GÜVENLİK UYGULAMALARINDA KULLANICI FARKINDALIĞI: BİR DURUM ÇALIŞMASI

[1]Atila Bostan
[1]Bilgisayar Mühendisliği Bölümü, Atılım Üniversitesi, Ankara
e-posta: abostan@atilim.edu.tr

Abstract

Existing server authentication mechanisms in secure web transactions rely heavily on user judgment. Although the usage of server side digital certificate provides significant means for server authentication, the protocol depends on the user's decision in SSL applications.

In this study, with a web phishing application in Atılım University we try to distinguish the rationale for the question "why people behave so careless in SSL server authentication process" and attempted to observe if technical education is sufficient in shaping the user conducts.

With the help of the findings in phishing application, the efficiency of web browsers' security warnings and current user habits are discussed. Several security advices are presented to improve browser-user interaction in reaching and maintaining a secure web communication.

Keywords: Security in server-side SSL, user awareness in IT security, pishing.

1. Giriş

Otomatik veri işleme tekniklerinden faydalanarak iş süreçlerinin geliştirilmesi ve modernizasyonu, bilgisayar ağlarını kullanmayı neredeyse alternatifsiz bir teknoloji haline getirmiştir. Günümüzde orta ve büyük ölçekli firmalar hem kendi iş süreçlerinin idaresi ve takibi için hem de müşterilerine verdiği hizmeti ve tanıtımı yaygınlaştırabilmek için bilgisayar ağlarından faydalanmaktadır. Her ne kadar sadece firma/kurum içi bilgisayar ağı kullanımı mümkün olsa da firma dışı sistemler ile entegrasyon, İnternet gibi çok yaygın bir ağın sağladığı ortam ve hizmetlere ulaşma ihtiyacı (firma/kurum fonksiyonlarını etkin olarak yerine getirebilmek için), İnternet ağına çevrim-içi erişmeyi gerektirmektedir. İnternet gibi genele açık ve kontrolü zor bir ortama bağlantı kurmak şüphesiz beraberinde bir çok güvenlik ihtiyacını da gündeme getirmektedir. Bu güvenlik ihtiyaçları temelde iki gruba ayrılabilir. Birinci ve öncelikli güvenlik ihtiyacı firma/kurum sistem ve verilerini zararlı uygulamalardan (bunlar kötü niyetli şahıslar tarafından veya bilgisiz kullanıcılar tarafından gerçekleştirilebilir) korunması, hizmet aksaması veri kaybı veya bozulmasına meydan verilmemsidir. İkinci güvenlik ihtiyacını ise firma/kurumun diğer sistemler ile olan tüm iletişiminin ve veri aktarma işlemlerinin güvenilir (dinlenemez, değiştirilemez ve kesintiye uğratılamaz) şekilde yapılması oluşturmaktadır.

Bilgisayar ağlarında güvenliğin sağlanması konusu sadece ağ ortamının (iletişim ortamı) yeterli güvenlikte olması konusunu içermemektedir. Çünkü ağ üzerinde çalışan bilgisayar sistemlerinde ve kullanıcı davranışlarında olan güvenlik zafiyetleri bilgi ve sistemlere zarar verebilecek uygulamalar için ortam yaratabilmektedir. Bilgisayar sistemlerinde ve iletişim ortamlarında sağlanması beklenen güvenlik gerekleri çoğunlukla teknik olmakla birlikte, sistem kullanıcılarının davranış boyutu psikolojik, sosyolojik ve örgütsel-kültür gibi teknik olmayan hususları da içermektedir. Her ne kadar insan davranışlarının şekillendirilmesi ve değiştirilmesinde eğitim önemli bir araç olsa da tek başına yeterli olmadığı durumlarla sıklıkla karşılaşılmaktadır. Daima göz önünde tutulması gereken bilgisayar ağlarında güvenliğin birbirine geçmiş bir çok sistemin uyum içerisinde çalışması ile sağlanabileceğidir. Unutulmamalıdır ki "Bir zincir en zayıf halkası kadar güçlüdür."

