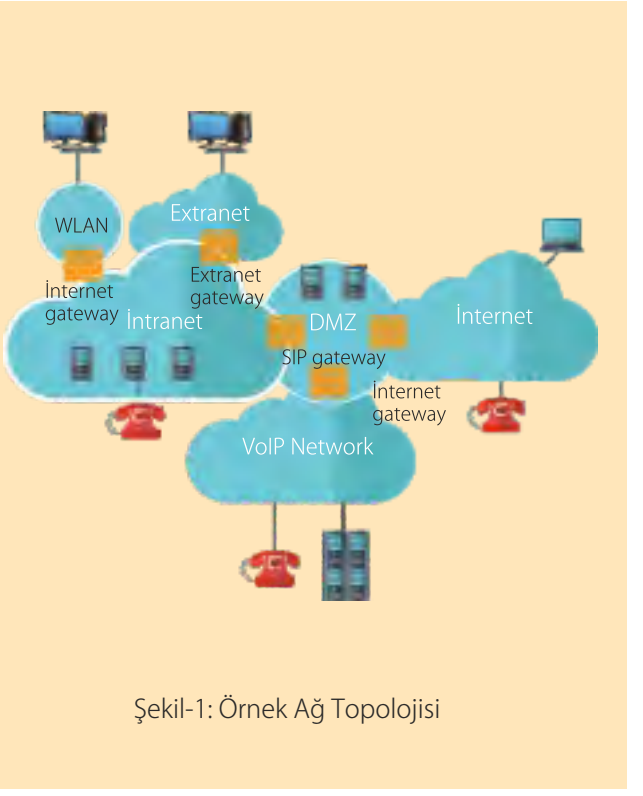
BİLGİ GÜVENLİĞİ
Yönetim Sistemi ve Güvenlik Ağ Geçitleri Kullanımı

Mehmet Kürşat Ünal
TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü

Kuruluşlar Bilgi Güvenliği Yönetim Sistemi'ni (BGYS) kurarlarken yararlandıkları ilk kaynak doküman TS ISO/IEC 27001 olmaktadır. Kuruluş bu standardın 6. bölümüne uygun olarak risklerini değerlendirdikten sonra haberleşme güvenliğini tehdit eden riskler için belli başlı güvenlik kontrollerini seçer. Risk işleme seçeneklerini tamamladıktan sonra bir nevi BGYS kapsamını belirten Uygulanabilirlik Bildirgesi ortaya çıkar. Genellikle bu dokümandaki güvenlik kontrolleri TS ISO/IEC 27002 dokümanında belirtilen 14 ana başlıkta toplanan güvenlik kontrollerinden oluşur. Haberleşme güvenliği için A.13 maddesini uygular.

Haberleşme güvenliği 'Ağ Güvenliği Yönetimi' ve 'Bilgi Transferi' olarak ikiye ayrılır. Ağ Güvenliği Yönetiminin amacı ağdaki bilgi ve destekleyici bilgi işleme olanaklarının korunmasını sağlamaktır. Makalemizde A.13.1.1 Ağ Kontrolleri başlığında güvenlik kontrolü ele alınmıştır. Buna göre sistemlerdeki ve uygulamalardaki bilgiyi korumak amacıyla ağlar yönetilmeli ve kontrol edilmelidir. Kuruluş eğer ağlarını güvenlik gereksinimlerine göre sınıflandırıp bölmüş ise bu ağlar arasındaki geçiş için 'Güvenlik Ağ Geçitlerini' kullanmaktadır. Örneğin kablosuz ağlarda alınabilecek önlemlerin kısıtlı olması sebebiyle kablolu ağlara göre gelebilecek tehditler daha fazladır. Bu yüzden kuruluşlar bu ağı kendi kritik sistemlerinden ayırırlar. Kuruluş açık bulut sistemlerini kullanıyorsa bulut sistemlerin çok kiracılı yapısından dolayı bulut sistemi kullanan kötücül sistemlerden gelebilecek tehditlerin kritik yapılardan izole edilmesi için iç ağ ile bulut sistemler arasında geçişin kontrol edilmesi gerekmektedir. VoIP telefonları kullanan bir kuruluşun ise VoIP telefon cihazlarını SIP ağ geçidi ile kamuya açık olan analog telefon şebekesinden ayırması gerekmektedir. Kuruluş internet üzerinden veya halka açık ağlar üzerinden bazı servislerinin kullanılmasına müsamaha gösterebilir. Bu servislere web sunucuları, mail sunucuları ve halka açık DNS sunucuları örnek gösterilebilir. Bu sunucular iç ağ ile dış ağ arasında bulunan DMZ denilen bölgeye konuşlandırılarak sunucuların dışardan ele geçirilmesi durumunda sunucuların iç ağı tehdit etmesinin önüne geçilmiş olunur. Yazının ilerleyen bölümlerinde bahsedileceği üzere birçok ağ geçidi mimarisi vardır. DMZ bölgesi oluşturabilmek için 'taranmış alt ağ geçidi mimarisi' kullanılmalıdır. Kuruluş, güvenlik ağ geçitlerine karşı olan tehditleri önlemek amacıyla TS ISO/IEC 27002 dokümanında da belirtildiği üzere TS ISO/IEC 27033 standardından yararlanabilir. Bu standart 5 bölümden oluşmaktadır. Bu bölümler sırasıyla "Genel Bakış ve Kavramlar", "Ağ Güvenliğinin Tasarımı ve Uygulanması İçin Tavsiyeler", "Referans Ağ Oluşturma Senaryoları - Tehditler, Tasarım Teknikleri ve Kontrol Konuları", "Güvenlik Ağ Geçitleri Kullanılarak Ağlar Arasında Güvenli İletişim" ve "Sanal Özel Ağlar (VPNs) Kullanılarak Ağlar Arasında Çapraz Güvenli İletişim".

Güvenlik ağ geçitlerine gelebilecek tehditler 4. bölümde ele alınmıştır. Bu bölüm ilk olarak Uluslararası Standardizasyon Teşkilatı (ISO) tarafından 2014 yılında yayınlanmış olup 2016'da kapağı Türkçeleştirilmiştir. Standardın ilk bölümündeki tarife göre güvenlik ağ geçidi güvenlik politikasına uygun koruma amacıyla farklı ağlar arasında veya ağ içindeki farklı alt grupların veya farklı güvenlik alanlarında bulunan yazılım uygulamalarının birleşme noktasıdır. Bu durum TS ISO/IEC 27033-4 Şekil-1'de aşağıdaki gibi gösterilmiştir.



Şekil-1: Örnek Ağ Topolojisi

Yukarıdaki örnek şekle bakarsak kırmızıyla yazılanların ağlar arasındaki birleşme noktası olduğu ve standarda göre de güvenlik ağ geçidi diye adlandırıldığını söyleyebiliriz. Bu şekil biraz yanıltıcı olup standardı okuyan kişinin güvenlik ağ geçidinin sadece güvenlik duvarından oluştuğu yanılgısına düşürmektedir. Oysa güvenlik ağ geçidi anahtarlar, yönlendiriciler, uygulama seviyesindeki ağ geçitleri,

güvenlik cihazları ve izleme fonksiyonuyla birlikte bir bütün olarak düşünülmelidir. Kuruluşlar ihtiyaçlarına göre bu cihazlarla farklı mimariler oluşturabilirler. Standardın 10.2 bölümüne göre paket filtrelemeli güvenlik duvarı/tarayıcı yönlendirici mimarisi, çift ağlı ağ geçidi mimarisi, taranmış ev sahibi mimarisi ve taranmış alt ağ ağ geçidi mimarisi olmak üzere 4 farklı mimari mevcuttur. Bu mimariler Şekil-2'de gösterildiği gibidir.

Standart ayrılan her bölge için kullanılan güvenlik ağ geçitleri için birer bilgi güvenliği politika dokümanı hazırlanmasını tavsiye eder. Bu doküman hazırlanırken aşağıda belirtilen hususlara dikkat edilmeli:

a) Güvenlik ağ geçitleri ile ilgili olabilecek ağ güvenlik tehditlerinin tanımlanması ve analiz edilmesi

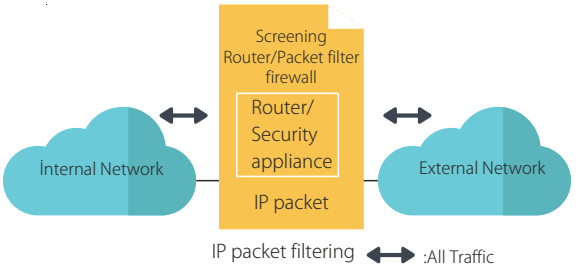
b) Tehdit analizine dayalı ağ güvenliği gereksinimlerinin belirlenmesi

c) Tipik ağ senaryolarıyla bağlantılı tehdit ve kontrol yönlerini ele alan tasarım ve uygulama teknikleri kullanma

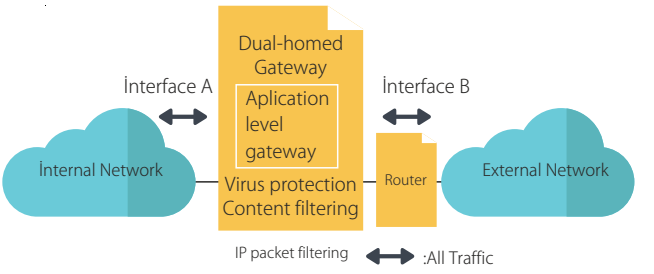
d) Güvenlik ağ geçidi kontrollerini gözden geçirme, uygulama, işletme ve izleme hususlarının ele alınması

Güvenlik gereksinimleri ve tehditleri standartta listelenmiş olup aşağıdaki tabloda da birbirleriyle eşleştirilmiştir.

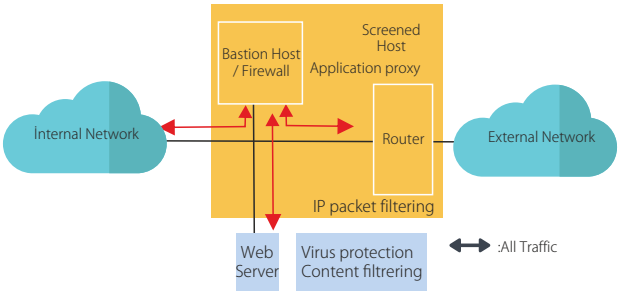
Güvenlik ağ geçidi mimarileri oluşturulurken yukarıdaki tehditlerin etkisini azaltmak için ağ cihazlarının yukarıda belirtilen gereksinimleri karşılaması gerekir. Bu gereksinimleri karşılama ve tehditleri azaltmada oluşturulacak mimarilerde standart belli başlı tekniklerin kullanılmasını tavsiye eder. Bu teknikler; ihtiyaca göre durum bilgisi olmayan paket filtreleme (stateless packet filtering), durum bilgisi olan paketin denetimi (stateful packet inspection), uygulama güvenlik duvarı, içerik filtreleme, saldırı önleme ve tespit sistemi ve güvenlik yönetimi uygulama programlama ara yüzü teknikleridir. Standardın son bölümü başlık olarak uygun ürünü seçmek olsa da burada anlatılanların uygulanmasıyla Tablo-1'de belirtilen gereksinimlerin karşılan-



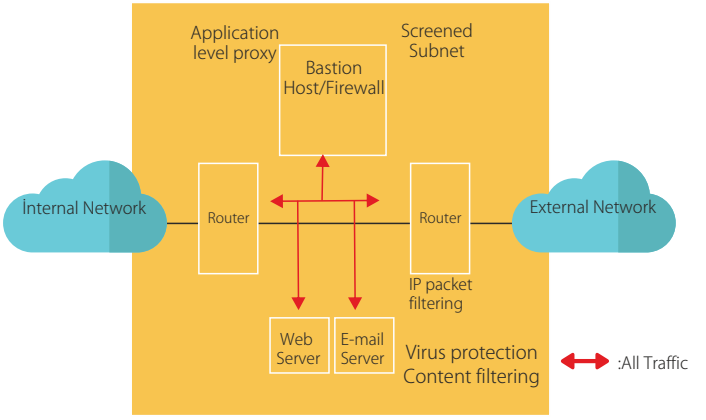
a)Paket filtrelemeli güvenlik duvarı/tarayıcı yönlendirici mimarisi



b) Çift Ağlı ağ geçiş mimarisi



c) Taranmış ev sahibi mimarisi



d) Taranmış alt ağ ağ geçidi mimarisi

dığından emin olunur. Bu anlatılanlar uygun güvenlik ağ geçidi mimarisinin seçimi, donanım ve yazılım platformunun seçimi, yapılandırma, güvenlik özellikleri ve ayarları, yönetim, günlük tutulması, denetim ve eğitim alanları olarak ayrılmışlardır. Bu alanların hepsi için geçerli olan tüm olası tehditlere (iç ağdan gelebilecek olanlara da), insan faktörüne dikkat edilmesi, konunun olabildiğince basitçe alınması ve güvenlik ağ geçidi bileşenlerinin doğru yapılandırma ve fonksiyonellikte kullanılması tavsiye edilir.

Yazımızda teknik olarak fazla detaya girmesek de güvenlik ağ geçitlerini sadece bir anahtar, yönlendirici veya herhangi bir başka ağ cihazından ibaret görmemeliyiz. Bu ağ cihazları eğer bir ağ alanı oluşturup bu ağa olan erişimi ve bu ağdan çıkan trafiği kontrol ediyorsa bu cihaza güvenlik ağ geçidinin bir bileşeni gözünde bakıp bilgi güvenliği politikasına uygun bir şekilde yapılandırıp yönetmemiz gerekmektedir. Sonuç olarak Bilgi Güvenliği Yönetim Sistemini sadece TS ISO/IEC 27001 ve TS ISO/IEC 27002 dokümanlarından oluştuğu gibi yanlış bir kanıya kapılmayıp kuruluş politikası gereği sürekli iyileştirme misyonuyla diğer kılavuz dokümanlarda belirtilen iyi uygulama örneklerini de kuruluş içinde uygulamak gerekmektedir.

	Gereksinim						
Tehditler	Mantıksal ağ bölümlemenin sağlanması	Mantıksal ağlar arasında oluşan trafiğin kısıtlanması ve analizi	Seçilen uygulamalardaki bağlantıları denetleyerek veya proxy işlemleri vasıtasıyla kuruluşun ağına ve kuruluşun ağından olan erişimin kontrolü	Kuruluşun ağ güvenlik politikasını zorunlu kılmak	Gelecek denetimler için trafiğin günlük kayıtlarının alınması	İç ağ, bilgisayar/ sistem ve uygulama mimarisinin saklanması	Ağ yönetim fonksiyonlarını kolaylaştırma kabiliyetini sağlamak
Yetkili kullanıcıların hizmet dışı kalması		X		X	X		X
Verilerin izinsiz değiştirilmesi	X	X	X	X	X		X
Verilerin yetkisiz olarak ifşa edilmesi	X	X	X	X	X		X
Yetkisiz olarak sistemin yeniden yapılandırılması			X	X	X	X	X
Kurumun kaynaklarının ve varlıklarının yetkisiz olarak kullanılması	X	X	X	X	X	X	X
Virus gibi kötücül yazılımlara sahip içeriğin yetkisiz olarak geçişi	X	X	X	X	X	X	X
Sanallaştırmanın ihlali	X	X	X	X	X		X
Güvenlik ağ geçitlerine karşı yapılan dağıtık hizmet dışı bırakma ve hizmet dışı bırakma saldırıları		X		X	X		X

Tablo: Güvenlik Gereksinimleri ve Tehditlerinin İlişkisi

TSEK 322

Güvenli Yazılım Geliştirme İçin Temel Kurallar

Aysun Kılıçlı ▶ TSE Sistem Yönetim Müdürlüğü

Ulusal Siber Güvenlik Eylem Planı 10 numaralı maddesinin alt eylemlerinden biri olan güvenli yazılım geliştirme temel kurallarının oluşturulması kapsamında, kritik altyapılar için geliştirilen yazılım projelerinde yazılım geliştirici ve proje yönetim ofisi tarafından rehber olarak kullanılmak üzere temel güvenlik kurallarının hazırlanması istenmiştir. Bu kriter, bir uygulama için programlama dilinden bağımsız olmak üzere, dokümanın oluşturulmasından, yazılımın tasarlanmasına, kodlanmasına, test edilmesine, kurulumuna ve kabul muayenesine kadar geçen süreçte, bu sürece müdahil tüm paydaşların yararlanabilecekleri, konulara bölünmüş kurallar dizininden oluşmaktadır. Yazılımı güvenli bir şekilde geliştirme adına paydaşlar tarafından hedeflenmesi gereken, bu kuralların tümünün yazılımda yer bulmasından ziyade yazılımın ve yazılımın kurulacağı ortamın ihtiyaçlarına göre bu dokümandaki kuralların incelenmeleri, sonrasında gerçeklenmeleri veya gerçeklenmelerine zemin hazırlanmasıdır.

Dokümandaki konu başlıkları, yazılım güvenliğinde önemli ve dikkat edilmesi gereken temel hususlar etrafında oluşturulmuştur. Bu başlıklar şu şekildedir:

- Verinin Korunması
- Kimlik Doğrulama
- Yetkilendirme
- Erişilebilirlik
- Sistem İzleme ve Denetimi
- Diğer Güvenlik Önlemleri

Verinin Korunması

Bu başlık, verinin yetkisiz kişilerin eline geçmesini engellemeyi, verinin hem bilgisayar sistemlerinde, hem saklama ortamlarında, hem de ağ üzerinde gönderici ve alıcı arasında taşınırken yetkisiz erişimlerden korunması, gizliliği ve bütünlüğü ile alakalı hususları içermektedir.

Kimlik Doğrulama

Bu başlıkta, kullanıcının sisteme/uygulamaya bağlanabilmesi veya uygulama içindeki birimlerin birbirlerini tanımaları için yapılması gereken işlem olan kimlik doğrulamanın güvenlik kuralları işlenmektedir.

Yetkilendirme

Bu başlıkta kimlik doğrulaması sağlanan kullanıcıların/yazılım birimlerinin sisteme, programa ve ağa hangi yetkilerle erişim hakkına sahip olduklarının belirlendiği yetkilendirme mekanizmaları ve bu mekanizmaların güvenlik unsurları işlenmektedir.

Erişilebilirlik

Bu başlıkta verinin her an ulaşılabilir ve kullanılabilir olmasını amaçlayan erişilebilirlik prensibi ele alınmaktadır. Bu kapsamda bilişim sistemlerinin kendilerinden beklenen iş sürekliliği ve bunun bilgi güvenliğine olan yansımaları madde madde işlenmektedir.

Uygulama servisleri 'noktadan noktaya' ya da 'uçtan uca' gizliliği ve veri bütünlüğünü desteklemelidir.

