2025-2026 BAHAR DÖNEMİ

TİC 110 – E-TİCARET

Elektronik Ticarette Güvenlik ve Ödeme Sistemleri

GİRİŞ

Dijitalleşmenin hızlanmasıyla birlikte e-ticaret, küresel ekonominin en hızlı büyüyen alanlarından biri haline gelmiştir.

- Online alışveriş hacmi her yıl artmaktadır,
- Mobil ticaret (m-commerce) yaygınlaşmaktadır,
- Dijital ödeme sistemleri gelişmektedir.

Ancak bu büyüme ile birlikte siber güvenlik riskleri ve ödeme güvenliği sorunları da artmaktadır.

Bu nedenle e-ticaret ekosisteminde ***güvenlik;***

- tüketici güveninin sağlanması,
- finansal işlemlerin korunması,
- Ve dolandırıcılık risklerinin azaltılması açısından kritik öneme sahiptir.

E-ticarette güvenlik yalnızca teknik bir konu değil aynı zamanda ekonomik ve ***stratejik*** bir konudur.

Güvenlik eksikliği şu sonuçlara yol açabilir:

- müşteri verilerinin çalınması,
- kredi kartı dolandırıcılığı,
- marka itibarının zarar görmesi,
- müşteri güveninin kaybedilmesi.

Bu nedenle işletmeler için siber güvenlik yönetimi e-ticaret stratejisinin önemli bir parçasıdır.

E-ticaret ortamında çeşitli siber tehditler ve güvenlik riskleri bulunmaktadır.

Başlıca tehditler:

- Kimlik avı saldırıları (Phishing)
- Kötü amaçlı yazılımlar (Malware)
- Hizmet reddi saldırıları (DDoS)
- Veri ihlalleri ve kart dolandırıcılığı

Bu tehditler hem tüketicileri hem de e-ticaret işletmelerini doğrudan etkileyebilir.

Kimlik Avı (Phishing) Saldırıları

Kimlik avı saldırıları, kullanıcıların sahte web siteleri veya e-postalar aracılığıyla kandırılması yöntemine dayanmaktadır.

Amaç:

- kullanıcı adı ve şifreleri ele geçirmek,
- kredi kartı bilgilerini çalmak,
- kişisel verilere erişmek.

Örneğin: Bir e-ticaret sitesine benzeyen sahte bir web sitesi üzerinden kullanıcı bilgilerinin toplanması.

- Bankadan gelmiş gibi görünen sahte linkler.

DDoS Saldırıları

DDoS (Distributed Denial of Service) saldırıları, bir web sitesine aşırı sayıda talep göndererek sistemin çalışamaz hale getirilmesini amaçlar.

Sonuçları:

- web sitesinin erişilemez hale gelmesi,
- satış işlemlerinin durması,
- işletmelerin finansal kayıp yaşaması.

Büyük e-ticaret platformları zaman zaman bu tür saldırıların hedefi olabilmektedir.

Veri İhlalleri ve Kart Dolandırıcılığı

E-ticaret sitelerinde meydana gelen veri ihlalleri sonucunda:

- müşteri verileri,
- kredi kartı bilgileri,
- ve ödeme bilgileri siber saldırganların eline geçebilir.

Bu durum finansal kayıplara, kimlik hırsızlığına ve müşteri güveninin azalmasına neden olabilir.

E-Ticarette Güvenliği Sağlayan Teknolojiler

E-ticaret sistemlerinde güvenliği artırmak için çeşitli teknolojiler kullanılmaktadır.

Başlıca güvenlik çözümleri:

- SSL / TLS şifreleme
- 3D Secure doğrulama
- İki aşamalı kimlik doğrulama (2FA)
- Güvenli ödeme ağları
- Fraud tespit sistemleri

SSL / TLS Şifreleme

SSL (Secure Sockets Layer) ve TLS (Transport Layer Security) internet üzerinden gönderilen verilerin şifrelenmesini sağlayan güvenlik protokolleridir.

Nasıl Çalışır?

