E-Ticarette Güvenlik Standartları

Ticaretin temellerinin dayandığı iletişim konusu, iletişimin üzerindeki kısıtların azalmasıyla en önce insan ilişkilerini, buna bağlı olarak da ticaretin gelişimini etkilemiştir. Elektronik devrimin dinamiğini oluşturduğu iletişim teknolojileri, ortaya, E-Ticaret kavramını çıkartmıştır.

E-Ticaret, teknolojinin sağladığı elektronik iletişim olanakları ile yapılan bir ticaret yapma biçimidir. Bunun günümüzdeki en büyük ve yaygın örneği İnternet üzerinden yapılanıdır. İnternetin gelişmesi ve yaygınlaşması sayesinde E-Ticaret de hayatımızın bir parçası haline gelmiştir.

E-Ticaret yapılırken en önemli nokta, para ve mal arasındaki yer değişimi döngüsünün kontrol edilmesidir. E-Ticaret platformları, alıcı ve satıcı arasındaki bir buluşma noktası olurken, satın alınan ürün veya hizmet olabilmektedir. Fiziksel ürünlerin elektronik ortama taşınması yanında da paranın da elektronik ortama taşınması getirmektedir. Madem para elektronik ortama aktarılmalı, o zaman paranın elektronik ortamdaki akışını sağlayacak bir sisteme, yani Ödeme Sistemlerine de gereksinim olmalıdır.

E-Ticarette kullanılan ödeme sistemlerini şu şekilde sıralayabiliriz:

- Kapıda nakit ödeme
- Kapıda kart / kredi kartı ile ödeme
- Havale / EFT ile ödeme
- Kart ile online ödeme
- Kredi kartı ile online ödeme
- Sanal kredi kartı ile online ödeme
- Kredi kartı ile 3D Secure online ödeme
- Mail Order (ödeme talimatı için kart bilgilerinin satıcıya doğrudan verilmesi) ile online ödeme
- Aracı kurumlar (PayPal vb.) ile online ödeme
- Mobil Ödeme (cep telefonu ile ödeme)

Kredi kartı ile ödeme: Kredi kartı hesabından ödeme tutarının online POS ile çekilmesi yoluyla gerçekleşir. Benzer şekilde, kart ile de ödeme vadesiz hesaplardan ödeme tutarı çekilerek ödeme yapılması söz konusudur. Ayrıca, sadece online alışverişlerde kullanılmak üzere üretilen sanal kredi kartları ile de ödeme yapılabilmektedir.

Sanal kredi kartı ile ödeme: Sanal kredi kartlarında da benzer şekilde bir süreç ile ödeme gerçekleştirilir. Sanal kredi kartları, fiziksel olarak var olmayan kredi kartlarıdır. Kişinin kredi kartı hesabına bağlı olarak alışveriş sırasında belli bir limit ile belirlenen ve alışveriş sonrasında limiti sıfırlanan kredi kartlarıdır.

Aracı kurumlar (PayPal) ile ödeme: İnternet üzerinde açılan sanal hesap cüzdanları arasında tek bir otoritenin denetimi altında para aktarımını sağlayan bir hizmetin markasıdır. Kredi kartı ya da banka hesap bilgileri bir kez girilerek PayPal hesabı açılır. Böylece, hesap bilgilerini alıcı veya satıcılarla paylaşılmadan online ödeme yapılmasını sağlar. PayPal ile alışveriş yapılırken, alıcılar nasıl ödeme yapmak istediklerini seçer (kredi kartı, nakit), PayPal parayı transfer eder, daha sonra satıcılar paralarını bankalarına aktarırlar.

Mobil ödeme: GSM operatörlerinin sanal cüzdanları tutan otorite olarak kullanıldığı ödeme şeklidir. Ödeme tutarı, cep telefonu faturasına yansıtılır. Düşük miktardaki ödemelerin cep telefonu üzerinden yapılması ve ödeme tutarının cep telefonu faturasına yansıtılması ile gerçekleştirilir. Böylece kredi kartı ya da banka hesap bilgisi kullanılmadan online alışveriş yapılabilir. Mobil alışveriş yapılırken, web üzerinden telefon numarası girilerek (ödeme SMS ile onaylanır) ya da SMS gönderilerek ödeme yapılabilir.

