MAKÜ

BURDUR MEHMET AKİF ERSOY ÜNİVERSİTESİ

OLAY KAYDETME ve İZLEME PROSEDÜRÜ

İçindekiler

1 Amaç 3

2 Kapsam 3

3 Sorumluluk 3

4 Tanımlamalar ve Kısaltmalar 3

5 İşlem Detayı 3

5.1 Olay Kaydetme 3

5.2 Kayıt Bilgisinin Korunması 4

5.3 Saat Senkronizasyonu 4

1 Amaç

Bu dokümanın amacı; Kapsam Analizi Dokümanı'nda belirtilen birimlerde işletilen sistemlerde olay takibi yapabilmek ve kanıt üretebilmektir.

2 Kapsam

Bu doküman, Kapsam Analizi Dokümanı'nda belirtilen birimlerdeki sistemleri kapsar.

3 Sorumluluk

Görev / Rol/Unvan	Dokümanın Hazırlanması	Dokümanın Kontrolü	Dokümanın Onaylanması	Dokümanın Yayınlanması	Dokümanın Güncellenmesi	Dokümanın Uygulanması	Dokümanın Uygulamadan Kaldırılması
Üst Yönetim			X			X	X
Üst Yönetim Temsilcisi			X			X	X
BGYS Yöneticisi	X	X		X	X	X	
BGYS Birim Sorumlusu	X	X				X	
Diğer Çalışanlar						X	

4 Tanımlamalar ve Kısaltmalar

Terim	Tanım/Açıklama
Kurum	Kuruluşumuzun Kapsam Analizi Dokümanı'nda belirtilen birimleri
BGYS	Bilgi Güvenliği Yönetim Sistemi

5 İşlem Detayı

5.1 Olay Kaydetme

Kurum bünyesinde oluşan kayıtları toplamak, izlemek ve 5651 sayılı kanuna uygun olarak saklamak için Log Yönetimi yazılımı kullanılmaktadır. Olay kayıtlarında, işlemin tespit edilebilmesi için olayın gerçekleştiği tarih, saat, kaynak ve olay detayları vb. bilgileri barındırılır. En az aşağıda çeşitleri verilen Olay Kayıtları tutulur:

- Oturum açma/kapama işlemleri kayıtları.

- Başarılı ve reddedilen sistem erişim girişimleri kayıtları.
- Dosya sunucusu üzerindeki dosyaların değiştirilme veya silinme kayıtları.
- Saldırı tespit sistemi kayıtları.
- Güvenlik duvarı kayıtları
- Merkezi anti virüs programı kayıtları.
- Kullanılan web uygulamaların işlem kayıtları.
- İşletim sistemi olay kayıtları.
- Elektronik posta trafiği kayıtları.
- Internet erişim trafiği kayıtları.
- IP dağıtım kayıtları.
- Uygulamaların kullanıcılar ve yöneticiler tarafından yaptığı işlem kayıtları.
- Ağ cihazları kayıtları

5.2 Kayıt Bilgisinin Korunması

Olay kayıtları yetkisiz erişimlere ve değiştirilmelere karşı korunur. Kurum, kayıtların korunması için Log Yönetimi yazılımı kullanmaktadır. Log Yönetimi yazılımı ile veriler alındığı andan itibaren tarih saat değerleri ile hashlenip saklanmaktadır. Hashleme mekanizması veriler alınır alınmaz uniq id kolonlar üzerinden çalışmaktadır. Bu yöntem ile verilerin değiştirilmesi engellenir. Kayıt dosyalarına günlük olarak zaman damgası yapılır.

5.3 Saat Senkronizasyonu

Kurum bünyesinde bütün bilgisayar ve sunucularda saat senkronizasyonu sağlayan NTP server kullanılmaktadır.

Revizyon Kayıtları

Rev. No	Tarih	Hazırlayan	Revizyon Nedeni /Sayfa No	Onaylayan	İmza
1					
2					
3					
4					
5					