E-ticaret Ödemesi Yapma

Amaçlar

- E-ticaret sistemi kullanıcıları için, ödemelerin güvenli ve adil bir şekilde yapılmasını sağlayın
- CNP işlemlerinden kaynaklanan dolandırıcılık oranını en aza indirin
- E-ticaret kullanıcıları için gizlilik ve güveni en üst seviyeye çıkarın
- Bütün yerel yasalara ve PCI (tüccar antlaşması) standartlarına uyun.

Uyum ve Yasalar

Eğer e-ticaret yapan bir tüccarsanız, vergi yasaları, ticaret uygulamaları, Mal Satışı (ve benzerleri), *lemon laws* (uygulanabildiği şekilde) vb gibi gibi bütün yerel yasalara uymanız gerekmektedir. Yetki hakkınız ile ilgili gereklilikleri öğrenmek için yasal danışma uzmanına başvurmalısınız.

Kredi kartı tüccarı iseniz, kredi kartı tüccar anlaşmalarını kabul etmişsiniz demektir. Genel olarak söz konusu anlaşmalar müsade edilen dolandırıcılık oranı ve CNP işlemleriyle ilgili kılavuz ilkeleri konusunda çok katıdırlar. Anlaşmanızı okumalı ve şartlarına uymalısınız.

Eğer anlaşmanızı anlamadıysanız, daha ayrıntılı bilgi için bankanızın tüccar destek hizmetinden yardım almalısınız.

PCI Uyumu

Kredi kartlarıyla ilgili en güncel yönetmeliklere uymak için, PCI Kılavuz İlkelerini ve tüccar antlaşmanızı yeniden incelemelisiniz. Kısacası, kredi kartı ödemesi yapacaksanız yerine getirmeniz gereken on iki gereklilik şunlardır:

Güvenli bir ağ kurun ve devam ettirin	Verilerinizi korumak üzere güvenlik duvarı konfigürasyonu kurun ve devam ettirin
	Sistem şifreleri ve diğer güvenlik parametreleri için satıcı tedarikli öntanımları kullanmayın

Kart sahibinin verilerini koruyun	Kaydedilmiş veriyi koruyun Kamu ağlarında kart sahibinin verilerini ve hassas bilgilerinin iletimini şifreleyin
Savunmasızlık Yönetim Programı Yerleştirin	Antivirüs yazılımı kullanın ve güncelleyin Güvenli sistemler ve uygulamalar oluşturun
Sağlam Erişim Kontrol Önlemleri Uygulayın	İş amaçlı bilgiye ulaşması gerekenlerin verilere erişimini engelleyin Bilgisayar erişiminde her bireye bir benzeri daha olmayan bir ID verin Kart sahibi verilerine fiziksel erişimi engelleyin
Ağları düzenli olarak izleyin ve test edin	Ağ kaynaklarına ve kart sahibi verilerine her türlü erişimi takip edin ve izleyin Güvenlik sistemlerini ve süreçlerini düzenli olarak test edin
Bilgi Güvenlik Politikası oluşturun	Bilgi güvenliğini sağlayacak bir politika yerleştirin

OWASP, “Güvenli sistemler ve uygulamalar oluşturun ve devam ettirin” şeklinde ifade edilen gereklilik kapsamında anılmaktadır.

> Açık Web Uygulama Güvenlik Projesi kılavuz ilkeleri gibi güvenli kodlama ilkelerine dayanan web yazılımları ve uygulamaları geliştirin. Kodlamada saldırıya açık noktaları belirlemek için alış veriş uygulama kodunuzu gözden geçirin. Bakınız www.owasp.org - “ Web Uygulama Güvenliğinde En Kritik On Saldırıya Açık Nokta.” Şunları içermek üzere,

yazılım geliştirme süreçlerinde, kodlamada yaygın saldırıya açık noktaları dikkate alın …

Bu Kılavuz, uygulamalarınızı güven altına almak için en iyi bilgi kaynağıdır. Faydalı da olsa, OWASP Top 10, uygulamanızın güvenliğini geliştirmek için sadece bir başlangıçtır, tam bir başvuru kaynağı değildir. Top 10, (bu kaynak yazılıdığı sırada) güncellenmekteydi.