Uluslararası güvenlik platformu (3D Secure): Sanal platformlarda ödeme sistemlerinde güvenliği artırma amacıyla çeşitli uygulamalar geliştirilmektedir. Bunların en yenilerden birisi 3D Secure olarak isimlendirilen Visa, Amex, Discover ve MasterCard ödeme sistemlerinin uygulamaya koyduğu Ulusal Güvenlik Platformu'dur. Siteden alışveriş yaparken kartı kullanan kişinin gerçekten kartın sahibi olup olmadığını anlamak amacıyla kullanılmaktadır. Sitede ödeme işlemi sırasında sadece kişinin kendisinin bildiği dört haneli şifre (pin numarasını) ve yine kendisinin belirlediği güvenlik sorusunun yer aldığı pop-up ekran alışveriş sitesi tarafından değil doğrudan bankanın kendi sisteminden kullanıcıya sunduğu bir hizmettir.

DPT'nin (2010) Bilgi Toplumu İstatistikleri raporuna göre, 2008'de işletmelerin İnternet üzerinden satışını kısıtlayan faktörlerin başında %48 oranı ile ödemelerle ilgili güvenlik problemleri gelmektedir.

Bu ödeme sistemlerinden kredi kartı ve onun güvenlik için uyarlanmış olan varyasyonlarının (3D Secure, Sanal Kredi kartı gibi) günümüzde yaygın kullanılan ödeme sistemlerindendir. Bunun nedeni, kredi kartı ile yapılan işlemlerin hızlı bir şekilde gerçekleşmesi ve kredi kartlarının gündelik ticaret hayatında da olan yaygınlığıdır. Bu kadar yaygın olan bir ödeme sisteminin güvenliği de son derece önemli bir konudur. Yaygınlığın getirdiği işlem hacmi beraberinde saldırganlara isteklendirme kaynağı olacak olan parayı

da getirecektir. Bu durumda yapılması gereken; alıcı, satıcı ve aracı kurumlar ile alt sistemler arasındaki bilgi güvenliğini sağlamaktır.

Temel anlamda kredi kartı bilgilerinin güvenliğini sağlamakta kullanılan sistemler araştırıldığında gündeme en çok gelen sistemin **SSL (Secure Sockets Layer)** olduğu görülmektedir. Hâlbuki SSL, sadece kredi kartı bilgilerinin saklanması için geliştirilmiş bir sistem değildir. SSL, ağ üzerinde hassas ve gizli kalması gereken bilgilerin geçtiği her yerde gizliliği sağlamak üzere geliştirilmiş bir şifreleme sistemidir. Bilgisayar teknolojisinde zaten hassas bilgilerin ağ trafiği içinde başkaları tarafından görülmemesi adına kullanılan bir yöntem olan SSL ile şifreleme, kredi kartı bilgilerinin geçtiği bilişim sistemlerinde bir standart ve disiplin olarak kullanılmaktadır.

SSL ile şifrelemenin gerçekleştiriliyor olması, kredi kartı bilgilerinin şifreleme yönteminin kırılarak başkaları tarafından görülemeyeceği anlamını taşımamaktadır. SSL ile şifreleme yapılırken dikkat edilmesi gereken teknik güvenlik unsurları mevcuttur. Eğer bu teknik güvenlik unsurları dikkatle yönetilmez ise, kredi kartı bilgilerinin gizliliğinin bozulması söz konusu olabilir. Bu unsurları şu şekilde bir arada toplayabiliriz:

- Zayıf algoritmalar ile şifreleme yapılması
- Kısa anahtar uzunlukları ile şifreleme yapılması
- Sertifika otoritesi kullanılmaması

Bahsi geçen bu teknik güvenlik unsurlarının her biri, şifreleme sisteminin aşılarak gizliliğin bozulmasına neden olabilecek türdendir.

