# OLTA Sistemi

Kenan KOÇ
Çağlar GÜLÇEHRE
TÜBİTAK ULAKBİM

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009

# OLTA Sistemi Ana Başlıkları

- OLTA Sistemi Nedir ?
- OLTA Sistemi Niçin Kuruldu ?
- Sizden Neler Bekliyoruz
- İstatistiksel Bilgiler

# OLTA Sistemi Nedir?

- Açılımı Olay Takipçisidir.
- OLTA olay kayıtlarının merkezi bir sistemde oluşturulup takip edilmesi için geliştirilmiş bir uygulamadır.
- OLTA sayesinde olay kayıtları üzerinde gerekli güncellemeler yapılarak hem olay kaydı sahibinin, hem şikayetçinin, hem de Ulak-CSIRT yetkililerinin bilgilendirilmesi sağlanmaktadır.

# OLTA Sistemi Nasıl Kullanılır I

1-Uca ait IPlerden birisiyle ilgili olay kaydı açıldığında abuse@uc_domain adresine bir bilgilendirme e-postası atılmaktadır.

2-Uç sorumlusu OLTA sistemine giriş yaptığında "Benim Açık Biletim" başlığı altında o uca ait henüz kapatılmamış olayları görecektir.

3-Olayın konu başlığına tıklayarak detayları incelenmelidir.

# OLTA Sistemi Nasıl Kullanılır II

4-Olay kaydı politikasında iki adet zaman kısıtı var.

a. İlk Tepki Süresi (Politikadaki tanım): Olay kaydının açılmasından olay üzerinde çalışmalara başlanıldığına dair bilgilendirmenin yapılmasına kadar geçen zamandır. Bilgilendirme, olay bildirimi e-postasında belirtilen web sayfası bağlantısı kullanılarak yapılmalıdır.

b. Olay Çözümü Süresi: Olayla ilgili uç tarafında yapılan işlemlerin yeterli görülmesi durumda Ulak-CSIRT üyeleri tarafından olayın kapatılması.

# OLTA Sistemi Nasıl Kullanılır III

5-Bu tanımlar doğrultusunda uç sorumlusu yeni bir olay bildirimi aldığında, olayın detaylarını incelemeli ve OLTA sisteminde "Cevapla" fonksiyonunu kullanarak olay araştırmasının başladığını belirtmelidir. (İlk Tepki Süresi Sonuna kadar).

6-Olay hakkında yeni bilgiler edindikçe yine aynı şekilde "OLTA sisteminde "Cevapla" fonksiyonu" kullanılarak olay güncellenmelidir.

7-Güncellemeler sonucu olayın çözüldüğüne karar verilirse, Ulak-CSIRT üyeleri olayı kapatacaktır.

# OLTA Sistemi Niçin Kuruldu ?

- OLTA Sistemi Olay Takibini kolaylaştırmak amacıyla kuruldu.

- ULAKNET kullanıcılarını için oluşturulan Olay Kayıtlarını daha düzenli hale getirmek ve ULAKNET uç sorumlularını bu konuda bilinçlendirmek amacıyla kuruldu.

# Eski Sistemin Zayıflıkları

- Her olay için bir link oluşturuluyor ve uç sorumlusuna gönderiliyordu.
- Uca ait tüm olaylar ve durumları görüntülenemiyordu.
- Kullanıcı bazlı olmayan yetkilendirme kullanılıyordu.
- Olay kaydı politikaları doğrultusunda otomatik bildirimler yapılması zordu.
- Kısaca eski sistem pek kullanıcı dostu değildi

**Olay Kaydı / Incident Record**

| | |
|---|---|
| Kayıt No / **Ticket Number** | 4 |
| Önem Seviyesi / **Incident Level** | 4 |
| Kayıt Tarihi / **Ticket Date** | 2006-07-01 21:49:49 |
| Kayıt Yapan / **Requester** | Kerem |
| eposta / **e-mail** | kerem |
| Tel / **Phone** | 31229 |
| Faks / **Fax** | |
| IP | 193.255. |
| Uc Kısa Adı | |
| Olay Tarihi / **Incident Date** | 01/07/2006 |
| Olay Saati / **Incident Time** | 21:48 |
| Zaman Dilimi / **Time Zone** | +2 |
| Saldırı Türü / **Attcak Type** | Diger |
| Ek Bigi / **Information** | Sunucularımıza sürekli olarak başarısız ssh bağlantısı yapmakta. Son bir ay içerisinde tek bir sunucumuza yapmış olduğu başarısız SSH bağlantı sayısı 6044. Bilgisayar aracılığı ile sunucularımıza kaba-kuvvet saldırısı yapıldığını düşünmekteyiz. |
| Durum / **Status** | Goruntulendi |
| Güncellemeler / **Updates** | |