Sistem İzleme ve Denetimi

Bu başlıkta, yazılımda herhangi bir sorun veya anomali ile karşılaşıldığında sorunun tespiti için kullanılan sistemler, bunların yazılım güvenliğindeki yerleri işlenmektedir.

Diğer Güvenlik Önlemleri

Bu başlıkta yazılımlara en sık gerçekleştirilen saldırılara karşı alınacak önlemler irdelenmektedir. Bu önlemlerin çoğu küçük kod örnekleri ile açıklanmışlardır. Bu konu başlıkları içindeki maddeler diğer konu başlıkları ile paralellik gösterebilir. Bu durumu göz önünde bulundurarak, dokümanın okunabilirliğini artırmak için her maddenin altına etiketler yerleştirilmiştir. Bu etiketlerden yola çıkılarak, o madde ile alakalı tüm güvenlik başlıkları görülebilir.

Bu yazıda güvenli yazılım geliştirmede en önemli unsurlar olan verinin korunması, kimlik doğrulama ve yetkilendirme kriterlerine değinilecektir.

Verinin Korunması

- Uygulama, ister veya tasarım dokümanlarında aksi belirtilmedikçe her türlü verinin gizliliğini korumalıdır.
- Uygulama servisleri 'noktadan noktaya' ya da 'uçtan uca' gizliliği desteklemelidir.
- Uygulama, kullanıcının kimlik bilgilerini taşıma esnasında korumalıdır. SSL veya benzeri teknolojileri tüm kimlik denetimi süreci esnasında kullanmalıdır.
- Uygulama 'noktadan noktaya' veya 'uçtan uca' veri bütünlüğünü desteklemelidir.
- Uygulama içindeki veriler ve çıktılar güvenlik sınıflandırmasına tabi tutulmalıdır.
- Uygulama başka kaynaklara (örneğin uygulama veri tabanına) bağlanırken, erişim için kullandığı parolaları şifrelenmiş (encrypted) bir halde saklamalıdır.
- Uygulama, son kullanıcıların ya da istemci durumundaki uygulama servislerini kullanan diğer sistemlerin kimliklerini doğrulamak için kullandığı parolaları kriptografik özet halinde (hash) saklamalıdır.
- Silinmiş verilere uygulama bileşenleri üzerinden tekrar ulaşım engellenmelidir. Bellekte ya da disk

sisteminde oluşturulan nesnelerin (objects) gizli veri içermesi engellenmelidir.

- Tasarım uyarınca, gerektiği durumlarda veriler şifrelenirken GİD'de belirtilen standartlara uygun ya da belirtilen otorite tarafından onaylanmış bir kripto ürünü* veya mekanizması kullanılmalı ve bu şekilde depolanmalıdır.
- Uygulama içindeki veri akışı kontrol politikası belirlenmeli ve uygulanmalıdır.
- Uzaktan çalıştırılabilen veya sistemin değişik parçaları arasında transfer edilen taşınabilir kodlar (mobile codes) dikkatli bir şekilde ele alınmalı, envanteri tutulmalıdır.
- GİD'de uygulama içindeki tüm verilerin korunması öngörülüyorsa, veriler uygulama bileşenleri arasında şifreli olarak (gizliliği korunarak) iletilmelidir.
- Uygulama, herhangi bir fonksiyonu çalışmaya başlamadan önce güvenlik fonksiyonlarının çalışır ve ayakta olduğunu garanti etmelidir.
- Uygulama veri dağıtım servisleri (DDS) kullanılıyorsa, bunlara kesinlikle gizliliği korunmuş bir kanal üzerinden (Örn. SSL kullanarak) erişmelidir.
- Uygulama varlıkları arasında karşılıklı bütünlüğü (referential integrity) sağlamakla yükümlü olmalıdır.
- Uygulama geri dönüşü olmayacak şekilde silinmiş verilerin artık uygulama içinde erişilememesini ve yeni üretilen verilerin, geri dönüşü olmayacak şekilde silinmiş bilgi içermemesini garanti etmelidir.
- Son kullanıcı, uygulamayı birden fazla ekranda kullanıyorsa bu ekranlar ya da raporlama ara yüzleri üzerinden sunulan bilginin tutarlılığını sağlamalıdır.

Kimlik Doğrulama

- Uygulama kimlik doğrulama yapmadan, anonim erişime kapalı olan servislerine/arayüzlerine/sayfalarına erişimi engellemelidir ya da bu tür erişimlerin denetlenebileceği ve yönetilebileceği mekanizmalar sunmalıdır.
- Uygulamanın, müşteri tarafından tanımlanmış olan kritik servisleri ve ayarları için 2 veya 3 faktörlü kimlik doğrulama kullanılmalıdır.
- Uygulama, önceden belirlenmiş sayıda yanlış kimlik doğrulama denemesinden sonra kullanıcıdan CAPTCHA talep etmelidir. DOS ya da kaba kuvvet

saldırısı (bruteforce) ihtimalinin olmadığı ortamlarda, önceden belirlenmiş hatalı kimlik doğrulama denemesinin ardından hesap kitlenmelidir. Uygulama hesabı tekrar aktive etmek için bir mekanizma sunmalıdır.

- Kimlik doğrulama esnasında ve hata durumlarında uygulama, kullanıcıya mümkün olduğunca az bilgi ile geri bildirim yapmalıdır.
- Uygulama, kimlik doğrulamaları yapılmış kullanıcılara kendi parolalarını ve güvenlik kontrolleri için kullanılan profil bilgilerini (Örn. e-mail adresi) değiştirme imkanı vermeli.
- Uygulama, kullanıcıya parola kurtarma (password recovery) mekanizmaları sunmalıdır. Parola kurtarma fonksiyonu güvenlik zafiyeti içermeyecek şekilde gerçeklenmelidir.
- Uygulama kullanıcısının parolasını unuttuğu veya başka bir nedenle mevcut parola ile uygulamada oturum açamadığı durumlar için kullanıcıya parolayı sıfırlayabileceği bir ekran veya fonksiyon sunmalıdır.
- Kullanıcıya uygulamaya erişebilmek için otomatik olarak verilen ilk parola, saldırılara dirençli, benzersiz ve sınırlı geçerlilik süresine sahip olmalıdır.
- Uygulama kullanıcıları, parola belirlerken veya mevcut parolalarını değiştirirken GİD'de belirtilmiş parola politikalarına uymaya zorlanmalıdır.
- En iyi uygulama tavsiyesi olarak (best practice) önerilen 'autocomplete=off' bayrağı kullanılarak internet tarayıcılarının kimlik bilgilerini tutmasının engellenmesidir.
- Kimlik doğrulama, parola sıfırlama vs. işlemleri sonrası uygulamanın başka bir sayfasına internet tarayıcının yönlendirilmesini (redirect) sağlamak amacıyla HTML 'HTTP-EQUIV=REFRESH' kullanmaktan kaçınılmalıdır.
- Uygulama tarafından bırakılan çerez (cookie) için 'httponly' aktive edilmelidir. Buna ek olarak, HTTPS protokolü kullanılan bağlantılarda çerezler için 'secure' parametresi aktif olmalıdır.
- Uygulamanın, kimlik doğrulamada Tek Giriş (Single Sign-On-SSO) teknolojilerini kullanması ön görülüyorsa, uygulamaya özel Tek Giriş mekanizması yazmaktan ziyade, piyasada hâlihazırda bir kısmı açık kaynaklı olarak sunulan Tek Giriş teknolojilerini kullanmak güvenlik açısından daha uygun olacaktır.
- Uygulama, oturum tekil tanımlayıcısını (Session ID) korumalıdır.
- Oturum tekil tanımlayıcısı (Session ID) URL'de gönderilmemeli veya referrer başlığı içine dâhil edilmemelidir.
- Oturum yönetimi için kullanılan ve uygulamayı kullanan bütün kullanıcılar için tekil olması gereken değerler (session id, token vb.) güçlü bir rastgele veri üretecinden temin edilmeli ve tahmin edilemez derecede karmaşık olmalıdır.
- Belirlenen süre boyunca aktif olmayan oturumlar otomatik olarak kapatılmalıdır. Uygulama, sistem yöneticilerine bu süreyi ayarlayabilecekleri bir ekran sunmalıdır.

Yetkilendirme

- Uygulama, kullanıcının sadece bilmesi gereken bilgilere erişim sağlayabilecekleri şekilde kısıtlamalar getiren mekanizmalar barındırmalıdır.
- Yetkilendirme sunucu tarafında yapılmalıdır. Sadece istemci tarafında yetkilendirme kontrolü yapılmamalıdır.
- Yetkilendirme yaparken 'rol bazlı' yetkilendirme tavsiye edilmektedir.
- Uygulamada, kullanıcıların yetkilerinin sistem yöneticisi ya da yetkilendirilmiş kişiler tarafından ayarlanabildiği kimlik yönetimi ekranı olmalıdır.
- Uygulamada kimlik yönetim ekranlarında belirlenen kullanıcılar ve yetkiler dışında yetkilendirme olmamalıdır.
- Uygulama dokümante edilmemiş ve sistemin çalışmasını etkileyebilecek parametreleri ya da kullanıcı hesaplarını içermemelidir.
- Güvenlik fonksiyonları ile alakalı görüntüleme ve yapılandırma ara yüzlerine/sayfalarına/servislerine sadece güvenlikten sorumlu ve yetkilendirilmiş hesaplar erişebilmelidir.
- Her bir iş nesnesi (business object) için read/write/modify/delete gibi yetkiler tanımlanmalıdır.
- Kimlik yönetim servisleri (kimlik doğrulama-aut-

hentication), yetkilendirme (authorisation) ve kimlik veri depoları (user data store) merkezileştirilmelidir.

- Yetkilendirme dinamik olmalı ve yetki kaldırıldığında nesneye ya da servislere erişim mümkün olmamalıdır.
- Kullanıcı organizasyondan ayrıldığında erişim izinleri ve yetkileri kaldırılmalıdır.
- Veriye ya da nesnelere erişim imkânı sunan bütün yollar erişim denetimine tabi tutulmalıdır.
- Bir kullanıcının birden fazla rolü var ise oturumu kapatmadan roller arası geçiş yapabilmesi sağlanmalıdır.
- Uygulama kullanıcıya sadece yetkisi ve izni olan fonksiyonları, servisleri ve nesneleri (sayfa, iş nesnesi, ekran vs.) göstermelidir.
- İşletim sistemi üzerinde bulunan bir araçla uygulama hesaplarına ait parolalarının doğrudan değiştirilmesini engelleyecek mekanizmalar sunulmalıdır.
- Canlı uygulama ortamı, test ve geliştirme veri tabanlarına (örneğin operasyonel, eğitim, alıştırma veri tabanları) bağlanmamalıdır. Aynı şekilde gerçek veri tabanı asla geliştirme ve test ortamlarında kullanılmamalıdır.
- Yığın görevleri (batch jobs) için yetkilendirme ve izleme yapılmalıdır.

Güvenlik fonksiyonları ile alakalı görüntüleme ve yapılandırma ara yüzlerine/sayfalarına/servislerine sadece güvenlikten sorumlu ve yetkilendirilmiş hesaplar erişebilmelidir

Çevik Yazılım Geliştirme Yaklaşımı ve SPICE Organizasyonel Olgunluk Modeli

Kerem Kemaneci ▶ TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü

1. Çeviklik ve Disiplin

Değişen dünyamızda her başarılı girişim hem çeviklik hem de disipline ihtiyaç duyar. "Eğer bir şirket, çevik olmadan güçlü bir disipline sahipse, sonuç durağanlık ve bürokrasi olacaktır. Sınırsız çeviklik ise faydasız bir hevesle enerjinin boşa harcanmasından öteye geçemeyecektir[1]."

Günümüz dünyasında her şey her zamankinden çok daha hızlı değişmekteyken, 2-3 yıla sığan başarı hikâyelerine şahitlik edebiliyoruz; aynı şekilde asırlık şirketlerin hızla çöküşlerine de şahit olmaktayız. Hızla değişen dünyada işletmeleri çok katı kurallara bağlamak, değişime ayak uyduramamak şirketlerin sonunu getirebilir (aşırı disiplin). Kuralları belirlenmiş sistem olmadan sınırsız çeviklik tahmin edil(e)meyen projeler, aşılan proje bütçeleri, geciken teslimat zamanları...kısacası "kaos", firmaları çıkmaz yollara götürebilir.

Çeviklik ve disiplin iki tarafı keskin kılıç gibidir, ortada bir yerlerde denge kurabilmek kaçınılmaz bir ihtiyaçtır. Çevik (atik, agile) yazılım geliştirme yapan firmalar zaman, bütçe, tasarım, kullanıcı istekleri konularında esnek olurken buna karşılık tahmin, kaynak kullanımı, risk yönetimi, kapasite, bütçe yönetimi gibi kritik süreçleri iyi yönetebilmelidir.

Çevik yazılım geliştirmenin ana prensiplerinden olan müşterinin her isteğine cevap vermek kulağa hoş gelse de, müşterinin sınırsız isteklerine sonuna kadar cevap vermeye çalışırken işletmenin kendi varlığını sürdürme gereksinimini göz ardı etmemelidir.

Çevik yazılım geliştiren işletmeler çevik yazılım prensiplerini uygularken, organizasyonel olgunluk modellerinin önerdiği uygulamaları da hesaba katarak çeviklik yeteneklerini olgun bir seviyeye çıkarmalıdırlar.

2. Organizasyonel Olgunluk Modeliyle Uyumlu Çevik Yazılım Geliştirmek

Çevik yazılım geliştirmenin ana prensiplerinden olan müşterinin her isteğine cevap vermek kulağa hoş gelse de, müşterinin sınırsız isteklerine sonuna kadar cevap vermeye çalışırken, işletmenin kendi varlığını sürdürme gereksinimini göz ardı etmemelidir.

Çevik yazılım geliştiren işletmeler çevik yazılım prensiplerini uygularken, organizasyonel olgunluk modellerinin önerdiği uygulamaları da hesaba katarak çeviklik yeteneklerini olgun bir seviyeye çıkarmalıdırlar.

Yazılım Geliştirme Olgunluk Modeli olarak dünyada en çok tanınan SPICE – TS ISO/IEC 15504 ve CMMI olmak üzere iki standart vardır. SPICE ve CMMI gibi Süreç Olgunluk Modelleri işletmelerin süreçlerinin belirlemesi, süreçlerin yetkinlik seviyelerinin tespit edilmesi, süreçlerin yetenek düzeylerinin daha üst seviyeye çıkarılması için rehberlik etmesi gibi alanlarda yardımcı olmaktadır. Çevik yazılım geliştirme modellerini uygulayan/uygulamak isteyen yöneticiler bahsi geçen olgunluk modellerinin bir kontrol listesi veya yazılı kurallar olmadığını unutmamalıdır. Bu standartlar işletmelere en iyi uygulamaları önerip işletmelere bir anlamda rehberlik ederken, işletmelerin süreçlerini ölçmeyi, değerlendirmeyi ve iyileştirmeyi amaçlar. Çevik yazılım geliştirme prensipleri sayesinde SPICE standardıyla belirlenmiş süreçlerin çeşitli performans göstergelerinde iyileştirme yapmak mümkün olabilir. Örneğin: Birim zamanda üretilen fonksiyon, hata oranlarının azalması, müşteriye geri dönüş süresi, değişiklik isteklerinin minimuma indirilmesi vs. çevik yazılım geliştirme yöntemleri ile iyileştirilebilir.

Çevik yazılım geliştirme prensipleri sayesinde SPICE standardıyla belirlenmiş süreçlerin çeşitli performans göstergelerinde iyileştirme yapmak mümkün olabilir.

3 İşletmeler İçin SPICE Standardı

İşletmelerin organizasyonel olgunluk modellerini uygulamaya koymak için genelde motivasyonu ihale şartnameleri olsa da, bu olgunluk modellerinde sertifikasyon sadece sonuç anlamına gelir. Yine de ihale nedeniyle sertifika almayı amaçlamış birçok firma, SPICE – TS ISO/IEC 15504 standardının, firmalarına kayda değer faydalar sağladığı ve yeni fikirler geliştirmelerinde etkili olduğunu beyan etmişlerdir. Belge alma amacı bir sebep olarak kalmış ve süreç yetenek düzeylerini daha yükseğe çekmek asıl motivasyon haline gelmiştir.

SPICE ISO/IEC 15504 standardı uyarlanırken firmanın devreye alması gereken uygulamalar kesin kurallara bağlanmamış ve uygulamaların nasıl, hangi yöntemle veya teknikle ele alınacağı firmaya bırakılmıştır. Bu açıdan işletmelere uygulama alanında çevik yazılım geliştirmek için büyük bir esneklik de sağlanmaktadır.

SPICE Organizasyonel Olgunluk Modeli (OOM) için ilk adım süreçlerin ve bu süreçlerin gerektirdiği temel uygulamaların belirlenmesidir. Olgunluk seviyesini birinci seviyede gerçekleştirmek için öncelikle yazılım geliştirmedeki temel süreçler seçilir. Bu süreçler daha çok mühendislik süreçlerinden meydana gelir ve bu süreçler gereksinim toplanması, gereksinim analizi, tasarım, kodlama, entegrasyon, test, sürüm yayımlama, kurulum ve bakım süreçlerinden oluşur.

Türkiye'de yazılım işletmelerinin %95'lik bir kısmı küçük ve orta boyutlu işletmelerden oluşmaktadır. Firmaların ortalama çalışan sayısı 9 kişiden oluşmaktadır[2]. Çevik yazılım geliştirme modellerinden en popüleri olan SCRUM'da takımların 3 - 9 kişiden oluşması da ilginç bir tesadüftür. Bu firmaların olgunluk seviyelerinin SPICE Seviye-1 düzeyine gelmesi ve böylece üretim süreçlerini SPICE standardına uyumlu hale getirmesi sayesinde üretim kalitesinin artacağı öngörülebilir bir durumdur.

Çevik yazılım geliştirmenin en önemli prensiplerinden biri de kısa çevrim süreleri ile erken safhalarda Prototip oluşturarak müşteriye sunmak ve müşterinin ihtiyaçlarını daha net şekilde anlamaktır. Bu da IKIWISI kuralına dayanır[3]. Standish Group tarafından gerçekleştirilen bir araştırmaya göre tipik yazılım sistemlerinde var olan özelliklerin %45 kadarının hiç kullanılmadığı, %19 kadarının da çok nadiren kullanıldığı tespit edilmiştir[4].

