E-Ticaret Güvenliği

Rahmetullah Yiğit[1], Şerif Bahtiyar[2]

[1] İstanbul Teknik Üniversitesi, Bilgisayar Mühendisliği Bölümü, Ayazağa, İstanbul

[2] Progress Ar-Ge Merkezi, Provus Bilişim Hizmetleri A.Ş., Şişli, İstanbul

yigitrahmetullah@gmail.com , serif.bahtiyar@provus.com.tr

Özet: E-Ticaret, mal veya hizmetlerin Internet veya diğer bilgisayar ağları gibi elektronik sistemler üzerinden alınıp satıldığı bir iş koludur. Özellikle son on yılda Internet kullanımının yaygınlaşması ve bilgisayar sistemlerinin daha kolay ulaşılabilir hale gelmesiyle e-Ticaret sektörü çok ciddi bir büyüme gösterdi. Artık neredeyse her türlü ürün ve hizmete elektronik yollarla ulaşılabiliyor. Bütün bankacılık işlemleri, bankaların Internet şubeleri üzerinden gerçekleştirilebiliyor. Ancak e-Ticaret uygulamalarının ortaya çıktığı ilk günlerden beri bu tür uygulamalar doğası gereği bilgisayar güvenliğine yönelik tehditlerin hedefi oluyor ve önemli bir müşteri kitlesi güvenlik endişeleri ile e-Ticaret hizmetlerini kullanmaktan kaçınıyor. Bu nedenle bu alandaki güvenlik politikaları ve uygulanmaları özel önem kazanıyor. Bu çalışmamızda, e-Ticaret uygulamalarında görülen genel güvenlik sorunlarını inceledik ve bunlara karşı olası çözüm yöntemlerine işaret ettik.

Anahtar Sözcükler: E-Ticaret, Güvenlik, Bankacılık.

E-Commerce Security

Abstract: Computer networks like the Internet have been a new commerce platform called e-commerce that is increasingly used to exchange goods and services for several decades. Particularly, e-commerce has attracted more people than ever and it has grown faster with the pervasive usage of the Internet and the availability of low cost computing equipments. Almost all financial operations and exchanges of goods have been carried on the electronic medium, such as payments by using online banking operations. On the other hand, e-commerce has been a target of attackers to make use of the electronic platform for malicious purposes since its invention. This circumstance makes some people suspicious about e-commerce and prevents them to use e-commerce services. Therefore, security is a significant issue to improve e-commerce. In this paper, we investigate security challenges and potential solutions related to e-commerce.

Keywords: E-Commerce, Security, Banking.

1. Giriş

Internet erişimi ve kullanımı dünyada hızla yaygınlaşıyor [1]. İstatistiklerine göre dünya genelinde Internet'in kullanıcı sayısı 2,4 milyarın üzerindedir [8]. Ülkemizde ise 35 milyonu aşmış durumdadır [8]. Bu kullanıcılar aynı zamanda e-ticaret uygulamalarının potansiyel müşterisi durumundadır. Bu kadar çok insanın e-ticaret'in yapması için e-ticaret uygulamalarına güvenmesi gerekir. Dolayısıyla, güveni sağlamak için e-ticaret uygulamalarında güvenlik çok önemli bir konudur. E-ticarette kullanılan varlıkların (kredi kartı numarası, para vs.) değerli olması da bu alandaki güvenliği ayrıca önemli kılıyor.

E-Ticaret genellikle Internet'le bütünleşmiştir. Bu nedenle e-ticarete yönelik tehditler genellikle izinsiz erişim (unauthorized access), veri bütünlüğünün bozulması (integrity violation) gibi Internet ve ağ güvenliği ile ilgili sorunları kapsıyor [2, 3]. Bundan dolayı, değerli varlıların korunması ve müşteri güveninin sağlanması için e-ticaret uygulamalarının güvenliği oldukça ciddi konudur.

Bu çalışmamızda, ikinci bölümde Internet ortamındaki genel güvenlik sorunlarını inceledik. Daha sonraki bölümde, e-ticarette güvenlik tehditlerini açıkladık. Dördüncü bölümde genel güvenlik önlemlerini sunduk. Son bölümü de sonuç ve önerilere ayırdık.

2. Genel Güvenlik Sorunları

Bir sistemin güvenli sayılabilmesi için sahip olması gereken üç temel özellik şunlardır, gizlilik, bütünlük ve erişilebilirliktir. Bunlara ek olarak gerçeklik ve izlenebilirlik bazı sistemler için zorunludur.

Gizlilik, e-ticaret açısından kullanıcının işlem sırasında kullandığı değerli bilgilerin ve kişisel bilgilerin başkaları tarafından görülmemesi şeklinde tanımlanabilir. Gizliliğin sağlanmaması müşterinin maddi kayba uğramasına veya kişisel bilgilerinin istenmeyen kişilerin eline geçmesine neden olabilir.

