Bilişim Etiği ve Hukuku

Prof. Dr. Eşref ADALI

E-ticarette

12

E-ticaret

- Büyük firmaların ticarette 1970'lerden beri bilgisayarlar arası iletişim yoluyla ticaret yaptıkları bilinmektedir. Bu tür ticaret bir özel ağ (VAN: Value Added Network) üzerinden gerçekleştirilmektedir. Genelağ'ın yaygınlaşmasının bir sonucu olarak daha çok bireysel kullanıma yönelik e-ticaret gelişmiştir. Bu yolla yapılan e-ticaret çok hızlı gelişmektedir. İnsanların alışveriş işlemini kolaylaştıran e-ticaret değişik sorunları da beraberinde getirmiştir.

- Ticaretin üç temel ilkesi vardır:
- Ticaret güvenli ortam ister.
- Alıcı ve satıcının birbirine güvenmesi gerekir.
- Alan ve satan alışverişten mutlu olmalıdır.

- Büyük kuruluşların kapalı bir ağ olan VAN üzerinden gerçekleştirdikleri, EDI belgelerini kullanarak yapılan e-ticarette yeterli güvenlik sağlanmaktadır ve taraflar birbirini çok iyi tanırlar.

TCP/IP Protokolü

Genelağ'da TCP/IP protokolü kullanılmaktadır. Bu protokol temel olarak İki katmandan; Üst Katman (TCP: Transfer Control Protocol) ve Alt Katman (IP: Internet Protocol) dan oluşur:

Üst Katman: Bilgisayarlar arasında iletilecek veri önce paketlere bölünür ve paketler alıcıya gönderilir. Alıcı gelen paketleri birleştirerek asıl veriyi elde eder.

Alt Katman: İletilmek istenen paketleri alıcının adresine iletir.

Üst katman içinde, Uygulama ve Taşıma katmanları yer alır.

Uygulama Katmanı: Farklı bilgisayarlarda bulunan uygulamalar arasındaki iletişimi sağlar.

Taşıma Katmanı: İki bilgisayar arasındaki veri akışını sağlar. Bu sunucudan sunucuya taşıma işlemidir.

Alt katman içinde Genelağ Katmanı, Ağ Erişim Katmanı ve Fiziksel Katman yer alır.

Genelağ Katmanı: Birbirine yönlendiriciler ile bağlanmış ağlar üzerinde, kaynak ve hedef bilgisayarlar arasında verilerin iletilmesini sağlar.

Ağ Erişim Katmanı: Bilgisayar ile ağ arasında mantıksal ilişkiyi kuran arabirim olarak değerlendirilir.

Fiziksel Katman: İletişim ortamının elektriksel ve fiziksel özelliklerini belirleyen katmandır.

TCP/IP Protokolünün Güvenliği - I

SYN Saldırıları: TCP/IP protokolünde bilgisayarlar üç aşamada oturum kurarlar. Sunucu dinleme konumundadır ve istemciden istek bekler. İstek SYN olarak gelir. İsteği alan sunucu 75 saniye kadar bekleme durumunda kalır. Genellikle sunucular ortalama 5 isteği karşılayacak durumdadır.

Sunucuyu meşgul etmeyi hedefleyen saldırganlar peş peşe bağlantı isteği göndererek sunucuyu meşgul ederek hizmet vermesini engelleyebilirler. SYN kandırması adı da verilen bu tür saldırılar TCP/IP protokolünün zayıf yönünden yararlanmaktadır.

IP Kandırması: IP kandırması olarak bilinen bu tür saldırılarda saldırgan kendi IP adresi yerine sahte bir adres kullanır. Saldırgan gönderdiği veri paketinin içine sahte bir IP adresi ekleyerek gönderir. Alıcı taraftaki IP katmanı gelen veri paketinin içindeki adresi gerçek adres olarak değerlendirir.

IP kandırması türündeki saldırılar genellikle sunucuların hizmet vermelerini aksatmak amacıyla yapılmaktadır (DDos).