IKIWISI Kuralı: "I Know when i see it" – "Ben gördüğümü bilirim" şeklinde Türkçe 'ye çevirebiliriz. Projenin başlangıcında henüz ortada hiçbir şey yokken müşteriden gereksinim istemek zordur. İlk prototipi oluşturup müşteri kullanımına hazır hale gelinceye kadar mutlaka eksik veya fazlalıklar olacaktır. IKIWISI kuralına göre müşteri ürünü çok erken görme şansına sahip olacak ve fikirlerini ve ihtiyaçlarını daha iyi ve daha doğru ifade edebilecektir. Bu sayede gereksinimlerin toplanması süreci ve ardıl süreçlerde harcanacak iş gücünde idealde ortalama %45'e kadar tasarruf gerçekleştirmesi sağlanabilecektir.

SPICE OOM Seviye-2 için karakteristik olarak her süreçte istenen performans metriklerinin belirlenmesi ve metriklerin doğru şekilde ölçülerek analiz edilmesi, süreç performansının devam ettirilmesi veya iyileştirilmesi gerekmektedir. Bu ölçümleri destekleyebilecek birçok ticari veya ticari olmayan yazılım geliştirilmiştir ve geliştirilmeye devam etmektedir. Birçok firma ise doğal olarak yazılım firması olmalarından kaynaklı kendi iş takip yazılımlarını yapmakta ve Organizasyonel Olgunluk Modeli gereksinimlerini karşılamaya yönelik özellikler eklemektedir. Performans ölçümleri sayesinde aksayan yönler daha kolay görülebilmekte ve klasik kalite metotlarının kullanımı da mümkün olabilmektedir.

Örneğin bir işletme iş takip yazılımları sayesinde hataları daha isabetli şekilde belirleyip, hataların kaynağını çözerek, öğrenilmiş dersler edinebilmektedir. Pareto Analizi'ne göre sorunların kaynağının %20'sini ortadan kaldırdığında hata sayısında %80'lere varan azalmalar görülebilmektedir. Bu da çevikte %40 - %50 oranında yeniden işleme masraflarını azaltabilmektedir.[5] Bu ölçümlerin yapılmadığı bir işletmede bu oranları da görmek mümkün olmayacağından yönetim açısından kapasite belirleme, kaynak aktarımı ve büyüme hedefleri belirleme gibi konularda belirsizlikler olacaktır. Süreçlerin belirlenip performans ölçümlerinin yapılmadığı bir işletmeyi yönetmek, adeta göstergeleri olmayan bir arabayı kullanmak gibidir.

Çeviklik disiplinli iş yapma ihtiyacı doğurur, bu disiplini sağlamak adına kurallar oluşturmak için SPICE Organizasyonel Olgunluk Seviyelerini hedef olarak belirlemek iyi bir seçenek olacaktır. Çevik yazılım geliştirme metodolojisi kullanan şirketler için risk yönetim stratejisi geliştirmek hayati bir öneme sahiptir. Çevik geliştirme modellerinin olumsuz yönlerinden sayılabilecek, bütçe, zaman, insan kaynağı limitlerinin aşılması riskleri görmezden geline-

mez. SPICE standardında yer alan risk yönetimi süreci bu noktada devreye girecektir.

Ülkemizdeki yazılım firmaları çoğunlukla sipariş üzerine müşteriye özel yazılım sistemleri geliştirmektedir. En büyük müşterilerden biri de kamu kurumları olmaktadır ve kamu kurumlarının yazılım satın alma süreçleri oldukça katı kurallara ve denetimlere tabidir. Bu açıdan da bakıldığında SPICE standardının isterlerinin bu süreçlerde destek olacağı tahmin edilebilir.

Yukarıdan aşağıya, aşağıdan yukarıya iyileştirme yaklaşımı[6]; çevik geliştirme metodolojisi kod geliştiricilerin kendilerine güvenlerini artırıp iş tatmini sağlarken, yönetim ise yapılan işlerin başarısı, performansı, çevrim süreleri gibi bilgilere ihtiyaç duyarlar. Sonuç olarak müşteriler kaliteli ürün ve hizmetlerle memnun edilirken, çevik metodolojiler kod geliştirici ve teknik ekibe işini sevdirecektir. SPICE standardı ile süreçleri ve kuralları doğru şekilde belirlenmiş işletmenin yöneticileri geleceği daha iyi görebilecek ve bu sayede işletmeyi belirlenecek hedefler doğrultusunda yönetirken kendilerine güvenleri artacaktır.

Açık Kaynak Kodlu Yazılımlar ve Kamuda Uygulanması

Abdullah Keskin ▶ TSE Bilşim Teknolojileri Test Müdürlüğü

Açık Kaynak Kodlu Yazılım çalıştırılması, kopyalanması, dağıtılması ve değiştirilmesi özgür bırakılmış yazılımları ifade eder.

Açık Kaynak Kodlu Yazılımlar

Açık kaynak, bir bilgisayar yazılımının makina diline dönüştürülüp kullanımından önce, programcılar tarafından okunur, anlaşılır, yeni amaçlara uygun değiştirilebilir halinin gizli tutulmayıp, açık halinde kamuyla paylaşılıyor olmasına verilen isimdir. Diğer bir deyişle Açık Kaynak Kodlu Yazılım çalıştırılması, kopyalanması, dağıtılması ve değiştirilmesi özgür bırakılmış yazılımları ifade eder. Bu tür yazılımlar genelde bir kişi ya da bir topluluk tarafından geliştirilir. Kaynak kodlarının ve farklı işletim sistemleri için uyarlanmış çalıştırılabilir (executable) paketlerin dağıtımı ve desteklenmesi genelde internet üzerinden (Github gibi) sağlanır.

En yaygın kullanılan özgür yazılım lisanslarının başında GNU GPL Lisansı gelmektedir. Aşağıda belli başlı bazı özgür yazılım lisansları listelenmiştir:

- GNU Genel Kamu Lisansı (GPL)
- GNU Kısıtlı Genel Kamu Lisansı (LGPL)
- BSD Lisansı
- Mozilla Kamu Lisansı (MPL)
- MIT Lisansı
- Apache Lisansı
- Eclipse Kamu Lisansı (EPL)
- Avrupa Birliği Kamu Lisansı (EUPL)

Bir yazılımın açık kaynak kodlu sayılması için gereken şartlar (Open Source Initiative, 2016):

Yazılımın ücretsiz dağıtılması

Yazılımın dağıtım lisansı hiçbir parçanın satılması ya da bu yazılımın kullanımı için başka bir ücretli programın yüklenmesi gibi bir zorunluluğu barındırmaması gerekir.

Kaynak Kod

Yazılımın açık kaynak kodlu olması, yazılımın derlenmiş halinin ücretsiz olarak sunulmasının yanı sıra kaynak kodunun da yazılımla beraber sunulması ve bu kaynak kodun kullanıcılar tarafından da dağıtılmasına bir engel olmaması anlamına gelir.

Yazılımın Geliştirilmesi

Yazılımın kaynak kodunda değişiklik yapılarak yine aynı lisans altında, aynı veya farklı isimle dağıtımına izin verilmesi gerekir.

Yazarın kaynak kodunun bütünlüğü

Bazı lisanslar yazılımın aynı isimle dağıtılmasına sadece yazarın kaynak kodunun orijinal halinin korunması şartıyla izin veriyor olabilir. Bu durumda eğer kaynak kod üzerinde bir geliştirme yapılıyorsa farklı isim ve/veya versiyon altında dağıtımı yapılabilir.

Kişiye bağlı kısıtlama

Lisans anlaşmasının belli bir kişi veya gruba has olmayıp, herkes için geçerli olması gerekir.

Yazılımın kullanım amacı

Yazılımın kullanım amacına yönelik bir kısıtlama bulunmaması gerekir. Yazılımın eğitim amaçlı kullanılabileceği gibi ticari maksatlarla da kullanılması lisans açısından problem teşkil etmemelidir.

Lisansın dağıtımı

Yazılıma erişen tüm kişilerin dağıtım konusunda da bir lisans kısıtlamasına tâbi tutulmaması gerekir.

Lisans bir ürüne özel olmamalı

Lisansın yazılımla üretilen belli bir ürüne has değil, yazılımın kendine has olması gerekir. Yazılımın kullanımı ya da dağıtımı belli bir ürünü kullanmaya bağımlı olmamalıdır.

Yazılımın teknolojik özellikleri

Yazılımın geliştirilmesi ya da kullanımı bir ürünün kullanımını zorunlu kılmamalıdır.

Ülkemizde Açık Kaynak Kodlu Yazılım Uygulamaları

Kamuda açık kaynak kodlu yazılım kullanımı 2003 yılında başlatılan e-Dönüşüm Türkiye Projesi kapsamında ele alınan önemli konulardan birisidir. Bu bağlamda, ilk olarak, 2005 Eylem Planı 7 numaralı "Kamu kurum ve kuruluşlarında açık kaynak kodlu yazılımların uygulanabilirliği" eylemi ile Kalkınma Bakanlığı Bilgi Toplumu Dairesi tarafından ilgili paydaşların katılımıyla konuya ilişkin bir rapor yayınlanmıştır. Bu raporda, açık kaynak kodlu yazılımın temel özellikleri, tarihçesi, kullanım alanları ve sağladığı avantajlar yer almakta, ayrıca açık kaynak kodlu yazılım hukuki ve mali yönden incelenmektedir. Raporda açık standartlara da vurgu yapılarak açık

kaynak kodlu yazılımın açık standartların gelişimi açısından önemli bir araç olduğuna dikkat çekilmektedir. Ayrıca bu rapora ek olarak söz konusu eylem kapsamında "Göç Planı Hazırlanması ve Uygulanması" raporu da yayınlanmıştır. Bu raporun kapsamı ise kamu kurum ve kuruluşları başta olmak üzere açık kaynak kodlu yazılıma geçmeyi planlayan kurumların göç adımlarını tasarlamalarını ya da uygun olmayan yazılımların geçişini elemelerini kolaylaştırmak için bir "Göç Planı" hazırlanmasıdır.

2006-2010 döneminde hazırlanan Bilgi Toplumu Stratejisi eki Eylem Planı'nda 74 numaralı "Kamuda Açık Kaynak Kodlu Yazılım Kullanımı" eylemi ile TÜBİTAK-BİLGEM (Türkiye Bilimsel ve Teknolojik Araştırma Kurumu – Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi) sorumluluğunda kamuda Açık Kaynak Kodlu Yazılım kullanımı için örnek oluşturmak üzere bir pilot uygulama yapılması ve bu uygulamada elde edilen tecrübelere göre Açık Kaynak Kodlu Yazılım kullanımının uygulanabilirlik analizinin gerçekleştirilmesi hedeflenmiştir. Bu kapsamda, Enerji Piyasası Düzenleme Kurumu'nda (EPDK) bir pilot uygulama yapılması için çalışmalar başlatılmıştır. EPDK'da yapılan çalışma kapsamında kuruma ait bilişim sistemleri TÜBİTAK-BİLGEM tarafından kurularak kurum sunucuları ile kullanıcı bilgisayarlarında Pardus kullanılmaya başlanmıştır. Proje takviminde önemli gecikmeler yaşanmış olup projeden henüz eyleme yönelik somut bir sonuç elde edilememiştir. Bununla birlikte, projenin kamuda açık kaynak kodlu yazılım kullanımına ilişkin önemli girdiler sağlayabileceği düşünülmektedir." (ÖZDAŞ, 2012)

Enstitümüz tarafında konu ile ilgili yapılan çalışmalara baktığımızda, TSE Bilişim Teknolojileri Test ve Belgelendirme Dairesinin girişimleriyle Aralık 2015'te TSE K 492 Pardus GNU/Linux Personel ve Firma Belgelendirmesi Kriteri oluşturulmuştur. Bu kriter temel alınarak yapılan belgelendirmelerde hem kamuda çalışan mevcut sistemlerin Pardus işletim sistemine aktarılması amacıyla "Pardus Göç Uzmanı" personel belgelendirmesi hem de bu işi firma olarak yapmak isteyenler için firma belgelendirmesi faaliyetleri başlatılmıştır.

Sayısal Kaynak Kod Emanetçilik Sistemi

Kaynak kodlar ve teknik dokümantasyonlar yazılım üreticilerine ait özel mülkiyet hükmündedirler ve gizli tutulurlar.

Mert Özkan Özcan
▶ TSE Bilişim Teknolojileri Test Müdürlüğü

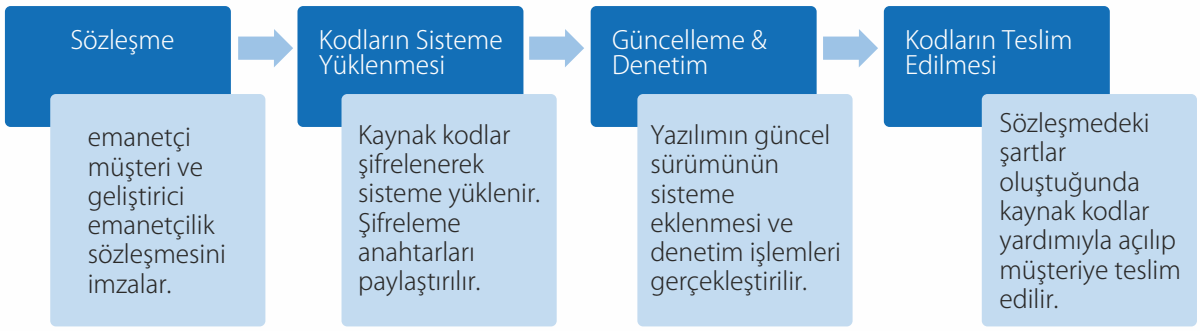
Ülkemizde ve dünyada gelişen bilişim teknolojileri ihtiyaçları doğrultusunda üretilen yazılımların karmaşıklıkları hızla artmakta, yazılımlardan beklenen fonksiyonel özellikler arttıkça bu durumdan yazılım geliştirme süreleri ve maliyetleri etkilenmektedir. Bu durum, yazılım geliştiricileri ve müşterileri arasındaki iş süreçlerinde de belirgin rol oynamaktadır. Yazılımlar, basitçe belirli bir programlama dilinde programcılar tarafından yazılmış 'Kaynak Kod' ve bu kaynak kodun işlemciler tarafından okunabilmesi için derlenip, '0' ve '1'lerin birleşimlerinden meydana gelen 'Derlenmiş Kod'dan oluşurlar. Derlenmiş kodlar insanlar tarafından kolayca okunamadıkları için yazılım geliştiriciler için esas önemli olan kaynak koddur. Kaynak kod ise kişilere yazılımda istedikleri değişiklikleri yapma imkânı vermektedir.

Yazılım geliştiriciler, müşterilerine çalışan uygulamaları ve uygulamanın çalışması için gerekli verileri verirler, fakat yazılıma ait kaynak kodu ve teknik dokümantasyonu müşterileri ile paylaşmazlar. Çünkü kaynak kodlar ve teknik dokümantasyonlar yazılım üreticilerine ait özel mülkiyet hükmündedirler ve gizli tutulurlar. Fakat bazı koşullar altında, müşteriler yazılıma ait kaynak koda ve teknik dokümantasyona erişmek isteyebilirler.

Geliştiriciler, kendi fikri mülkiyetleri olan yazılımların kaynak kodlarını müşterileriyle paylaşmak istememekte, müşteriler ise iş sistemlerini üzerine kurguladıkları yazılımların sürdürülebilirliğini garanti altına almak istemektedirler. Bu noktada ortaya çıkan karşılıklı güven ihtiyacını gidermek için soruna özel bir yedieminlik sistemine gerek duyulmuştur.

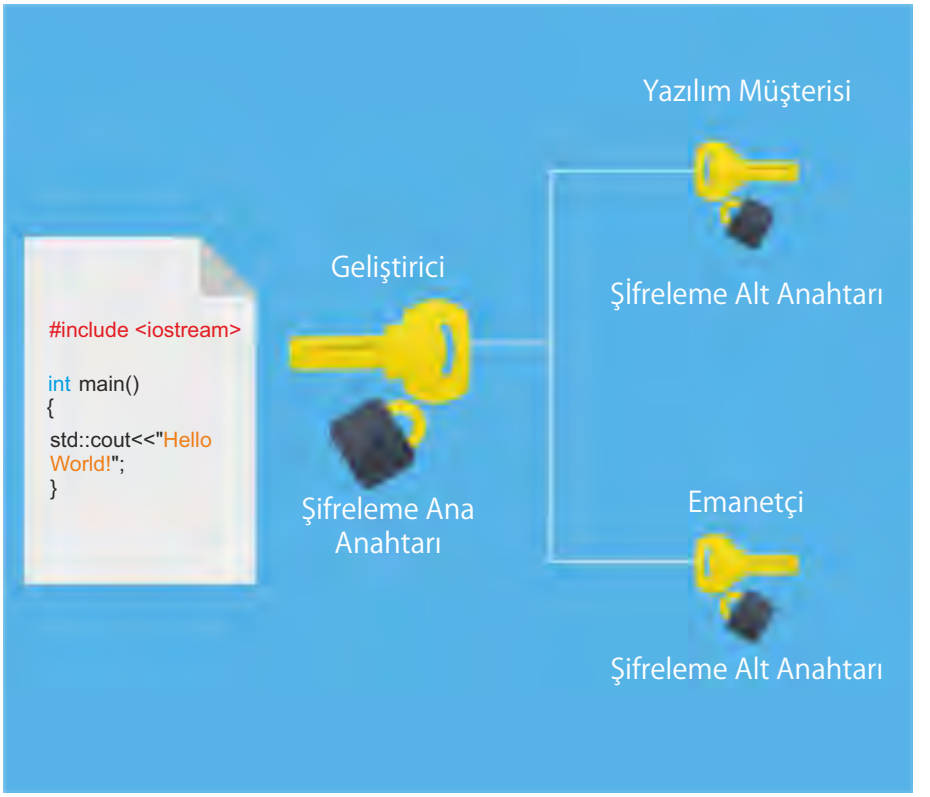
Yedieminlik, hukuksal durumu çekişmeli olan bir malın veya eserin iki taraf arasında imzalanan temel bir sözleşme ile sözleşmedeki şartlar oluşana kadar tarafların güvendiği üçüncü bir kişide saklanması olarak tanımlanabilir. Sayısal kaynak kod emanetçilik hizmeti ise basitçe yedieminlik sisteminin yazılım kaynak kodu için uygulanmasıdır.

Süreç, tarafların kaynak kod emanetçilik sözleşmesini imzalamacıyla başlar. Kaynak kod emanetçilik sözleşmesinin tarafları ve süreçten kazanımları aşağıdaki tabloda listelenmiştir.



Taraflar	Kazanımlar
Yazılım Müşterisi	Sözleşmede belirtilen koşullar gerçekleştiğinde yazılıma ait kaynak kodlara erişim hakkı kazanır. Yazılım geliştirici sözleşmedeki sorumluluklarını yerine getiremeyecek durumda olduğunda bu varlıklara erişim sağlanarak yazılımın devam ettirilmesi sağlanır.
Yazılım Geliştirici	Sözleşmede belirtilen sorumluluklarını yerine getirdiği sürece kendi fikri mülkiyeti olan yazılım kaynak koduna erişim olmayacağından ve böylelikle bu kodların kâr amaçlı kullanılmayacağından emin olur.
Emanetçi	Sağladığı emanetçilik hizmet kalemlerinden maddi gelir elde eder.

