Kurumlarda güvenlik açıkları yönetimi

Kadir Kesgin1,\*

1 Gönen Meslek Yüksek Okulu, Bandırma Onyedi Eylül Üniversitesi, Türkiye

2 Department of information Technologies, Program of Information Security Technologies Bandırma Onyedi Eylül Üniversitesi Bandirma, Türkiye

\* Correspondence: kadir@bandirma.edu.tr

**Özet:** Kurumlardaki güvenlik açıkları yönetimi, saldırı daha oluşmadan onu tanımlamaya, değerlendirmeye ve gerekli adımları atarak önceden engellemeye yönelik bir süreçtir. Günümüz koşullarında hiçbir kurumun güvenlik saldırıları nedeniyle saygınlık, zaman ve para kaybına tahammülü yoktur. Kritik bilgilerin istenmeyen kişilerin eline geçmesi kurum için çok zor bir süreç başlatacağı gibi devletimiz için de sorunlar oluşturabilmektedir. Bu gibi sorunların en kısa sürede etkisiz hale getirilebilmesi için güvenlik açıklarının yönetimi zorunlu hale gelmiştir. Bilgiye sürekli erişimi sağlamak son kullanıcının bu bilgiyi değişikliğe uğramadan kaynaktan çıktığı şekliyle almasını sağlanması gerekmektedir. Verinin çıkış noktasından varış noktasına kadar veri bütünlüğünün korunması, ayrıca sadece yetkili kişilerin erişimi sağlanması ve de verinin gizliliği ve mahremiyeti korunması gerekmektedir. Güvenlik açıkların en büyük nedeni insandır bundan dolayı kurumların bilgi güvenliği için bir politikaları olması gerekmektedir. Bilginin tehdit ve tehlikelerden korunarak gelebilecek zararlı etkilerinden arındırılması gerekliliği doğmuştur. Bu çalışmada belirli başlı güvenlik açıklarının nedenleri, değerlendirme ve önlem alınması için neler yapılabileceği incelenmiş ve değerlendirilmiştir.

**Anahtar Kelimeler: Güvenlik, Güvenlik açığı, Saldırı, Güvenlik açığı yönetimi,**

The management of security vulnerability in institutions is a process of recognition, evaluation and blocking attacks before they occur. Today, any institution does not have the endurance of losing prestige, time and money because of security attacks. The critical information being fallen into the hands of undesirable people may start a hard process not only for the institutions but also for the government. The management of security vulnerability has become compulsory to neutralize this kind of problems as soon as possible. It is a necessity for the institution to constant reach of the last user to the information without any change, as it get out of the source. It is necessary to protect the data integrity from the exit point to arrival point, to enable the reach of only authorized people and to protect the data privacy. The most important reason of security vulnerability is human being; so, institutions need to have a policy for information safety. It is a necessity that the information has to be protected from threats and risks and clarified from the threatining effects. The reason of this security vulnerability, evaluation and what to do to take precautions are studied and evaluated in this research.