Kredi Kartları

Her hafta, yeni bir işletmenin en nihai utancı yaşadığını okuyoruz – müşterilerinin bütün kredi kart verilerinin çalınmış olduğunu öğreniyoruz... Bu noktada, çoğunlukla işletmenin sonu demek olduğu açıklanmamaktadır (bakınız *Daha ayrıntılı bilgi* bölümü - Visa ve AMEX tarafından feshedilen KartSistemleri). Müşteriler, kredi kartlarını değiştirmek, bankalarının kart servislerine günlük ya da haftalık çevrimlerini fakslamak zorunda bırakılmaktan hiç hoşlanmazlar. Müşteri uygunsuzlukları yanında, tüccarlar, yetersiz güvenlikleri olduğunda, tüccar antlaşmalarını bozarlar. Hiçbir tüccar antlaşması, modern İnternet destekli işler için kara haber değildir.

Bu bölüm, ödeme işlemlerini nasıl ypmanız ve kaydetmeniz gerektiği ile ilgilidir. Şans ki, bunları yapmak yanlış yönde gerçekleştirmekten daha kolaydır.

Doğru Uygulamalar

- Işlemleri online olarak hemen gerçekleştirin ya da işlemin yapılmasını bankanıza bırakın.
- **CC numaralarını hiçbir zaman saklamayın. Eğer kaydedilmeleri gerekiyorsa, PCI mektup ilkelerini takip etmeniz gerekmektedir. Kredi kartları bilgilerini kayıtlı tutmamanızı önemle hatırlatıyoruz.**
- **Siteniz için paylaşılan bir sunucu kullanıyorsanız, PCI kılavuz ilkelerine uyamazsınız. PCI kılavuz ilkelerine uyum sağlamak için kendi altyapınızın olması gerekmektedir.**

Pek çok işletme kolay yolu seçerek müşterilerinin kredi kartı numaralarını kayıtlı tutarlar, çünkü ihtiyaçları olduğuna inanırlar. Bu doğru bir davranış değildir. Kredi kartı numaralarını kayıtlı tutmayınız.

Yetki numaraları

Işleminizi başarıyla gerçekleştirdikten sonra, size bir yetki numarası verilmektedir. Bu her işleme ait özel bir numaradır ve kendine has hiçbir değeri yoktur. Bu değeri kayıtlı tutmak, kayıtlara yazmak, çalışanlara sunmak ve müşteriye e-posta ile göndermek güvenlidir.

Tekrarlanan Ödemeleri Gerçekleştirmek

Kredi kartı numaralarını kayıt altında tutmanın işe bazında geçerli tek gerekçesi tekrarlanan ödemelerdir. Ancak, tekrarlanan ödemeleri desteklerken üzerinize düşen bazı sorumluluklarınız bulunmaktadır:

- Tüccar antlaşmanızın şartlarına uymanız gerekmektedir. Pek çok ticaret antlaşması kredi kartı sahiplerinden alınmış imzalı orijinal yetkilendirme temin etmenizi gerektirir. Bu imzalı belge, müşterinizin sizin ücretlerinizi zora sokması halinde size destek olacaktır.
- Yapılması gereken en doğru uygulama kredi kartı numaralarını şifrelemektir. Bu uygulama, PCI kılavuz ilkeleri kapsamında zorunlu bir şarttır.
- Özellikle CNP işlemleri kullanıyorsanız, tekrarlanan ödeme süresini bir yıldan uzun olmayacak şekilde sınırlayın.
- Antlaşma sona erdiği anda kredi kartı bilgilerini silin.

Şifreleme konusunda yaşayacağınız sorun ise iş süreci sırasında verinizin daha sonra şifresini çözebiliyor olmanızdır. Kartları şifreli bir şekilde kayıtlı tutacaksanız, öncü web sunucusunun bunların şifresini çözebiliyor olması için hiçbir neden yoktur.

Kredi kartının bazı bölümlerini görüntülemek

PCI, sadece ilk altı (BIN) ya da son dört hanenin sunulmasına izin verir. Eğer mümkünse, kredi kartını hiç görüntülememenizi önemle tavsiye ederiz.

