Standartlar ve Güvenlik Açısından Log Yönetimi

Log yönetimi -101

Huzeyfe ÖNAL <huzeyfe@lifeoverip.net>

11/13/2009

[Log yönetimi hakkında 2008 yılında BeyazŞapka dergisi için hazırladığım yazı]

Contents

Log Yönetimi

Bir uçağın karakutusu ile bilişim sistemleri için ayrıntılı log tutmak aynı manaya gelir. Ne karakutusuz bir uçak kazası ne de sağlıklı loglama yapılmamış bir ortamdaki bilişim olayı istenildiği gibi aydınlatılamaz.

Loglama konusunun diğer güvenlik konuları arasındaki önemini gün geçtikçe daha iyi anlıyoruz. Büyük ölçekli şirketlerin 2009 yılı güvenlik bütçesindeki en büyük payın loglama sistemlerine ait olduğu bilgisi log yönetiminin gittikçe artan önemini kanıtlar niteliktedir.

Eskiden daha çok sistem yöneticilerinin sorun giderme amaçlı kullandığı loglama bugünlerde –ve bundan sonrası için- daha çok güvenlik, forensik analiz ve standartlara uyumluluk için kullanılmaya başlanmıştır.

Loglamanın Adını Koymak

Şüphesiz ki loglama tek başına bir değer ifade etmez. Nasıl ki tarladan toplanan hasat işlenmeden bir işe yaramıyorsa koleksiyon amacı ile toplanan ve izlenip değerlendirilmeyen loglar da pek birşey ifade etmez.

Loglanan verilerin izlenmesi ve yorumlanması kısaca log yönetimi ile birlikte bir değer ifade eder ki bu da piyasa dilinde SIM/SEM/SIEM(Önceleri SIM ve SEM kavramı kullanılırdı , şimdilerde SIEM kavramında karar kılınmış gözüküyor) olarak adlandırılıyor.

Burada SIEM(Security Information and Event Management) ve log yönetimi kavramları farklı olarak düşünülse de hedefledikleri amaç benzer olduğundan yazı boyunca birbirlerinin yerine kullanılmıştır.

2004 yılından bu yana 4 farklı SIEM/Log yönetimi projesinde çeşitli pozisyonlarda çalışma fırsatı buldum ve projelerde kullandığımız ürünler Gartner gibi saygın kurumların raporlarında hep en üst seviyelerde idi. Yaptığımız projeleri eleştirel bir gözle değerlendirdiğimde tam manası ile başarıya ulaşmış bir proje göremiyorum.

Bu konudaki temel sorun loglama konusunda yapılan çalışmaların hep log toplama üzerine olması, toplanan logların nasıl değerlendirileceği konusunun ertelenmesidir. Yeni yeni biraz da standart ve kanunların zorlaması ile toplanan loglarla ne yapılacağı konusu değerlendirilmeye başlamıştır. Loglama konusu da diğer güvenlik operasyonları gibi kaynak, zaman ve ilgi isteyen bir konudur ve alınacak verim bu bileşenlerle doğru orantılıdır.

Loglama niçin önemlidir?

İsterseniz bu başlığı loglama niçin gereklidir diye de okuyabilirsiniz.

Tekrar hatırlatacak olursak loglama konusu önceleri system yönetimi, sorun giderme, sonraları güvenlik ve şimdilerde standartlar, kanun ve düzenlemelerle yürütülüyor. En etkilisi de son şık olan standarlar. Zira kanun ve standartlar diğer tüm gereksinim ve yaptırımlardan daha etkilidir.

Loglama konusuna standartların ne kadar önem verdiğine örnek olarak PCI veri güvenliği standartını verebiliriz. PCI DSS altı ana başlıkta on iki gereksinim ister. Bunlardan bir tanesi tamamen loglama ve log yönetimine ayrılmıştır.

Bununla birlikte Health Insurance Portability and Accountability Act (HIPAA), Federal Information Security Management Act (FISMA), SOX, 5651 sayılı T.C kanunu, ISO 17799 vs gibi ismini sıkça duyduğumuz kanun/standart/düzenlemeler de loglama konusunu zorunlu tutmuştur.

Log yönetimi projeleri öncesinde bilinmesi gerekenler

Loglama konusunda bazı önemli noktalar dikkate alınmazsa yapılan projeler boşa gidebilir. Log yönetimi konusunda proje yapmadan önce bazı ana noktaları belirlemekte ve projenin planını ona göre şekillendirmekte fayda var.

