

Ulak-CSIRT Dünü, Bugünü, Yarını

Murat SOYSAL
TÜBİTAK ULAKBİM

İçerik

- Ulak-CSIRT nedir?
- I.Yıl: Şubat 2006 - Nisan 2007
- II.Yıl: Nisan 2007 – Mayıs 2008
- III.Yıl: Mayıs 2008 - Mayıs 2009
- Yarını: Mayıs 2009 - ?
- Sorular & Yorumlar

Ulak-CSIRT



ULAKNET bünyesinde bilgi güvenliği konusundaki bilincin artırılması, yaşanan bilgisayar güvenlik olayları sayısının azaltılması ve ağın kurulduğu tarihten beri sürdürülen çalışmaların daha koordineli bir hale getirilmesi için UlakNet Bilgisayar Olaylarına Müdahale Birimin kurulmasına karar verilmiştir. Dünyadaki benzerleri ile paralel bir organizasyona sahip bu birim, Ulak-CSIRT (<http://csirt.ulakbim.gov.tr>) olarak adlandırılmış ve Subat 2006'da faaliyetlerine başlamıştır.

Amaçlar (Şubat 2006 - Nisan 2007)

Dün I



Amaçlar

- Bilgi güvenliği bilinci sağlamak
- Ağ güvenli hale getirmek
- Saldırgan tespitinin koordinasyonu
- Güncel açıkları ve çözümlerini bildirmek
- Türkçe doküman sağlamak
- Ağın saygınlığını dış dünyada artırmak

İş Planı (Şubat 2006 - Nisan 2007)

Dün I



- Olay bildirim formu işletimi (trouble ticket)
 - Her saldırı için bir giriş yapılması
 - Hedefini bilgilendirme
 - Kaynak ağ yöneticisinden talep
 - Sonuç aşamasına kadar koordinasyon
- Türkçe doküman organizasyonu
 - Mevcut dökümanların toparlanması
 - Eksik alanların belirlenmesi
 - Çeviri ya da üretim koordinasyonu
- Güncel açıkların izlenmesi
 - Web sayfasında anonslar yayınlanması
 - Türkçe uyarılar sağlanması
- Hukuki konularda takip ve bilgilendirme
 - Mevcut yasalar
 - ULAKBİM ve uçların hukuki sorumlulukları

Amaçlar (Nisan 2007 – Mayıs 2008)

Dün II



Yol haritasında 2006 yılı için yer alan hedeflerin bir çoğunu başarıyla gerçekleştiren birim çalışmalarında öngördüğü ivmeyi yakalamıştır. Ulak-CSIRT üyeleri ilk etapta belirlenen çalışma konularında gelinen nokta sonrası çalışma konuları ve birimin yapısı konusunda güncellemelere gidilmesi ihtiyacını hissetmiştir.

Bu güncelleme isteğinde ülkemizde 2006 yılı içerisinde bilişim suçlarının popülerleşmesi ve bağlı olduğumuz Avrupa Akademik Ağı (Geant) kapsamında yürütülen çalışmalar sonucu ülke akademik ağlarına ait CSIRT benzeri oluşumlara verilen önemim açıkca ifade edilmesi önemli bir yer tutmaktadır.

4 farklı çalışma grubu kurularak yeni bir organizasyona gidilmiştir.

Amaçlar (Nisan 2007 – Mayıs 2008) Dün II



TÜRKİYE'nin ilk akredite güvenlik birimi.

Ulak-CSIRT (Turkey) entered into "accredited" status on 2007-07-14.



3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009



İş Planı – (Nisan 2007 – Mayıs 2008)

Dün II



- Ağ Erişim Kontrolü (Network Access Control) Çalışma Grubu
Koordinatör : *Hüseyin YÜCE*
- Bal Küpü Tuzağı (Honeypot) ve Kara Delik (Black Hole) Çalışma Grubu
Koordinatör: *Murat SOYSAL*
- Web Güvenliği ve Zayıflık Tarama Sistemleri (Vulnerability Analysis) Çalışma Grubu
Koordinatör: *Enis KARAARSLAN*
- PC Yönlendirici ve Güvenlik Merkezi Çalışma Grubu
Koordinatör: *Gökhan ERYOL*

Amaçlar (Mayıs 2008 - Mayıs 2009) Bugün



- Çalışma gruplarına ULAKNET uçları katkısı sınırlı seviyede olmuştur.
- Ç.G. İş planlarının çoğu Ulak-CSIRT üyeleri tarafından gerçekleştirilmiştir.
- İş planları yeniden gözden geçirilerek her grup için zaman aşama planı yapılmıştır.
- Uç yöneticilerine yönelik eğitimler
- Güvenlik olay takibinin geliştirilmesi