Bütünlüğün korunması için sistem sağlayıcı veya başka bir kötü amaçlı yazılım veya kişinin kullanıcının bilgilerini isteğin dışında değiştirmemesi gerekir.

Erişilebilirlik, servis sağlayıcının veya verinin erişime kapanmaması şeklinde tanımlanabilir. Güvenlik önlemleri sisteme veya veriye erişimi engellememelidir.

Gerçeklik, söz konusu varlığın ya da özelliğin orijinal, doğrulanmış ve güvenilir olmasını gerektirir.

İzlenebilirlik ise varlığın hareketlerinin ve gerçekleştirdiği işlemlerin takip edilebilir olmasını gerektirir.

3. E-Ticaret Güvenlik Tehditleri

3.1 Müşterinin Kandırılması

Saldırganlar genellikle kullanıcı adı ve şifre gibi kullanıcıya ait hassas bilgileri hedef alırlar. Bu bilgiler ile sunucu veri tabanlarına erişerek kullanıcı hakkında daha fazla bilgiyi ele geçirmeleri veya kullanıcı adına işlem yapmaları mümkündür. Eğer bilgileri ele geçirilen kullanıcı sistemde yönetici yetkilerine sahipse hasar daha büyük olabilmektedir.

Kullanıcıların bilgilerini ele geçirmek için çeşitli aldatma teknikleri kullanılmaktadır. Gönderilen sahte e-postalar ile kullanıcılardan çeşitli bahanelerle kullanıcı bilgileri istenmektedir. Sosyal medya kullanımın yaygınlaşmasından sonra bu saldırganlık tipi de sosyal medya uygulamalarına taşınmış, kullanıcı bilgileri genellikle kullanıcılara tanıdıkları biri veya güvendikleri bir uygulama tarafından gönderilmiş gibi yapılan sosyal medya mesajları ile hassas bilgileri istenmeye başlamıştır.

Bazı durumlarda teknik bilgisi yüksek saldırganlar kullanıcının hâlihazırda kullanmakta olduğu bir e-ticaret uygulaması ara yüzünün kopyasını geliştirmekte, kullanıcılar bu kopya sayfalara yönlendirilip orijinal sisteme giriş yaptığını düşündürülerek kullanıcı bilgileri ele geçirilmektedir.

3.2 Ağ ve Internet Güvenliği İhlalleri

E-ticaret uygulamaları genellikle Internet üzerinden servis sağlamaktadır. Bu nedenle, operasyonun tarafları arasındaki veri alış-verişi Internet'te çeşitli bilgisayar ağları üzerinden geçmektedir be bu ağların çoğunluğu hem servis sağlayıcının hem de kullanıcının bilgi ve kontrolü dışında bulunan güvensiz ağlardır. Bu güvensiz ağlarda veri ağ dinlemesine maruz kalabilir ve bu şekilde istenmeyen kişilerin eline geçebilir.

3.3 Servis Sağlayıcıya Yapılan Saldırılar.

Saldırılar sadece kullanıcıyı veya iletişimi değil servis sağlayıcıyı da hedef alabilir. Bu tür saldırılar çok sayıda kullanıcının verisi bulunan sistemleri hedef aldığı için daha tehlikelidir.

Hizmeti Engelleme Saldırıları (Denial of Service Attacks - DoS) servis sağlayıcıyı hedef alan, veri çalmaktan çok sistemin erişilebilirliğini hedefleyen saldırılardır [4]. 199 yılında Minessota Üniversitesine yönelik saldırıda 300 civarında bilgisayar sisteminden 10 dakika içerisinde 2 milyonun üzerinde paket gönderilerek üniversitenin servis sağlayıcıları bloke edilmiştir [1]. Bu gün gelişen teknolojiler ile bu rakamlar çok daha yukarılara çıkabilmekte, servisler uzun süre iş göremez hale getirilebilmektedir. Bu tür saldırılar ile servis sağlayıcıya bir veya birden fazla bilgisayar kullanılarak çok sayıda istek gönderilerek gerçek kullanıcılardan gelen istekleri bloke etmeye çalışılır. Bu şekilde hem servis sağlayıcı maddi zarara uğrar hem de istemci işlemini zamanında gerçekleştirememiş olur.

Servis sağlayıcılar virüsler ve Truva atları (Trojan horse) ile direk olarak da hedef alınabilirler. Servis sağlayıcıya bulaşan bir virüs sitemdeki verinin bütünlüğünü bozabilir. Daha da tehlikelisi virüsler servis sağlayıcıdan kullanıcılara yayılabilirler. Örneğin, Asprox virüsü etkilenen servis sağlayıcıdaki web sayfalarını ziyaret eden bütün sistemlere bulaşabilir.