- Kullanıcı bir web sitesine girer (https://),
- Tarayıcı ile sunucu arasında şifreli bir bağlantı kurulur,
- Gönderilen veriler (şifre, kart bilgisi vb.) şifrelenerek iletilir,
- Üçüncü kişiler bu verileri okuyamaz.

Bu sayede:

- kullanıcı bilgileri korunur,
- ödeme verileri güvenli şekilde iletilir,
- veri hırsızlığı riski azaltılır.

Tarayıcıda görülen ***https*** ibaresi güvenli bağlantıyı gösterir.

3D Secure Ödeme Sistemi

3D Secure (3 Domain Secure), internetten yapılan kredi kartı ödemelerinde kullanılan bir ek güvenlik doğrulama sistemidir.

3 farklı taraf (domain) vardır:

1. Kart sahibi (siz)
2. Satıcı (e-ticaret sitesi)
3. Banka (kartı veren kuruluş)

Ödeme sırasında kullanıcıdan:

- SMS doğrulama kodu ve,
- mobil bankacılık onayı istenir.

3D Secure Ödeme Sistemi

3D Secure sisteminin kullanıcılar ve firmalar açısından birçok avantajı vardır:

- Çalıntı kartlarla işlem yapılmasının önüne geçer.
- Kart sahibine özel doğrulama sayesinde güvenliği artırır.
- Müşteri memnuniyetini ve güvenini artırır.
- Online alışverişte yasal güvence sunar.

İki Aşamalı Kimlik Doğrulama (2FA)

2FA (Two-Factor Authentication – İki Faktörlü Kimlik Doğrulama), kullanıcıların bir sisteme giriş yaparken iki farklı doğrulama katmanı kullanmasını zorunlu kılan bir güvenlik yöntemidir.

Amaç, sadece şifreye dayalı güvenliği aşarak hesabı daha güçlü şekilde korumaktır.

Örneğin: Kullanıcı adı ve şifre + SMS doğrulama kodu

E-Ticarette Ödeme Sistemleri

E-ticaret işlemlerinin temel unsurlarından biri güvenli ve kullanıcı dostu ödeme sistemleridir.

Başlıca ödeme yöntemleri:

- Kredi ve banka kartları,
- Dijital cüzdanlar,
- Banka havalesi / EFT,
- Mobil ödeme sistemleri.

Dijital Cüzdanlar

Dijital cüzdanlar, kullanıcıların ödeme bilgilerini güvenli şekilde saklayan sistemlerdir.

Örnekler:

- Apple Pay
- Google Pay
- PayPal

Avantajları:hızlı ödeme, güvenli işlem, kullanıcı kolaylığı.

Mobil Ödeme Sistemleri

Mobil ödeme sistemleri, kullanıcıların akıllı telefonları üzerinden ödeme yapmalarını sağlar.

Örnekler:

- QR kod ile ödeme,
- mobil bankacılık uygulamaları,
- temassız ödeme sistemleri.

Mobil ticaretin gelişmesiyle birlikte bu yöntemler hızla yaygınlaşmaktadır.

Güvenli E-Ticaret İçin Alınması Gereken Önlemler

Kullanıcılar için

- güçlü ve benzersiz şifreler kullanmak,
- şüpheli e-postalara dikkat etmek,
- güvenilir e-ticaret sitelerini tercih etmek,
- iki aşamalı doğrulama kullanmak.

İşletmeler için

- güvenlik standartlarını uygulamak,
- SSL ve 3D Secure sistemlerini kullanmak,
- müşteri verilerini şifrelemek,
- düzenli güvenlik kontrolleri yapmak.

E-ticaret ekosisteminin sürdürülebilir şekilde gelişebilmesi için güvenlik ve ödeme sistemleri kritik öneme sahiptir.

Siber tehditlerin sürekli gelişmesi nedeniyle:

- güvenlik protokollerinin güncellenmesi,
- güvenilir ödeme sistemlerinin kullanılması ve,
- kullanıcı farkındalığının artırılması gerekmektedir.

Bu önlemler, güvenli ve sürdürülebilir bir e-ticaret ortamının oluşmasına katkı sağlar.