Sıra Numarasını Tahmin Etme: TCP protokolüne uygun olarak sağlanan bağlantıda kullanılan sıra numarası (Initial Sequence Number: ISN) 32 bit uzunluğundadır. Dolayısıyla bu numarayı tahmin etme olasılığı düşüktür. Kaynak bilgisayar tarafından üretilen bu numara belli bir kurala uyularak üretiliyor ise tahmin etmek kolaylaşır. Unix çekirdeği tarafından üretilen ISN'nin belli bir kurala göre hesaplandığı bu nedenle bir önceki bağlantıda kullanılan ISN biliniyor ise bir sonraki ISN numarasının hesaplanabileceği açıklanmıştır. Saldırganlar bu zayıflıktan yararlanmak üzere çok sayıda ISN'yi denemektedirler.

Kaynak Yönlendirme: Yanıtın hangi yolla, hangi IP'ye ulaşması gerektiğini gönderen belirlediği bir durumdur. Günümüz yönlendiricileri kaynak yönlendiricisini belirleyebildikleri için bu konu sorun olmaktan çıkmıştır.

TCP/IP Protokolünün Güvenliği - II

Bağlantıyı Ele Geçirme: Bağlantıyı ele geçirme ya da Aradaki Adam olarak adlandırılan bu yöntemde saldırgan bağlantıda olan iki bilgisayarın arasına girmektedir. IP kandırması yöntemi, Unix parolası, Keyberos ve TKP gibi ek güvenlik bilgilerini iki taraf arasında aktaramaz. Ancak bu yöntemde saldırgan iki bilgisayar arasındaki asıllama işleminin sürmesini sağlar ve bağlantıyı ele geçirir. Aradaki adam yönteminin çalışabilmesi için aradaki adamın bağlantıdaki iki bilgisayarın iletişim yolu üzerinde bulunması gerekir. Aradaki adam iki taraftan gelen veri paketlerini birbirine aktarır.

Yönlendirme Saldırısı: TCP/IP protokolünde kullanılması kesinlikle gerekli olmayan ancak kullanılan Yönlendirme Bilgisi Protokolü (Routing Information Protocol: RIP) sıkça kullanılmaktadır. RIP ağ üzerindeki en kısa ya da önerilen yolu tanımlamaktadır. RIP içinde asıllama işlemini barındırmamakta, dolayısıyla doğrulamaya çalışmamaktadır.

Bu açıklardan yararlanan saldırganlar ileti paketinin geldiği ve gideceği adresleri değiştirebilmektedirler. Böylece saldırganlar ileti paketlerini ele geçirebilmekte ve içeriğini istediği gibi değiştirebilmektedir.

ICMP Saldırısı: Alıcı tarafı uyarmak üzere gönderilen mesaj Genelağ Denetim Mesaj Protokolü (Internet Control Message Protocol: ICMP) olarak adlandırılır. Bu mesaj genellikle ping atmak olarak adlandırılır. Ping atıldıktan sonra gönderen taraf karşı tarafın yanıt vermesini bekler. ICMP mesajı içinde asıllama bilgisi yoktur. Bu nedenle hizmet aksatma türü saldırılarda kolaylıkla kullanılmaktadır.

Alan Adı Hizmeti Saldırısı: Alan Adı Hizmeti (Domain Name Service: DNS) Genelağ'da yaygın olarak kullanılmaktadır. İnsanların kolayca belleyebildiği alan adlarını, Genelağ Protokolünün anladığı IP adreslerine dönüştüren işleme DNS ve bu işlemi yapan sunuculara da DNS sunucusu adı verilmektedir. Böylece kullanıcıların web sayfalarına ve sunuculara kolayca erişimi sağlanmaktadır. Genelağ saldırganları Alan Çalma adı verilen yöntemle bir sunucunun ya da web sayfasının IP adresini ele geçirmektedirler. Daha sonra DNS sunucusuna erişerek DNS'in karşılığı olan IP adresini değiştirirler. Böylece kullanıcıları farklı bir sunucu ya da web sayfasına yönlendirebilirler.