Truva atları, istenen bir hizmeti yerine getirir gibi görünürken diğer yandan sistemin güvenliğine zarar veren zararlı programları tanımlamak için kullanılır. Truva atları uzaktan erişim, veri bütünlüğünün

bozulması, FTP ve e-posta gibi servisleri ele geçirmek veya izlemek, güvenlik yazılımlarını servis dışı bırakmak için kullanılabilir.

Servis sağlayıcıya yönelik bir başka saldırı çeşidi de veri tabanına yönelik saldırılardır. Bu saldırılara örnek olarak SQL-Injection saldırılarını gösterebiliriz. Bu saldırılarda, kullanıcı tarafından gönderilen girdiler ile servis sağlayıcı veri tabanında değişiklik yapılmaya çalışılır.

4. Genel Güvenlik Önlemleri

4.1 Güçlü Güvenlik Politikası

Bir sistemin güvenliğini sağlamanın ilk ve en önemli adımı sağlıklı bir güvenlik politikası ortaya konulmasıdır. Sisteme ilişkin riskler iyi bir şekilde anlaşılmalı ve risklere karşı gerekli tüm önlemleri kapsayan bir güvenlik politikası oluşturulmalı, gerekli güvenlik yazılımları bu politika doğrultusunda gerçeklenmelidir.

4.2 Eğitim

Bilgisayar güvenliğin her alanında eğitim en hassas unsurudur. Bütün diğer güvenlik önlemleri başarı ile uygulansa dahi kullanıcı bilgisizliği güvenlik ihlallerine sebep olabilir.

Kişiler, sahibi oldukları uygulamanın güvenlik ihtiyaçlarını ve sektördeki genel güvenlik risklerinin farkında olmalıdır. Kurumlar, yapılarını oluştururken ve uygulamayı geliştirecek yazılım ekiplerini kurarken bu güvenlik ihtiyacını karşılayabilecek yetkinlikte kişileri tercih etmelidir.

Geliştiriciler sistemler için güçlü güvenlik politikaları geliştirebilecek ve bu politikaları başarıyla gerçekleyebilecek teorik ve pratik bilgiye sahip olmalı, bunun yanında geliştirecekleri uygulamaya ilişkin güvenlik risklerini bilmelidir.

Kullanıcılar Internet veya e-ticaret ortamında bilgilerinin gerekli önlemler alınmadığı takdirde güvende olmayacağını bilmelidir. Operasyondaki personel kendi tarafları ile ilişkili basit ancak etkili önlemleri bilmeli ve bu önlemleri uygulayabilecek temel bilgiye sahip olmalıdır.

4.3 Şifreleme

Yukarıda bahsedildiği gibi e-ticaret uygulamalarında veri alış-verişi genellikle Internet üzerinden gerçekleşmektedir. Bu güvensiz hat üzerindeki iletişimi güvenli hale getirmenin en önemli ayağı şifrelemedir. Genel olarak şifreleme metotları ikiye ayrılır, gizli anahtar ile şifreleme ve açık anahtar ile şifrelemedir.

E-ticaret ve daha genel olarak web uygulamaları için açık anahtar ile şifrelemeye dayalı yaygın bir metot olarak SSL (Secure Sockets Layer – Güvenli Giriş Katmanı) kullanılmaktadır. Bu şekilde iletişim ağ dinlemeye karşı güvenli hale getirilmektedir.

Netscape tarafından 1994 yılında geliştirilen SSL protokolü web tarayıcısı ile servis sağlayıcı arasında açık anahtar tabanlı şifrelenmiş güvenli bir bağlantı sağlar. SSL protokolü web tarayıcı ile servis sağlayıcı arasındaki işlemin güvenliğini garanti eder [3]. Bu gün yeni sürümleri ile birlikte SSL, TLS (Transport Layer Security) olarak adlandırılmaktadır.

4.4 Güvenlik Duvarları ve İhlal Algılama ve Önleme Sistemleri

Güvenlik duvarları (Ateş Duvarı - Firewall) bir bilgisayara gelen ve giden trafiği izleyerek tanır ve gerektiğinde engelleyen bilgisayar programlarıdır [4]. Güvenlik duvarları gerçeklenirken iletişimin hangi durumlarda engelleneceği ya da izin verileceği belirlenerek program bu kurallar doğrultusunda gerçeklenir. Güvenlik duvarları servis sağlayıcıların hizmet engelleme saldırılarına karşı korunmasında ve kullanıcının kişisel bilgisayarının güvenliğinin sağlanmasında kullanılabilir.