Bu çalışmada sistem, ağ ve kullanıcı olarak üç sınıfa böldüğümüz güvenlik alt unsurlarından, kullanıcı davranışları sorgulanmıştır. Atılım Üniversitesi içerisinde yapılan bir ağ güvenlik saldırısına kullanıcıların verdiği tepkiler incelenmiş ve kullanıcı davranışlarının nedenleri araştırılmıştır. Takip eden bölümde web hizmeti sunumunda SSL tekniği ve bu tekniğin sağladığı güvenlik kazanımları konusunda bilgi verilmektedir. Daha sonra, yapılan güvenlik saldırısının yapılma şekli ve uygulanan yöntem konusunda bilgi verilmekte ve bu saldırıya karşı kullanıcıların davranışları incelenerek nedenleri yorumlanmaktadır. Sonuç bölümünde ise kullanıcı davranışlarının daha güvenli hale gelebilmesi için görüş ve öneriler belirtilmiştir.

2. HTTP İletişim Güvenliğinin Sağlanmasında SSL Tekniği

Hiper Metin Aktarım İletişim Protokolünde (Hyper Text Transport Protocol-http) kullanıcı bilgisayarı ile sunucu arasındaki iletişimin güvenli şekilde yapılabilmesi için kullanılan tekniklerden birisi de SSL (Secure Sockets Layer)'dir. SSL aslında IETF (Internet Engineering Task Force) tarafından onaylanan gönderim katmanı seviyesi güvenlik protokolü [1] (Transport Layer Security-TLS)'nün bir uygulamasıdır. SSL Netscape firması tarafından geliştirilmiştir. SSL protokolünün en güncel sürümü SSL V3.0'dır ve tanımlaması [2]'de verilmiştir. SSL protokolü kullanıcı ve sunucuların kimliklerinin doğrulanmasını ve bu iki bilgisayar

arasındaki iletişimin üçüncü şahıslar tarafından anlaşılamamasını temin etmektedir.

SSL tekniği iletişim güvenliğinin sağlanmasında Açık Anahtar Altyapısı (Public Key Infrastructure-PKI) ve sayısal sertifika yönetim esaslarından faydalanmaktadır. Sayısal sertifikalar sunucu ve kullanıcının kimliklerini doğrularken PKI açık anahtarlarının karşıdaki bilgisayara iletilmesinde kullanılmaktadır. İletişimin şifrelenmesi ise, hesaplama sürati kazanımı sebebiyle, simetrik bir anahtar ile yapılmaktadır. Ancak, her oturum için yeniden belirlenen simetrik anahtarın kullanıcı-sunucu arasında güvenli şekilde iletilmesinde, sayısal sertifika içerisinde bildirilen karşı bilgisayar açık anahtarı kullanılmaktadır. Bu çalışmada SSL iletişimi sunucu tarafı sayısal sertifikası seçeneği ile kullanıldığı için takip eden bölümde bu tekniğin detayları hakkında bilgi verilmektedir. İlgilenen okuyucular sunucu ve kullanıcı sayısal sertifikası kullanımı detayları için [2]'i ve bu çalışma kapsamında yer almayan SSL kullanıcı tarafı sayısal sertifikası kullanımı güvenlik açıkları için [3]'ü inceleyebilirler.

Sayısal sertifika ile kimlik doğrulamanın temelinde, iletişimde bulunan bilgisayarların güvendikleri üçüncü bir unsurun varlığı yatmaktadır. Bu güven duyulan unsur, sunucu bilgisayarın kimliğini (İnternet ortamında bilgisayar kimliği onun DNS kayıt ismi olarak ele alınmaktadır) garanti altına alan bir sayısal sertifika üretir. Üretilen bu sayısal sertifikanın güvenliği ise sertifika üreticisinin (güven duyulan unsur) sayısal imzası ile sağlanmaktadır. SSL iletişiminde sunucu bilgisayar, kullanıcı bilgisayarının da güvendiği bir otoriteden almış olduğu ve içerisinde kendi DNS kayıt isminin olduğu sertifikayı kullanıcı bilgisayarına iletir. Kullanıcı bilgisayarı aldığı bu sertifika üzerinde bir dizi kontrol işlemi yapar. Öncelikle bu sertifikanın kendisinin güvendiği bir otoriteden alınıp alınmadığını ve sertifika içerisindeki imzanın tutarlılığını kontrol eder. Daha sonra yine sertifika içerisinde belirtilen geçerlilik süresinin dolup dolmadığına bakar. Bu kontrolü takiben, sertifika üreticisi tarafından yayımlanan sertifika iptal listesine, yine sertifika içerisinde belirtilen adresten, ulaşarak bu sertifikanın herhangi bir sebeple sertifika otoritesi tarafından iptal edilip edilmediğini kontrol eder. Bütün bu kontrollerin olumlu sonuçlanması durumunda, kullanıcı bilgisayarı kendisinin ulaşmak istediği bilgisayar adı (İnternet DNS kayıt adı) ile sertifika içerisinde belirtilen bilgisayar kimliğinin aynı olup olmadığını kontrol eder. Böylece irtibat kurmuş olduğu sunucu bilgisayarın kendisinin ulaşmak istediği bilgisayar olduğunu güvendiği bir otoritenin garantisi altında doğrulamış olur.