Disk alanı

Log yönetimi konusundaki en büyük çıkmazlardan birisi loglanacak sistemlerin ne kadar log üreteceği ve bu loglar için ne kadarlık disk alanı ayrılacağıdır. Genelde yapılan hata; logların uzun süreli saklanmasına ihtiyaç hissedilmediği düşünülerek yeterli disk alanı ayrılmaması şeklinde oluyor.

PCI DSS üzerinden gidecek olursak bir yıllık log saklama gereksinimiz aşağıdaki gibi bir hesaplama ile ortaya çıkacaktır. PCI kapsamına giren sistemleriniz için benzer hesaplamalar yaparak toplam gereksinim hesaplanbilir.

Bir yıllık loglama için ortalama disk alanı = 365 gün x 24 saat x 3600 saniye x 100 (yoğun sistemler saniyede çok daha fazla log üretecektir) x 200 byte = 580~ gigabyte / yıl . Tabi bu değer sıkıştırılmamış ham veridir. İyi bir sıkıştırma ile bu değer küçültülebilir. Eger loglar için veritabanı kullanıyorsanız bu sayıyı iki üç ile çarpmak gerekir.

Loglamanın performansa etkisi

Loglama yapan sistemin durumuna gore performans etkileri değişir. Eğer sistem üzerinde yapılan tüm işlemleri logluyorsa ve bu logları ağ üzerinden olduğu gibi gönderiyorsa hem sistem üzerinde hem de ağ üzerinde bir performans problemi oluşabilir. Bunun için genelde ajan mantığı ile çalışan sistemlerde loglar biriktirilerek belirli arlıklarla merkezi loglama sistemine gönderilir.

Veritabanı sistemlerinin loglaması konusunda da dikkatli olmak ve sadece ilgili işlemleri loglamak gerekir. Yoksa veritabanınız loglama yapayım derken asıl işlevini yerine getiremez. Veritabanında loglamanın performansa etkisini ölçmek için veritabanında tüm select sorgularını loglatmayı ve bu loglamanın size performans açısından kaybını ölçün. Bu işlem veritabanının durumuna gore ortalama %30 civarında bir performans kaybına yol açacaktır.

Ağ ve güvenlik sistemlerinde yapılacak yanlış loglama ile sistemin kendisini DDOS'a açmış oluruz. Loglar eğer diske yazılıyorsa gelecek ağır bir trafikte diske yazma işleminden dolayı sistem devre dışı kalabilir. Benzer şekilde logları ağ üzerinden merkezi bir loglama sistemine gönderiyorsa loglama sistemi kısa sürede cevap veremez hale gelebilir.

Mesela saniyede 30.000 paket gönderen bir araç yardımı ile firewall/güvenlik cihazı çok rahatlıkla devre dışı bırakılabilir.

Neleri Loglamalıyız?

Log ve olay yönetim proseslerinin can alıcı bölümü nelerin loglanacağı konusudur. Bu her şirketin uymakla yükümlü olduğu güvenlik politikaları, standart, kanun ve düzenlemelere bağlı olarak değişiklikler gösterse de genelde ortak noktada buluşurlar.

UNIX/Linux ve Windows sistemlerde loglama

UNIX sistemlerde loglama genellikle syslog aracılığı ile olur. Sistemde çalışan uygulamalar syslog aracılığı ile sistem üzerine ya da uzak sisteme loglarını gönderebilir. Fakat bu klasik loglama yöntemi ile sistem üzerinde yetkili kullanıcıların çalıştırdığı komutlar ve dosyalar üzerindeki değişiklikler kontrol edilemez.

Ticari UNIX sistemlerin hemen hepsi kendine has bir audit altyapısına sahiptir ve bu altyapı kullanılarak sistemde işletilen komutlar log olarak alınabilir. Mesela PCI DSS'in loglama konusunda istediği veriler BSM altyapısı kullanılarak rahatlıkla alınabilir. Yine Linux ve FreeBSD'de de Solaris BSM benzeri audit altyapısı kullanılarak istenilenler elde edilebilir.

Solaris BSM için aşağıda yapılacak konfigurasyonlarla PCI gereksinimleri karşılanabilir.

/etc/security/audit_control
Dosyasına aşağıdaki satırı eklemek

```
flags:lo,-fr,+fc,+fd
```

ve

/etc/security/audit_user

Dosyasına aşağıdaki satırları eklemek.

```
root:ex,fr,fw,+aa:no
    yetkili_kullanici: ex fr,fw,+fm:no
```

Windows sistemlerde loglama biraz daha kolay olmasına rağmen ortaya çıkan loglar çok anlaşılır değildir. İşlemler komut satırı aracılığı ile yapılmadığından geriye yönelik bir olay araştırmasında zorluklarla karşılaşılacaktır.

