

KURUMLARDA LOG YÖNETİMİNİN GEREKLİLİĞİ

Ender ŞAHİNASLAN

Bilgisayar Mühendisliği
Trakya Üniversitesi, Edirne
ender@bankasya.com.tr

Arzu KANTÜRK

Bilgi Güvenlik Uzmanı
BANK ASYA, İstanbul
akanturk@bankasya.com.tr

Rembiye KANDEMİR

Bilgisayar Mühendisliği
Trakya Üniversitesi, Edirne
rembiyeg@trakya.edu.tr

Önder ŞAHİNASLAN

Bilişim Bölüm Başkanlığı
Maltepe Üniversitesi, İstanbul
onder@maltepe.edu.tr

ÖZET

Günümüzde güvenlik noktasında önemi artan konulardan biri de log yönetimidir. Log yönetimi, Bilgi Teknolojileri yönetimin altyapı bileşenlerinden biri olmasına rağmen kurumlar tarafından gözardı edilmektedir. Birçok kurumda loglar sadece kayıt altına alınmaktadır fakat log analizi yapılmamaktadır.

ISO 27001, Bilgi Güvenliği(BG) Yönetim Standardında log(iz kaydı) yönetimin önemi vurgulanmaktadır. Bilgi güvenliği ihlalleri ve vakaları arttıkça log yönetiminin önemi ve gerekliliği daha iyi anlaşılmaktadır.

Bu çalışmada; BG açısından log yönetiminin önemi ve gerekliliği, kurumda etkin bir log yönetiminin nasıl sağlanabileceği konuları kapsar.

Anahtar Kelimeler: Bilgi Güvenliği, Log Yönetimi, Log Analizi, Kurumlarda Log Yönetiminin Gerekliliği

ABSTRACT

Today Log management gain ground about safety issue day by day. Although log management is one of substructure components of BT management, it is ignored by institutions. Logs only is written down in a lot of institutions but log analysis is not tested.

ISO 27001, the significance of log management is emphasized on BG management standard. If information safety deviations and its events increase, the significance of log management and its necessity are better understood.

This study includes the importance of log management ve its necessity in terms of BG how to enable log management efficiently in the institution.

Key Words: Information Security, Log Management and Its Analysis, The Necessity of Log Management in the Institutions

1. GİRİŞ

Eskiden sadece sistem sorunlarının çözmek amacıyla log kayıtları alınırken günümüzde güvenlik ve standartlara uyum için loglama yapılmaktadır.

FISMA, HIBAA, SOX, COBIT, ISO 27001 gibi uluslararası standartlar log yönetimini zorunlu kılmaktadır. Kanunlar ve standartlar tüm yaptırımlardan her zaman daha etkin bir role sahiptir.

Ayrıca, 04.05.2007 tarihli 5651 sayılı kanunda internet suçlarını önlemeye yönelik olarak kurumların log yönetimi ile ilgili yükümlülükleri belirlemiştir.

PCI veri güvenliği standardı da log yönetimini zorunlu kılan standartlara örnek verilebilir. PCI DSS Standartı 6 başlık altında 12 gereksinim ister. Bunlardan biride log yönetimine aittir.

Her kurumun güvenlik politikasına, standart, kanun ve düzenlemelere göre bu konuda ortak bir noktada bir araya gelinir. Kurumların log yönetimi prosedürünü logların hangi noktalardan alınacağı ve neler olacağı konusunu kapsamaktadır.

2. LOG YÖNETİMİ ve ANALİZİ

Loglar, güvenlik denetimi sağlamak amacıyla merkezi olarak kaydedilmeli ve arşivlenmelidir. Bir sistemde kayıt altına alınabilecek olaylardan bazıları aşağıda verilmektedir.

- ❖ Uygulamalara ait olaylar
- ❖ Ağ cihazlarına ait olaylar
- ❖ Veritabanı olayları
- ❖ Yedekleme
- ❖ Hatalar
- ❖ DHCP kayıtları
- ❖ Web Aktiviteleri vs..

Sistemde hangi logların tutulacağı ihtiyaca göre belirlenmeli ve log yönetimi ve analizi bağımsız bir birim tarafından yapılmalıdır. Günümüzde log yönetimi, bilgi güvenliği çalışanlarının sorumluluğunda yapılmaktadır.

Örneğin; logların sistem yöneticisi tarafından alınması ve analiz edilmesi bir güvenlik riski oluşturur. Çünkü log kayıtları istediği gibi değiştirebilir ve üzerinde oynanabilir. Bu durumda bilginin bütünlüğüne aykırı bir durumdur. Malesef çoğu kurum bu konuda hassasiyet göstermemektedir.

Bilgi güvenliği çalışanları, kurumsal ağ üzerindeki tüm sunucular, istemci iş istasyonlarındaki olası güvenlik açıkları ve bilgi sızdırılmasıyla ilgili sebep ve çözümler için log kayıtlarını kritik bir kaynak olarak kullanmaktadır. Tüm log kayıtları kaydedildiği takdirde ortaya çıkan zor bir iş var demektir. Buda log kayıtlarının analizidir. Bu noktada, ihtiyaca uygun log analiz programları kullanılmalıdır.

