Bölüm 7

AĞLARDA SALDIRI TESPİT VE ÖNLEME SİSTEMLERİ

Mesut PEK[1]

GİRİŞ

Güvenlikle ilgili tehditlerin sayısının ve türlerinin hızla artmasıyla birlikte, güvenlik teknolojilerinde de hızlı bir gelişim yaşanmaktadır. Bilgisayarların güvenliğini sağlamak, yetkili olmayan kişilerin sistemlere girip bilgileri ele geçirmelerini veya değiştirmelerini engellemek için ilk olarak kimlik doğrulama ve erişim kontrolü gibi güvenlik mekanizmaları geliştirilmiştir. Bu tip mekanizmalar güvenliğin ilk basamağını oluşturmaktadır. İnternet'in yaygınlaşmasıyla birlikte bilgi sistemlerine yönelik tehditlerde de ciddi artışlar ve saldırıların tiplerinde genişlemeler olmaktadır. Artan tehditler nedeniyle, yukarıdaki mekanizmalar dışında yeni mekanizmaların varlığına gerek duyulmuştur. Güvenlik duvarları (firewall), güvenlik tarayıcıları (vulnerability scanner) ve saldırı tespit sistemleri(STS) güvenlik mekanizmalarının ikinci basamağını oluştururlar. Bu güvenlik teknolojilerinden hiçbiri tek başına tam olarak yeterli değildir; çünkü her biri farklı güvenlik noktalarına odaklanmıştır. Güvenli bir sistem için bu yapıların birbirini destekleyecek şekilde birlikte kullanılması gerekir (itü, 2018).

Kurumsal bilgi güvenliğinin sağlanabilmesi amacıyla bilgi güvenliği yaşayan bir süreç olarak ele alınmalı, sistemler güncellenmeli, eğitimler alınmalı, oluşabilecek yeni riskler karşısında yatırımların zamanında ve doğru bir şekilde yapılması gerekmektedir. Ayrıca tüm bu evrelerde güvenlik seviyesinin istenilen düzeyde sağlanıp sağlanamadığının saptanması, varsa mevcut zafiyetleri açığa çıkarmak, açık kapıları bulmak, uygulanan kurumsal bilgi güvenliği politikalarında yeni açıklar olup olmadığını anlamak amacıyla belirli zaman dilimlerinde sistemlerin gözden geçirilmesi gerekmektedir. Kurumsal bilgi sistemlerinin güvenliğinin sağlanmasında zafiyetlerin erken tespitinin önemi büyüktür. Saldırı gelmeden önce güvenlik zafiyetlerinin tespit edilerek giderilmesini sağlayan güvenlik testleri kurumsal bilgi güvenliğinin sağlanması açısından büyük önem taşımaktadır. Güvenlik testlerinin sınıflandırılarak kurumların ihtiyaçları doğrultusunda, belirli bir yöntem ve disiplin çerçevesinde etik kurallara saygılı güvenlik uzmanları ta-

[1] Bilgi İşlem Müdürü, Şişli Meslek Yüksekokulu, mesutpek@gmail.com

nını düzenli olarak günceller. SRX Serisi aygıt, paket çekimi (PCAP) verilerini, trafiğinden PCAP Syslog Kombinasyon Protokolünü kullanarak Juniper Secure Analytics (JSA) cihazına iletebilir (juniper, 2018)

KAYNAKLAR

1. Eyupcelik (2018), XSS Saldırısı, http://eyupcelik.com.tr/guvenlik/403-derinlemesine-xss-dom-stored-reflected-saldirisi
2. Gülmüş, M. (2010). Kurumsal bilgi güvenliği yönetim sistemleri ve güvenliği. Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü Yüksek Lisans Tezi.
3. ipfs.io (2018), Man in the middle attack, (29.01.2019 - https://ipfs.io/ipfs/QmT5NvUtoM-5nWFfrQdVrFtvGfKFmG7AHE8P34isapyhCxX/wiki/Man-in-the-middle_attack.html)
4. İtü(2018), Saldırı Tespit Sistemleri, (11.01.2018, http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/sald%C4%B1r%C4%B1-tespit-sistemleri),
5. İtü(2018), Sızma Belirlemede Anormallik Tespiti Kullanımı, (28.01.2018 - http://web.itu.edu.tr/orencik/SizmaBelirlemedeAnormallikTespitiKullanimi.pdf)
6. İtü(2018), Virüs solucan ve Truva atı, (28.01.2018 - http://bidb.itu.edu.tr/seyir-defteri/blog/2013/09/07/vir%c3%bcs-solucan-ve-truva-at%c4%b1)
7. itway.com (2018), HP TippingPoint Saldırı Önleme Sistemi (IPS)
8. , (28.01.2018 - http://www.itway.com/generale/Itway_Turkey/TippingPoint/Tippingpoint.pdf)
9. juniper.net (2018), IPS ve IDS nedir , (28.01.2018 - https://www.juniper.net/us/en/products-services/what-is/ids-ips/)
10. Karaarslan, E., Tuğlular, T., & Şengonca, H. Web Saldırı Saptama ve Engelleme Sistemi Temelleri. Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, 2(1).
11. Latha, S., & Prakash, S. J. (2017, January). A survey on network attacks and Intrusion detection systems. In 2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS) (pp. 1-7). IEEE.
12. Odtu (2018), Snort , (28.01.2018 - http://cisn.odtu.edu.tr/snort.php)
13. Özgür, A., & Erdem, H. (2012). Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması. Bilişim Teknolojileri Dergisi, 5(2), 41-48.
14. Packetstormsecurity(2018), Web uygulama güvenliği, (20.08.2019, https://dl.packetstormsecurity.net/papers/web/webappsec-101.pdf)
15. Vural, Y., & Sağıroğlu, Ş. (2008). Kurumsal Bilgi Güvenliği ve Standartlari Üzerine Bir Inceleme. Gazi Üniversitesi Mühendislik-Mimarlık Fakültesi Dergisi, 23(2).
16. Wikipedia(2018), Bilgisayar Virüsü, (01.02.2019, https://tr.wikipedia.org/wiki/Truva_at%C4%B1_(bilgisayar))
17. Wikipedia(2018), Truva Atı, (01.02.2019, https://tr.wikipedia.org/wiki/Truva_at%C4%B1_(bilgisayar))