**Yeni Güncellemeler** Güncelle

# Kullanım Politikası

ULAKBİM Kabul Edilebilir Kullanım Politikası
5.7 Maddesine göre

ULAKBİM bünyesinde faaliyet gösteren ULAK-CSIRT (Computer Security Incident Response Team), dış ağlardan ULAKNET'e veya ULAKNET'den dış ağlara yapılabilecek güvenlik ihlallerini önleme, gerçekleşen saldırı ve sorumlularını tespit etme ve saldırıyla karşılaşan ağın yöneticileriyle bilgileri paylaşmakla sorumludur. Kullanıcı Kuruluşlar, ULAK-CSIRT tarafından önem seviyesine göre belirlenerek talep edilen süre içerisinde istenilen bilgileri sağlamakla, gerekli önlemleri alarak güvenlik ihlalini engellemekle ve bilgi akışını sağlamakla sorumludur.

http://www.ulakbim.gov.tr/ulaknet/kullanim-politikasi2007.pdf

# Olay Kaydı Politikası I

TÜBİTAK ULAKBİM

**Seviye Tespiti**

| Önem Seviyesi | Belirtiler | Örnekler |
|---|---|---|
| Seviye 1 - Kritik | • Çok sayıda hedefin etkilenmesi<br>• Servis kesintisine sebep olması<br>• Olaya sebep trafiğin devam etmesi | • UlakNET omurga cihazlarının çalışmasını engelleyen trafikler<br>• Devam eden DdoS saldırısı<br>• Devam eden sızma çabası |
| Seviye 2 - Ciddi | • Belirli bir hedef grubunun etkilenmesi<br>• Servis yavaşlamasına sebep olması<br>• Olaya sebep trafiğin devamı | • Erişime açık sunucu tesbiti<br>• Relay 'e açık e-posta sunucusu<br>• Devam eden port taraması |
| Seviye 3 - Orta | • Sınırlı sayıda hedefin etkilenmesi<br>• Olaya sebep olan trafiğin kesilmiş ancak tekrar başlaması çok muhtemel olması | • Copyright uyarısı |
| Seviye 4 - Düşük | • Çok az sayıda hedefin etkilenmesi<br>• Olaya sebep olan trafiğin kesilmiş olması | • İstenmeyen e-posta<br>• Virus sebepli tarama |
| Seviye 5 - Özel | • Ulak-CSIRT üyeleri tarafından diğer seviyelerle sınıflandırılamayan olaylar | • Süreli adli yazı ile kullanıcı bilgi talebi |

* Her bir olay kaydı için seviye tespiti ULAK-CSIRT tarafından yapılacak ve olay kaydı bildirim e-postasında olay detayları ile beraber ilgili kuruma iletilecektir.



ULAK CSIRT
UlakNet Computer Security Incident Response Team

# Olay Kaydı Politikası II

**Seviye Süreleri**

| Önem Seviyesi | İlk Tepki Süresi * | Olay Çözümü Süresi |
|---|---|---|
| Seviye 1 | 1/2 Saat | 1 saat |
| Seviye 2 | 1 saat | 4 saat |
| Seviye 3 | 4 saat | 24 saat |
| Seviye 4 | 12 saat | 48 saat |
| Seviye 5 | Olaya özel belirlenecektir | Olaya özel belirlenecektir |

* İlk Tepki Süresi; olay kaydının açılmasından olay üzerinde çalışmalara başlanıldığına dair bilgilendirmenin yapılmasına kadar geçen zamandır. Bilgilendirme, olay bildirimi e-postasında belirtilen web sayfası bağlantısı kullanılarak yapılmalıdır.

# Olay Kaydı Politikası III
## Yaptırımlar

| Önem Seviyesi | İlk Tepki Süresinin Aşılması Durumu | Çözüme Ulaşılamaması Durumu |
|---|---|---|
| Seviye I - Kritik | Tepki süresi sonunda otomatik tekrar bildirim ve ilgili Ulak-CSIRT üyesi tarafından telefonla bildirim ile tepki süresinin yarısı kadar zaman tanıma* | Erişim engellenmesi (NAT benzeri uygulamalar sebebiyle uç trafiğinin tamamen etkilenecek olması durumu dahil) |
| Seviye II - Ciddi | Tepki süresi sonunda otomatik tekrar bildirim ve ilgili Ulak-CSIRT üyesi tarafından telefonla bildirim ile tepki süresinin yarısı kadar zaman tanıma* | Erişim engellenmesi (NAT benzeri durumlarda uç yöneticisi ile iletişime geçerek çözüm süresinin yarısı kadar daha zaman tanıma)** |
| Seviye III - Orta | Tepki süresi sonunda otomatik tekrar bildirim ile tepki süresi kadar zaman tanıma* | Çözüm süresi sonunda otomatik tekrar bildirim ile çözüm süresinin yarısı kadar zaman tanıma ** |
| Seviye IV - Düşük | Tepki süresi sonunda otomatik tekrar bildirim* | Çözüm süresi sonunda otomatik tekrar bildirim ile çözüm süresi kadar zaman tanıma ** |
| Seviye V - Özel | Olaya özel belirlenecektir | Olaya özel belirlenecektir |