File System Auditor, OSSIM, Kiwi Syslog Daemon, Swatch, Infraskope, Manage Engine Event Log Analyzer gibi birçok log analiz programları bulunmaktadır.

Bu tür yazılımlar, log kayıt bilgilerinin etkin ve kural tabanlı bir şekilde toplanmasını sağlarlar. Bu şekilde gereksiz log kayıtları elenir ve sadece kurumun güvenlik ilkeleriyle ilgili kritik olaylar kayıt altına alınır. Farklı kaynaklardan toplanan bu log bilgileri üzerinde tek noktadan kurumsal kayıt tutma süresi uygulanabilir.

Ayrıca USB bellek kullanımı, alınan ekran görüntüleri, önemli dokümanları yazdırma, HTTP tunneling, VPN, bluetooth, mesajlaşma uygulamaları, dial up ya da diğer ağ arayüzleri, Mac adres değişiklikleri ve sniffer, gibi kötü niyetli yazılımlara ait bilgiler işletim

sistemleri tarafından loglanmamaktadır. Bu olayları gözlemleyebilmek içinde log yönetim sistemi gereklidir.

Log yönetim sistemlerinde gerçek zamanlı izleme ve uyarı mesajları ile bu tür tehlikeleri tanımlamak ve harekete geçip gerekli güvenlik önlemleri alarak açığı kısa sürede kapatmak mümkündür.

3. KURUMLARDA LOG YÖNETİM SİSTEMİNİN GEREKLİLİĞİ

Tüm kurumlar açısından değerlendirildiğinde, bilgi ve bilgi güvenliği kurumun en büyük değerleridir. Bu sebepten kurumlarda log yönetimi belli bir merkezde toplanmalı ve analizi bağımsız tek bir noktadan yapılmalıdır. Bir güvenlik olayında savcılık aşağıdaki bilgileri X kurumdan istediğinde ve X kurumu aşağıdaki türdeki, sorulara cevap veremediğinde kurum sıkıntıya düşecektir.

Kim hangi saatde ne yapmış?

Hangi dosyalar üzerinde değişiklik yapmış?

Sistemde nereye erişmiş?

Kimler hangi programlar çalıştırıyor?

USB kullanıldı mı?

Hangi dosyalar yazıcıya yollandı? vs..

BT altyapısını oluşturan log kayıtlarını toplayan, inkar edilemez bir şekilde saklayan, analiz yapan ve tanımlanan koşulların oluşması durumunda haber veren bir log yönetim sistemi kurumlarda mutlak şekilde kurulmalıdır.

Aşağıdaki tabloda, 2008 CSI Computer Crime & security anketine göre %51'lık bir oranda log yönetimi sistemi kullanıldığı görülmektedir.

Kullanılan Teknolojiler	2008
Antivirüs yazılımı	97%
Anti spyware yazılımı	80%
Uygulama Seviyesinde Güvenlik Duvarları	53%
Biometrik	23%
İçerik Filtreleyici	32%
Şifreli veri gönderme	71%
Şifreli veri depolama	53%
Son kullanıcı güvenlik yazılımı	34%
Güvenlik duvarları	94%
Saldırı Tespit Sistemi	69%
Saldırı Önleme Sistemi	54%
Log Yönetimi Yazılımı	51%
Açık anahtar altyapı sistemleri	36%

Şekil 1: Log yönetimi

Fakat bu oran zorunluluk ve bilgi güvenliği önemi arttıkça daha da artacaktır.

4. SONUÇ

Kurumlarda, log yönetimi gittikçe önemi artan konulardan biridir. Güvenliğin en zayıf halkası olan insan unsurun faaliyetlerin izlenmesi ve loglarının alınması, herhangi bir güvenlik ihlalinde inkar edilemezlik politikasına uygun olarak ihali yapanın bulunması ve uygun yaptırımın verilmesini sağlayacaktır. Bilgi güvenliğinin sağlanması ve risklerin minimize edilmesi açısından bu çok büyük önem arz etmektedir.

Sonuç olarak; kurumlarda log yönetim sistemi muhakkak olmalı ve bağımsız bir birim tarafından yapılmalıdır. Kesinlikle sistem üzerinde tüm yetkilere sahip olan bir sistem yönetici tarafından yönetilmemelidir.

5. KAYNAKÇA

[1] **ISO/IEC 27001 Information Security Management System**

[2] **2008 CSI Computer Crime & Security Survey**
<http://www.gocsi.com/>

[3] <http://www.beyazsapka.org/dergi.aspx?id=152>

[4] <http://www.karmasis.com>

[5] **Log Management**
<http://www.sans.org/logmgmtsummit07/>

[6] **Guide to Computer Security Log Management**
<http://74.125.47.132/search?q=cache:SeBNxBAiw1QJ:csrc.nist.gov/publications/nistpubs/800-92/SP800-92.pdf+log+management&hl=tr&ct=clnk&cd=2&gl=t>

[7] **Log Management**
http://74.125.47.132/search?q=cache:4EXluajThyAJ:www.infosecwriters.com/text_resources/pdf/Six_Mistakes_of_Log_Management_AChuvakin.pdf+log+management&hl=tr&ct=clnk&cd=7&gl=tr

[8] <http://bt-stk.org.tr/k5651.html>