Kaynak kod kontrolü için bir diğer alternatif ise yazılım geliştirici ve yazılım müşterisinin üzerinde uzlaştığı bağımsız bir denetçidir.



Sözleşme imzalandıktan sonra yazılım kaynak kodların, emanetçinin güvenliğini sağlamakla yükümlü olduğu sisteme aktarılması işlemleri gerçekleştirilir. Emanetçi, yazılım geliştirici ve yazılım müşterisi bir araya gelerek kaynak kodları sisteme yüklerler. Ancak bu noktada sisteme yüklenecek olan kaynak kodların müşterinin kullanmakta olduğu sahada çalışan yazılıma ait olup olmadığı sorusu ortaya çıkmaktadır. Emanetçi söz konusu yazılımın kullanıcısı olmadığından dolayı kaynak kod denetimini gerçekleştirmesi pratik olarak mümkün değildir. Yazılım müşterisi ise yazılımın sahadaki kullanıcısı olduğundan yazılım geliştiricisinin gözetiminde kaynak kodları inceleyip, doğruluğunu kontrol edip onaylayabilir. Kaynak kod kontrolü için bir diğer alternatif ise yazılım geliştirici ve yazılım müşterisinin üzerinde uzlaştığı bağımsız bir denetçidir. Her iki durumda da emanetçi, yazılım geliştiricisinin getirdiği kaynak kodları sistemlerine yüklemeden önce yazılım müşterisinin onayını almalıdır. Yazılım müşterisinin onayladığı kaynak kodlar sisteme aktarılması süreci adımları aşağıda sıralanmıştır:

1. Kaynak kodların şifrelenmesi için kullanılacak olan rastlantısal (random) ana anahtarın üretilip, yazılım geliştiriciye teslim edilmesi

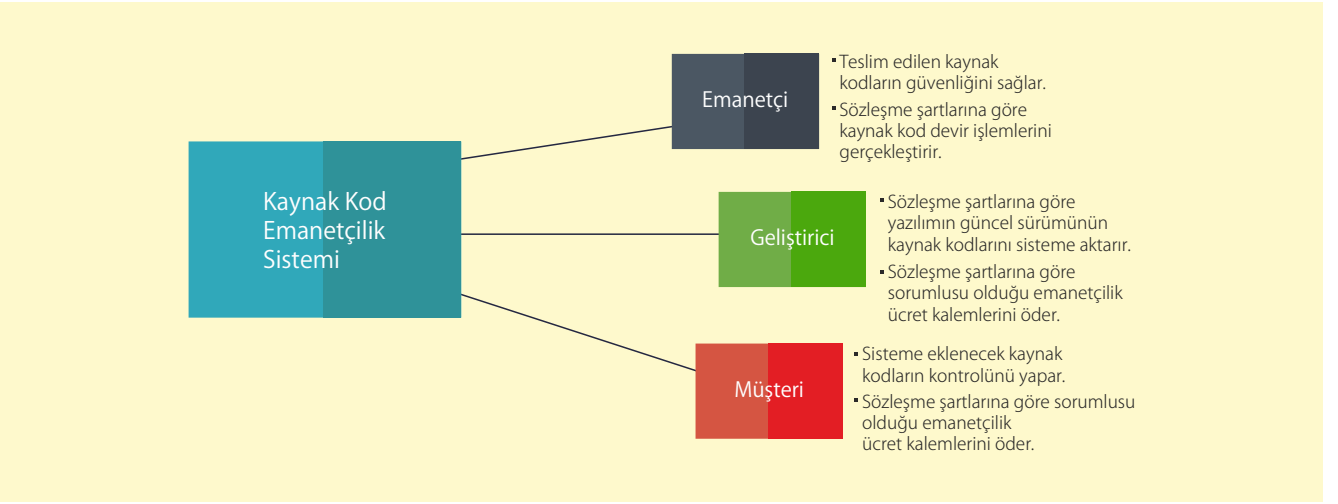
2. Ana anahtardan iki alt anahtar üretilip bir tanesinin yazılım müşterisine, diğerinin emanetçiye teslim edilmesi

3. Kaynak kod tesliminde ve denetimlerde kullanılması amacıyla kaynak kodun şifreleme işlemi öncesi ve sonrası hash değerlerinin hesaplanması

4. Yazılım geliştiriciye teslim edilen ana anahtar ile kaynak kodların şifrelenmesi

Yukarıdaki işlemlerin gerçekleştirilmesi sonrasında kaynak kodlar şifrelenmiş bir şekilde emanetçinin güvenli sistemlerine aktarılır. Bu noktada dikkat edilmesi gereken husus, yazılımın fikri mülkiyet hakları sahibi konumundaki geliştiricisi haricindeki tarafların tek başlarına kaynak koda doğrudan erişme imkânlarının bulunmamasıdır.

Şifrelenen kaynak kodların açılması için yetkili ana anahtar sadece geliştiriciye teslim edilmekte, ema-



netçi ve müşteriye teslim edilen alt anahtarlar tek başlarına bir anlam ifade etmemekte ve bir araya getirilmeden şifrelenmiş kaynak kodlar açılamamaktadır. Günümüzde kullanıcıların yazılımlardan beklentileri sürekli artmakta ve değişmektedir. Bu durum, yazılımların yaşayan süreçler olması zorunluluğunu ortaya çıkarmaktadır. Kullanıcı taleplerine cevap veremeyen yazılımları bekleyen 'son' düşünüldüğünde, emanetçilik sistemine yüklenen yazılımın güncelliğinin sağlanması önem arz etmektedir. Yazılım geliştirici, emanetçilik sözleşmesi kapsa-mında belirlenen aralıklarla sistemde bulunan kaynak kodları güncellemelidir. Emanetçilik sisteminde yazılım güncelleme işlemleri yazılım müşterisinin onayı ve geliştiriciye teslim edilmiş ana anahtarın güncel yazılım kaynak kodlarını şifrelemesi için kullanılması süreçlerinden oluşmaktadır.

Emanetçilik sistemine teslim edilen kodlar için yazılım müşterilerinin belirli aralıklarla denetim taleplerinin olması mümkündür. Denetim işlemleri genellikle iki seçenekli yapılmaktadır. İlk seçenekte emanetçilik sistemine şifreli şekilde eklenmiş kodlar üzerinde eşlik denetimi yapılmakta, işlem sonucu kaynak kod tesliminde taraflara teslim edilmiş olan hash değerleriyle karşılaştırılmaktadır. İkinci seçenekte yazılım geliştiricinin getirdiği ana anahtar vasıtası ile kaynak kodlar açılıp yazılım müşterisinin geliştirici gözetiminde kaynak kodları incelemesi sağlanmaktadır.

Süreç başlangıcında imzalanan kaynak kod emanetçilik sözleşmesinde kaynak kod devir şartları belirlenmektedir. Yazılım müşterisi bu şartlardan herhangi birisinin oluştuğunu yasal bir dayanak (mahkeme kararı vb.) ile emanetçiye bildirmek zorundadır. Müşterinin sunduğu yasal dayanak, emanetçi tarafından incelenerek olumlu bulunduğu takdirde, emanetçide ve yazılım müşterisinde bulunan alt anahtarlar yardımıyla kaynak kodlar açılır ve sözleşmede kaynak kod devir işlemlerini gerçekleştirir. Kaynak kod devir şartlarına bazı örnekler aşağıda listelenmiştir:

1. Yazılım geliştirici firmanın iflas etmesi

2. Yazılım geliştirici firmanın ticaretten çekilmesi

3. Yazılım geliştirici firmanın lisans veya destek anlaşmasının şartlarını ihlal etmesi

4. Geliştirici firmanın yapısının değişmesi ya da sahibinin değişmesi

5. Yazılım geliştiricinin ürünü geliştirmeyi durdurması

KAYNAKÇA

- TSE Escrow Analiz Raporu – Yelda ÜNAL (ARALIK 2013)
- Agreement, Source Code Escrow, Dilşad KESKİN.
- "KAYNAK KOD (SOURCE CODE) ESCROW SÖZLEŞMESİ.
- " Yücel, Meriç, and Burak Üstündağ. "Sayısal Veri ve Kaynak Kodu Emanetçilik Sistemi, 4." Ulusal Yazılım Mühendisliği Sempozyumu.

TS 13298 Elektronik Belge ve Arşiv Yönetimi Standardının Kamu Kurumlarına Etkisi

Serkan BİLECEN

▶ TSE Bilişim Teknolojileri Belgelendirme Müdürlüğü

Türk Standardları Enstitüsü (TSE) Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığının en eski ve en faal hizmetlerinden birisi olan TS 13298 Elektronik Belge ve Arşiv Yönetimi Sistemi Ürünleri Belgelendirmesi, 2010 yılından beri gerçekleştirilmektedir. Standart kapsamında yapılan çalışmalar, kamu kurumlarındaki tüm faaliyetlerin hızını ve kalitesini doğrudan etkilemekte olup, bundan dolayı TSE'nin bütün kamu kurumlarındaki faaliyetler üzerinde önemli bir rol oynamasını sağlamaktadır.

Standardın temel amacı, modern çağın gereklerine uygun olarak faaliyetlerinin hızlandırılması gereken kamu kurumlarında üniversitelerde, belediyelerde ve diğer kurumlarda; belgelerin geleneksel fiziksel ortamdan elektronik ortama geçişinin sağlanması, teknolojik gerekliliklerin yerine getirilmesi, belgelerde bulunması gereken diplomatik niteliklerin elektronik ortamda da uygulanabilirliğinin gerçekleştirilmesini sağlamaktır. Belgelerin hukuki geçerliliğinin sağlanması da önemli bir kriterdir. Standardın kapsamında başlıca; Dosya Tasnif Planı ve Saklama Planları ile ilgili Yönetim Özellikleri, E-Arşiv Modülü, Güvenli Elektronik İmza, Kayıtlı Elektronik Posta, E-Yazışma Paketi gibi teknolojik gereksinimler ile ilgili şartlar, kullanım özellikleri, üst veri yönetimi ve yetkilendirme tanımlamaları bulunmaktadır.

Ülkemizdeki birçok kamu kurumu, standardın adını ilk olarak 2008/16 Sayılı T.C. Başbakanlık Genelgesi'nde duymuştu. Adı verilen Genelgede, kamu adına görev yapan kurum ve kuruluşların faaliyetlerinin TS 13298 standardına göre gerçekleştirilmesi, ayrıca üretmiş oldukları e-belgenin kurumlar arası paylaşımını www.devletarsivleri.gov.tr adresinde belirlenen kurumlar arası elektronik belge paylaşım hizmeti kriterlerine göre gerçekleştirilmesi gerekliliği belirtilmiştir. Bu kapsamda tüm kamu kurum ve kuruluşlarının 2 yıl içinde standarda uyumlu hale getirilmesi istenmiştir.

Takip eden yıllarda ise kamu kurumlarının büyük bir kısmı standarda uygun yazılım ürünlerini kullanmaya başlamıştır. Geliştirici firmalar arasında rekabetin yüksek olduğu bir piyasa oluşmuş olup, Ekim 2015'te hayata geçirilen TS 13298:2015 ve Şubat 2016 tarihinde eklenen T1 tadilatı ile standardın E-Arşiv, Kayıtlı Elektronik Posta ve E-Yazışma Paketi gibi yeni eklenen teknolojilerle zenginleştirilmesi sağlanmıştır. Aynı zamanda yapılan bu yeniliklerle Kurum Yeterlilik Sertifikasyonu tanımı standartta oluşturulmuş ve sadece geliştirici firma ile kurumların değil, aynı zamanda Elektronik Belge Yönetim Sistemi (EBYS) yazılımlarını kullanan kamu kurumlarının da standarda uygun kullanımının belgelendirilmesi gerçekleştirilmektedir.

Bir dönem belgelendirilmiş firma sayısı 38'e kadar çıkmış olup, Ocak 2017 itibarıyla 34 yazılım geliştirici firma ve kurum TS 13298 ürün belgelendirmesinden sertifika sahibidir. 1 adet belediye de TS 13298 Kurum Yeterlilik Sertifikasyonu almıştır. Bütün bu süreçte, standardın tanınırlığı ve yaygınlığı geniş kitlelere ulaşacak şekilde artmıştır.

Standart kapsamındaki ürün belgelendirmesi; TSE Bilişim Teknolojileri Test ve Belgelendirme Daire Başkanlığı tarafından standarda uygunluk denetimi ve denetimin takibinde ilgili yazılım ürününün fonksiyonel yeterlilikleri, performans testi (işlem hızları) ve siber güvenlik özellikleri açısından test edilmesi vasıtasıyla gerçekleştirilmektedir. Standardın gereklerini sağlayan ve belgelendirilen yazılım ürünlerinin kullanımı, kamu kurum ve kuruluşlarının gerçekleştirdiği tüm faaliyetlerinde şu faydaları sağlamaktadır:

- Nitelikli ve sürdürülebilir kurumsal hafızanın tesis edilmesi
- Bilgiye erişimin kolay ve şeffaf hale getirilmesi
- EBYS'nin güvenlik ve arşivleme ile ilgili kötü ve niteliksiz kullanımının, bilgi manipülasyonunun ve belge sahteciliğinin önüne geçilmesi
- Merkezi sistemlerle entegrasyon (Kurumlar ve farklı yazılımlar arası belge paylaşımı, E-Devlet, Kaysis vb.)
- E-arşiv yapısının büyük veri analitiği açısından kullanılabilir hale gelmesi
- Faaliyetlerin kanıtı, tarihsel gelişimin kaynağı olan belgeler için standart bir kalite yakalanabilmesi
- Kamuda standart bir yapı oluşturulmasına katkı sağlanması
- Yöneticilerde -Long Term Thinking- uzun vadeli düşünebilme vizyonuna katkı sağlanması

Modern teknolojinin gerekleri açısından TS 13298 standardı, 2015 revizyonu ile EBYS yazılımlarının güvenlik testlerinin yapılmasını da artık zorunlu tutmaktadır. Güncel Türkiye ve Dünya basınında siber güvenliğin ne kadar önemli olduğuna ve güvenlik önlemlerinin ihmal edilmesinin ne gibi sıkıntılara yol açtığına dair günlük bazda sansasyonel haberlerle karşılaşılmaktadır. TS 13298 ile belgelendirilecek yazılım ürünlerinin, siber güvenlik kapsamından daha kaliteli bir duruş sergilemesini sağlamak açısından TSE, bu eklemenin mecburi olduğuna hükmederek 2015 revizyonunda güvenlik kriter ve gereksinimlerini tanımlamıştır. Bu kapsamda, belgelendirilecek yazılım ürünlerinin TS ISO/IEC 15408 Ortak Kriterler (Common Criteria) standardından en az EAL 2 güvenlik seviyesinde ya da TSEK 505 Temel Seviye Güvenlik Belgelendirmesinden yeterlilik sağlaması gerekmektedir.

TSE'ye bilgi ve belge yönetimi konusunda uzun süredir destek veren Marmara Üniversitesi Fen-Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü'nde, bir dönem Bölüm Başkanlığı da yapmış olan Prof. Dr. Hamza Kandur, TS 13298 standardına yapılmış olan 2015 revizyonu ile güncellenmesi nedeni ile ilgili olarak aşağıdaki görüşlerini bildirmişlerdir:

"2015 yılındaki güncelleme ihtiyacının altında yatan faktörler özetlenecek olursa; TS 13298:2009 elektronik belgelerin üretilmesi ve yönetilmesini içeriyordu. Elektronik belgelerin arşivlenmesi ile ilgili temel gereksinimler tanımlanmamış, standardın yaygınlaşması ve anlaşılması beklenmişti. 2015'teki en önemli yenilik, elektronik arşiv ile ilgili maddeler olmuştur. Bu, bir anlamda sistem içerisinde üretilen e-imzalı belgelerin bir bütün içinde ve ispat gücünü de muhafaza ederek uzun süreler korunabilmesi gereksinimini karşılamaya yönelik bütünleyici bir ekleme olmuştur. Çok köklü bir arşiv geleneğine sahip olan Türkiye, bu anlayışı hangi ortamda belge üretimi yapıldığı önemli olmaksızın devam ettirmek ve gelecek kuşakların tarih konusunda birincil kaynaklar elde etmesini sağlayacak tedbirleri almakla mükelleftir.

E-arşiv ile ilgili eklenen bölümler, sadece organik olarak oluşan arşiv malzemesinin korunması ve yönetilmesine yönelik değil, aynı zamanda derleme arşiv malzemesinin de korunması ve yönetilmesine yönelik olanakları beraberinde sunmaktadır. Yani kurum ve kuruluşlar belge, doküman, görüntü, ses vb. türdeki materyallerini tek bir sistem üzerinden yönetebilecek ve erişebileceklerdir. Bu bütünleşik yapının sağlamış olduğu avantajlar hem arşiv boyutu ile hem de sosyal boyutu ile değerlendirilmelidir. TS 13298:2015 aynı zamanda sistem içerisinde üretilen belgelerin sistemler arasında paylaşımını mümkün kılan gelişmelere de ayak uyduracak şekilde revize edilmiştir. Bu anlamda e-posta yönetimi ve dijital görüntüleme sistemleri bölümleri güncellenmiştir. E-yazışma ve KEP gibi kamuda iletişimi artıracak önemli projeler ve bu projelerin EBYS ile olan bağıntıları bölümler halinde izah edilmiş ve belgenin üretiminden nihai tasfiyesine kadar olan süreç bir bütün olarak tanımlanmış

ve bununla ilgili kurallar, çerçeveler oluşturulmuştur. Ayrıca 2 Şubat 2015 tarihinde güncellenen Resmi Yazışmalar Hakkında Uygulanacak Usul ve Esaslar Yönetmeliği ile eş güdümlü hale getirilmiştir.

TS 13298:2015, aynı zamanda standarttaki maddeleri sağlama yükümlülüğünün kimlerin sorumluluğunda olduğuna dair bazı belirteçler içermektedir. Bazı maddeler, hatta bölümler seçmeli hale getirilmiş; bazı maddeler sadece üretici sertifikasyonu için zorunlu hale getirilirken, bazı maddeler de kamu kurumları için zorunlu hale gelmiştir."