* Sürenin bitiminde olay çözümü süresi aşılana dek bir işlem yapılmayacaktır.
** Ek süre bitiminde erişim engellenmesi yapılacaktır.

# OLTA Sisteminde Olay Kaydı Nasıl Oluşturuluyor

1- csirt/abuse/olta@ulakbim.gov.tr adresine gelen saldırı şikayeti epostaları,

2- Balküpü Servisinden gelen bildirimleri

3- Diğer yollarla gelen şikayetleri

değerlendirip, geçerli bulur isek Olay Kaydı açıyoruz.

# OLTA Sisteminin Yapısı I

- Bu Bölümü Olta Sistemini ULAK-CSIRT için geliştiren **Çağlar GÜLÇEHRE** arkadaşımızın anlatmasını isterdim. Fakat bu hafta uygun olmadığı için ben anlatacağım.

- RTIR Nedir: CERT' lerin Olay Takibi için dünyanın birçok yerinde kullanıldığı paket programdır.

# OLTA Sisteminin Yapısı II

RTIR programında ne gibi değişiklikler yapıldı.

1- Tüm ULAKNET kullanıcılarının bilgileri girildi.

2- ULAKNET Olay Kaydı Politikası kuralları Olta Sitemine girildi.

3- Şikayete konu IP'yi kullanan ULAKNET Ucu ve o ucun Sorumlusu ile ilgili bilgilerin veri tabanından çekilmesi için modüller eklendi.

4- Şifre hatırlatma modülü eklendi.

5- Otomatik vade dolumu hatırlatması eklendi

# Sizden Ne Beklemiyoruz

TÜBİTAK ULAKBİM

- Olay kaydı ile ilgili cevapları aşağıdaki gibi ucu açık cevaplar değil de, yaptığınız çalışmaları detaylı bir şekilde yazmanızı istiyoruz.
- *Kısa süre zarfında olaya müdahale edilecektir.*
- *Olay kaydı ile ilgilenilecektir.*
- *Olay kaydı ile ilgili çalışmalara başlanacaktır.*



ULAK CSIRT
UlakNet Computer Security Incident Response Team

# Sizden Ne Bekliyoruz I

- Açılan olay kayıtlarını cevaplar yazarak olay kayıtlarının çözüm aşamasına gelmesini sağlamanızı istiyoruz.

- Olay kayıtları cevaplarına birkaç örnek verelim.

# Sizden Ne Bekliyoruz II

## Örnek Cevaplar

Spam yaratan 193.140…… nolu IP adresi ……. MYO lunda çalışmaktadır.IP , dhcp server tarafından otomatik olarak verilmekte olduğundan kimlik tespit edilememiştir……. merkezinde çalışanlar bu konuda uyarılmışlardır.

# Sizden Ne Bekliyoruz III

Örnek Cevaplar

- …….. Yüksek okulunda öğrencilerin kullanımında olan bir bilgisayara ait. bilgisayar ağdan devre dışı bırakıldı. yeniden formatlanıp antivürüs programı kurulduktan sonra sisteme dahil edilecek.
- Bir kullanıcının şifresi ele geçirildiği tespit edilmiştir.Spam amacıyla kullanılmıştır. Gerekli işlemler yapılmıştır

# Sizden Ne Bekliyoruz - IV

TÜBİTAK ULAKBİM

## Örnek Cevaplar

- Saldırıyı gerçekleştiren IP 193.140……. dur. www……..edu.tr dir. 193.140……. nolu ip adresinden herhangi bir saldırı FW loglarında görünmemektedir. İlgili IP ye sahip lokasyonumuzda çözüme yönelik çalışmalar yapılmaktadır.

  Tşkler...