Bu sebepten dolayı Windows sistemlerde -özellikle kritik sistemler- tüm ekranı olduğu gibi kaydetme sıkça başvurulan yöntemlerden biridir. Bir haftalık tam kaydetmeyi görüntü kalitesinden ödün vermeden bir dvd'ye sığdırabilen uygulamalar bulunmaktadır.

Ağ ve Güvenlik Cihazlarında Loglama

Router, switch, wireless, VPN sistemleri, firewall, IPSler bu kategoriye girer ve bu tip sistemler üzerine genelde ek program kurulamayacağından dolayı syslog kullanılarak uzak sistemlere log gönderimi yapılır.

Veritabanı loglama

Veritabanı loglamada tercih edilen iki yöntemden biri veritabanının audit altyapısı kullanılarak loglama diğeri de veritabanı sunucuya giden trafiği pasif olarak izleyen ve sorgulamaları vs anlamlı bir sekilde kaydeden sistemlerdir.

Tercih kullanılan veritabanının sağladığı olanaklara göre ve gereksinimlere göre yapılmalıdır. Performans konusunda ciddi endişeleriniz varsa pasif loglama sistemleri tercih edilebilir fakat bu tip sistemlerin maliyeti yüksektir. Veritabanının kendi audit mekanizması kullanılacaksa dikkat edilmesi gereken en önemli husus gereksiz işlemlerin loglanmamasıdır.

Uygulamalarda loglama

Loglama konusunda en sıkıntılı bileşenler genelde özel geliştirilen uygulamalardır. Bu tip uygulamalar gereksinime göre yazıldığından loglama özelliğinden yoksundurlar. Bu tip uygulamalar için arkada kullanılan veritabanı üzerinde loglama yapılarak bir nebze çözüm üretilebilir fakat uygulama yazılımcılarına loglama konusundaki isteklerinizi belirtmek ve yeni alınacak uygulamalarda loglama konusunun açık olarak belirtilmesi daha sağlıklı bir çözüm olacaktır.

Mesela üzerinde hiçbir şekilde log tutmayan ve uzaktan telnet ile yönetilen bir uygulamanın logları Snort aracılığı ile alınabilir. Aşağıdaki Snort kuralı tüm telnet bağlantılarını ve bu bağlantılarda geçen anlaşılır karekterleri uygun bir şekilde kaydedecektir.

```
log tcp any any <> $SERVER_IP 23 (session: printable;)
```

Diğer uygulamaları (ftp, sql vs) de benzeri yöntemle pasif olarak loglatabilirsiniz.

Logları ne kadar süreli saklanmalı?

Bu da yine standart ve kanunlara göre değişse de genel kabul görmüş süre 90 günlük online log ve bir yıllık arşiv log tutmaktır.

Logların bütünlüğü

Merkezi olarak toplanan logların birbirleri ile karşılaştırılması ve korelasyon yapılabilmesi ancak bu logların aynı zaman değerini kullanması ile mümkündür. Log kaynakları arasındaki zaman uyumsuzluğu korelasyon işleminin başarısız olmasına sebep olur.

Logların bütünlüğü ile ilgili diğer önemli husus da logların değiştirilmemesi ve bunun ispatlanmasıdır. UNIX altında dosyaları sadece ekleme modunda çalışacak şekilde değiştirebiliriz. Böylece log dosyasına sadece ekleme yapılabilir, içeriğinde değiştirme yapılamaz hale gelir. Arşive alınan log dosyalarının teyplere yedeklenmeden önce elektronik zaman damgasının alınması da logların alındığı tarihten sonrasında değiştirilmediğini ispat için önemlidir.

Standartlar açısından loglama

Bilgi güvenliğini amaçlayan standart, kanun, düzenlemeler ve raporlar incelendiğinde hemen hepsi loglama konusuna önem vermiş ve bu konuda aksiyonlar alınmasını zorunlu tutmuştur.

Her standart loglama açısından farklı şeyler istese de temel de hedef aynı olduğundan tek bir log yönetimi sistemi ile çoğu standarta uyum sağlanabilir.

Loglama konusunda yapılan hatalar.

Loglama konusunda yapılan hataları aşağıdaki başlıklarda inceleyebiliriz;

- Logların eksik alınması
- Logların incelenmemesi
- Logların kısa süreli kaydedilmesi
- Logların normalize edilmemesi
- Uygulama sistemlerinin loglarının olmaması.

Kaynaklar:

NIST Loglama politikası - NISTSP800-92

http://www.sans.org/reading_room/whitepapers/logging/

http://chuvakin.blogspot.com/