Kredi kartı numarasını takip etme, gönderme ya da sunmayı kullanışlı yapan pek çok sebep bulunabilir, ancak kredi kartlarını güvenli bir şekilde sunmak mümkün değildir:

- Büyük bir organizasyonun çok sayıda başvurusu varsa ve hepsi, kredi kartlarının belirleyici bölümlerini göstermek için farklı işlemsel süreçler gerektiriyorsa, kart açıklanacaktır.
- E-posta düzeninde fatura göndermek, müşterileri kredi kartları karşılığında belirlenen ücretler konusunda bilgilendirmek için kullanılan düşük maliyetli bir yöntemdir. Ancak e-posta yöntemi güvenli değildir.
- Pek çok işyerinde, çağrı merkezi çalışanları genellikle oldukça yüksek alım satım oranlarına sahip gezici kişilerden oluşmaktadır.
- Kayıtlar, kanıtları yok etmek için değil, ek gizli bilgi elde edebilmek amacıyla saldırıya maruz kalır.
- Az sayıda bankacılık kuruluşları bulunan ülkelerde, kurumsal BIN numaraları sınırlıdır. Bu nedenle, kart numarasının büyük bir kısmı gizlenmiş bile olsa, işler durumdaki BIN numaralarını tahmin etmek ve yeniden oluşturmak mümkündür.

Pek çok kredi kartı 16 haneden oluşmaktadır (Amex gibi örnekler 14 ya da 15 haneli olabilmektedir):

```
XXXX XXYY YYYY YYYC
```

C, sağlama toplamıdır. X, BIN numarasıdır ve kartı düzenleyen kurumu belirtir. Y ise müşterinin kart numarasıdır.

CCV, CCV2 ve PVV (ya da PIN Doğrulama Değerini) kayıtlı bulundurmamalısınız. Bunlar, pek çok ağ geçidi tarafından, basılı dolandırıcılığa karşı korumak amacıyla kullanılan kredi kartı geçerlilik alanıdır, çünkü değer kartın arkasındadır. 3.2.3 ve 3.4 numaralı bölümlerde de belirtildiği gibi, bu değerin kayıtlı tutulması yasaktır.

Bütün bu sebeplerden dolayı, kullanıcı ya da çalışanınıza açık ya da gizlenmiş kredi kartlarını sunmamanız önemle hatırlatılır. Ancak, kredi kartının hiçbir hanesini görüntülememenizi, yalnızca geçerlilik tarihini görüntülemenizi tavsiye ediyoruz.

Kredi Kartı Borç Bilgisi Okuma

Bu bölüm web uygulaması geliştirenlerin pek çoğu için uygulanabilir olmamakla birlikte bir kez daha hatırlamakta fayda bulunmaktadır.

Müşteri kartını iki defa geçirmek yasaktır. Elektronik fon transfer terminalinden daha sonra da satış sisteminden kartı geçirmek yaygın bir uygulamadır. Müşterilerin, kredi kartlarına çok defa okutan insanlara alışmasını kısmen engellemek üzere uygulanmaktadır; çünkü müşteri kartı hile yoluyla kopyalamak ve kötüye kullanmak için bir ilk adımdır.

Manyetik şerit içeriğini ya da kayıtlı değer chip'ini kaydetmek yasaktır.

Yama ve Onarma

PCI, sisteminizin herhangi bir bölümü için, yamanın mümkün olduğunda bir ay içerisinde yama yapmanızı gerektirir. Böylece, kredi kartı işlemlerini gerçekleştirmeniz ya da kaydetmeniz kolaylaşacaktır.

Ters Kayıtlar

Ters kayıtlarla ilgili iki potansiyel dolandırıcılık çeşidi vardır: organizasyonun içinden birinin hesatan para çekerek üçüncü bir tarafa aktarması ya da organizasyon dışından birinin, borçlu olunmayan bir meblağı "ödemek" için otomasyonlu ters kayıt sürecini nasıl kullanacağını başarılı bir şekilde çözmesi- örneğin, negatif numaralar kullanılarak gerçekleştirilebilir.

Tesr kayıtlar her zaman elle yapılmalıdır, ayrıca iki ayrı çalışan ya da grup tarafından imzalanmalıdır. Böylece hem içeriden hem de dışarıdan yapılabilecek dolandırıcılık riski azaltılmış olacaktır.

Bütün değerlerin sınırlar dahilinde tutulmasının ve imza atacak yetkilinin uygun bir şekilde belirlenmesinin esas olduğu unutulmamalıdır.

Örneğin, 2001 yılında Avustralya'nın Melbourne kentinde, güvenilir bir çalışan, bir spor organziasyonundan 400,000 Dolar çekmek için mobil bir EFTPOS terminali kullanmıştı. Eğer bu kişi bu kadar açgözlü olmasaydı, hiçbir zaman yakalanamayacaktı.

Organizasyonun dolandırıcılığa ne kadar hoşgörülü yaklaşacağını bilmek de çok önemlidir.