İletişim güvenliğinin sağlanması ise, irtibat kurulan sunucunun ulaşmak istenen sunucu olduğunun onayını müteakip, şifreli iletişimin kurulması aşamasına geçilir. Kullanıcı bilgisayarı sunucu tarafından kendisine iletilen sayısal sertifika içerisinde sunucu bilgisayarının PKI açık anahtarını da almış durumdadır. Kullanıcı bilgisayarı sadece aktif olan oturumda geçerli olacak ve karşılıklı olarak mesajların şifrelenip açılmasında kullanılacak simetrik şifreleme anahtarını üretir ve bu anahtarı sayısal sertifika içerisinde bildirilmiş olan sunucu açık anahtarı ile kapatarak sunucuya gönderir. PKI matematiği gereği bir açık anahtar ile şifrelenen mesaj, ancak o açık anahtarın karşılığı olan kişisel anahtar ile açılabilmektedir (burada hesaplama gücü ve hesap için gereken zaman önemli parametrelerdir). PKI anahtarlarının kullanımı ve sağladığı güven konusunda detaylı bilgi [4,5]'ten edinilebilir. Böylece kullanıcı bilgisayarı tarafından üretilen simetrik anahtarın sunucuya güvenli şekilde iletilmesi sağlanmış olur. Bu aşamadan sonra oturum sonuna kadar tüm trafik bu simetrik anahtar aracılığı ile şifrelenir ve çözülür.

Değişik web tarayıcıları ve bu tarayıcıların faklı sürümlerinde aynı olmamakla birlikte, kullanıcı bilgisayarı ile sunucu arasında başarılı şekilde kurulan bir SSL iletişimi genellikle web tarayıcılarında durum çubuğunda veya adres satırı yanında kilit sembolü ile gösterilir.

3. Uygulama

Bu çalışma kapsamında bilgisayar kullanıcılarının güvenlik uygulamalarına karşı hassasiyetleri ve bilgi güvenliği ile ilgili kurulan sistemlerin günlük hayatta kullanılma şekillerini incelemek üzere bir web pishing (bilgi çalma/yemleme) uygulaması yapılmıştır. Uygulama Atılım Üniversitesi içerisinde gerçekleştirilmiştir.

Uygulamada hedeflenen; güvenli web iletişimi için kullanılan SSL altyapısının ve bu altyapının dayandığı güvenlik sistemlerinin günlük hayatta nasıl kullanıldığının ortaya konması olmuştur. Bu amaçla, uygulamada güvenlik saldırısının hedef kitlesi olarak üniversitenin Bilgisayar, Yazılım ve Bilişim bölümlerinde öğretim elemanı ve öğretim görevlisi olarak çalışmakta olan personelin bir kısmı seçilmiştir (yabancı uyruklu personel uygulama dışı bırakılmıştır). Hedef kitlenin bu bölüm öğretim elemanlarından seçilmesinin sebebi, karşılaşılacağı umulan güvenlik ihlallerinin teknik bilgisizlikten kaynaklanma olasılığını en aza indirmektir. Seçilen üç bölüm öğretim elemanlarının SSL güvenlik uygulamaları ve kullandıkları web tarayıcısının güvenlik uyarı mesajlarına aşina oldukları varsayılmıştır.