Prof. Dr. Hamza Kandur, aynı zamanda kamu kurum ve kuruluşlarının EBYS'ye yaklaşımını aşağıdaki şekilde yorumlamıştır:

"Kamu kurum ve kuruluşları nitelikli ve sürdürülebilir bir yapının kurulmasında önemli bir yere sahiptirler. Bu nedenle lisanslı bir ürünü alıp kendi iş ve fonksiyonlarına göre uyarlama ve uygulama sürecinde standardın ruhunu yansıtacak bazı unsurları göz ardı etmemeleri gerekmektedir. Yapılan gözlemlerde kamu kurum ve kuruluşlarının EBYS ile ilgili yapılandırma süreçlerinde alışkanlıkları gereği, standart dışı bazı uygulamaları, üretici firmalardan istedikleri gözlemlenmiştir. Gerek EBYS sürecinin yapılandırılmasında gerek kamuda EBYS'ler açısından birlikteliğin sağlanmasında kamu kurum ve kuruluşlarının da TS 13298:2015 kapsamında akredite olmaları oldukça önemli hale gelmiştir."

TSE'nin yapmış olduğu TS 13298 belgelendirme faaliyetleri ilk başladığında inceleme metodunun tanımlanmasında belirleyici rol oynayan Marmara Üniversitesi Fen-Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü Öğr. Gör. Dr. Bahattin Yalçınkaya'ya, TSE'nin konu ile ilgili sahip olması ge-reken ideal yaklaşımı ve incelemelerin Bilgi ve Belge Yönetimi biliminin esaslarına uygunluğuna dair görüş sorulduğunda kendisinden aşağıdaki şekilde yanıt alınmıştır:

"Türk Standardları Enstitüsü belgelendirme ile ilgili ürün incelemelerinde nicel analiz başlığı altında bulunan unsurları incelemektedir. İncelemeler ve testler sonunda yeterli görülen yazılımlar Bilişim Teknolojileri Belgelendirme Komitesi kararı ile lisanslamaya tabi tutulmaktadır. TS 13298 standardında yapılan incelemelerde, konunun hassasiyetinden dolayı genellikle bir yazılım uzmanı ve bir belge yönetimi uzmanının beraber tetkik gerçekleştirmesi ideal olmaktadır.

Nicel Analiz

- Sistem Kriterleri
- Belge Kriterleri
- E-Arşiv Kriterleri
- Güvenlik Profili
- Üstveri (Metadata)

Kamu kurum ve kuruluşlarında, nicel analiz kısmında bulunan bazı maddeler incelemeye konu olmakla beraber, nitel analiz kısmında yer alan unsurlar kapsamlı bir şekilde incelenmekte, şartları sağlayan kurum ve kuruluşlara kalite yönetiminin bir unsuru olarak Kamu Yeterlilik Sertifikası verilmektedir.

Nitel Analiz

- Kullanım kolaylığının incelenmesi
- İşlem – süreç analizi ve belge form yapılarının yeterliliği
- Ölçümleme standart bir değerin bulunmadığı konuların rapor edilmesi (arşiv politikası vb. gibi)
- Dijitalleştirme projelerinin değerlendirilmesi"

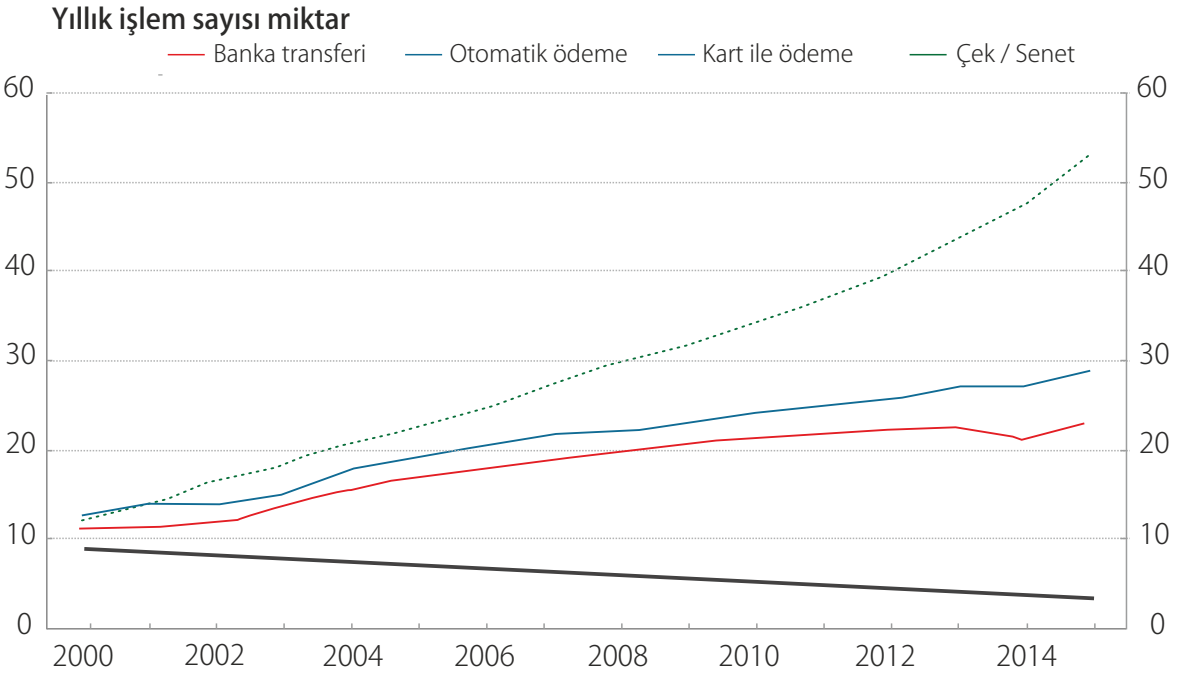
Yorumları ve katkıları için Marmara Üniversitesi Fen-Edebiyat Fakültesi Bilgi ve Belge Yönetimi Bölümü'nün değerli akademisyenleri Prof. Dr. Hamza Kandur ve Öğr. Gör. Dr. Bahattin Yalçınkaya'ya teşekkür ederim.

Sistem içerisinde üretilen e-imzalı belgelerin bir bütün içinde ve ispat gücünü de muhafaza ederek uzun süreler korunabilmesi gereksinimini karşılamaya yönelik bütünleyici bir ekleme olmuştur.

Banka/Kredi Kartları ve Güvenlik Önlemleri

İbrahim Halil Kırmızı ▶ TSE Siber Güvenlik Belgelendirme Müdürlüğü

Ticaretin ilk yapıldığı günden bugüne alışverişin nasıl olacağı, mal veya hizmet karşılığının ne olduğu sürekli gelişen bir sistem olmuştur. Bu süreçte paranın icat edilmesi, insanoğlunun en büyük adımlarından biri kabul edilir. Tarih boyunca bu konudaki ilerlemeler sürekli devam etmiştir. Paranın icat edilmesiyle tuz, deri gibi mallarla yapılan alışveriş yerini altın, gümüş gibi değerli madenlerden üretilen paralara bırakmıştır. İlk kez 1661 yılında İsveç'te basılan kâğıt para, otorite bir kuruluş tarafından onaylıdır ve günümüzde kullandığımız banknotun temelini oluşturmaktadır. 1946 yılında günümüz anlamında ilk kredi kartının hayatımıza girmesiyle alışveriş işlemleri başka bir boyut kazanmış, zamanla mobil ödeme sistemleri, son zamanlarda ise "Cryptocurrency" denilen ve şifrelemeye dayanan para birimleri hayatımıza girmiştir. Avrupa Birliği tarafından yayınlanan rapor incelendiğinde kart ile yapılan ödemelerin diğer ödemelere oranla hızla arttığı görülmektedir.



Neden Güvenlik

Günümüzde yaygın olarak çipli kartlar ve manyetik şeritli kartlar kullanılmaktadır. Her iki kart tipi de read-only (yazma korumalı) olmasına rağmen, manyetik şeritli kartların kopyalanmasının daha kolay olması, yerini zamanla çipli karta bırakmasına sebep olmuştur. Yine de kart teknolojisinin gelişimi, kötü niyetli kişilerin geliştirdiği ataklardan daha hızlı olmadığı için zaman içerisinde çevresel bileşenler üze-rinde geliştirmeler yapılmıştır. Ödeme Kaydedici Cihazlar ile ilgili regülasyonlar bunların başında gelmektedir. Ayrıca 1990'lı yıllardan beri kullanılan SMS doğrulaması bir güvenlik katmanı oluşturmaktadır. İnternet bankacılığının yaygınlaşması ile birlikte internet bankacılığı için kullanılan 'internet bankacılığı şifresi', 'mobil imza' gibi başka önlemler alınmıştır. Kötü niyetli kişiler ise, bu sistemdeki en zayıf halka olan 'insan faktörü' üzerinden giderek saldırı tipleri geliştirmişlerdir. Sosyal mühendislik ya da telefon dolandırıcılığı yoluyla bankacılık bilgilerinin ele geçirilmesi, ATM cihazlarına yerleştirilen maliyeti düşük sistemler ile kart ve parola bilgilerinin çalınması bu saldırı tiplerinden en önde gelenleridir. Kart bilgilerini çalan saldırganlar, kişiyi dolandırmakla kalmayıp bu bilgileri internet forumlarında birkaç dolar gibi fiyatlara satmaktadırlar. Kötü niyetli kişilerin geliştirdiği tüm bu saldırılara rağmen çipli kartlar için de birçok önlem alınmıştır.

Donanımsal Önlemler

- Çip devresi üzerinde aktif koruma kalkanı bulunmaktadır. Kartlar, bu devreyi bozacak herhangi bir donanım ya da lazer gibi dış etkeni tespit edebilmektedir.
- Kartlar, kriptografik işlemler ve diğer bazı işlemleri yaparken donanımsal olarak akıllı kart devresinde bulunan Rasgele Sayı Üreteçlerini kullanmaktadırlar. Ortak Kriterler sertifikasyon süreçlerinde, üreticilerin iddiası doğrultusunda kullanılan algoritmaların rastgeleliğini ölçen test paketleri (Test Suite) uygulanmaktadır.
- Kartlar, işlem saat hızının artırılması (over-clocking) ve azaltılmasını (under-clocking) tespit edebilir niteliktedir.
- Kartların çalıştığı voltaj aralıkları (2.3V - 6.3V) dışındaki bir seviyede oluşan gerilim, kartlar tarafından tespit edilebilmektedir.
- Kartlar, donanımsal olarak yapılan araya girme (Glitch, Spike) ataklarını tespit edebilmektedir.

▪ Kartlar, çok düşük ya da çok yüksek sıcaklıklarda yapılan atakları tespit edebilmektedir.

▪ Kartların arka yüzündeki CVV numarası; kart numarası, geçerlilik tarihi ve sadece kartı sağlayan kuruluş tarafından bilinen bir anahtarın parametre olduğu belirli bir algoritma yoluyla (ve 3DES kullanılarak) elde edilmektedir. CVV değeri, deterministik değildir.

Yazılımsal Önlemler

▪ Kartın ve üzerinde koşan işletim sisteminin belirli geliştirme aşamalarında dizayn karmaşıklaştırılmaktadır (Obfuscation).

▪ RSA-2048, ECC, ECDH gibi kaliteli ve nitelikleri FIPS 186-3, IEEE-P1363 gibi standartlarla belirlenmiş kriptografik algoritmalar kullanılmaktadır.

▪ Yazılımlar, Sonlu Durum Makinaleri şeklinde tasarlanmıştır; yani belirli bir komut zinciri vardır ve her durum için işlem sırası bellidir.

▪ Hem çevrimiçi hem de çevrimdışı sistemlerde kartlara uygulanacak kimlik doğrulama mekanizmaları EMV topluluğu tarafından geliştirilmiş ve standardize edilmiştir.

Ulusal ve Uluslararası Düzenlemeler

2007 yılında Resmi Gazete'de yayımlanan Banka Kartları ve Kredi Kartları Hakkında Yönetmeliğe göre POS cihazları asgari olarak PCI tarafından yayınlanan POS PIN Giriş Cihazı Güvenlik Gereksinimleri standardının gereklerini sağlamak zorundadır. Yine aynı Yönetmeliğe göre POS cihazının bankanın kendi sistemiyle iletişiminde PCI tarafından yayınlanan Veri Güvenliği Standardının şifrelemeyle ilgili gerekleri karşılanmak zorundadır.

Bankacılık Düzenleme ve Denetleme Kurulu (BDDK) tarafından 2009 yılında yayımlanan Genelge'de ATM güvenliği ile ilgili olarak şu ifade yer almaktadır: "Müşterilere uygulanan kimlik doğrulama mekanizması birbirinden bağımsız en az iki bileşenden oluşur. Bu iki bileşen; müşterinin 'bildiği', müşterinin 'sahip olduğu' veya müşterinin 'biyometrik bir karakteristiği olan' unsur sınıflarından farklı ikisine ait olmak üzere seçilir. Müşterinin 'bildiği' unsur olarak PIN bilgisi gibi bileşenler, 'sahip olduğu' unsur olarak ATM kartı gibi bileşenler kullanılabilir. Bileşenler tamamen müşterinin şahsına özgü olmalı ve bunlar sunulmadan kimlik doğrulama gerçekleştirilememeli, hizmetlere erişim sağlanamamalıdır."

Gelir İdaresi Başkanlığı (GİB), yayımlanan tebliğlerle özellikle son yıllarda banka kartı veya kredi kartı kullanarak yaptığımız alışverişlerde önemli bir yer tutan Yeni Nesil Ödeme Kaydedici Cihazlarda güvenlik ile ilgili kuralları belirlemiştir. 2012 yılında Resmi Gazete'de yayımlanan Tebliğ'de bu cihazlarda yayında olan Ortak Kriterler Koruma Profili'ne uyum aranacağı belirtilmiştir. Ayrıca hem Yeni Nesil Ödeme Kaydedici Cihazlar hem de bu cihazlar ile GİB arasındaki ilişkiyi yöneten TSM (Trusted Service Manager) Merkezleri için Teknik Kılavuzlar yayımlanmıştır. Konuyla ilgili olarak Ödeme Kaydedici Cihazların harici donanım ve yazılımlar ile iletişiminin güvenliğinin tanımlandığı bir Mesajlaşma Protokolü (GMP) de oluşturulmuştur.

Ayrıca yine GİB tarafından akaryakıt pompalarında kullanılacak Yeni Nesil Ödeme Kaydedici Cihazlar için de Koruma Profili hazırlanmaktadır.

Geçtiğimiz Ekim ayında (2016), EMV tarafından 3D Secure v2.0 standardının tanıtımı yapılmıştır. Bu standart ile internet alışverişlerinde hâlihazırda kullanılan 3D Secure v1.0 standardının bazı eksiklikleri giderilmiştir. Yeni standarda göre artık 3D Secure sadece web tarayıcı tabanlı değil, uygulama içi satın almaları da destekleyecektir. Aynı zamanda alışveriş yapılan web sitesinin de banka ve müşteri ile haberleşirken alması gereken önlemler artırılmıştır. Bu standardın da yakın zamanda Mastercard, Visa gibi kuruluşlar aracılığıyla hayatımıza gireceği beklenmektedir.

Kartlara Yapılabilecek Saldırılar

▪ Koruma Kalkanı Saldırıları: Yukarıda sıralanan güvenlik önlemlerine karşın, saldırganlar da atak türleri geliştirmektedirler. Birkaç bin doları geçmeyecek donanımlar kullanılarak koruma kalkanları aşılabilmektedir. Fakat daha profesyonel saldırılar yapmanın bedeli zamanla artmaktadır. Değeri 1 milyon doların üzerinde olan FIB (Focused Ion Beam) cihazı ile çipler analiz edilebilmektedir. Bu cihazlar genellikle Ortak Kriterler Değerlendirme Laboratuvarları ve çip üreticileri tarafından kullanılmaktadır.

▪ Hata Saldırıları: Kartın işleyişinde hata meydana getirerek mantıksal işleyişinde olmayan bir duruma getirmeye yönelik saldırılardır. Bu saldırı yöntemine önlem olarak kartlar ve kart işletim sistemleri Sonlu Durum Makinaları şeklinde tasarlanmaktadır.

▪ Yan-Kanal Saldırıları: Güç tüketimi, elektromanyetik sızıntılar ya da zamanlama bilgisi üzerinden karta yapılabilecek ve kriptografik anahtar, PIN bilgisi gibi bilgilerin elde edilmeye çalışıldığı saldırılardır.

▪ Donanım Saldırıları: Donanımsal olarak araya girme yoluyla yapılan saldırılardır.

Tüketici Olarak Alabileceğimiz Önlemler

▪ Kartı teslim alır almaz arka taraftaki imza panelini imzalamamız gereklidir. Bu önlem, imza ile yapılan alışverişlerde tüketiciyi korumak için geliştirilmiştir.

▪ Kart PIN numarası, internet bankacılığı şifresi gibi bilgileri bir yerde yazılı halde tutmamalıyız.

▪ Kolayca tahmin edilebilecek doğum tarihi gibi sayıları PIN olarak kullanmamalıyız.

▪ Kart bilgilerini; Whatsapp, e-posta ya da telefon yoluyla herhangi biriyle paylaşmamalıyız. Cep telefonumuzda ya da bilgisayarımızda bulunan bir zararlı yazılım, bu bilgilere erişiyor olabilir.

▪ İnternet bankacılığı işlemi gerçekleştirdiğimiz bilgisayarlarda mutlaka çalışır durumda bir antivirüs yazılımı olmasına dikkat etmeli ve işletim sisteminin güncelliğinden emin olmalıyız.

▪ İnternet bankacılığı kullanırken web sitesi adres satırına dikkat etmeliyiz.

▪ İnternet bankacılığı kullandığımız web tarayıcının güncelliğinden emin olmalıyız.

▪ İnternet bankacılığı kullanırken güvenilir web sitelerini tercih etmeliyiz.

▪ Sanal kredi kartı ile alışveriş yaparken kısa süre geçerli limitler belirlemeliyiz.

▪ E-posta yoluyla gelen ve bankacılık log-in sayfasına yönlendiren ya da kart bilgilerini talep eden herhangi bir linke güvenmemeliyiz. Oltalama saldırıları en çok bu yolla gerçekleşmektedir.

▪ İnternet bankacılığı kullandıktan sonra mutlaka log-out olarak çıkış yapmalıyız.

▪ ATM makinalerini kullanırken tuş takımı, kart giriş ünitesi ya da kamera gibi çevresel bileşenlerde şüpheli bir durum hissedersek işlem yapmamalıyız.

▪ Dokunmatik ekranlı ATM makinelerini kullanırken şüpheli bir durum hissedersek ATM önünden ayrılmadan telefonla bankaya ulaşmalıyız. Dokunmatik ekranlara kimyasal dökme yoluyla müşterinin erişiminin engellendiği saldırı tipleri olduğu bilinmektedir.