Kredi kartı bilgilerinin güvenliği söz konusu olduğunda, süreçlerin güvenlik standartlarını belirlemeye yarayan PCI-DSS konusuna da değinmek gerekir. Payment Card Industry (PCI) Data Security Standart (Ödeme Kartları Endüstrisi Veri Güvenliği Standardı), Mastercard ve VISA tarafından belirlenmiş verinin kullanımı, korunması, saklanması ve iletimi ile ilgili ortak güvenlik standardıdır. Kısaca PCI-DSS olarak adlandırılmaktadır. Kredi kartları ile işlem kabul eden tüm işyerleri ve bankalar PCI-DSS standardına uymak zorundadır.

Kredi kartı bilgilerini ve böylece kredi kartı sahiplerini korumaya yönelik hazırlanan PCI-DSS, standartlara uymayanlar için bazı cezai yaptırımları da yanında beraber getirmektedir.

Kredi kartı bilgilerinin güvenliğinin nasıl sağlanması gerektiğini belirten PCI-DSS standardı, gerçek anlamda kredi kartı bilgilerinin nasıl korunmasını gerektiğine dair geliştirilmiş bir güvenlik standardıdır. Bu standart, teknik olarak SSL ve diğer şifreleme yöntemlerinin nasıl ve nerede kullanılacağına açıklık getirerek, günümüzde kullanılan teknik altyapıların nasıl yönetileceğine dair yol göstermektedir. SSL ise bu teknik altyapılardan

sadece birini oluşturmaktadır ve kamuoyundaki yanılgının aksine SSL, başlı başına bir güvenlik standardı değildir.

Teknik olarak hassas bilgilerin saklanması adımlarının her biri kredi kartı bilgilerinin veri tabanı üzerinde saklanması aşamasında da kullanılmaktadır. Kredi kartı bilgisini veri tabanına alan bir şirket, bu bilgiyi şifreli olarak saklamakla yükümlüdür. Benzeri teknik uygulamalar diğer hassas bilgiler için de kullanılmaktadır.

Ödeme sistemlerinde güvenliği sağlamak için mantıksal yapılar da geliştirilmiştir. Yukarıda bahsi geçen veri tabanı üzerinde şifreleme yapılması örneği, aracı bir şirketin kredi kartı bilgilerini kendi veri tabanında tutarak riski üstlendiğini göstermektedir. Bu riski bertaraf etmek için kullanılan mantıksal birkaç güvenlik sistemi, yani güvenli ödeme sitemleri de mevcuttur. **Bu sistemlere örneklerden den biri Sanal POS uygulaması, diğeri de Secure 3D'dir. Sanal POS uygulamasında banka girilen kredi kartı bilgisinin doğruluğunu onaylar ve yine banka tarafında bütün işlemler gerçekleştirildikten sonra satıcıya bu işlemlerin gerçekleştirildiğine dair bilgi yollanır. Bu durumda satıcı kredi kartı bilgilerini bir veri tabanı üzerinde saklama gereği duymaz ve bu riski üzerine almamış olur.**

Benzer ödeme yöntemlerinden biri de PayPal ve benzeri aracı kurumlarla yapılanıdır. Bu sistemlerde para transferi sanal krediler üzerinden yapılır. Bu kredileri elde etmek için kişiler yine diğer ödeme türlerini kullanarak (kredi kartı, havale vb.) hesaplarına kredi yüklerler. Bu kredileri başkalarının hesaplarındaki kredilere aktarımı ile birlikte transfer işlemi gerçekleşmiş olur.

Güvenlik konusunda bu sistemleri kullanan alıcı ve satıcıların bilinçli olması beklenir. Her ne kadar teoride bu durumun böyle olacağı varsayılsa da aslında uygulamada işler farklı şekilde gelişmektedir. Bunun farkında olan bankalar ve aracı kurumlar, yeni güvenli ödeme sistemlerini geliştirmeye ve satıcı ile alıcı arasındaki bilgi güvenliğini tehdit edecek etkenleri minimuma indirmeye yönelik çalışmalar yapmaktadır.