ULAK CSIRT
UlakNet Computer Security Incident Response Team

# İstatistiksel Bilgiler I
## Açık Olay Kaydı Sayısına Göre

| Sıra | Üniversite Adı | Toplam Olay Kaydı Sayısı | Toplam Açık Olay Kaydı Sayısı | Toplam Çözülmüş Olay Kaydı Sayısı |
|---|---|---|---|---|
| 1 | İzzet Baysal Üniversitesi | 124 | 124 | 0 |
| 2 | Yıldız Teknik Üniversitesi | 77 | 77 | 0 |
| 3 | Balıkesir Üniversitesi | 63 | 63 | 0 |
| 4 | Ağrı İbrahim Çeçen Üniversitesi | 56 | 56 | 0 |
| 5 | Mustafa Kemal Üniversitesi | 43 | 43 | 0 |
| 6 | Dicle Üniversitesi | 27 | 27 | 0 |
| 7 | Karamanoğlu Mehmetbey Üniversitesi | 27 | 27 | 0 |
| 8 | Atatürk Üniversitesi | 28 | 25 | 3 |
| 9 | Boğaziçi Üniversitesi | 34 | 20 | 14 |
| 10 | Mersin Üniversitesi | 19 | 18 | 1 |

# İstatistiksel Bilgiler

## Çözülmüş Olay Kaydı Sayısına Göre

| Sıra | Üniversite Adı | Toplam Olay Kaydı Sayısı | Toplam Açık Olay Kaydı Sayısı | Toplam Çözülmüş Olay Kaydı Sayısı |
|---|---|---|---|---|
| 1 | Yüzüncü Yıl Üniversitesi | 65 | 0 | 65 |
| 2 | Marmara Üniversitesi | 41 | 2 | 39 |
| 3 | Süleyman Demirel Üniversitesi | 37 | 0 | 37 |
| 4 | Uludağ Üniversitesi | 23 | 0 | 23 |
| 5 | Hacettepe Üniversitesi | 24 | 1 | 23 |
| 6 | Sabancı Üniversitesi | 22 | 0 | 22 |
| 7 | Çukurova Üniversitesi | 20 | 0 | 20 |
| 8 | Selçuk Üniversitesi | 23 | 4 | 19 |
| 9 | Dumlupınar Üniversitesi | 16 | 0 | 16 |
| 10 | Boğaziçi Üniversitesi | 34 | 20 | 14 |

# İstatistiksel Bilgiler
## Toplam Olay Kaydı Sayısına Göre

TÜBİTAK ULAKBİM

| Sıra | Üniversite Adı | Toplam Olay Kaydı Sayısı | Toplam Açık Olay Kaydı Sayısı | Toplam Çözülmüş Olay Kaydı Sayısı |
|---|---|---|---|---|
| 1 | İzzet Baysal Üniversitesi | 124 | 124 | 0 |
| 2 | Yıldız Teknik Üniversitesi | 77 | 77 | 0 |
| 3 | Yüzüncü Yıl Üniversitesi | 65 | 0 | 65 |
| 4 | Balıkesir Üniversitesi | 63 | 63 | 0 |
| 5 | Ağrı İbrahim Çeçen Üniversitesi | 56 | 56 | 0 |
| 6 | Mustafa Kemal Üniversitesi | 43 | 43 | 0 |
| 7 | Marmara Üniversitesi | 41 | 2 | 39 |
| 8 | Süleyman Demirel Üniversitesi | 37 | 0 | 37 |
| 9 | Boğaziçi Üniversitesi | 34 | 20 | 14 |
| 10 | Atatürk Üniversitesi | 28 | 25 | 3 |



ULAK CSIRT
UlakNet Computer Security Incident Response Team

# Bugüne Kadar Açılan Olay Kayıtları

| Sıra | Olay Türü | Toplam Olay Kaydı Sayısı | Toplam Açık Olay Kaydı Sayısı | Toplam Çözülmüş Olay Kaydı Sayısı |
|---|---|---|---|---|
| 1 | Balküpü | 570 | 357 | 213 |
| 2 | Spam | 265 | 100 | 165 |
| 3 | Copyright | 172 | 101 | 71 |
| 4 | Port | 15 | 0 | 15 |
| 5 | Giriş | 14 | 0 | 14 |
| 6 | Phishing | 12 | 0 | 12 |
| 7 | Virus | 9 | 2 | 7 |
| 8 | DoS | 7 | 0 | 7 |
| 9 | Diğer | 5 | 3 | 2 |

# Sorular & Yorumlar


Ulusal Akademik Ağ
Bilgisayar Olaylarına Müdahale Birimi
Ulak-CSIRT

*Enis Karaaslan* - *Ege Üniversitesi*
*Gökhan Akın* - *İTÜ*
*Gökhan Eryol* - *ULAKBİM*
*Hüseyin Yüce* - *Marmara Üniversitesi*
*Hüsnü Demir* - *ODTÜ*
*Murat Soysal* -*ULAKBİM*

*Kenan Koç* -*ULAKBİM*
**http://csirt.ulakbim.gov.tr**
**http://blog.csirt.ulakbim.gov.tr**
**http://viki.csirt.ulakbim.gov.tr**
**csirt@ulakbim.gov.tr**