**Key Words: Security, Security Vulnerability, Attack, The Management of Security Vulnerability**

1. **Giriş**

Günümüzdeki en değerli varlık bilgidir. Bütün stratejiler bilginin doğru ellerde olması ve doğru şekilde aktarılması için kurulmuştur. Güvenlik açığı tanımını (NIST)[1] ,bir yazılım zayıflığının sistemi kendi çıkarları doğrultusunda bozmak isteyen bir kişinin kullanacağı açıklar olarak tanımlar. Açık tanımını ise Gartner, bilgi teknoloji güvenliğini tehlikeye atmak için kullanılabilecek bir zayıflık olarak tanımlayarak insanlar ve süreçler açısından da ele alarak biraz daha genişletir. Hangi tanım referans alınırsa alınsın yazılım da ki bu kusurlar teknolojilerin kötüye kullanımı ile kötü niyetli kişilerin elinde çalınabilir bilgiler bulundurmak sağlayabilmektedir. Bu şekilde bir durum Bilişim Teknoloji ve iş süreçlerini çalmak, değiştirmek veya geciktirmek için kullanılabileceği gibi kurumlardan faydalanmak için de kullanılabilir. Bu da kurum için güven kaybını zaman kaybını ve para kaybını beraberinde getirir. Güvenlik açıklarının anlık olarak değişkenlik gösterdiğini düşünürsek güvenlik açıklarını gidermek ve kötü kişilerin bu açıklardan yararlanmasını engelleme işi döngüsel bir iş yükü getirmektedir. Ortalama olarak her ay 300 adet yeni açığın ortaya çıktığı bilinmektedir [1]. Bu veri ele alındığında bütün kurumların kendileri için önemli olan verilerini çok daha sık taraması ve güvenlik açıklarını olabilecek en kısa zaman da gidermeleri gerekmektedir. Cert/CC istatistiklerine göre; güvenlik saldırıları, yamaları yayınlanmış fakat güncelleme yapılmamış güvenlik açıklarından gerçekleşmektedir. Bu şekilde bir tehditin varlığı kurumunuzu her an risk altında tutarken entegre bir çözüm kullanarak sistem zaaflarının ve güvenlik açıklarının tehditlere karşı sürekli taranması ihtiyacı doğmuştur. Sadece saldırı tespit sistemi kullanmanın yeterli olmayacağı bunun dışında kurumlar da güvenlik açıklarının belirli bir yönetim sürecinin de bulunması gerekliliği Gartner Araştırmacıları tarafından öngörülmektedir. Araştırmalara göre güvenlik açıkları yönetim süreci işleten kurumlara yapılan saldırıların başarıya uğrama olasılığı sadece saldırı tespit sistemi kullanan kurumlardan yüzde 90 daha azdır. Kurumların belli güvenlik yönetimi stratejileri ve yönetimi için belirlenen yöntemleri bulunmaması yalnızca güvenlik açısından değil, iş süreçlerinin yönetimi açısından da çok fazla zorluk yaşatacaktır. [2]

1. **Güvenlik Açıkları**

Tarihte etkisinin direk olarak hissedildiği ilk siber saldırı Stuxnet diyebiliriz. Windows’un güvenlik açığından ve de insan faktörünü kullanarak İran’da bulunan bir uranyum santralindeki santrifüjleri çalışmaz hale getiren bir dosya sızdırılması ile yapılmıştır. Bu örnek insan olan her yerde güvenlik açığının olacağının bir kanıtıdır [3]. Saldırılan ne zaman ve ne kadar süreceği bilinmediğinden dolayı anlık tepki verilebilmelidir. Anlık tepkiler doğabilecek sıkıntıları en aza indirebilmektedir. Bundan dolayı kurumlarda en kısa sürede tepki verebilmek için iyi planlama yapılmalı ve bunlar için ekipler kurulmalıdır. Dünya’da bu konuda ilklerden olarak CERT/CC gösterilmektedir. Türkiye’de de bu gibi saldırıların en kısa sürede çözümlenmesi ve de engellenmesi için SOME birimleri bulunmaktadır. Her türlü kötü amaçlı saldırıyı engellemek için tek bir yaklaşımın başarılı olamayacağını tarih bize göstermiştir. Kurumlar stratejik bir yaklaşım ile paylaşımcı olarak kötü amaçlı yazılımlara karşı korunabilirler.[4]