Geri ödeme

Pek çok işletme, satış dilinde “puan” olarak bilinen çok küçük marjinlerde işlem yaparlar. Örneğin, "6 puan" brüt maliyet üzerinden %6 kar anlamına gelmektedir. Aslında bu oran, sabah yataktan kalkmanıza değmeyecek kadar küçük.

Bu nedenle, mallarınızı sevk ettikten sonra çok sayıda geri ödemeyle karşı karşıya kaldığınızı görürseniz, bir işlemden kazanacağınız kârdan fazlasını kaybetmişsiniz demektir. Perakendecilik dilinde ifade etmek gerekirse, buna “fire” adı verilmektedir. Ancak, polis bu durumu dolandırıcılık olarak adlandırır. Geri ödemeler için yasal sebepler de vardır ve yerel tüketici yasalarından bu hakların neler olduğunu öğrenebilirsiniz. Ancak, pek çok düzenleyici yüksek geri ödeme oranına sahip tüccarlarla ilgili çok net olmayan fikre sahiptirler. Bu durum, onlara büyük zaman ve para kayıplarına mal olmakla birlikte dolandırıcılık kontrollerinin bulunmadığını da göstermektdir.

Riskinizi azaltmak için aşağıdaki kolay önlemleri alabilirsiniz:

- Para negatif bir şey değildir. Sıfır ya da olumlu sayıları hızlandırmak, negatif sayıları engellemek için dayanıklı basım kullanın.
- Negatif değerlerin yolunu açarak, ödeme işlevini ters kayıt haline getirecek şekilde aşırı yüklemeyin.
- Bütün geri ödemeler ve ters kayıtlar kayıt olma, denetleme ve manüel yetkilendirme gerektirir.
- Web sitenizde ters kayıtlar ya da geri ödemeler için hiçbir kod bulunmamalıdır.
- Ödeme ağ geçidinden yetkilendirme belgesi almadan mallarınız sevk etmeyin.
- Kredi kartlarının büyüyk bir çoğunluğunun BIN numaralrı ve düzenleyen kurumun bulunduğu ülke arasında sıkı bir ilişki vardır. Ülke dışındaki BIN kartlarına mal göndermemeyi ciddi olarak dikkate alın.
- Yüksek değerli mallar için, telefon üzerinden ya da faks aracılığıyla ödemeye yapmayı dikkate alın.

Bazı müşteriler, tek seferde çok sayıda geri ödeme almayı deneyeceklerdir. Geri ödeme talep eden müşterilerinizi dikkatle izleyin ve fazla risk teşkil edip etmediklerini belirleyin.

Düzenleyen kuruluşun müşteri ile ilgili edindiği müşteri e-posta adresi ve telefon numarasını isteyin. Bu size diğer tehlike bayrakları açıldığında yardımcı olacaktır.

10 sentlik bir imza, binlerce dolarlık güvenlik altyapısına bedeldir. Web sitenizde, dolandırıcılığı yasaların bütün gerekleri doğrultusunda dava ettiğiniz ve bütün işlemlerin tamamen kayıtlı olduğu konusunda kesinlikle bilgi verin.

Daha ayrıntılı bilgi için lütfen aşağıdaki kaynakları inceleyiniz

- PCI ihlâlleri için Visa ve AMEX KartSistemlerini feshediyor: http://www.theregister.co.uk/2005/07/19/cardsystems/
- **AMEX, Visa, Mastercard, Discover, JCB, Diner's Club – Kart Endüstrisi Kart Endüstrisi Veri Güvenlik Standardı**

  http://www.visa-asia.com/ap/center/merchants/riskmgmt/includes/uploads/AP_PCI_Data_Security_Standard_1.pdf
  https://sdp.mastercardintl.com/pdf/pcd_manual.pdf
- **Visa**

  Kart Sahibi Bilgisi Güvenlik Sistemi
  http://usa.visa.com/business/accepting_visa/ops_risk_management/cisp.html
  Hesap Bilgisi Güvenlik Programı
  http://www.visa-asia.com/ap/sea/merchants/riskmgmt/ais.shtml

  CISP'tan PCI'ya
  http://usa.visa.com/download/business/accepting_visa/ops_risk_management/cisp_Mapping_CISPv2.3_to_PCIv1.0.pdf

Dökümanın Aslı : OWASP GUIDE 2.0.1

Çeviri : Çiğdem Akanyıldız - acigdema@yahoo.com