Tekil Kimliğin Yokluğu: Genelağ'ın kullanılmaya başlandığı ilk dönemlerde IP yöntemiyle her bilgisayara bir adres verilebileceği öngörülmüştür. Ancak bir süre sonra bunun yetersiz kaldığı görülmüştür. Günümüzde konuma bağlı veya geçici olarak tanımlanan IP adresleri sunucular veya adres dönüştürücüler tarafından değiştirilmektedirler. Dolayısıyla yere bağlı ya da geçici IP adresine dayalı güvenlik sistemleri saldırılara karşı zayıf kalmaktadır.

Güvenli Elektronik Ödeme

- Secure Electronic Transaction (SET) protokolünün ana ilkesi Genelağ üzerinden yapılacak ödemenin müşteri tarafından satıcıya doğrudan yapılmaması, bunun yerine ödemenin bir aracı kuruluş (ödeme kanalı) üzerinden yapılmasıdır.

- Güvenli ödeme sisteminde hem müşteri hem de satıcı için SYB gerekmektedir. SET içinde SYB kullanıldığı için müşteri, satıcı ve banka arasında güvenilir ve gizli bir iletişim sağlanmaktadır. Ödeme işlemi güvenli biçimde kurulmakta, sorunsuz sürdürülmekte ve sahteciliği engellemektedir. Satıcı kredi kartı hakkında bilgi edinemediğinden ancak kartın çalınmış ya da sahte olduğuna karar verebilir.

SSL'nin sorunları

- SSL müşteriyi kulak misafirlerinden korumaktadır, buna karşın sahte satıcılardan koruduğu söylenemez. Bazı satış siteleri sahte veya yanıltıcı site olabilmektedir. Bu tür siteler müşterileri dolandırmak amacıyla kurulurlar. Müşterilerini iki türlü dolandırırlar:

  1- Tanınmış bir satıcının taklidini yaparak ya da

  2- Tümüyle yalancı bir site oluşturarak.

- Bu tür dolandırıcılıkların önüne geçebilmek üzere 3 boyutlu güvenlik sistemleri geliştirilmiştir. Üç boyutlu güvenlik sisteminde kredi kartı ile ödeme anında müşterinin cep telefonuna bir sayı gönderilmekte ve müşterinin bu sayıyı ödeme ekranındaki alana girmesi istenmektedir. Böylece kredi kartı ile ödeme yapmak isteyenin gerçek müşteri olup olmadığı kararı verilmektedir.