2020 yılına kadar 200 milyar ağa bağlı cihaz, 5 Milyar çalınmış veri ve 6 trilyon dolar siber güvenlik maliyeti olması beklenmektedir. Ayrıca dünyadaki veri sayısının 4 milyar zetabyte’tan 96 zetabyte dolaylarına çıkması, her 40 saniye de bir işletme fidye saldırısına maruz kalırken bu 15 saniyeye kadar düşmesi öngörülmektedir. Sadece fidye zararlıları yüzünden FBI verilerine göre 1 milyar dolar maliyet bulunmaktadır [5]. Her 39 saniye de bir hack saldırısı gerçekleşmektedir [6]. 2016 yılında yapılan saldırıların yüzde 95 i kamu kurumlarına, teknoloji şirketlerine satış mağazalarına olduğu görülmektedir [7]. 2016 yılında toplamda dünya genelinde 1 milyar kişinin hesabına veya kayıtlarına saldırı yapıldığı düşünülmektedir [8]. Siber saldırıların %43 ü küçük ölçekli firmalara yapılmaktadır [9]. Şirketlere yapılan saldırıların %64'ü web tabanlı saldırılar olmakla beraber %62 si kimlik ağı ve sosyal mühendislik saldırıları, %59'u kötü niyetli kod ve botnet saldırıları olarak ayrılmaktadır. 2013 yılından bu yana her gün 3.809.448, her saat 158.727, her dakika 2.645 ve her saniye 44 kayıt çalınmaktadır [10]. Büyük çaptaki DDoS atakları 2016'nın 4. çeyreğinde %140 oranında artış göstermiştir [11].

Kurumlarda görünen en önemli güvenlik açıklarını aşağıdaki gibi sıralayabiliriz:

* Kullanılan şifrelerin kolay tahmin edilebilir olması

Kurum iç ağındaki kullanılan kullanıcı şifrelerinin kolay tahmin edilebilir olması en basit saldırılar ile bile kurum ağının başka kişilerin eline geçmesini sağlayabilecektir. Kurum içinde kullanılan sistemlerin şifrelerinin ilk kurulum anındaki standart şifresi ile bırakılması kolay tahmin edilebilirliği arttırmaktadır. Kurum ağındaki yetkili bir hesabın ele geçirilmesi bütün sistemlere erişimin önünü açacak ve bütün sistemin istenmeyen kişilerin eline geçmesi sonucunu doğurabilecektir.

Kurum kendi sisteminde olan bütün kullanıcılar için belli bir şifre politikası belirlemelidir. Sistemde yetkili kullanıcıların özellikle şifre politikasına uygunluğu belli hizmetler ile kontrol edilmeli ve testlere tabi tutulmaları sağlanmalıdır. Şifreleme sistemlerinde en az iki boyutlu doğrulama yapılmalıdır. (sms, token gibi) Kurumun şifre politikası zorunlu olarak uygulanmalıdır.

* Sanal Özel Ağ Sunucularının yanlış ayarlanması sonucu ortaya çıkan hatalar

Sanal özel ağ (VPN) bağlantıları, kullanıcının bağlı olduğu güvensiz bir ağın kurum içinde ki güvenli ağa bağlantı yapması için güvenli iletişim tünellerine verilen addır. Kullanım alanlarına baktığımızda kurum dışındaki bir kullanıcın kurum kaynaklarına ulaşması için veya kurumlar arası bağlantının kurulması için kullanılabilirler. Zayıf şifreleme algoritmalarının kullanılması çok büyük bir zafiyete neden olabilmektedir. Eğer kullanılan sanal özel ağda güvenlik açığı var ise, bunu kullanan bir kişi kurum ağına kolaylıkla sızabilir ve kurum içindeki ağ yapılandırmasına zarar verebilmektedir. Kullanılan VPN sunucuları kendilerine ait olan bir ağda ve firewall aracılığı ile yerel ağa bağlantı yapabilmelidir. Kullanıcı kendine ait izole bir ağ ile güvenlik duvarı aracılığıyla yerel ağa bağlanmalıdır. Kullanıcılardan alınan bilgilerin şifreleme yöntemi kolay kırılmayan algoritmalardan seçilmelidir. Sanal özel ağlarla bağlanan kullanıcıların sadece gerekli olan erişimleri sağlanmalı internete çıkışları ve farklı sunuculara erişimleri engellenmelidir.