Web pishing uygulamasında taklit edilecek web sitesi olarak, üniversite öğrenci bilgi sistemi seçilmiştir. Öğretim elemanları bu siteye kendilerine tahsis edilmiş olan kullanıcı adı ve şifre ile giriş yapmakta ve iletişim, sunucu tarafı sayısal sertifikası kullanan SSL uygulaması ile güvenlik altına alınmaktadır. Üniversitemizde kullanılmakta olan bu sitenin uygulama için seçilmesinin en önemli sebebi ise site sunucusu tarafından kullanılan sayısal sertifikanın uygun olmayan kullanımı nedeni ile güvenlik uyarı mesajlarının oluşturduğu duyarsızlıktan faydalanmaktır.

Öğrenci bilgi siteminde kullanılan sunucu sertifikası, öncelikle site DNS adını tanımlamak için üretilmemiş, bilgi sistemleri sistem yöneticilerinden birisinin adına (şahıs adına) üretilmişti. Dolayısıyla, siteye ulaşmak isteyen tüm web tarayıcıları bir sertifika uyarısı

vermekteydi. Kullanıcılar için de bu sitede web tarayıcılarının sertifika hatası vermesi kanıksanmış bir durumdu.

Yapılan güvenlik saldırısında okul elektronik posta sunucusu üzerinden hedef kullanıcılara bir sahte elektronik posta gönderilerek, bu posta içerisine konan bir bağlantı aracılığı ile öğrenci bilgi sistemine giriş yaparak sistemi ve kullanıcı adı-şifre'lerini test etmeleri talep edilmiştir. Hedef kullanıcılara gönderilen elektronik posta, böyle bir talebi yapması çok kuvvetli olan üniversite bilgi işlem müdürünce gönderilmiş gibi gösterilmiştir. Ayrıca, posta metni içeriğinde oldukça resmi bir ifade kullanılarak yapılan talebin inandırıcılığı artırılmıştır. Elektronik posta içerisindeki bağlantının kullanıcıları yönlendirdiği bilgisayarda ise orijinal öğrenci bilgi sistemi giriş sayfasının bir koyası yaratılarak SSL üzerinden yayımlanmıştır. SSL hizmet uygulamasında, sunucu tarafı sayısal sertifika kullanımı (orijinal öğrenci bilgi sistemi hizmetinde olduğu gibi) seçeneği uygulanmıştır. Ancak, orijinal öğrenci bilgi sisteminin kullanmakta olduğu hatalı sertifika kullanılabilecek olmasına rağmen, kullanıcıların bu sertifikayı da kontrol edip etmediklerini incelemek amacı ile tamamen farklı bir sayısal sertifika üretilmiş ve SSL uygulamasında sunucu bilgisayar sertifikası olarak kullanılmıştır. Sahte web sitesine ulaşarak giriş yapan kullanıcıların kullanıcı adı ve şifreleri kaydedilerek, takip eden işlemler için orijinal sitenin kullanılması (sahte sunucu aracılığı ile) sağlanmıştır.

Uygulamada saldırı hedefi olarak 16 öğretim elemanı seçilmiştir. Bu personelin üniversite elektronik posta sunucusundaki posta adreslerine göndericisi değiştirilmiş bir elektronik posta gönderilmiş ve öğretim elemanlarının bu posta içerisindeki bağlantı aracılığıyla sahte web sitemize giriş yapmaları beklenmiştir. Elektronik postanın gönderilmesinden itibaren üçüncü gün mesai saati bitiminde uygulamaya son verilmiştir. Elektronik posta gönderilen 16 öğretim üyesinden 11'i sahte siteye giriş yaparak kullanıcı adı ve şifreleri tarafımızdan öğrenilmiştir. Üç gün içerisinde siteye giriş yapmayan 5 öğretim elemanının 4'ü elektronik postayı hiç açmamış, birisi ise varsayılan web tarayıcısının MS Internet Explorer olmaması sebebi ile posta içerisindeki bağlantıya ulaşmaya çalıştığı halde hizmete ulaşamamıştır (bu orijinal öğrenci bilgi sisteminde de böyledir. Sadece MS IE tarayıcıları ile siteye ulaşılabilmektedir). Üçüncü gün sonunda sahte web sitemize ulaşarak kullanıcı adı ve şifrelerini öğrendiğimiz öğretim elemanlarına yapılan uygulama konusunda bilgi verilmiş ve sistemdeki şiflerini değiştirmeleri istenmiştir.