SET Protokolü

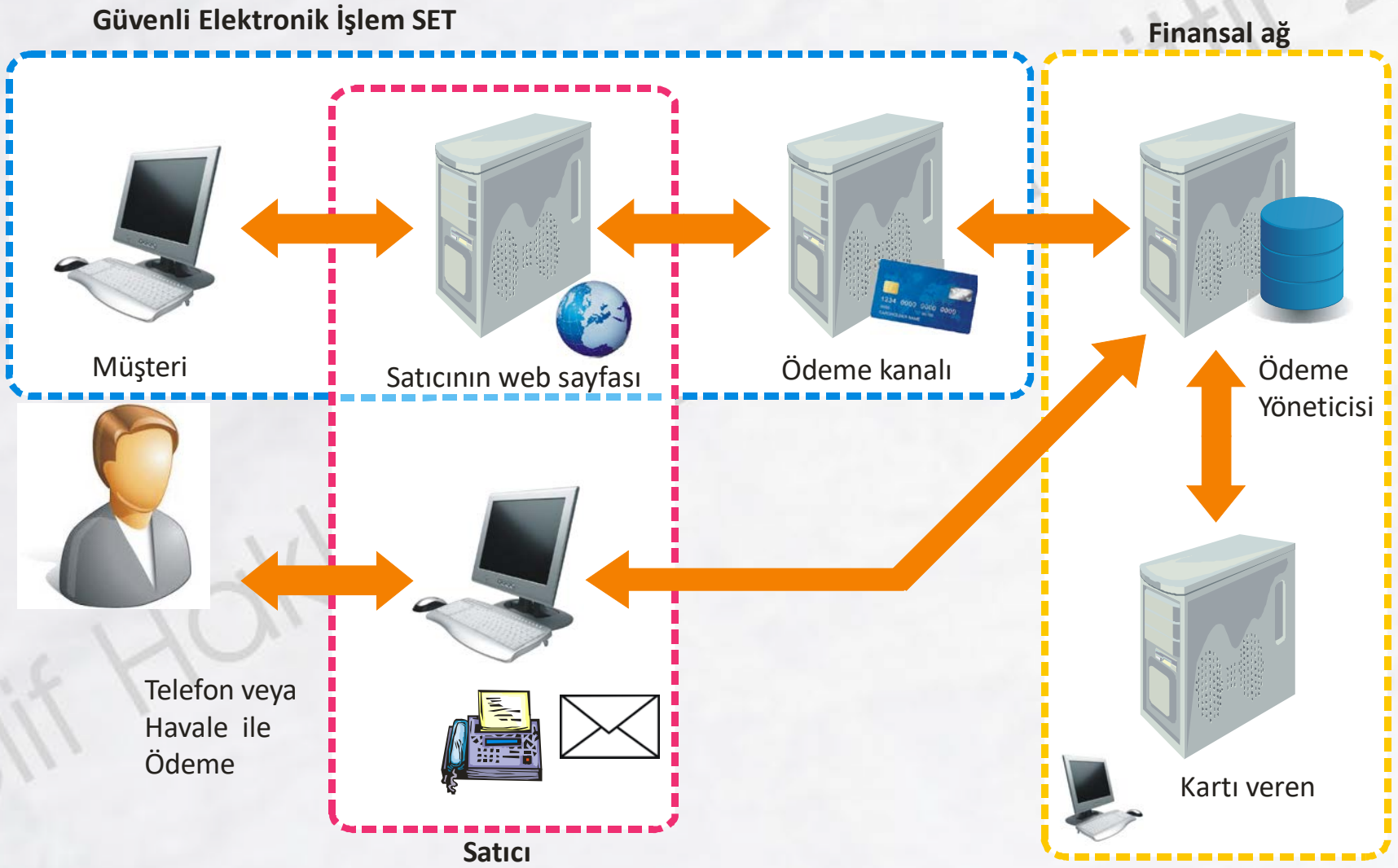
Temel ilkeler

- Sipariş ve ödeme bilgilerinin gizliliğini sağlamak.
- Ödeme işlemi ve hizmetler ile ilgili verilerin bütünlüğünü sağlamak.
- Müşteri kredi kartı hesabının asıllamasını sağlamak.
- Satıcının asıllamasını sağlamak.