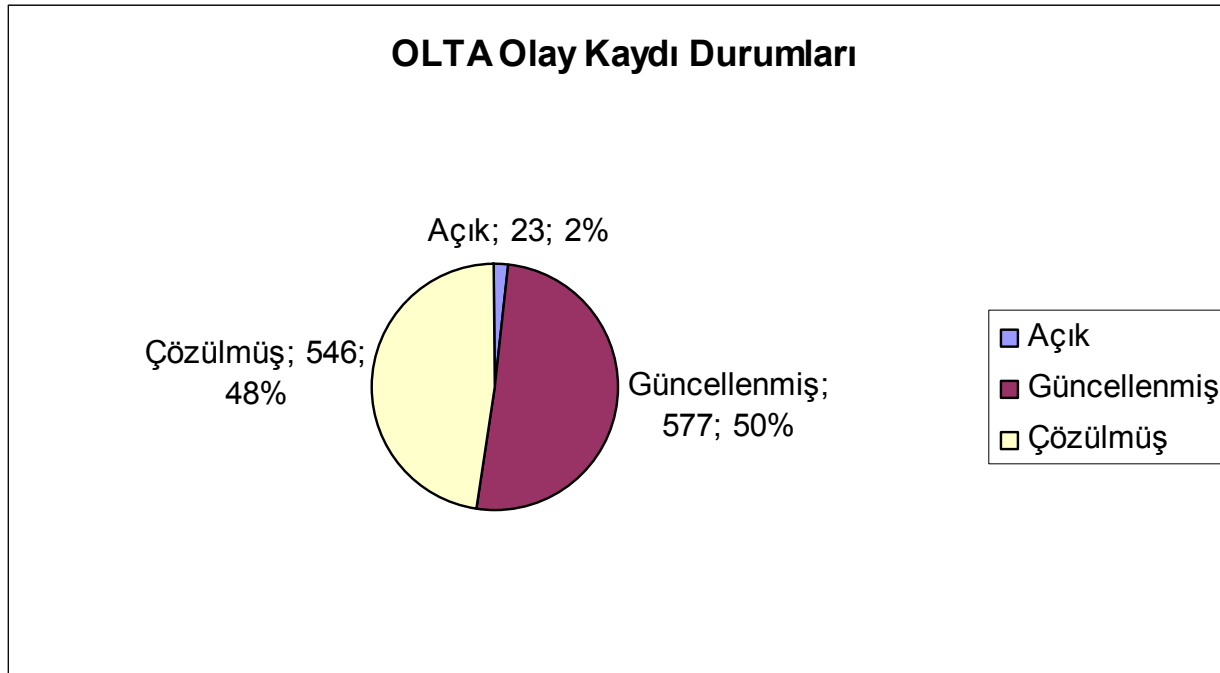
İş Planı – (Mayıs 2008 - Mayıs 2009)

Bugün



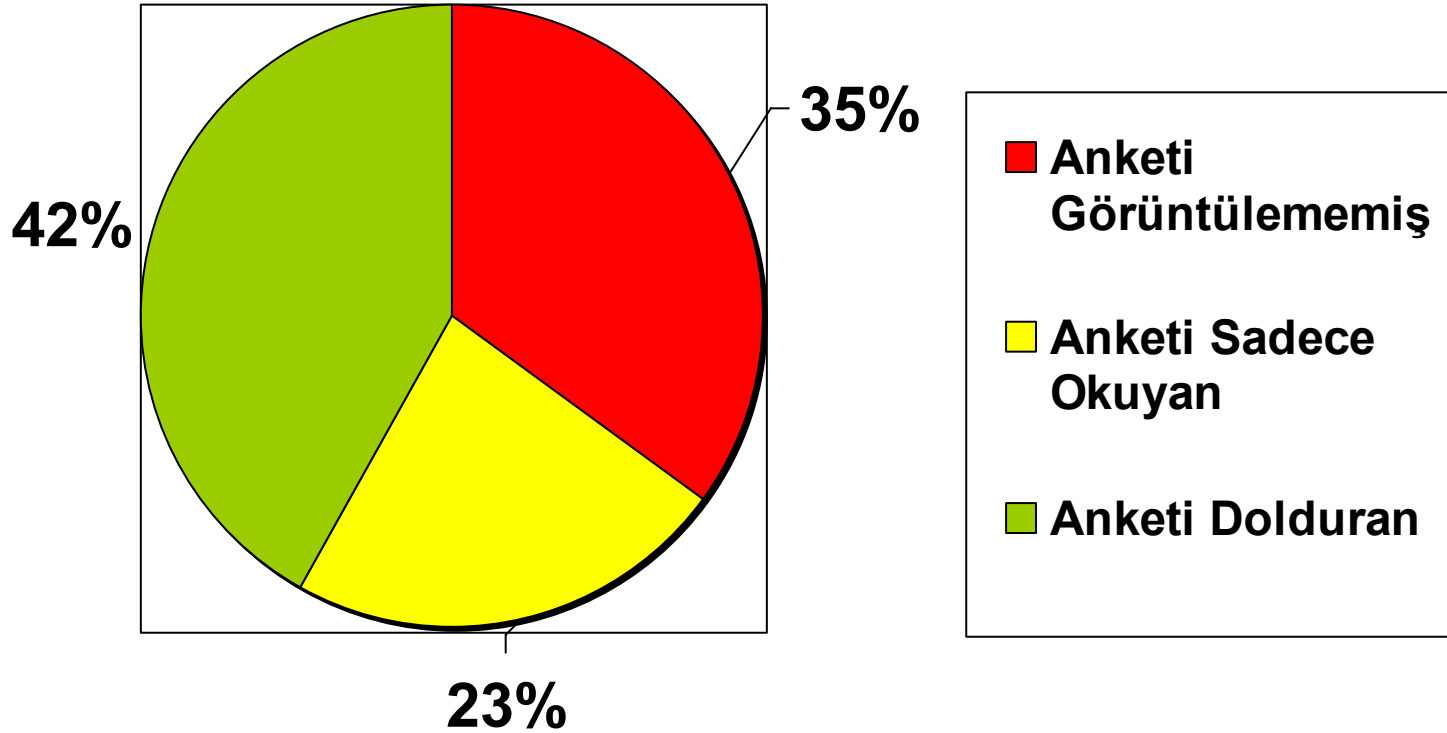
- *OLTA sistemi kurularak Olay Takibi konusunda önemli yol katedilmiştir.*
- *Kenan KOÇ 'un Olay Takip sistemi üzerinde çalışmaya başlamıştır.*
- *OLTA üzerinde hazırlanan ULAKNET Uç bilgileri sistemi*
 - *ULAKNET İstatistikleri*
 - *ULAKNET eposta listeleri*
 - *ULAKNET ağ yöneticilerinin kullandığı veri tabanları ile birleştirilerek her uç için en güncel bilgilerin uç sorumluları tarafından girilmesi sağlanmıştır.*
- *PC-Yön ve Balküpe Ç.G. Faaliyetlerini tamamlayarak ULAKNET servisi haline gelmiştir.*
- *Ulak-CSIRT Blogundan çok sayıda aktif paylaşım yapılmıştır*