4. Değerlendirme

Kullanıcıların güvenlik konusunda eğitilmiş olması otomatik bilgi işleme ve iletişim sistemlerinde güvenliğin sağlanmasında önemli bir noktadır. Zira, kullanıcının içinde yer almadığı bir güven mekanizması henüz oluşturulamamıştır. SSL protokolü ile sağlanmaya çalışan güven modelinde de kullanıcı önemli bir unsur olarak yer almaktadır [6]. Ağ ve bilgi sistemi kullanıcılarına güvenlik eğitimi verilmesi, güvenlik politikası oluşturulması ve güvenlik tedbirleri geliştirilmesinin önemi, ayrıca bir farkındalık yaratılmasının gerekliliğine Sukhai tarafından dikkat çekilmektedir [7]. Sadece kullanıcıların değil, lisans seviyesinde bilgi teknolojileri eğitiminde de güvenlik eğitimine önem verilmesi ve güvenlik eğitiminin sadece teknik boyutları değil teknik olmayan boyutlarını da içerek şekilde yapılanması gerektiği Yang tarafından belirtilmektedir [8]. Bütün bu çalışmaların dikkat çekmek istediği nokta bilgi sistemlerinde güvenlik eğitiminin ayrı bir boyut olduğudur. Ancak güvelik gereklerini ve tekniğin nasıl uygulanacağını bilmek kullanıcı davranışlarının her zaman güvenli sınırlar içerisinde olacağını garanti etmemektedir. Mevcut uygulamalar ve alışkanlıklar bazen bilgi ve mantıklı davranışların önüne geçebilmektedir.

Yapılan uygulama sonuçlarının hedef kullanıcılar ile paylaşılması esnasında, öğretim elemanlarının SSL sayısal sertifikasının kullanım tekniği ve sağladığı güvenlik konusunda bilgileri değerlendirilmiş, maruz kaldıkları güvenlik saldırısına neden engel olmadıkları incelenmiştir.

Kullanıcı adı ve şifresi elde edilen öğretim elemanlarından 9'unun SSL tekniği ve sayısal sertifikaların kullanımı konusunda yeterince bilgi sahibi oldukları öğrenilmiştir. Bu personelden sadece 2'si SSL'in güvenli bir web iletişimi sağladığını bildikleri ancak sayısal sertifikanın kullanım şekli ve güvenlik sağlama mekanizmasını bilmediklerini belirtmişlerdir. Bu çalışma kapsamında elde edilen sonuçlar dikkate alındığında, teknik eğitimin güvenliğin sağlanmasında tek başına yeterli olamadığı, kullanıcı davranışları ve alışkanlıkların belirleyici faktör olduğu belirlenmiştir. Çünkü, kullanıcı adı ve şifresi öğrenilen 9 öğretim elemanı sayısal sertifika kullanımı konusunda teknik bilgiye sahip olmalarına karşılık, web tarayıcılarının verdiği sertifika uyarı mesajlarını önemsemeden işlemlerine devam etmişler ve güvenlik saldırısının başarılı olmasını sağlamışlardır. Bu kullanıcılardan hiç birisi, sahte sitenin kullandığı sertifikanın orijinal sitenin sertifikasından farklı olduğunu fark etmemiştir.

Benzer şekilde, almış oldukları elektronik posta içersinde belirtilen bağlantının kendilerini sahte bir siteye yönlendiriyor olabileceğinden hiçbir öğretim elemanı şüphelenmemiş, ne elektronik postanın gerçekten bilgi işlem müdürü tarafından gönderilip gönderilmediğini ne de posta içerisindeki bağlantı adresini (posta içerisinde görünen adres öğrenci bilgi siteminin adresi olmasına rağmen bağlantı IP adresi olarak farklı bir adrese yönlendirmekteydi) kontrol etmiştir.

Kullanıcılarla yapılan görüşmelerde, üniversite içerisinde bir güvenlik politikasının oluşturulmadığı, kullanıcıların kurumsal güvenlik mekanizmaları konusunda bilgisinin bulunmadığı da tespit edilmiştir. Üniversite içerisinde bir güvenlik uyarı ve ihbar sistemi bulunmamasının yanında, öğretim elemanlarının çoğu karşılaştıkları güvensiz veya tehlikeli uygulamaları sadece yakın çevresi ile paylaşmakta kurumsal bir uyarı ve tedbir sitemi işletilmemektedir.