İhlal algılama sistemi (Intrusion Detection System) sistem güvenliğinde bir açık meydana geldiğinde bunu tespit etmeyi hedefleyen sistemlerdir. İhlal önleme sistemleri (İntrusion Prevention System) ise bu ihlalleri engellemek, durdurmak ve raporlamak için geliştirilmiş sistemlerdir.

Günümüzde bütün bu sistemleri içinde servis olarak barındıran modern bütünleşmiş güvenlik yazılımları mevcuttur. Bu tür yazılımların kullanımı her servis sağlayıcı hem de müşteri tarafında riskleri azaltacaktır.

4.5 Veri Tabanı Güvenliğine Yönelik Önlemler

Veri tabanlarına yönelik en önemli saldırılar SQL-Injection saldırılarıdır. Bu tür ve benzer saldırılara önlem almak için kullanıcı tarafından sağlanan girdilerin kontrol edilmesi gerekmektedir. Kullanıcıdan gelen verinin veri tabanında bir hasar ya da istenmeyen bir değişikliğe neden olup olmayacağını kontrol etmek için verideki karakterler, kelimeler ve işaretler incelenerek belli sorgu ve

işaretler engellenebilir. Örneğin, SQL veri tabanında "DROP DATABASE" ifadesi içeren sorguların gönderilmesini engellemek için bu iki kelimeyi içeren girdiler yasaklanabilir.

Veri tabanlarına yönelik saldırıları engellemek için çeşitli yöntem ve algoritmalar mevcuttur.

5. Sonuç ve Öneriler

Güvenli bir e-ticaret operasyonu için en az aşağıdaki şartların sağlanması gerekir:

Güvenilir Servis Sağlayıcı: Kullanıcılar hizmet aldıkları ve kişisel bilgilerini verdikleri, üzerinden para ve kaynak transferi gerçekleştirdikleri servis sağlayıcının güvenliğinden emin olmalıdır. Bunun için servis sağlayıcın sistem ve veri tabanı güvenliğine dair gerekli sistemlere sahip olması gerekmektedir.

Güvenli İletişim: Haberleşmenin iki tarafı arasındaki iletişim üçüncü tarafların erişimine karşı korumalı olmalıdır. Bunun için iletişimin şifrelenmesi en basit ve etkili yöntemdir. Şifreleme için artık bir endüstri standardı haline gelmiş olan SSL kullanımı minimum gereksinim olmalıdır. Bunun dışında başka güvenli iletişim metotları kullanılabilir.

Güvenli İstemci: Servis sağlayıcıya isteğin gönderildiği sistemin güvenliği de şarttır. Bu sistem yine zararlı yazılımlara karşı gerekli araçlarca korunmalıdır.

Bütün bunların yanında sistem güvenliği en üst düzeyde tutulsa dahi operasyonun her tarafında yer alan iş sahipleri, geliştiriciler ve en önemlisi kullanıcılar e-ticaret güvenliği ve olası riskleri hakkında bilgi sahibi olmalıdır. Zira kullanıcının basit şifre seçimi dahi tek başına bütün güvenlik önlemlerini devre dışı bırakabilerek zarara neden olabilir.

Teşekkür

Bu çalışma EUREKA ITEA2 projesi ADAX (proje no. 10030) ve TEYDEB projesi AKFİS (proje no. 1130018) tarafından desteklenmiştir.

6. Referanslar

[1] Randy C. Marchany, Joseph G. Tront, " E-Commerce Security Issues", **Proceedings of the 35th Hawaii International Conference on System Sciences,** (2002).

[2] Dai, W., Wei, J., " Research on the Security of an improved E-commerce Model", **2010 International Conference on E-Business and E-Government**, (2010).

[3] Jie, Z., Hong, X., "E-Commerce Security Policy Analysis", **2010 International Conference on Electrical and Control Engineering**, (2010).

[4] Matbouli, H., Gao, H., "An Overview on Web Security Threats and Impact to E-Commerce Success", **International Conference on Information Technology and e-Services**, (2010).

[5] McCole, P., Ramsey, E., Williams, J., "Trust considerations on attitudes towards online purchasing: The moderating effect of privacy and security concerns", **Journal of Business Research 63,** (2010).

[6] Kumar, P. A. R., Selvakumar, S., "Distributed denial of service attack detection using an ensemble of neural classifier", **Computer Communications 34,** (2011).

[7] Tian, Z., Xu, N., Peng, W., "E-commerce Security: a Technical Survey", **Second International Symposium on Intelligent Information Technology Application**, (2010).

[8] "World Internet Users Statistics Usage and World Population Stats.", (28 Dec. 2013) http://www.internetworldstats.com/stats.htm.