ÖN BİLGİ

Bu belge

- https://www.bgasecurity.com/makale/standartlar-ve-guvenlik-acisindan-log-yonetimi/

resmi adresindeki veya linkin kırık olması ihtimaline karşın alternatif olarak

- https://www.includekarabuk.com/kitaplik/indirmeDeposu/Siber_Guvenlik_Teknik_Makaleler/Teori/BaskalarinaAitMakaleler/Standartlar%20ve%20Bilgi%20A%C3%A7%C4%B1s%C4%B1ndan%20Log%20Y%C3%B6netimi.pdf

adresindeki makaleye çalışılarak elde edilen notlarımı kapsamaktadır. Bu çıkarılan notlar belgemde alıntılar ve/veya kişisel ilavelerim mevcuttur.

1)

Bir uçağın kara kutusu neyse bilişim sistemlerinin log'u da odur. Nasıl bir uçağın yaptığı kazanın nedeni kara kutusunda saklı ise bir bilişim sisteminin çökmesinin nedeni de log'larda saklıdır. Nasıl kara kutuyu inceleyen uzmanlar uçağın bir saldırı sonucu mu yoksa teknik bir aksaklıktan dolayı mı düştüğünü saptayabiliyorsa log'ları inceleyen bilişim uzmanı da sıkıntının teknik bir sorundan mı yoksa bir siber saldırıdan dolayı mı kaynaklandığını saptayabilir.

(Page 3)

2)

Eskiden daha çok sistem yöneticilerinin sorun giderme amaçlı kullandığı log'lama bugünlerde daha çok güvenlik analizi, adli analiz ve standartlara uyumluluk için kullanılmaktadır.

(Page 3)

3)

Log'lar işlenmediği takdirde işe yaramayan bir büyük veridir. Log'lanan verilerin izlenmesi ve yorumlanabilmesi için eskiden SIM veya SEM denilen, fakat şu aralar SIEM olarak lanse edilen analizin icra edilmesi gerekmektedir. SIEM'in açılımı Security Information and Event Management'tır.

(page 3)

4)
SIEM ve Log Yönetimi iki ayrı kavram olsa dahi hedefledikleri amaç benzer olduğundan yazı boyunca birbirlerinin yerine kullanılacaklardır.

(Page 3)

5)

SIEM/Log Yönetimi projelerinde Türkiye'de genellikle başarıya ulaşamamaktadır. Bunun temel nedeni log'lama konusunda yapılan çalışmaların hep log toplama üzerine odaklanması, toplanan log'ların nasıl değerlendirileceği konusunun ertelenmesidir.

(Page 3-4)

6)

Log'lama konusunda bazı önemli hususlar - disk alanı, ağ kullanılıyorsa ağı meşgul etme oranı vs... - dikkate alınmazsa yapılan projeler boşa gidebilir. O nedenle log yönetimi konusunda projeye başlamadan önce bazı ana noktaları belirlemekte ve projenin planını ona göre şekillendirmekte fayda vardır.

(Page 4-5)

7)

Veritabanınızı log'lama için kullanmayı düşünüyorsanız var olan işlevini engelleyecek derecede bir yoğunluk yaşar mı yaşamaz mıyı test edebilmek için uygulamanızdaki tüm select sorgularını log'latmayı deneyebilirsiniz. Bu işlem veritabanınızın durumuna göre ortalama %30 civarında bir performans kaybına yol açacaktır.

(Page 5)

8)

Log'lar eğer diske yazılıyorsa gelecek ağır bir trafik sonucu - mesela DDOS sonucu - diske yazılan devasa log'lardan ötürü sistem devre dışı kalabilir. Benzer şekilde log'lar eğer ağ üzerinden merkezi bir log sunucusuna gönderiliyorsa log'lama sistemi kısa sürede cevap veremez hale gelebilir. Örneğin saniyede 30.000 paket gönderen bir araç yardımı ile hedef firewall (güvenlik) cihazı kolaylıkla devredışı bırakılabilir.

(page 5)

9)

Unix/Linux Sistemlerde Log'lama
UNIX sistemlerde log'lama genellikle syslog aracılığıyla olur. Sistemde çalışan uygulamaların oluşturduğu log'lar syslog aracılığıyla mevcut sisteme veyahut uzak bir sisteme gönderilebilir. Fakat bu klasik log'lama yöntemi sistemde yetkili olan kullanıcıların çalıştırdığı komutları ve manipule ettikleri dosyalar üzerindeki değişiklikleri kontrol etmez. Ticari UNIX sistemlerinin hemen hepsi kendine has bir audit altyapısına sahiptir ve bu altyapı kullanılarak sistemde işletilen komutlar log olarak alınabilmektedir.

(Page 6)

10)

Windows Sistemlerde Log'lama
Windows sistemlerde loglama biraz daha kolay olmasına rağmen ortaya çıkan log kümesi çok anlaşılır değildir. Windows sistemlerde işlemler komut satırı aracılığıyla yapılmadığından dolayı

geriye yönelik bir olay araştırmasında zorluklarla karşılaşılmaktadır. Bu sebepten dolayı Windows sistemlerde - bilhassa kritik makinaların windows sistemlerinde - ekran tamamıyla kaydedilmektedir. Bu sıkça başvurulan yöntemlerden biridir.

NOT: Bir haftalık tam ekran video kaydedici yazılımların çıktıları bir DVD'ye sığabilmektedir.

(Page 6)

11)

Ağ ve Güvenlik Cihazlarını Log'lama
Router, switch, wireless, firewall, IPS ve VPN Sistemler üzerinde genellikle ekstra program kurulamayacağı için üzerlerinde mevcut olan klasik syslog yardımıyla log'lar belirlenen bir sisteme aktarılmaktadır.

(Page 7)

12)

Log'ların Bütünlüğü
Logların bütünlüğü ile ilgili önemli bir husus logların değiştirilmemesi ve değiştirilmediğinin ispatlanmasıdır. UNIX altında dosyaları sadece ekleme modunda çalışacak şekilde ayarlayabilmekteyiz. Yani bu ayarı yaptığımız takdirde log dosyasına sadece ekleme yapılabiliriz, içeriğinde değiştirme yapamayız. Tek yönlü bir kilit söz konusu. Arşive alınan log dosyalarının teyplere yedeklenmeden önce elektronik zaman damgasından geçirilmesi de log'ların teslim alındıktan sonraki tarihlerde değiştirilmediğine dair ispat için önemlidir.

(Page 8)

13)

Log'lama Konusunda Yapılan Hatalar

• Log'ların Eksik Alınması
• Log'ların Normalize Edilmemesi
• Uygulama Servislerinin Log'larının Olmaması
• Log'ların incelenmemiş halde bırakılması
• Log'ların çok kısa süreliğine kaydedilmesi

(Page 8)