Yapılan güvenlik saldırısının başarıya ulaşmasında belki de en önemli etken, orijinal öğrenci bilgi sisteminde sunucu sertifikasının uygun kullanılmamasıdır. Sertifika kullanımında iki adet teknik yanlışlık bulunmaktaydı. Bunlardan birincisi sunucu sertifikasının site DNS adına üretilmemiş olması, ikincisi ise sertifikayı veren sertifika otoritesinin web tarayıcılarında güvenli kökler (veya güven zinciri) içerisinde bulunmamasıdır. Bu durum kullanıcıların siteye her bağlanmalarında tarayıcıların sertifika problemini uyarmasına sebep olmakta ve kullanıcılar tarayıcıların devam etmek istiyor musunuz sorusuna olumlu yanıt vererek işlemlerine devam etmelerini gerektirmektedir. Bu kullanım şeklinin kullanıcılarda bir duyarsızlaşma yaratarak, kullanıcıların uyarı sebebini araştırmaya gerek duymadıkları tespit edilmiştir. Yapılan görüşmelerde bu alışkanlığın sadece bu sitedeki uygulamaya özel olmadığı, benzer kullanımların İnternet'te yaygın olarak bulunmasından dolayı bu kullanıcı davranışının genel bir yaklaşım olduğu görülmüştür. Çünkü, uzun bir süredir bahsedilen site mevcut şekli ile kullanılmasına karşılık, uygulamaya katılan öğretim elemanlarının hiç birisi uyarı sebebini aştırmamış, sertifika güvenlik uyarısının neden verildiğini incelememiştir (orijinal sitede verilen uyarının da sebebi öğretim elemanlarınca bilinmemektedir). Genelde yapılan yorum, SSL hizmetlerinde kullanılan sunucu sertifikalarının bazı kanuni gerekler ve maddi yüklerden dolayı web tarayıcıları ile tam uyumlu çalışmadığı ve bu kullanım şeklinin (uyarıdan sonra devam etmeyi seçmek) iletişim güvenliğini tehlikeye atmadığı olmuştur. Bu yorumda doğru olan, açıklanan kullanım şeklinin web iletişimini üçüncü şahıslara karşı şifrelenmiş olması ve bu güvenlik parametresinde bir geri adımın söz konusu olamamasıdır. Ancak kullanılan sertifikanın bağlantı kurulan sunucunun, arzulanan sunucu olduğunu garanti etmediği göz ardı edilmektedir.

Computer Security Institute (CSI)'ın ABD'de yapmış olduğu 2008 Bilgisayar Suçları ve Güvenlik anketi sonuçlarına [9] göre, web hizmetleri günümüzde en çok güvenlik gerektiren uygulamalar olarak tespit edilmiştir. Web güvenlik açıkları olarak ise en önde belirtilen husus pishing (bilgi çalma/yemleme) yöntemi olarak belirtilmektedir. Bu yönteme karşı mevcut en etkin savunma/güvenlik önlemi ise kullanıcı farkındalığı yaratmaktır. Ancak, yine aynı araştırmada güvenlik harcamaları içerisinde kullanıcı farkındalık eğitimi için %1'den az harcama yapan firma/kurumlar %42 oranında yer alırken firma/kurumların %13'ü bu konuda yaptıkları harcama miktarını belirleyememiştir. Bu parametreler yapılan güvenlik harcamalarının büyük bölümünün teknik donanım ve uygulama (yazılım) konularında olduğunu göstermektedir. Bu araştırmada yapılan tespitlerden bir diğeri de, güvenlik saldırısına uğrandığı zaman gösterilen tepkilerde "kullanıcıların saldırganı tespit edilmeye çalışması" %60 oranında yer alırken, "durumu kanuni görevlilere bildirmek" seçeneğinin ise %27 oranında olmasıdır.

5. Sonuçlar

Bu uygulamadan elde edilen sonuçlar, güvenlik uygulamalarında başarının sadece teknik eğitimle elde edilemeyeceğini, kullanıcı farkındalığı ifadesinde başka unsurların da yer aldığını göstermektedir. SSL uygulamalarında sertifika hatası tespit edilmesine rağmen, web tarayıcılarının kullanıcı onayı ile işleme devam etmesi uygulaması kullanıcı farkındalığını olumsuz etkilemektedir. Tarayıcıların ürettiği hata mesajlarındaki detayların içerdiği güvenlik riskleri çok net olarak anlaşılmamakta ve alınabilecek kontrol tedbirleri tam olarak bilinmemektedir.