▪ Özellikle POS cihazları ile alışveriş yaparken tuşlara tıkladıktan sonra elimizi bir miktar daha tuş takımı üzerinde ya da rasgele bir sayı üzerinde bekletmeliyiz. Cep telefonlarına takılan termal kamera aparatları kullanılarak kart şifrelerinin ele geçirildiği saldırı tipleri olduğu bilinmektedir.

▪ Otobüs, metro gibi yerlerde olabilecek ataklara karşı Temassız (NFC) özelliği olan kartlarda işlem limitimizi en düşük seviyeye çekmeliyiz.

Her geçen gün yeni bir saldırı vektörünün üretildiği günümüzde, almamız gereken önlemler de her geçen gün artmakta ve çeşitlenmektedir. Hızlı yaşam koşullarında mümkün olduğunca temkinli ve bilinçli birer tüketici olmak ve çevremizdeki kişileri uyarmak, bu tarz suçların gerçekleşmesi ihtimalini en aza indirmek için önem taşımaktadır.

KAYNAKÇA

- http://www.telegraph.co.uk/finance/businessclub/money/11174013/The-history-of-money-from-barter-to-bitcoin.html
- http://www.ecb.europa.eu/press/pdf/pis/pis2015.pdf
- http://www.commoncriteriaportal.org/files/ppfiles/pp0035b.pdf
- http://www.bddk.org.tr/WebSitesi/turkce/Mevzuat/Bankacilik_Kanununa_Iliskin_Duzenlemeler/94956001atm_lere_iliskin_genelge_05022009.pdf
- http://www.gib.gov.tr/node/103997 http://www.gib.gov.tr/sites/-default/files/fileadmin/duyurular/YN_OKC_-GMP3.pdf

Nesnelerin İnterneti (IoT) ve Siber Güvenlik

Sezen Selin SÖZEN
TSE Bilişim Teknolojileri Test Müdürlüğü

Bugünlerde sıkça duyduğumuz ve ileride daha fazla duyacağımız bir kavram olan 'Nesnelerin İnterneti (IoT)', ilk olarak 1999 yılında Kevin Ashton tarafından kullanılmıştır. Bu kavram gelişen teknoloji ile birlikte, ortaya çıktığı günkü halinden daha geniş bir kitleye ulaştı. Nesnelerin İnterneti, "nesnelerin kendi aralarında oluşturduğu bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbirleriyle haberleşmeleri" olarak tanımlanmaktadır. Ayrıca; çeşitli iletişim protokolleri sayesinde birbirleri ile iletişim kuran ve birbirine bağlanarak, bilgi paylaşarak akıllı bir ağ oluşturmuş cihazlar sistemi olarak da tanımlamak mümkündür.

1991 yılında Cambridge Üniversitesi'ndeki akademisyenlerin kahve makinasını görebilmek için kurduğu kameralı sistem çevrimiçi ve gerçek zamanlı olması sebebiyle Nesnelerin İnterneti ve bağlı nesnelerin varlığının ilk örneğini oluşturmuştur. 2001 yılına kadar kullanılan sistem, kahve makinasının görüntüsünü dakikada üç kez bilgisayar ekranlarına gönderiyordu. 1999 yılında Kevin Ashton, yaptığı sunumda RFID teknolojisi uygulamasının firmaya faydalarını sıralayarak kullanılmasını önerdi. Bu sistem radyo dalgaları ve sensörlere dayalı bir sistemdi.

Nesnelerin İnterneti uygulamaları, sensörlerin tek tek erişilebilir olmasından başka, pek çok sensörün verisinin birleştirilerek değer üretilmesi amacıyla da kullanılmaktadır. Fiziksel ortamlardan gelen yüksek miktardaki sensör verilerinin, yapılan değerlendirmelerin ardından bilgi olarak operatörlere veya ilgili kişilere iletilmesi ya da verinin sistemler yardımıyla işlenerek bir faaliyet icra edilmesi sağlanmaktadır. Bu açıdan bakıldığında Nesnelerin İnternetinin 'Büyük Veri' kavramları ve uygulamaları ile iç içe olduğu görülmektedir. 'Nesne' kavramı, çok geniş bir cihaz yelpazesini ifade etmektedir. Bunların içinde kalp izleme cihazları, çiftlik hayvanları üzerindeki çipler, araba bilgisayarları, ev aletleri, akıllı termostatlar, izleme sistemleri, yangın erken uyarı sistemleri gibi aklınıza gelecek veya gelmeyecek yüzlerce değişik cihaz bulunmaktadır. Bilgi teknolojileri standartlarıyla ilgili çalışmalar yapan 1. Ortak Teknik Komite'ye bağlı Özel Çalışma Grubu 5 IoT hakkında çalışmalar gerçekleştirmiştir. Yapılan çalışmalar JTC 1 tarafından 'Nesnelerin İnterneti Ön Raporu' halinde yayınlanmıştır.

Nesnelerin İnterneti, "nesnelerin kendi aralarında oluşturduğu bir ağ ve bu ağdaki nesnelerin belirli bir protokol ile birbirleriyle haberleşmeleri" olarak tanımlanmaktadır.

Nesnelerin İnterneti kavramının altyapısı:

- Sensör Sistemi: Kullanılan sistemin dış dünya ile iletişimini sağlar. Isı, basınç, gaz, hareket vb. sensörler kullanılabilir.
- Veri Analizi: Sensörlerden alınan verilerin analiz edilerek bilgi olarak iletilmesi anlamına gelmektedir.
- Veri Toplama: Hangi sensörlerden nasıl veri toplanacağı, merkezi sunuculara nasıl veri iletileceği, veri iletişim protokolleri, karar mekanizmalarının planlanması faaliyetleri bu başlık altında gerçekleştirilmektedir.
- Veri İletişimi: En az enerjiyle en verimli iletişimi sağlayabilecek olan yapıların, sistemin gereksinimine göre belirlendiği bölümdür.
- Veri Gizliliği ve Güvenlik: Bu verilerin gerekli analizler yapıldıktan sonra kullanıcıya iletilirken yazılan algoritmalar yardımıyla şifrelenip sadece istenilen kullanıcıya gitmesinin sağlandığı bölümdür.

Nesnelerin İnterneti kavramının başlıca uygulama alanları:

▪ Çevre İzleme: Sensörler yardımı ile çevre koşullarının izlenmesidir. Su kirliliği, atmosferik olaylar, baraj doluluğu, orman yangını değerlendirilebilir ve ayrıca toplanan ilgili veriler yardımıyla deprem, tsunami erken uyarısı yapılabilir.

▪ Altyapı İzleme: Köprüler, açılır-kapanır köprüler (gemi yaklaştığında açılması gibi), demiryolu rayları, rüzgâr santralleri sürekli izlenerek, işletmeleri ile ilgili sorunlar ya da tehlikeli durumlar belirlenebilir.

▪ Endüstriyel Uygulamalar: Üretim tesislerinin ve üretim döngülerinin kontrolü yapılabilir. Bu durum yeni ürün üretme sürecini hızlandırabilir. Ulusal elektrik ağı ile bağlantı kurulup, üretimin enerjinin daha az talep gördüğü ya da daha ucuz olduğu saatlere kaydırılması sağlanabilir.

▪ Kamu Düzeni ve Güvenliği: Ani kalp durması gibi bir rahatsızlık geçiren birinin durumunda; birbirleri arasında çabucak bilgi transferi yapan cihazlar, acil durumlarda yardımcı olacaktır.

▪ Enerji Yönetimi: Elektronik cihazların internete bağlı olması, aynı zamanda uzaktan da kumanda edilebilmelerine olanak sağlayacaktır. İlerde evinizden uzaktayken internet üzerinden ısıtma/soğutma sisteminizi, fırınınızı ya da evin ışıklarını açıp kapayabilmek gibi olanaklarınız olacaktır.

▪ Medikal Servisler: Nesnelerin internetinin en önemli kullanım alanları, uzaktan izleme ve acil durum bildirme sistemleri olacak. Tansiyon, şeker, kalp ritmi, kalp pillerinin ya da gelişmiş işitme cihazlarının izlenmesi ile genel sağlık durumunu izlenebilmektedir. IoT, sağlık durumuna bağlı olarak önlem alma, görüntüleme ve teşhis koyma aşamasında çeşitli çözümler sunmaktadır. Cihazlar bireylerin kilo, gövde kitle, uyku düzeni ve günlük aktivite oranı gibi kendi sağlık durumlarını denetlemelerinde yardımcı olmaktadır.

▪ Ev ve Bina Otomasyonu: Ev otomasyonunda aydınlatma, ısıtma, soğutma, iletişim, eğlence ve güvenlik sistemlerini kontrol etmek mümkün olabilmektedir.

▪ Ulaşım ve Taşımacılık: Araçlar ile iletişim, akıllı trafik düzenlemeleri, akıllı otopark sistemleri, elektronik geşeler (OGS, HGS gibi), lojistik ve araç filosu yönetimi, yol yardımı gibi bir kısmını zaten kullandığımız, bir kısmını ise gelecekte daha yoğun kullanmaya başlayacağımız pek çok teknoloji bulunmaktadır. Sensörler yardımıyla yol üzerindeki araçları sayan, yolculuk süresini hesaplayan, çukurları tespit eden ve park yerlerinin kullanılma süresini hesaplayan akıllı ulaşım sistemleri kurulabilir.

Nesnelerin İnterneti hayatımıza girdikçe ve uygulama alanları arttıkça birçok problemi de beraberinde getirmektedir. Bunlardan belki de en önemlisi siber güvenlik alanında meydana gelebilecek problemlerdir. Siber güvenlik, internet çağının en büyük sorunlarından biri olarak kabul edilmektedir. İnternetin her geçen gün daha fazla yaygınlaşmasıyla daha da büyük bir sorun haline gelmeye devam ediyor. Günümüzde siber güvenlik, devletlerin ve büyük şirketlerin bile başını ağrıtabilecek kadar kritik bir öneme sahiptir. Federal Ticaret Komisyonu Nesnelerin İnternetini günlük kullanımımızda olan nesnelerin internete bağlanıp veri gönderip alması kabiliyeti olarak tanımlamış ve her gün kullandığımız cihazlara sensörler konulmasının ve bu cihazların bütün aktiviteleri kaydetmesinin büyük güvenlik risklerini ortaya çıkaracağını raporlamıştır.

IoT teknolojisi, bireylerin çevreleri ile ilişkilerini yeniden şekillendirmektedir. Bu gelişme ile kişiler, evler, araçlar ve kurumlar yüksek güvenlik riski ile karşı karşıya kalmaktadır. Akıllı binalarda ve cihazlarda kullanılan birçok teknolojinin çok düşük güvenlik önlemlerine sahip olması, söz konusu cihazların normal çalışmalarını sekteye uğratabilecek saldırılarla karşı karşıya gelmesine ve güvenlik sorunlarına neden olmaktadır. Şirketlere ya da kişilere ait verilerin çalınması/sızdırılması uygulamaların sekteye uğratılmasından daha ciddi bir sorun teşkil etmektedir. Bu duruma neden olan başlıca etkenler hızlı yazılım üretme eğilimi, kullanılmayan standartlar ve ucuz parça kullanımıdır. Bu zafiyet çözülmesi gereken önemli bir sorundur.

Tüm bu güvenlik zafiyetlerine rağmen Nesnelerin İnterneti kavramının gelişmesi desteklenmeli, gerekli önlemler alınarak birbiri ile bağlantılı nesnelerin iletişiminin kontrollü bir şekilde yönetilmesi ve bütünlüğün sağlanması için çalışmalar başlatılmalıdır. Kullanılacak güvenlik ve kontrol uygulamaları ile alınacak basit önlemler sayesinde cihazlar yönetilebilir, üretilen verinin toplanması ve depolanması sağlanabilir. Bu durumda, Nesnelerin İnterneti kavramının gelişmesi için güvenli bir ortam oluşturulabilir.

Bağlı cihazların sebep olduğu 3 temel risk

Sürekli her yerden bilgi toplama

Bilgilerin beklenmeyen şekilde kullanılması

Siber güvenlik

KAYNAKÇA

- http://www.karel.com.tr/blog/internet-things-nesnelerin-interneti-nedir-cihazlarin-etkilesim-trendleri
- http://www.karel.com.tr/blog/hacklenen-nesnelerin-interneti-internet-hacked-things-nedir http://www.karel.com.tr/blog/nesnelerin-interneti-iot-ve-sensor-uygulamalari
- //tr.wikipedia.org/w/index.php?title=Nesnelerin_%C4%B0nternet%27i&oldid=17722740 Kutup, N. Nesnelerin İnterneti; 4H Her yerden, Herkesle, Her zaman, Her nesne ile bağlantı.
- https://www.ftc.gov/system/files/documents-/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet
- https://www.isaca.org/Journal/archives/2015/Volume-2/Pages/internet-of-things-offers-great-opportunities-and-much-risk-turkish.aspx

Adli Bilişim
ve Standardizasyon

İnan Özkan ▶ TSE Bilişim Teknolojileri
Test Müdürlüğü

Bilişim araçlarının hayatımızda kapladığı alan artık insanlarla olan iletişimimizin neredeyse tümünü kapsamaya başladı. Tüm arkadaşlarımız sosyal medyada, telefon rehberimizde, mesajlaşma uygulamalarımızda, tüm yakınlarımızı onunla olan ilişkilerimizin yakınlığına göre kendi elimizle yine bu araçlar vasıtası ile etiketlenmiş şekilde hazır durumdadır. Elbette tüm bu yenilikler kendileri ile beraber hayatımıza yeni suç tipleri ve klasik suçların farklı şekillerde işlenme yöntemlerini de getirmiş bulunmaktadır. Tam bu noktada iletişim araçları üzerinde bıraktığımız her iz suç ve suçlunun tespitinde veya uyuşmazlıkların çözümünde önemli birer delil haline gelmiş durumdadır. Emniyet güçlerimiz, hukukçularımız ve özel laboratuvarlarımız bu alan ile ilgilenmiş ve bu alan ile ilgili uzmanlar yetiştirmek zorunda kalmışlardır. Elbette her bir birimimizin kendi oturmuş süreçleri ve alışkanlıkları mevcuttur. Ancak bu alışkanlıklarını ve süreçlerini ancak sorunlar ile yüzleştikleri vakalarda değiştirmek zorunda kalırlar. İşte bu değişikliği standardize ederek ortak bir tavır takınabilmek için adli bilişim alanında standardizasyon olmazsa olmaz bir konu olarak önümüze çıkmaktadır.

Bu tespitler sonrasında adli bilişimin tanımına bakacak olursak farklı yaklaşımlar bulmamız mümkündür. Örneğin adli bilişim, "elektronik ortamlardan elde edilen bulguların, bilişim teknik ve teknolojileri kullanılarak hukukî delillere dönüştürülme süreci" olarak tanımlanabilirken diğer yandan adli bilişimi, "elektronik ortamlarda muhafaza edilen veya bu ortamlarda tutulan, saklanan, işlenen, iletilen, silinen veya bulundurulan düz metin, ses, resim, görüntü gibi veri ve bilgilerin bir kısmı veya tamamının birleşiminden oluşan her türlü nesnenin, bir suç dolayısıyla, delil niteliği taşıyacak şekilde tanımlanması, elde edilmesi, saklanması, incelenmesi, ayrıştırılması, raporlanması ve mahkemeye sunulması çalışmalarıdır" şeklinde veya "adli olayların sayısal sistemler üzerinde incelenmesi ve delillendirilmesi süreçlerini kapsayan adli bilişim, bilişim hukuku alt alanına yardımcı bir disiplindir" şeklinde de tanımlamak mümkündür.

Adli bilişim alanındaki çalışmaların dünya genelinde ilk olarak 1970'li yıllarda başladığı bilinmektedir. Ülkemizde ise bu alanda hukukçuların ilgisi ilk olarak 1990'lı yıllarda görülebilir. 2000'li yıllarda da güvenlik güçlerinin bu konuda uzmanlaşmış birimler kurmaya başladıkları bilinmektedir. Ancak bu alandaki uzmanlaşma ve laboratuvar ekipmanının yüksek maliyet gerektirmesi nedeniyle örneğin Emniyet Genel Müdürlüğü'nde, İstanbul, Ankara ve İzmir'de Bilişim Suçları ve Sistem Şube Müdürlükleri tarafından yürütülürken diğer tüm illerimizde bilgisayar ve ağ sistemlerini işletmekle görevli Bilgi İşlem Bürolarınca takip edilmektedir. Bu tespit ile emniyet içerisinde yapılan çalışmaların genelinin mahiyetinin sadece bilgisayar gibi bilişim araçlarına el koymak ve bu araçların suç içeriği barındırıp barındırmadığının incelemesini sadece bilgisayarcı gözü ile yapmak olduğu açıktır. 1992 yılında da belirtildiği gibi "eğitim ve bilinçlenme yanında uzman – denetçi bilirkişi kadrosunun oluşması" günümüzün de sorunları arasında hala yerini korumaktadır. Örneğin 2015 yılında, özel bir firma olan ADEO tarafından kurulan Adli Bilişim Laboratuvarı hakkında çıkan haberlerin neredeyse tamamında "Türkiye'nin ilk özel adli bilişim laboratuvarı" olduğu vurgusu bulunmaktadır. Her ne kadar bu laboratuvardan daha önce de benzer girişimler yapılmış olsa dahi bu haber bile bizlere adli bilişim konusunda daha işin çok başında olduğumuzu göstermektedir. Henüz işin başında iken adli bilişim alanında yapılacak olan çalışmaları standartlar çerçevesinde geliştirmek, işe başlamak için en doğru adım olacaktır.

1. Adli Bilişimin Bileşenleri ve Standardizasyon

Adli bilişim temelde dört bileşen altında incelenebilir. Bunlar;

- Adli Bilişim Soruşturma Süreçleri
- Adli Bilişim Laboratuvarları
- Adli Bilişim Uzmanı
- Adli Bilişim Yazılımları

1.1. Adli Bilişim Soruşturma Süreçleri

Adli bilişimin tanımı, ülkemizde çok yeni bir alan olması ve hukuki boyutunun ardından yeniden adli makamlar tarafından işletilen adli bilişim süreçlerine bakacak olursak, bir zorunluluk veya mevzuatta bu

konu ile ilgili herhangi bir özel tanımlama olmadığı görülmektedir. Sıradışılığı açısından ve ceza hukuku açısından yeni olması nedeniyle oldukça tartışmalara yol açan adli bilişim soruşturma yöntemleri hakkındaki problemler, sistematik bir çalışma ve etkin yönetim metotları ile çözüme ulaştırılabilir.

