



**Akademik Bilişim '09**  
11 - 13 Şubat 2009  
HARRAN ÜNİVERSİTESİ - ŞANLIURFA



http://ab2009.harran.edu.tr

## Kurumlarda 'Log' Yönetim Gerekliliği

### Akademik Bilişim 2009






**Ender ŞAHİNASLAN**

**Arzu Kantürk Dr.Rembiye Kandemir Önder Şahinaslan**

Ender ŞAHİNASLAN 11-13 Şubat 2009



### Eğitimci [Ender Şahinaslan]

2007 - Devam	BANK ASYA - Bilgi Güvenliği - Müdür Yardımcısı
2005 - 2007	BANK ASYA Organizasyon, Kalite ve Sistem Geliştirme Müdürlüğü - II.Müdür
2004 - 2005	BANK ASYA - Yazılım Geliştirme Müdürlüğü - Sistem Analist
2000 - 2004	SABANCI ÜNİVERSİTESİ - Bilgi Teknolojileri - Uygulama Sorumlusu
1999 - 2000	MALTEPE ÜNİVERSİTESİ - Bilgisayar Mühendisliği - Öğretim Görevlisi
1997 - 1999	GEBZE YÜKSEK TEKNOLOJİ ENSTİTÜSÜ - Bilgisayar Mühendisliği - Arş.Grv.
1995 - 1996	GAZİ ÜNİVERSİTESİ - Fen Bilimleri Enstitüsü - Araştırma Görevlisi

- **Doktora**, Trakya Üniversitesi - Bilgisayar Mühendisliği - 2008 - Devam
- **Yüksek Lisans**, Gebze Yüksek Teknoloji Enstitüsü - Bilgisayar Mühendisliği - 1998
- **Lisans**, Trakya Üniversitesi - Bilgisayar Mühendisliği - 1995

Ender ŞAHİNASLAN 11-13 Şubat 2009


### Gündem



- Log-Kayıt İzi Toplamının Önemi
- Bazı Log Kayıtları
- Log Yönetimi ve Analizi
- Gereklilikleri (İş ve Uyum)
- Log Yönetim Metodolojisi
- Sonuç ve Öneriler

Ender ŞAHİNASLAN 11-13 Şubat 2009

### Log Toplamının Önemi



- **Uçak düştüğünde**
  - Kara kutu
- **Park yerinde bir araç infilak ettiğinde**
  - Güvenlik Kamerası
- **Size ait bir IP adresinden YÖK'ün internet sitesine bir saldırı olduğunda**
  - Unix tabanlı işletim sistemleri ve modern ağ cihazları tarafından üretilen iz kayıtları
- ...vb her türlü bilişim suçlarını araştırmada
- **Ana ihtiyaç duyulan şey.. Denetim İzleri - Log kayıtları**

Ender ŞAHİNASLAN 11-13 Şubat 2009

## Log- İz Kayıtlarından Bazıları

- ➔ Windows EventLog
  - ➔ Temel olarak işletim sistemi ve uygulamalar tarafından üretilen kayıtları tutar
- ➔ Dosya olarak tutulan iz kayıtları
  - ➔ ISS, IAS(VPN), e-posta sistemleri ve bir çok diğer uygulamalar tarafından üretilen iz kayıtları
- ➔ SysLog Kayıtları
  - ➔ Unix tabanlı işletim sistemleri ve modern ağ cihazları tarafından üretilen iz kayıtları
- ➔ Özel Olaylar (USB cihaz yazılımları, Ağ dinleyen yazılımlar ..)

Ender ŞAHİNASLAN 11-13 Şubat 2009

## Log yönetimi ve Analizi

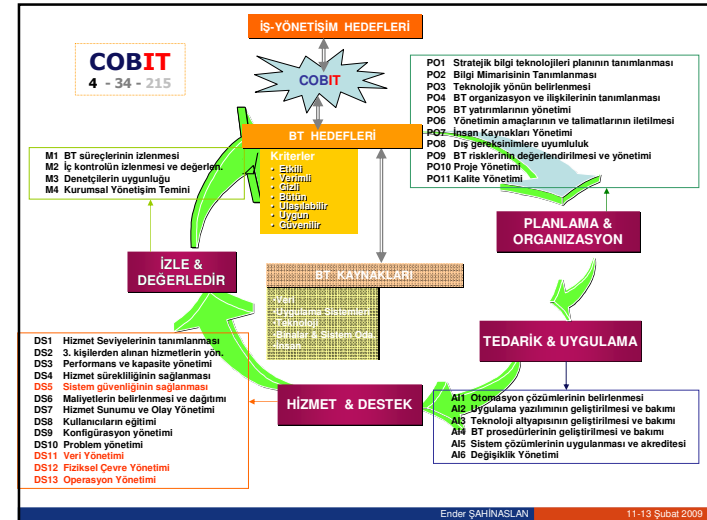
- ➔ Loglar, güvenlik denetimi sağlamak amacıyla **merkezi olarak kaydedilmeli ve arşivlenmelidir**
- ➔ Kayıt Altına alınması gereken bazı olaylar
  - ➔ Uygulama kayıt olayları, sistem giriş kayıtları
  - ➔ Ağ cihaz olayları,
  - ➔ Veri tabanı olayları
  - ➔ Yedeklemeler,
  - ➔ Hatalar
  - ➔ İnteraktif aktiviteler, kamera kayıtları .....

Ender ŞAHİNASLAN 11-13 Şubat 2009

## Hangi Log Kayıtları?

- ➔ İhtiyaçlara göre belirlenmeli
- ➔ SOX, COBIT, ISO 27001, PCI, ITIL, HIBAA beklentileri
  - ➔ Kullanıcı oturum açma işlemleri, Grup oluşturma vb
  - ➔ Finansal hareketler,
  - ➔ Bilgi oluşturma, erişim, değiştirme, silme olayları
  - ➔ ...
- ➔ Uyum Gereklilikleri (COBIT, Finansal Denetim, 5651 vb)
  - ➔ DHCP- IP dağıtım log kayıtları
  - ➔ İnternet aktivite kayıtları vb. (http, ftp, e-posta)

Ender ŞAHİNASLAN 11-13 Şubat 2009



Ender ŞAHİNASLAN 11-13 Şubat 2009

## Log yönetim yazılımı kullanım durumu

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%

Kaynak: 2008 CSI Computer Crime & Security Survey

Ender ŞAHİNASLAN

11-13 Şubat 2009

## Log yönetim metodolojisi

- Log Yönetimi hazırlık ...
  - Plan (Hangi iz kayıtlarının hangi süreyle ne sıklıkta alınacağını belirle, planlanın yapılması, sorumlulukların atanması)
  - Uygulama
  - Kontrol (düzenli gözden geçirme)
  - Önlem al

Ender ŞAHİNASLAN

11-13 Şubat 2009

## Sonuç ve Öneriler

- Artan bilgi ve güvenlik ihlalleri, yasal uyumluluk gerekleri, deneyimler, çeşitli standartlar ve günün koşulları log yönetimini gerekli kılmakta,
- Log yönetimi bir BT sorun yada görevi değildir,
- Denetim ve izleme BT'den bağımsız gruplar tarafından yapılmalı ve yönetilmeli
- Artık günümüzde olay sonrası log kayıtlarını izleme yerine olay gerçekleşmeden önce risk önleyici olarak kullanılması tercih edilmekte bunun içinde yönetimi şart.

Ender ŞAHİNASLAN

11-13 Şubat 2009



## SORULAR & CEVAPLAR TEŞEKKÜRLER



Ender ŞAHİNASLAN

11-13 Şubat 2009