Web erişimi esnasında kullanıcıların bir an önce hizmete ulaşmayı hedeflemeleri ve günümüze kadar olan "uyarı mesajlarına onay vererek" hizmet almaya devam etme alışkanlığı mevcut uyarı sisteminin etkinliğini azaltmaktadır. Bu tarz güvenlik uyarılarının web tarayıcısı içerinden değil işletim sistemi (ve/veya durum çubuğu) üzerinden verilmesi (ağ bağlantı durum bilgileri, yazılım güncelleme bilgilerinin verilmesi gibi) ve bu uyarıların belirli zaman dilimleri (1-2 dakika) aralıkları ile açılır pencere veya uyarı baloncukları şeklinde tekrar edilmesi kullanıcı dikkatinin çekilmesi açısından uygun olabilir.

Bir güvenlik politikası oluşturularak, güvenlik ihlallerinin veya şüpheli uygulamaların bildirilebileceği kolay ulaşılır, fonksiyonel erişim sistemlerinin kurulması ve bunların tüm kullanıcılar tarafından bilinmesi, güvenliğin tesis edilmesinde ve sürekliliğinin sağlanmasında kilit rol oynamaktadır.

Bütün bu destekleyici tedbirlerin yanında kullanıcıların teknik bilgi eksikliğinin tamamlanması gerekmektedir. Ancak, sadece teknik bilginin davranışların şekillendirilmesinde yeterli olmadığı unutulmamalıdır. Kullanıcıları yanlış ve güvensiz kullanım alışkanlıklarından kurtarmak ve bu tür alışkanlıklara sebep olabilecek uygulamaları sürdürmemek en önemli güvenlik tedbirleri arasında yer almaktadır.

Mevcut SSL protokolü kullanıcıların bağlandıkları sitenin gerçekliğini/doğruluğunu onaylayabilecekleri varsayımı üzerine kurulmuştur. Bu kabulün çalışması için kullanıcının teknik olarak bilgili ve onay işlemini bilinçli olarak (diğer araçlar ile kontrol ederek) yapması gerekmektedir. Yapılan bazı bilimsel çalışmalar bu modelin etkin şekilde çalışmadığını göstermektedir[6]. Web sunucusu onay sisteminin kullanıcı seçiminden çıkarılarak, tamamen otomatik olarak yapılabilmesi için yeni protokol, tarayıcı ve güven mekanizmaları tasarlamak bu problemin uzun vadede çözülmesi için umut vaat etmektedir.

Kaynakça

[1] RFC 5246 TLS Version 1.2, http://tools.ietf.org/html/rfc5246 adresinden en son 27.10.2009 tarihinde erişilmiştir.

[2] SSL Protokolü Versiyon 3.0, http://www.mozilla.org/projects/security/pki/nss/ssl/draft302.txt adresinden en son 27.10.2009 tahinde erişilmiştir.

[3] Marchesini, John, S.W. Simith, Meiyuan Zhao, Keyjacking: The Surprising Insecurity of Client-side SSL, Dartmouth Computer Science Technical Report TR2004-498, 2004

[4] Carlisle Adams, Steve Lloyd, Understanding Public-Key Infrastructure: Concepts, Standards, and Deployment Considerations**,** Macmillan Technical Publishing, 1999, ISBN:157870166X.

[5] Andrew Nash, William Duane, Celia Joseph, PKI: Implementing and Managing E-Security, McGraw-Hill, Inc. New York, NY, USA, 2001, ISBN:1590610008.

[6] Ye Eileen Zishuang, Yougu Yuan, Sean Smith, Web Spoofing Revisited: SSL and Beyond, Dartmouth Computer Science Technical Report TR2002-417, 2002.

[7] Sukhai Natalia B., Hacking and Cybercrime, InfoSecCD Conference '4, 2004.

[8] Yang T.Andrew, Computer Security and Impact on Computer Science Education, Consortium for Computing in Small Collages, 2001.

[9] 2008 CSI Computer Crime & Security Survey, Computer Security Institute, http://i.cmpnet.com/v2.gocsi.com/pdf/CSIsurvey2008.pdf adresinden en son 13.01.2010 tarihinde erişilmiştir.