* Hatalı Kablosuz Ağ Yapılandırması

Günümüzde olmazsa olmaz ağların en tepesinde kablosuz ağlar bulunmaktadır. Kullanımı oldukça artmış olan kablosuz ağlar, kurum iç ağının büyük bir parçası olmuştur. Ancak güvenlik gereksinimleri düşünmeden tasarımların yapılmış olması çok fazla sorunu da beraberinde getirmektedir. Kablosuz ağ kullanıcıların kimlik denetimi yapılmaksızın internete çıkarılması, güvenlik duvarı ile denetlenmemesi, kablosuz ağlara sızmayı kolaylaştırmaktadır. Kablosuz ağın kurumdaki diğer ağlar ile etkileşimi kısıtlı olmalıdır. Her kablosuz ağa katılan kişi kurumun diğer ağlarına yetkisi yoksa ulaşamamalıdır. Kablosuz ağlara sızabilen bir saldırgan, kurumun yerel ağına girerek, yerel ağdaki bütün sunuculara saldırı yapabilir ve tüm ağı izleyerek eğer açık bulabilirse değiştirebilir. Kurum içi kablosuz ağ planlaması sırasında, kablosuz ağ kullanıcılarının mutlaka güvenlik duvarından geçirilerek kimlik kontrolüne tabi tutulması sağlanmalıdır. Ayrıca mutlaka kayıtlar tutulmalı ve zaman damgası ile damgalanmalıdır.

* Web Uygulamalarında Başka Siteden Kod Çalıştırma

Cross-Site Scripting hatası olarak bilinen bu hata bir saldırganın bir web sitesi aracılığı ile ziyaretçilerin sisteminde komut çalıştırabilmesine olanak sağlamaktadır. Bu saldırılarda ziyaretçilerin tarayıcı açıklarından yararlanılabilir ve/veya java ve VBScript komutları çalıştırılabilir. Web site çerezlerine ulaşılabilir ve bunlar alınabilir hale gelir. Bu şekilde tarayıcıda kaydedilmiş şifreler ele geçirilebilir. Bankacılık sistemleri için sahte web sayfaları oluşturularak kullanıcının yanıltılması ve bilgilerinin alınması sağlanabilmektedir.

Uygulama alanında ki büyün değişkenler mutlaka bir kontrolden geçirilmeli ve veri türleri karşılaştırılmalıdır. Kullanıcının girdi bilgileri ile beklenen girdiler karşılaştırılmalı ve beklenen girdi gelmediği takdirde girdi reddedilmelidir.

* SQL sorgularının değiştirilebilir yapıda olması

Yazılım geliştiriciler sunucularda gerekli olan bilgileri SQL veritabanları vasıtasıyla saklayabilmektedir, SQL sorgularında SQL için anlam ifade edebilecek &#&#‘ gibi karakterlerin açıklara sebebiyet vermemesi için önlem alınması gerekmektedir. Bu şekilde bir SQL açığı ortaya çıktığında kötü niyetli kişiler SQL sorgularını değiştirebilir ve bütün verilere çok kolay ulaşabilmektedir. Bu şekilde web sitelerine ve uygulamalara ulaşım sağlayarak zararlar verilebilmektedir.

Uygulamalarda girilen bir bilginin beklenen bir bilgi türü mü olduğu mutlaka kontrol edilmeli, türü farklı olan girdiler mutlak suretle reddedilmelidir. Alan kontrolleri yapılmalı ve girdi kabulü bundan sonra yapılmalıdır.