SET protokolünde, bir alışveriş süreci 9 adım olarak tanımlanmıştır

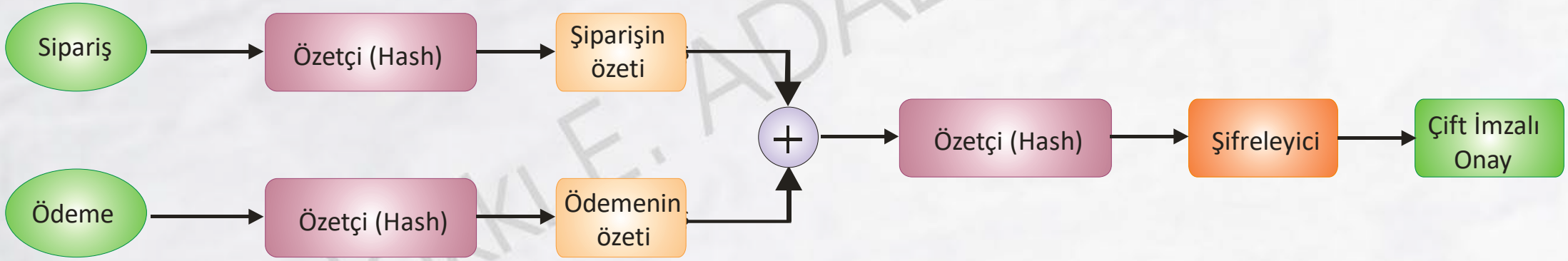
1. Müşteri satıcının web sayfasına bağlanır.
2. Müşteri satın almak istedikleri ile ilgili olarak iki parçadan oluşan sipariş ve ödeme bilgilerini gönderir. Parçalardan birincisi alışveriş ile ilgilidir ve satıcıya gönderilir. İkinci parça kredi kartı bilgisidir ve bu bilgi satıcının müşterisi olduğu bankaya gönderilmek üzere satıcıya gönderilir.
3. Satıcı kredi kartı bilgilerini kendi bankasına iletir.
4. Satıcının bankası müşterinin kredi kartının bu kartı veren kuruluşa bağlanarak onaylanmasını ister.
5. Kredi kartını müşteriye vermiş olan kuruluş, satıcının bankasına onay gönderir.
6. Satıcının bankası satıcıya onay gönderir.
7. Satıcı siparişi tamamlar ve müşteriye onay bilgisini gönderir.
8. Satıcı bankasından alışveriş ile ilgili işlem kaydını alır.
9. Kredi kartını müşteriye veren kuruluş müşteriye kredi kartı ödeme belgesini (fiş ya da fatura) gönderir.

SET Protokolünün Çalışma Biçimi



Sipariş ve Ödeme Bilgilerinin Birleştirilmesi

Sipariş ve Ödeme bilgileri iki parça hâlindedir. İlk parça alışveriş ile ilgilidir. Bu parçaya sipariş adını veriyoruz ve bu parça satıcıya gönderiliyor. İkinci parça ödeme ile ilgilidir. Ödeme adını verdiğimiz bu parça kredi kartına ilişkin bilgileri içerir ve satıcının bankasına gönderilir. Satıcının ödeme ile ilgili bilgileri daha açık bir ifadeyle kredi kartı bilgilerini görmemesi gerekir. Bir alışverişin tamamlanabilmesi için bu iki parçanın birleştirilmesi gerekir.



E-ticarette Tarafların Birbirine Güvenmesi-I

Genel ağ üzerinden yapılan e-ticaret üç sınıfta toplanmaktadır:

Kuruluşlar arası e-ticaret (k-k): VAN yerine Genelağ'ı kullanan kuruluşlar, birbirini tanımakta, genellikle uzun süredir aralarında ticaret yapmaktadırlar. Bu nedenle önemli sorunları olduğu söylenemez.

Satıcı ve müşteri arası e-ticaret (s-m): Günümüzdeki en yaygın e-ticaret uygulamasıdır. Tanınmayan kuruluşların ve bireylerin gerçek olamama olasılığı vardır. Bu nedenle sorunlar yaşanmaktadır.

Bireyler arası e-ticaret (b-b): İki tarafın da gerçek olduğunun kanıtı yoktur. Bu nedenle en riskli e-ticaret yoludur.

Kuruluşlar Arası E-ticaret

VAN üzerinde büyük firmalar arası yapılan ticarette, firmalar birbirini tanımakta ve kullandıkları iletişim ağı kapalı ve güvenlidir. Dolayısıyla etik ve hukuk açısından önemli bir sorun kaynağı değildir.

E-ticarette Tarafların Birbirine Güvenmesi-II

Kuruluş ve Birey Arası E-ticaret

Genellikle az bilinen e-ticaret firmaları ile yaşanan sıkıntılar:

- **Ayıplı ürün gönderilmesi**: E-ticaret sayfasında beğenilip seçilen ürün müşteriye gönderilmektedir. Ancak gönderilen ürün kullanılmış, bozuk, arızalı ya da tamir edilmiş bir ürün olabilmektedir. Ürün geri gönderildiğinde yenisini gönderen firmalar olabildiği gibi hiç yanıt vermeyenler de olabilmektedir. Özellikle ayıplı ürünü bilerek gönderen firmalardan yeni ve sağlam bir ürün beklemek saflık olur.
- **Taklit ürün gönderilmesi**: Dış görünümü bilinen bir ürüne çok benzer olan bir ürün gönderilmektedir. Taklit ürün gönderenlerin dolandırıcı oldukları kesindir. Dolayısıyla ürünü geri göndermek ve gerçek ürünün gönderilmesini beklemek anlamsızdır.