Kurumların E-Ticaret yaparken dikkat etmesi gereken hem teknik hem de sürece dayalı olan birçok güvenlik unsuru vardır. Bu unsurların birçoğunun uygulanmıyor olması, kurumun hukuki sorunlarla karşı karşıya kalmasına neden olabilir.

PCI Standardı nedir?

PCI herhangi bir Ödeme Kartını kabul eden işletmeler için hazırlanmış bir standarttır. Burada birincil amaç "Müşteri Verilerinin Korunmasıdır". Bu veriler, kartın üzerinde yazılı, manyetik şerit üzerinde veya kart içerisindeki çip'de bulunmaktadır. PCI Standartları, Müşterilerin verilerinin korunması için teknik ve operasyonel bazı gereksinimleri ortaya koyar. Standartların

uygulanması, işletmeye bağlantılı herhangi bir satış/işlem noktasındaki, işlemler ve iletilen Kart Sahibi Verilerini kapsar.

Her Standardın olduğu gibi PCI'ın da bir yöneticisi vardır. PCI Standardı "Ödeme Endüstrisi Güvenlik Standartları Konseyi" (PCI SSC) tarafından geliştirilmekte, yönetilmekte, eğitmekte ve farkında lığı sağlamaktadır. Konsey, 2006 yılında başlıca kart markaları tarafından kurulmuştur. Her marka, müşteri verilerinin güvenliğinin sağlanmasında PCI'ı bir standart kabul ederek uyumlu olmak için gerekli olan çalışmaları yapmayı taahhüt etmişlerdir.

SSL (Secure Socket Layer)

SSL network üzerindeki bilgi transferi sırasında güvenlik ve gizliliğin sağlanması amacıyla Netscape tarafından geliştirilmiş bir güvenlik protokolüdür. 1996 yılında 3.0 versiyonunun çıkarılmasıyla hemen bütün Internet tarayıcılarının (Microsoft Explorer, Netscape Navigator vb) desteklediği bir standart haline gelmiş ve çok geniş uygulama alanları bulmuştur.

SSL gönderilen bilginin kesinlikle ve sadece doğru adreste deşifre edilebilmesini sağlar. Bilgi gönderilmeden önce otomatik olarak şifrelenir ve sadece doğru alıcı tarafından deşifre edilebilir. Her iki tarafta da doğrulama yapılarak işlemin ve bilginin gizliliği ve bütünlüğü korunur.

Veri akışında kullanılan şifreleme yönteminin gücü kullanılan anahtar uzunluğuna bağlıdır. Anahtar uzunluğu bilginin korunması için çok önemlidir. Örneğin; 8 bit üzerinden bir iletimin çözülmesi son derece kolaydır. Bit, ikilik sayma düzeninde bir rakamı ifade eder. Bir bit, 0 veya 1 olmak üzere 2 farklı değer alabilir. 8 bit ise sadece 28=256 olası farklı anahtar içerir. Bir bilgisayar bu 256 farklı olasılığı sıra ile inceleyerek bir sonuca ulaşabilir. SSL protokolünde 40 bit ve 128 bit şifreleme kullanılmaktadır. 128 bit şifrelemede 2128 değişik anahtar vardır ve bu şifrenin çözülebilmesi çok büyük bir maliyet ve zaman gerektirir. Kötü niyetli bir kişinin 128 bit'lik şifreyi çözebilmesi için yüksek Mevla da para ve zamana ihtiyacı var.

KMK BİLGİ TEKNOLOJİLERİ A.Ş.
Mersis No: 0564057618200015 - Ticaret Sicil No: 970475
DAP Royal Center Altayçeşme Mahallesi Çam Sokak No:16 D. Blok Daire:28 Kat:7
Maltepe / İSTANBUL