1. **Güvenlik Açıkları Yönetimi**

Güvenlik açık yönetimi için dört aşamalı sistem uygulanmalıdır:

1. İlkeler belirlenmelidir:

Kurum tarafından kullanılan bütün ağa bağlı cihazlar belli bir kural çerçevesinde yapılandırılmalı, bu noktada güvenlik açıkları değerlendirilmesi ve yama kontrolleri yapılması sağlanmalıdır. Son kullanıcı şifreleri belli standartlara kavuşturulmalı ve belli sürelerle değiştirilmesi zorunlu hale getirilmelidir. Kurumdaki bütün cihazların belli bir kurala göre kurgulanması ve de bu kurgu üzerinden ayarlamaların yapılması gerekmektedir.

1. Önleme:

Bu aşamada; kötü amaçlı yazılımları tanımlamak ve filtrelemek için gerçek zamanlı koruma tekniklerinin uygulanması gerekmektedir. Anlık olarak taramalar yapılmalı bütün ip ve url taramaları genele yayılmalıdır. Kod analizleri ve kum havuzu (sandbox) çözümleri kullanılarak sanal sistemlerde kodlar denenmelidir.

1. Algılama:

Bu aşamanın amacı, son kullanıcı noktasında halihazırda bulunan tehditlerin varlığına işaret eden anormallikleri tespit etmektir. Bu aşamada hızlı algılama gerekmektedir. Kurum içindeki bütün ağa bağlı cihazların açık taramalarını düzenli olarak yapılması gerekmektedir. Ağa bağlı cihazlarda ki açıklar tespit edilerek açıların giderilmesi için çalışmalar yapılmalıdır.

1. İyileştirme:

Bu aşama, hasarı onarmaya ve öğrenilen dersleri uygulamaya odaklanmaktadır. Kurum bir saldırı ile karşılaştığında bu konuda mutlaka dersler almalı ve eğer bu saldırıdan zarar görmüşse bu şekilde bir saldırının yeniden gerçekleştiğinde zarar görmemek için düzenlemeler yapmalıdır [12].

**Referanslar**

[1] CERT, Carneige Mellon University Software Engineering Institute, <http://www.cert.org/faq/>, (E.T. 22/02/2018)

[3] P.W. Singer & Allan Friedman, “Siber Güvenlik ve Siber Savaş”, Buzdağı Yayınları, 2014

[2] Tipton H. F., Krause M. (2007). Information Security Management Handbook. Auerbach Publications USOM, Ulusal Siber Olaylara Müdahale Merkezi, https://www.usom.gov.tr/index.html, (E.T. 22/02/2018)

[4] Gartner EPP Magic Quadrant 2016, <https://www.inisi.com/documents/magic-quadrant-for-endpoint-protection-platforms.pdf>, (E.T. 22/02/2018)

[5] <https://cybersecurityventures.com/2015-wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf>, (E.T. 22/02/2018)

[6] <https://www.securitymagazine.com/articles/87787-hackers-attack-every-39-seconds>, (E.T. 22/02/2018)

[7] <http://www.techrepublic.com/article/forrester-what-can-we-learn-from-a-disastrous-year-of-hacks-and-breaches/>, (E.T. 22/02/2018)

[8] [http://www.techrepublic.com/article/forrester-what-can-we-learn-from-a-disastrous-year-of-hacks-and-breaches/](http://www.techrepublic.com/article/forrester-what-can-we-learn-from-a-disastrous-year-of-hacks-and-breaches/#_blank), (E.T. 22/02/2018)

[9] <https://smallbiztrends.com/2017/01/cyber-security-statistics-small-business.html>, (E.T. 22/02/2018)

[10] <https://nudatasecurity.com/blog/scary-cyber-halloween/>, (E.T. 22/02/2018)

[11] [http://gsnmagazine.com/node/47957?c=cbrne\_detection](http://gsnmagazine.com/node/47957?c=cbrne_detection#_blank), (E.T. 22/02/2018)

[12] <https://www.fireeye.com/content/dam/fireeye-www/global/en/current-threats/pdfs/rpt-world-eco-forum.pdf>, (E.T. 22/02/2018)