Bazı Uzakdoğu ülkesi firmaları lisanslı programları (özellikle işletim sistemlerini) ucuz fiyatla satmaktadır. Gelen ürün bilgisayara lisanslı bir ürün gibi kurulabilmektedir. Bu tür programların piyasa fiyatlarının altında nasıl satılabildiği araştırıldığında şu sonuçla karşılaşılmıştır: İşletim sistemi üreten firmalar bilgisayar donanımı üreticisi firmalara bu programların bir aslını vermekte ve çoğaltma hakkı tanımaktadırlar. Her bir çoğaltma için de lisans numarası tanımlamaktadırlar. İşletim sistemi programının kopyasını elde etmek satıcı için kolaydır. Bunun kopyalarını CD veya DVD üzerine hazırlayıp aslı gibi etiketlemektedirler. Donanım üreticilerinden elde ettikleri lisans numaralarını da pakete ekleyip pazarlamaktadırlar.

- **Eksik ürün gönderilmesi**: Bazı ürünler paketler hâlinde satılmakta ve her paketin içinde kaç tane olduğu belirtilmektedir. Dolandırıcı firmalar paketlerin içine web sayfasında yazan sayıdan daha az koymaktadırlar.
- **Sahte ürün gönderilmesi**: Disk yerine demir kütle, ilaç yerine toz kireç, kitap yerine, kitabın kapağının geldiğini söyleyen insanları duyuyoruz.

E-ticarette Tarafların Birbirine Güvenmesi-III

- Genelağ üzerinden sürdürülen bankacılık işlemleri kuruluş ve birey arası ticaret sayılabilir. İnsanlar paralarını bankalara güvendikleri için yatırırlar. Genelağ bankacılığında insanların paralarının çalınması bankanın bir eylemi değildir. Müşterinin hesap bilgilerini ve parolasını çalan soyguncuların işidir.

- Müşterilerin satıcıları kandırdığı olaylar da görülmektedir. Genellikle kredi kartı ile yapılan ödemelerde kandırmalar olmaktadır. Kredi kartının yapısı bilindiğinde, geçerli bir kart numarasını oluşturulabilir. Bunun için Genelağ'da hazır programlar da bulunmaktadır. Bilgisayarlı kredi kartının kullanılmadığı ve 3 düzeyli güvenliğin uygulanmadığı ülkeler için geçerli bir kredi kartı numarası üretip bunun ile alışveriş yapılabilmektedir. Satıcı firmaların bu tür kartlar ile alışveriş yapmak isteyenlere karşı özel önlemler alması gerekir.

Değerlendirme

Sonuç olarak s-m türü e-ticarette satıcının güvenilir olup olmaması çok önemlidir. Geçmişi bilinen ve güven kazanmış e-ticaret firmalarının SYB'leri vardır ve çoğunlukla SET protokolünü kullanırlar. Dolayısıyla bu firmalardan güvenli alışveriş yapılabilir. Adı sanı bilinmeyen firmalardan alışveriş yapmaktan kaçınılmalıdır. Bireysel müşterilerin SYB'lerinin olması gerekmediğinden satıcılar sahte kredi kartlarına karşı önlem almak zorundadırlar.

E-ticarette Tarafların Birbirine Güvenmesi-IV

Bireyler Arası E-ticaret

E-ticaretin en riskli olan biçimi bireyler arası olan biçimidir. Çünkü iki tarafın da SYB'si yoktur ve olması da beklenmemektedir. Bireyler arasındaki ödemeyi güvence altına almak üzere geliştirilmiş düzenlemeler vardır. Bunlar alıcı ve satıcı arasındaki para aktarımı işini üstlenen kuruluşlardır. Alıcı ve satıcı anlaştıktan sonra alıcı parasını aracıya gönderir. Alıcı ürünü aldığını söylemeden aracı kuruluş satıcıya ödemeyi aktarmaz.