Adli bilişim soruşturmasına denk gelebilecek olan güvenlik ihlali olayları ile ilgili standartlar şunlardır:

▪ ISO/IEC 27037:2012 Bilgi Teknolojisi – Güvenlik Teknikleri – Dijital Delilin Belirlenmesi, Toplanması, Elde Edilmesi ve Korunması

Standart, sayısal delillerin toplanması ile ilgili süreçleri anlatmakta ve rehber olarak kullanılabilmektedir. Standart içerisinde bölümler halinde tanımlamalar, sayısal delil elde etme süreci, sayısal delilin belirlenmesi, toplanması, edinimi ve korunmasının ana bileşenleri ile farklı sayısal delillere bu standardın uygulanması ile ilgili rehberlik sunmaktadır.

▪ ISO/IEC 27041 Bilgi Teknolojisi – Güvenlik Teknikleri – Olay Soruşturma Metotlarının Güvence Uygunluğu ve Yeterliliği Hakkında Rehber

Bu standart ile kurum içerisinde ya da laboratuvarlar tarafından oluşturulacak ya da benimsenecek olan ihlal olayı yönteminin uygunluğunu ve yeterliliğini nasıl sağlayacağımız hakkında bilgilendirme yapılmaktadır.

▪ ISO/IEC 27042 Bilgi Teknolojisi – Güvenlik Teknikleri – Dijital Delillerin Analizi ve Yorumlanması Hakkında Rehber

Standart genel olarak dijital delillerin devamlılık, geçerlilik, tekrar üretilebilirlik ve tekrar edebilirlik açısından analizi ve yorumlanması hakkında rehber niteliğindedir. Analitik proseslerin seçimi, tasarımı ve uygulanması konusunda pratik uygulamalar içerir ve soruşturma, statik analiz, imaj alınabilen ve kopyalanabilen sistemlerin canlı analizi, imaj alınamayan ve kopyalanamayan sistemlerin canlı analizi, yorumlama ve yorumlamayı etkileyen faktörler, raporlama ve tavsiye edilen rapor içeriği, yetkinlik ve yeterlilik konularını ele almaktadır.

▪ ISO/IEC 27043 Bilgi Teknolojisi – Güvenlik Teknikleri – Olay Soruşturma Prensipleri ve Süreçleri

Standart, dijital delilleri kapsayan çeşitli soruşturma senaryoları için olay soruşturma süreçleri hakkında rehber niteliğindedir. Standart önemli bir içerik sunmakta ve süreçler ile ISO standartları arasında ilişki kurmaktadır.

1.2. Adli Bilişim Laboratuvarları

Adli bilişim laboratuvarlarının akreditasyonu için kullanılabilecek olan akreditasyon standardı "TS EN ISO/IEC 17025 Deney ve Kalibrasyon Laboratuvarlarının Yeterliliği İçin Genel Şartlar" standardıdır. 17025 akreditasyonu numune alma, deney ve kalibrasyon kalitesini güvence altına almak için yürütülen bir faaliyettir. Standart ile hedeflenen kalifiye personelin doğru raporlama yapabilmesi, uygun fiziki mekanlarda uygun numunelerin teste tabi tutulabilmesi, izlenebilir ölçümler için uygun donanım kullanılabilmesi ve gözetim ve iyileştirme ile geçerli deney metotlarının kullanılabilmesi sonucunda kalite yönetiminin gerçekleştirilebilmesidir.

1.3. Adli Bilişim Uzmanlarının Belgelendirilmesi

Adli bilişim incelemesi gerektiren herhangi bir soruşturma içerisinde hangi niteliklere sahip bilirkişilerin bulunması gerektiği ile ilgili olarak herhangi bir zorlayıcı şart ortaya konulmamıştır. Ülkemizde bu yönde bir çalışma Türk Standardları Enstitüsü (TSE) tarafından Siber Güvenlik Özel Komiteleri altında kurulan Adli Bilişim Komitesi tarafından yapılmış, kriter numara almış ancak sektörden destek görememesi nedeniyle henüz yayımlanamamıştır. Kriter ile adli bilişim uzmanı eğitimleri, sınavları ve belgelendirmesi gerçekleştirilmesi hedeflenmiştir. Kriterin yayımlanması halinde alacağı isim TSE K 489 Adli Bilişim İncelemeleri Yapan Personel ve Firmalar İçin Şartlar olacaktır.

1.4. Adli Bilişim Yazılımlarının Belgelendirilmesi

Adli bilişim süreçlerinin akredite laboratuvarlar tarafından konusunda uzman belgelendirilmiş kişilerce takip edilmesinin önemi üzerinde durduk. Ancak gelinen son noktada adli bilişim incelemeleri için aslında uzmanlar tarafından yine bilişim araçları yani adli bilişim yazılımları kullanılmaktadır.

Kullanılan yazılımların verdiği sonuçlar vasıtası ile uzmanlar sonuca gitmekte, bir suç unsuru veya suçun delili olabilecek bir durumun varlığına veya yokluğuna karar vermektedirler.

Uzmanların kullandıkları yazılımların da belli standartlar çerçevesinde doğrulanabilmesi gerekmektedir. Zaten 17025 akreditasyonu içerisinde yaşanacak olan zorluklardan birisi de standardın içerisinde bulunan ölçüm araçlarının kalibrasyonunun yapılmasıdır. Adli bilişim laboratuvarlarına uyum açısından yazılımların belgelendirilmesi bu maddenin de doğrudan sağlanmasına fırsat sağlayacaktır. Böyle bir çalışma şu anda sadece ABD tarafından gerçekleştirilmektedir. National Institute of Standards and Technology (NIST) tarafından yürütülmekte olan "Computer Forensics Tool Testing Program" tam olarak bu işlemi gerçekleştirmektedir. ABD'de herhangi bir yazılım ya da donanımın adli bilişim makamlarında yasal olarak kullanılabilmesi için NIST tarafından kabul edilmesi gerekmektedir. Ülkemizde bu konuda bir yetkilendirme veya test makamı bulunmamaktadır. Ancak konu ile ilgili süreç standardı/kriteri yazılarak yetkili bir makam oluşturulmalı ve gerekli testler yapılmadan herhangi bir yazılım adli bilişim yazılımı olarak kullanılmamalıdır.

KAYNAKLAR

- Arslan, Çetin (2014), Hukuk Öğretiminde Adlî Bilişim
- http://fbe-infosec.gazi.edu.tr/posts/view/title/prof.-dr.-seref-sagiroglu'nun-biltekhaber%E2%80%99le-yaptigi-soylesi-128469 son erişim tarihi 24.01.2017
- Şengül, G., Atsan, F.K., Bostan, A. (2014), Adli Bilişim Alanındaki Mevcut Problemler, Çözüm Önerileri ve Gelecek Öngörüleri
- http://www.wavefrontcg.com/A_Brief_History_of_Cybercrime.html son erişim tarihi 24.01.2017
- Yücel, Mustafa (1992), Bilişim Suçları
- Çiçek, İ., OKATAN, A., Ülkemizde Adli Bilişim Laboratuvarı Kurulumu ve Bilişim Suçlarıyla Mücadeleye Katkıları
- http://www.milliyet.com.tr/turkiye-nin-ilk-ozel-adli-bilisim-teknoloji-2019229/ son erişim tarihi 24.01.2017
- Carrier, B., Spafford, E.(2003), Getting Physical with the Digital Investigation Process
- Kırmızı, İ.H.(2016), Dünyada Adli Bilişim Uzmanı Belgelendirme ve Türkiye'deki Çalışmalar
- Karataş, S. (2015), TS EN ISO/IEC 17025 Standardı ve EA 2/17 Revizyon Değişiklikleri
- http://www.telepati.com.tr/agustos12/konu8.htm son erişim tarihi 24.01.2017

BULUT BİLİŞİM
VE RİSKLERİ

Eda Bitlisli ▶ TSE Siber Güvenlik Belgelendirme Müdürlüğü

Günümüzde teknolojinin gelişmesiyle beraber bulut bilişim de gelişmekte ve tüm dünyada olduğu gibi Türkiye'de de bulut bilişime olan ilgi artmaktadır. Yüksek erişilebilirlik, platform bağımsızlık, donanım kaynaklı problemlerin bulunmaması ve düşük maliyet gibi sağladığı birçok avantajın yanı sıra bulut bilişim beraberinde bazı riskleri de barındırmaktadır.

Bulut Bilişim Nedir?

Bulut bilişim (cloud computing), bilgisayarlar ve diğer cihazlar için, istendiği zaman kullanılabilen ve kullanıcılar arasında paylaşılan bilgisayar kaynakları sağlayan, internet tabanlı bilişim hizmetlerinin genel adıdır [1].

Bulut Bilişim Servis Modelleri

Servis modeli kuruluşun kapsamını, bilişim ortamı üzerindeki kontrolünü ve kullanılan soyutlama seviyesini belirler. Bulut bilişim sağlayıcılarının en sık kullandıkları üç servis modeli şunlardır:

Altyapı Hizmeti (Infrastructure-as-a-Service)

Uygulamaların geliştirilip çalıştırılması için ihtiyaç duyulan sunucu, yazılım ve ağ ekipmanlarından oluşan temel bilişim altyapısının sağlandığı modeldir. Esas amacı temel yazılım ve donanımı satın alıp barındırmaktan kaçınıp, yerine bir hizmet arayüzü ile kontrol edebilmektir [3]. Bu modelde işletim sistemleri ve uygulama yazılımlarının onarımından, sürdürülmesinden ve güvenliğinden bulut hizmetini alan sorumludur.

Platform Hizmeti (Platform-as-a-Service)

Bu modelde uygulamaların geliştirilip yayınlanması için ihtiyaç duyulan programlama dili yürütme ortamı, veri tabanı sunucu ve işletim sistemini içeren platform temin edilmektedir. Platform hizmetinin en temel avantajı uygulama geliştiricileri gerekli donanım ve yazılım bileşenlerini satın alma ve barındırma zahmetinden kurtarıp maliyetleri düşürmektir. Güvenliğin bir bölümünden hizmet sağlayıcı, bir bölümünden ise müşteri sorumludur.

Yazılım Hizmeti (Software-as-a-Service)

İhtiyaç duyulan uygulamaların ve çalışmalarını sağlayacak kaynakların sağlandığı modelidir. Bulut altyapısını kontrol etmek, yönetmek ve güvenliğini sağlamak büyük oranda hizmet sağlayıcının sorumluluğundadır.

Bulut Bilişim Yayılma Modelleri

Yayılma modelleri, bilişim kaynaklarının yönetimi ve müşterilere tahsisi konularının yanı sıra müşteri sınıflarının ayrıştırılmasını da detaylıca tanımlar [3]. Yayılma modelleri, bilişim kaynaklarının yönetimi ve müşterilere tahsisi konularının yanı sıra müşteri sınıflarının ayrıştırılmasını da detaylıca tanımlar [3].

Genel Bulut (Public Cloud)

Genel bulut uygulamalarında depolama ve diğer kaynaklar bir hizmet sağlayıcı tarafından genel kullanıcılara sunulurlar. Bu hizmetler ücretsiz erişimlidir veya kullanım başına ödeme modeliyle ücretlendirilirler. Genel olarak Amazon AWS, Microsoft ve Google gibi genel bulut sağlayıcıları kendi altyapılarını işletir ve sadece internet aracılığıyla erişim sunarlar (doğrudan bağlantı sunulmaz) [1]. Verileriniz hizmet sağlayıcının veri merkezinde tutulduğundan yönetiminden ve bakımından ilgili sağlayıcı sorumludur.

Özel Bulut (Private Cloud)

Özel bulut birden çok tüketici içeren sadece tek bir organizasyon için işletilen bulut altyapısıdır; dâhilî olarak veya üçüncü parti tarafından yönetilebilir, işletilebilir ve yine dâhilî veya haricî olarak barındırılabilir [2]. Dinamik ve öngörülemez ihtiyaçları olan işlerde (yaşamsal yazılımlar, güvenlik alarmları) özel bulut avantajlı olmasına karşın doğal afet ve veri hırsızlığı gibi durumlarda güvenlik açıklıklarına meyilli olabilmektedir.

Hibrit Bulut (Hybrid Cloud)

Hibrit bulut iki veya daha fazla bulutun (özel, topluluk veya genel) birleşimidir. Bu farklı bulutlar müstakil olarak bulunmaktadır fakat birbirlerine bağlıdırlar, böylece çoklu yerleştirme modellerinin imkânlarını sunarlar [2]. Genellikle büyük ölçekli işletmelerde kullanılmaktadır.

Topluluk Bulut (Community Cloud)

Topluluk bulut ortak ilgi ve endişeleri (güvenlik ge-

reklilikleri, politika vb.) olan özel bir topluluktaki çeşitli organizasyonlar için sağlanan bulut altyapısıdır. Topluluk içindeki bir veya birden çok organizasyon tarafından işletilip yönetilebileceği gibi üçüncü taraflar tarafından da barındırılıp yönetilebilir. Topluluk bulutun amacı toplulukta bulunan organizasyonların genel bulutun çok kullanıcılı, kullandıkça öde yapısına ek olarak özel bulutun gizlilik, güvenlik avantajlarını sağlamasıdır.

Bulut Bilişim Riskleri

Sunduğu avantajların yanı sıra bulut bilişim beraberinde belirli riskleri de getirmektedir.

Veri Güvenliği ve Gizliliği

Bulut bilişim hizmetlerinde fiziksel kaynakların birçok kullanıcı tarafından ortak olarak kullanılıyor olması, veri gizliliği ve güvenliği açısından risk yaratabilmektedir. Bulut içindeki farklı kullanıcıların, ortak kaynaklar üzerindeki depolama, bellek alanlarını birbirinden ayırmaya yarayan iç mekanizmalarda ortaya çıkabilecek açıklık ve hatalar, yapılacak saldırılar sonucu kullanıcıların özel ve gizli verilerinin ele geçirilmesine sebebiyet verebilir. Ayrıca, bulut bilişimde kaynakların dinamik olarak ayrılıp bırakıldığı düşünüldüğünde, çoğu işletim sisteminde uygulandığı gibi, silinen verilerin fiziksel olarak silinmeyip sadece mantıksal seviyede silinmesi durumunda, bırakılan depolama kaynağının başka bir kullanıcıya tahsis edilmesi sonucu, bu fiziksel olarak silinmeyen verinin başka kullanıcılar tarafından ele geçirilmesi mümkün olabilmektedir [4]. Fakat veri gizliliğine zarar verecek bu saldırıların çoğu verilerin bulutta şifreli şekilde saklanması, sanal yerel ağ kullanımı ve ağ içi güvenlik duvarı kullanımı yöntemleri ile engellenebilir.

Hizmetin Devamlılığı

Bulut bilişim hizmet sağlayıcılarında meydana gelebilecek yazılımsal, donanımsal ya da dışardan gelecek saldırılardan kaynaklı hizmet kesintileri, bu sağlayıcıdan hizmet alan tüm kullanıcıları etkileyecektir. Hatta tüm altyapı ve hizmetleri bu sağlayıcıdan temin eden işletmelerde bu durum faaliyetlerin durmasıyla bile sonuçlanabilmektedir. Hazi-Haziran 2008'de Google AppEngine'de meydana gelen bir programlama hatasından dolayı 6 saat, Temmuz 2008'de ise Amazon S3'te tek bir bit hatasından kaynaklanan bir hatadan kaynaklanan 8 saatlik hizmet kesintileri yaşandı [4].

Bulut Bilişim hizmet sağlayıcılarında meydana gelebilecek hizmet kesintilerinin bir diğer sebebi de dışardan gelebilecek DDoS yani dağıtılmış hizmet dışı bırakma saldırılarıdır. Bu saldırı türünde birçok bilgisayar aynı anda aynı noktaya istek yönlendirilip, sunucuların bu isteklere cevap veremez hale getirilmesini sağlamaktadır. Böylelikle bulut bilişim hizmet sağlayıcıları hizmet veremez hale gelebilmektedir. Fakat günümüzde bulut bilişim sağlayıcıları bu tarz saldırılara karşı koruma mekanizmaları geliştirerek saldırının geldiği noktaları tespit edip önleme yönünde önlemler almaktadır.

Servis Sağlayıcı Bağımlılığı

Bir bulut bilişim servis sağlayıcısından diğerine geçiş yapmak istenmesi durumunda, bulut bilişim servis sağlayıcılarının yazılım programlama ara yüzlerini istenen seviyede standartlaştırmamış olmaları ve verilerin servis sağlayıcılara özel veri tabanı şemalarında tutulmaları gibi sebeplerle, veri ve yazılımların taşınmasında büyük zorluklarla karşılaşılmaktadır [4]. Ayrıca servis sağlayıcısının değiştirilmesi durumunda mevcut servis sağlayıcının bulundurduğu kullanıcı bilgilerini kullanması şüphesi de kullanıcıları servis sağlayıcılara bağımlı hale getiren sebeplerden bir diğeri.

Bant Genişliği ve Veri Transferi

Şirket verilerinin bulut hizmet sağlayıcısına aktarılması yoğun bir veri trafiği demektir. Bant genişliğinin sınırlı olması hem veri transfer süresini hem de maliyeti artırmaktadır. Bu durum bulut yoluyla hizmet alımı önündeki engellerden biridir. Bu engelin çözümü olarak veri disklerinin fiziksel olarak taşınması, uygulanan çözümlerden biridir.

Veri Kaybı

İnsani sebepler (iflas, dava vb.) veya ekipman kaynaklı (sistem çökmeleri, donanım arızası vb.) sorunlar veya tedbirsizlikler nedeniyle kalıcı veri kayıpları yaşanabilmektedir.

Yönetim Arayüzü ve Uzaktan Erişim

Bulut bilişim hizmet sağlayıcıların kullanıcılarının hizmetlerini yönettikleri ara yüzler, internet üzerinden erişilebilir olmaları ve geniş yönetim imkânları barındırmaları sebebiyle, internet tarayıcıların ve uzaktan erişimin zayıflıkları düşünüldüğünde, yüksek güvenlik riski taşımaktadırlar [4]. Saldırganlar tarafından gerçekleştirilen çeşitli saldırı yöntemleriyle (man-in-the-middle, sniffing vb.) verilerin dinlenmesi, kullanıcı oturumlarının elde edilmesi, şifrelerinin çalınması mümkün olabilmektedir.

Bulut Bilişim hizmet sağlayıcılar tarafından, bulut temelli güvenlik modeli oluşturularak bulut-içi ("in-the-cloud") tarama hizmetleri sayesinde bulut kullanıcılarının bulut içindeki saldırılara karşı korunması sağlanmaya çalışılmaktadır.

TSE'nin Bulut Bilişim Alanındaki Çalışmaları

7 Mart 2014 tarihinde Türk Standardları Enstitüsü (TSE) bünyesinde faaliyet gösteren 'Siber Güvenlik Özel Komitesi Bulut Bilişim Çalışma Grubu' tarafından hazırlanmış olan 'Bulut Bilişim Güvenlik ve Kullanım Standardı' taslağı yayınlanmıştır. Bu standardın amacı bulut ortamındaki riskleri ve koruma yöntemlerini belirterek bu teknolojilerin kullanımıyla ilgili karar vermek için gereken bilgi ve anlayışı sağlamaktır. Standart taslağı kamu ve özel sektörde ilgili kurumlara görüş almak için gönderilmiştir.