Bireyler arası ticarette de bir önceki kısımda anlatılan sorunlar yaşanabilir:

- Ayıplı ürün gönderilmesi
- Taklit ürün gönderilmesi
- Eksik ürün gönderilmesi
- Sahte ürün gönderilmesi

E-ticarette Tarafların Mutluluğu

Bir ticaretin, ticaret sayılabilmesi ve sürdürülebilir olması için alıcı ve satıcının yapılan alışverişten mutlu olması gerekir. Güvenlik sorunu olmadığını bilen bir müşteri güvendiği bir satıcıdan ürün almayı her zaman yeğler. Çünkü:

- Ürünü seçmek için satıcının yerine gitmesi gerekmez. Özellikle, özellikleri bilinen ve ölçünlere uygun olarak üretilmiş ürünleri elle incelemek ve denemek gerekmediğinden e-ticaret sitesinden seçmek yeterlidir. Oturduğu yerden istediği zaman sipariş vermek ve ürünün ayağına kadar getirilmesi müşteriyi mutlu eder.
- Satın aldığı ürünü hiçbir gerekçe belirtmeden değiştirebileceğinin garantisini bilmesi alışveriş kararını daha kolay ve hızlı vermesini sağlar. Geri gönderme yükünün satıcıya ait olması kararını daha da etkiler. Bu kolaylık birden fazla ürün sipariş etmesinin yolunu açar. Gönderilen ürünlerden beğenmediklerini belli süre içinde geri gönderebilir. Böylece ürünleri ve satıcıyı ayağına kadar getirmiş duygusuyla mutlu olur.
- E-ticarette satıcı ürünleri sergilemek üzere geniş alanlara gereksinim duymaz. Hatta ürünleri kendi deposunda saklaması da gerekmeyebilir. Siparişi aldıktan sonra üreticiden isteyebilir. Bu yöntemle işletme giderlerinden çok büyük tasarruf sağlar. Yerinde satış için gerekli olan satış elemanı ve ortamı ısıtma, soğutma ve aydınlatma gibi giderler de olmayacaktır. Giderleri çok azalacak bir kuruluş için e-ticaret yöntemiyle ürün veya hizmet satmak son derece kârlıdır.
- E-ticaret ile dünya geneline ürün ve hizmet satılabilmektedir. Dolayısıyla firmaların ciroları e-ticaret sayesinde artmaktadır. Bu da satıcı için mutluluk vericidir.

E-ticaretteki Etik ve Hukuk Sorunları-I

Güvenliğin Sağlanması

Ticaret ortamının güvenliğini sağlamak kamunun görevidir. Genelağ üzerindeki ticaretin güvenliğini sağlamak da müşterilerin ve satıcıların görevi değildir. İlgili kısımda anlatıldığı gibi e-ticaretin güvenliğini sağlamak üzere epey çalışma yapılmıştır. Müşteriler kimlik ve kredi kartı bilgilerini ve parolalarını çaldırmadıkları sürece sorun olmaması gerekir. Güvenliği kırarak yaşanan olaylar ve değerlendirmeleri şöyledir:

- Kullanıcının kimlik bilgileri ve parolasının çalınması, genellikle bankacılık işlemlerinde kullanılan hesap bilgisi ve parolanın çalınması ile gerçekleştirilen soygun türüdür. 3. bölümde bu tür soygunlar hakkında örnekler anlatılmıştır. Kısaca hatırlamak istersek: soyguncu müşterinin bilgisayarına casus programının yüklenmesini sağlamakta ve bu program sayesinde müşterinin hesap numarası ve parolasını öğrenebilmektedir.