23 Kasım 2015 tarihinde de TSE ve TÜBİTAK BİLGEM işbirliği ile 'Bulut Bilişim Standartları Çalıştayı 2015' düzenlenmiştir. Çalıştaya ülkenin önde gelen bulut hizmeti sağlayan ve bulut hizmeti alan özel sektör, kamu, üniversite yetkilileri katılım sağlamışlardır. 2015 Bulut Bilişim Standartları Çalıştayı ile ülkemizde devam eden standardizasyon çalışmaları üzerine mevcut durum analizi gerçekleştirilmesi, katılımcı kurumların/kuruluşların bulut bilişim çalışma alanlarında yetkinlik tablolarının oluşturulması amaçlanmıştır.

Yasal Düzenlemeler

Kişisel verilerin işlenmesinde başta özel hayatın gizliliği olmak üzere kişilerin temel hak ve özgürlüklerini korumak ve kişisel verileri işleyen gerçek ve tüzel kişilerin yükümlülükleri ile uyacakları usul ve esasları düzenlemek amacıyla 6698 sayılı 'Kişisel Verilerin Korunması Kanunu' 7 Nisan 2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Bulut bilişim hizmet sağlayıcıları bulut içindeki kişisel verilerin korunmasında bu Kanun'daki hükümlülüklere uymakla mükelleftir.

Değerlendirme

Her teknolojinin olduğu gibi bulut bilişimin de avantajları ve riskleri vardır. Kuruluşlar bulut ortama geçiş kararı vermeden önce bulut ortama uygunluğu maliyet, kritiklik ve hassasiyet gibi kriterleri göz önüne alarak önceliklendirmeli ve bulut bilişimle ilgili kararları bu kriterlerin risk analizi sonucunda vermelidir. Ayrıca günümüzde 'Kişisel Verilerin Korunması Kanunu', 'Bulut Bilişim Güvenlik ve Kullanım Standardı' taslağı ve çalıştaylar benzeri birçok önemli çalışma olmasına karşın bu alandaki standardizasyon çalışmaları, denetim mekanizmaları ve yasal düzenlemeler henüz yeterli değildir.

Bulut bilişim hizmetlerinde fiziksel kaynakların birçok kullanıcı tarafından ortak olarak kullanılıyor olması, veri gizliliği ve güvenliği açısından risk yaratabilmektedir.

KAYNAKÇA

[1] Bulut Bilişim https://tr.wikipedia.org/wiki/Bulut_bili%C5%9Fim

[2] The NIST Definition of Cloud Computing http://faculty.-winthrop.edu/-domanm/csci411/Handouts/NIST.pdf

[3] "Bulut Bilişim Güvenlik ve Kullanım Standardı" Taslak

4] "Bulut Bilişim Risk Değerlendirmesi - I" https://www.bil-guvenligi.gov.tr/guvenlik-teknolojileri/bulut-bilisim-risk-degerlendirmesi-i.html

Sosyal Mühendislik

Omuz Sörfü

Ferhat Işık ▶ TSE Siber Güvenlik Belgelendirme Müdürlüğü

Omuz sörfü sosyal mühendislik yöntemlerinden biridir. Sosyal mühendisliği açıklamak gerekirse; insanlar arasındaki iletişimdeki ve insan davranışındaki açıklıkları tanıyıp, bunlardan faydalanarak güvenlik süreçlerini atlatma yöntemine dayanan müdahalelere verilen isimdir [1].

Omuz sörfü denildiğinde aklınıza ilk ne gelir? Kısa bir süre düşündüğümüzde omuz sörfü aslında aklımıza gelen şeyden çok da farklı değil. Omuz sörfünü araştırdığımızda tanımlarda, "Şifre yazılırken ya da erişim kısıtlı sistemlere erişilirken saldırıların izlenmesi" gibi açıklamalarla karşılaşmaktayız.

Peki, günlük hayatta omuz sörfüne nasıl maruz kalıyoruz?

1. İşyerinde illaki meraklı ya da kötü niyetli olarak omuz sörfü gerçekleştirmeye çalışan insanlar vardır. Bu kişiler; iş arkadaşlarımız, amir ve müdürlerimiz, işyerine dışarıdan gelen kişiler vb. olabilir.

2. Kafede otururken, restoranda yemek yerken, bankta arkadaşınızı beklerken, otobüste yolculuk ederken yanınızda oturan ya da arkanızdaki kişiler tarafından size omuz sörfü yapılabilir. Genellikle anlık mesajlaşmalarınızı okumaya çalışırlar, Facebook'ta incelediğiniz bildirilere, Twitter'dan okuduğunuz tweetlere göz atarlar.

İletişim bilgilerinizi, Facebook'taki adınızı, telefon numaranızı, mesajlaştığınız kişinin adını (acaba sevgilisiyle mi konuşuyor merakından dolayı) öğrenmeye çalışır. Ayrıca omuz sörfü ile kötü niyetli kişilerin elde edebileceği daha kritik bilgiler de olabilir.

3. Kredi kartı veya bankamatik kartı hırsızlığı öncesi kartın şifresini öğrenmek için denenen yöntemlerden biri de omuz sörfüdür. ATM'lere para çekmeye gittiğimizde ya da işlem yapmaya çalıştığımızda yanımızdaki ATM'de işlem yapmaya çalışan ya da arkamızda sıra bekleyen kişi tarafından omuz sörfüne maruz kalabiliriz. Bu kişiler bizim kart bilgilerimizin yanı sıra kart şifremizi, hesabımızdaki para miktarını ve diğer bilgilerimizi öğrenebilir.

ATM'lere para çekmeye gittiğimizde ya da işlem yapmaya çalıştığımızda yanımızdaki ATM'de işlem yapmaya çalışan ya da arkamızda sıra bekleyen kişi tarafından omuz sörfüne maruz kalabiliriz.

Omuz sörfüyle ilgili daha birçok örnek vardır. Peki, omuz sörfüne karşı ne gibi önlemler alabiliriz?

1. Sizden başka birinin ortamda bulunduğu durumlarda şifrenizi girmeyin. Zaruri durumlarda hızlı bir şekilde tuşlara basınız [2].

2. Yanınıza gelen kişiler olduğunda ve başkasının görmemesi ya da paylaşmamanız gereken şeyler olduğunda önlemler almanız gerekir. Eğer ekranı değiştirmeye zamanınız yok ise monitörü tamamen kapatabilir, masanızdaki evrakların ters yüzünü çevirebilir ya da nazikçe müsaade etmesini isteyebilirsiniz.

3. ATM'lerde işlem yapmak için gireceğiniz şifrenizi elinizle saklamaya çalışabilir ya da ATM'ye daha da yaklaşarak diğer kişilerin görüş açısını daraltabilirsiniz.

REFERANSLAR

[1]https://www.bilgiguvenligi.gov.tr/sosyal-muhendislik/sosyal-muhendislik-saldirilari-3.html

[2] Granger S., Social Engineering Fundamentals, Part I: Hacker Tactics, SecurityFocus In-focus, Article No: 1527. 2001.

Elektronik İmza

Cem Erdivan ▶ TSE Siber Güvenlik Belgelendirme Müdürlüğü

İmza genel olarak bir belgenin kişi tarafından yazıldığını veya okunduğunu böylece onaylandığını belirtmek için yapılan her türlü işarettir. İmza ile ıslak imza birbirinden farklıdır. İmza geniş anlamda kullanılır ve faks, e-posta, kağıt vs. atılan tüm imzaları kapsar. Islak imza ise kişinin elektronik iletişim araçları kullanmaksızın kendi eliyle attığı imzasıdır. Borçlar Kanunu'nun 13'üncü maddesi, "Tahriri olması icap eden akitlerden borç deruhte edenlerin imzaları bulunmak lazımdır" demekte, 14'üncü maddesi de 'imza'yı düzenlemektedir. Buna göre imza üzerinde borç alan kimsenin el yazısı olmak zorundadır. Hukuki bakımdan asıl olan kişinin kendi el yazısı ile atmış olduğu ve ıslak imza olarak da bilinen imzadır. Bu manada imza, yazılı bir irade açıklamasının kendisine ait olduğu ifade etmek amacıyla, bir kimsenin ismi için kullandığı özel biçimdeki çizi ve harflerden kurulu bir işarettir.

İlk olarak 1969 yılında ilk ağların kurulup bunun 1973 yılında bilim çevrelerine tanıtılması ile oluşan internet, veri iletim ağlarının en yaygın ve en geniş parçasıdır. Sanal alan ise, bilişim sistemleri ve bunları birbirine bağlayan her türlü veri iletim ağından ve sayısal verilerden oluşan bir ağdır. İletişim teknolojilerinin gelişmesi bilgi ve iletişim teknolojilerinin iş ilişkilerine de uygulanmaları ile elektronik ticaret ortaya çıkmıştır. Önceleri kapalı ağlar (closed networks) üzerinden yapılan elektronik ticaret, internet ile birlikte açık ağlar (open networks) üzerinden yapılmaya başlanmış ve kısa sürede önemli bir büyüklüğe ulaşmıştır. Ancak elektronik ticaretin büyümesi güvenlik problemlerini de beraberinde getirmiştir. Bu nedenle firmalar ve bireyler açık ağlar üzerinden iletişime geçmek için güvenlik (security), kişiliğin belirlenmesi (identification), bütünlük (integrity) ve doğruluk (authentication) sorunlarının çözülmesini beklemeye başlamışlardır. Bu gelişmeler sonucunda 'elektronik imza' kavramı ortaya çıkmıştır.

Kişinin gerçek hayatta kendisini tanıtan ve imzalanan metnin kendisi tarafından okunduğunu ve onaylandığını belirten imzasının elektronik ortamda gerçekleştirilmesi yöntemlerine elektronik imza adı verilmiştir. Ancak elektronik ortamda güvenlik ve kimlik gibi sorunların halledilmesi için elektronik imzanın geliştirilmiş şifreleme (kriptografi) yöntemleri ile gerçekleştirilmesi gerekmiştir. Bu ise 'dijital imza'nın oluşumunu getirmiştir. Dijital imza, gerçek hayatta kullandığımız imzanın elektronik ortama aktarılmış şekli değil; gerçek hayatta kullandığımız imzanın elektronik ortamda da hüküm ve sonuç doğuracak şekle getirilmesi ile oluşturulmuş dijital formatıdır. Elektronik imzanın geliştirilmesi ve yaygınlaştırılması elektronik ticaret ve elektronik devlet gibi kavramların gelişmesinin de vazgeçilmez bir gereği olmuştur. Bu amaçlarla Avrupa Birliği, 13 Aralık 1999'da 1999/93/AT sayılı Avrupa Parlamentosu ve Konseyi Elektronik İmza Direktifi'ni kabul etmiş ve 19 Ocak 2000 tarihinde yürürlüğe sokmuştur. Türkiye de Avrupa Birliği'ne aday bir ülke olarak ve Dünyadaki gelişmelere ayak uydurmak amacıyla 15.01.2004 tarihinde 5070 sayılı Elektronik İmza Kanunu'nu kabul etmiş ve 23.07.2004 tarihinde yürürlüğe sokmuştur.

Elektronik İmzanın Tanımı ve Kullanım Şekilleri

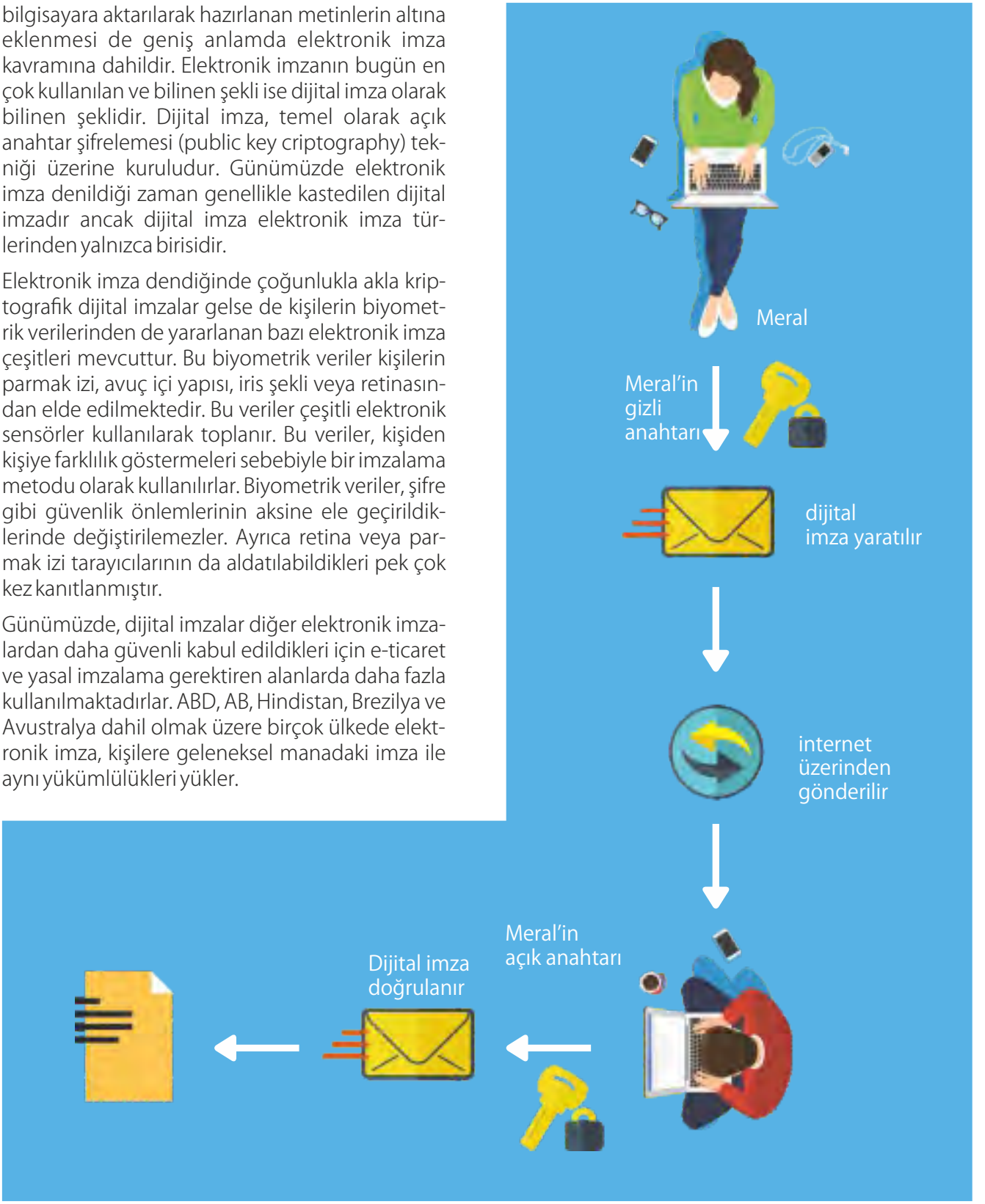
Elektronik imza, başka bir elektronik veriye eklenen veya elektronik veriyle mantıksal bağlantısı bulunan ve kimlik doğrulama amacıyla kullanılan elektronik veridir. E-imza olarak da bilinir. Elektronik ortamlarda imza yerine kullanılabilen yasal kimlik doğrulama sistemidir. Elektronik imza sayesinde imzalanmış verinin, kimin tarafından imzalandığı ve güvenilirliği kontrol edilmiş olur. Elektronik imza; bir bilginin üçüncü tarafların erişimine kapalı ortamda, bütünlüğü bozulmadan ve tarafların kimlikleri doğrulanarak iletildiğini elektronik veya benzeri araçlar ile garanti eden harf, karakter veya sembollerden oluşur. Bilgi ve iletişim teknolojilerinin gelişmesi ile birlikte ortaya çıkan elektronik ticaret, elektronik devlet ve elektronik sözleşme gibi kavramlar elektronik ortamda işlem yapılmasını da kaçınılmaz kılmıştır. Ancak yapılan bu işlemler esnasında yapılacak sözleşmelerin ve beyan ve irade açıklamalarının kim tarafından oluşturulduğunun anlaşılabilmesi için tarafların imzalarının elektronik metinlerde de yer alması gerekli olmuştur. Elektronik imza geniş anlamda en basitten en komplekse kadar kişinin elektronik ortamda tanınmasını sağlayan her türlü işaretidir. Bu manada en basit çözüm olarak kişinin kendi el yazısı ile attığı imzanın 'tarayıcı' vasıtasıyla

.

bilgisayara aktarılarak hazırlanan metinlerin altına eklenmesi de geniş anlamda elektronik imza kavramına dahildir. Elektronik imzanın bugün en çok kullanılan ve bilinen şekli ise dijital imza olarak bilinen şeklidir. Dijital imza, temel olarak açık anahtar şifrelemesi (public key criptography) tekniği üzerine kuruludur. Günümüzde elektronik imza denildiği zaman genellikle kastedilen dijital imzadır ancak dijital imza elektronik imza türlerinden yalnızca birisidir.

Elektronik imza dendiğinde çoğunlukla akla kriptografik dijital imzalar gelse de kişilerin biyometrik verilerinden de yararlanan bazı elektronik imza çeşitleri mevcuttur. Bu biyometrik veriler kişilerin parmak izi, avuç içi yapısı, iris şekli veya retinasından elde edilmektedir. Bu veriler çeşitli elektronik sensörler kullanılarak toplanır. Bu veriler, kişiden kişiye farklılık göstermeleri sebebiyle bir imzalama metodu olarak kullanılırlar. Biyometrik veriler, şifre gibi güvenlik önlemlerinin aksine ele geçirildiklerinde değiştirilemezler. Ayrıca retina veya parmak izi tarayıcılarının da aldatılabildikleri pek çok kez kanıtlanmıştır.

Günümüzde, dijital imzalar diğer elektronik imzalardan daha güvenli kabul edildikleri için e-ticaret ve yasal imzalama gerektiren alanlarda daha fazla kullanılmaktadırlar. ABD, AB, Hindistan, Brezilya ve Avustralya dahil olmak üzere birçok ülkede elektronik imza, kişilere geleneksel manadaki imza ile aynı yükümlülükleri yükler.



Şekil – 1: Dijital imzanın çalışma mantığı

KOSGEB | TSE

BELGELENDİRME DESTEK ORANI

%100'E ÇIKARILDI!

KOBİ ve Girişimcilerin, **TSE**'den alacakları belgeler akreditasyon şartı ve **bölge farkı aranmaksızın destekleniyor.**

kosgeb

kosgebim

www.kosgeb.gov.tr
444 1 567