- Bu tür soygunların sonunda açılan davalarda konu çok tartışılmıştır. Müşteriler bankanın itibarlı ve güvenilir bir kuruluş olduğunu dolayısıyla soygundan sorumlu olmaları gerektiğini söylemişlerdir. Buna karşın bankalar müşterinin bankaya girişte kullandığı anahtar bilgileri saklaması gerektiğini savunmuşlardır. Aslında iki taraf da haklıdır. Ancak bankaların güvenilir ve sorumlu kuruluş olmaları onları güvenliği artırmak üzere yeni ve etkin çözümler bulmaya itmiştir.

- Genelağ'ın güvenliğinden kaynaklanan soygunlarda eğer müşterinin bir kastı ya da belirgin bir kusuru yok ise satıcılar sorumlu tutulur. Gerekli güvenlik önlemlerini sağlamaları gerektiği söylenir.
- Bu arada müşterilerin bilerek kendi hesaplarında soygun yaptırabilecekleri de unutulmamalıdır.

E-ticaretteki Etik ve Hukuk Sorunları-II

Satıcının Güvenilirliği

Ayıplı ürün gönderilmesi: Bir satıcı bilerek ayıplı ürün gönderiyor ise o satıcının dolandırıcı olduğu söylenebilir. Dolayısıyla ürünü geri gönderip yenisini istemek boşuna bir çaba olur. Bu durumda hukuk yolunu denemek de çok anlamlı değildir. Satıcının ilk tepkisi şöyle olacaktır: Biz sağlam ürün gönderdik; siz onu bozdunuz diyecektir. Müşteri ürünü teslim alırken yanında tarafsız bir tanık olmayacağı için bu savı çürütmesi çok zordur. Satıcı ile müşterinin farklı ülkelerde olması durumunda mahkemede hak aramak daha da zordur. Aynı ülkede yaşanan olaylarda aynı firmanın benzer şekilde ayıplı ürün sattığı kanıtlanır ise mahkeme suçlu bulabilir.

Taklit ürün gönderilmesi: Bir satıcının web sayfasında asıl ürünü sergileyip müşteriye taklidini göndermesi açıkça dolandırıcılıktır. Bu tür satıcıların e-ticaret sitesi kurmaktaki amaçları dolandırıcılıktır. Dolayısıyla bunlar ile hukuk yolu kullanılarak başa çıkmak zordur. Firmalarını kısa süre sonra kapatıp yeni adla yeni e-ticaret sitesi açarlar.

Eksik ürün gönderilmesi: Eksik ürün gönderen satıcılar içinde aynı değerlendirmeyi yapabiliriz.

Sahte ürün gönderilmesi: Disk yerine demir kütle, ilaç yerine kireç tozu gönderen firma için dolandırıcılık sıfatı bile yetersiz kalır.

Müşterileri bu tür yerlerden alışveriş yapmaya yönelten nedenler;

1- Fiyatlarının her yerden ucuz olması;

2- Başka yerlerde bulamadıkları ürünleri buralarda bulmalarıdır.

Müşteri ürünün ucuz olmasının bir nedeni olduğunu düşünmelidir. Bu arada satıcı konusunda Genelağ'da araştırma yapmasında yarar vardır. Başka yerlerde satılmayan bir ürünün bu tür sitede bulunmasının iki nedeni olabilir: Ya bu ürünün yasal olarak satışı yoktur ya da satıyoruz dedikleri ürün sahtedir.

E-ticaretteki Etik ve Hukuk Sorunları-III

Müşterinin Güvenilirliği

Müşteri kılıklı kişilerin satıcıları dolandırdıkları da görülmektedir. Hatta bu tür dolandırıcılıkları örgütlü biçimde yapanlar da vardır. Örneğin Genelağ'daki banka dolandırıcılığı eylemlerinin bazıları örgütler tarafından yapılmaktadır. Bunlarda karşı önlemleri satıcı firmaların almaları gerekir. Soygun amaçlı örgütler genellikle bulundukları ülkenin dışında bu tür soygunları yapmaktadırlar. Böylece yasalardan kaçabilmektedirler.