İş Planı – (Mayıs 2008 - Mayıs 2009) Bugün



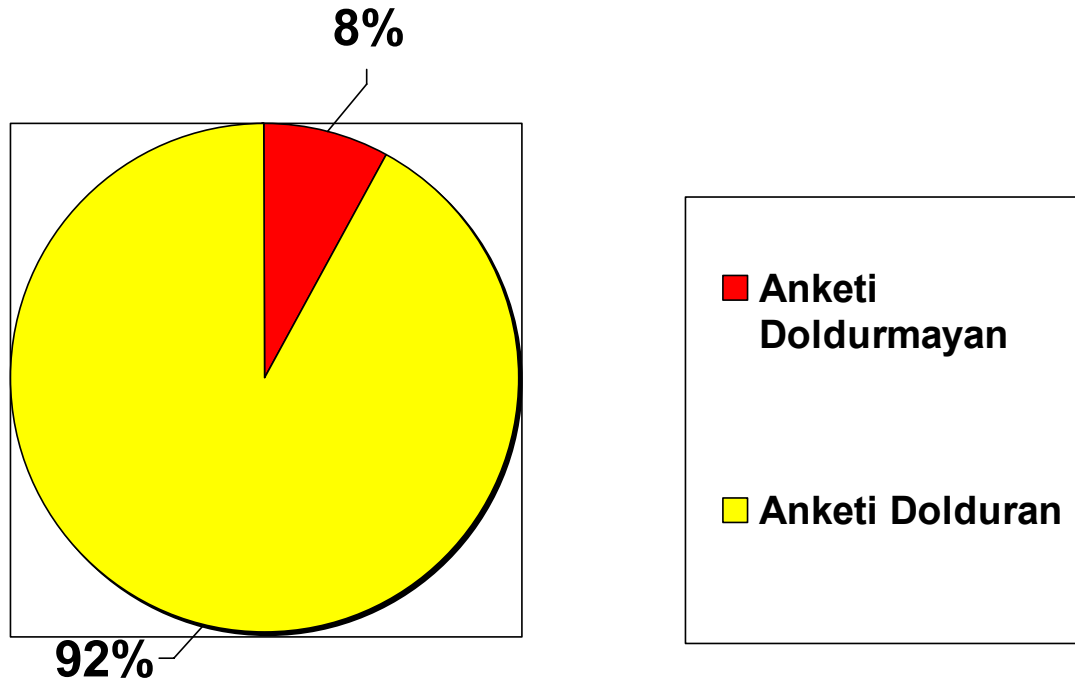
2006 dan bir örnek

Ağ yöneticileri ile iletişim



2009 dan bir örnek

Ağ yöneticileri ile iletişim



İş Planı – (Mayıs 2008 - Mayıs 2009) Bugün



Ulak-CSIRT Tr-CERT işbirliği

82 Farklı uçtan 91 kişi eğitime katılım sağlanmıştır.

Eğitimin Konuları

Sınır Güvenliği

Microsoft Sistemleri Güvenliği

Linux \ Unix Güvenliği

Kablosuz Ağ Güvenliği

- 23-27 Haziran 2008: 30 kişi katılmıştır.*
- 07-11 Temmuz 2008: 31 kişi katılmıştır.*
- 15-20 Şubat 2009 : 30 kişi katılmıştır.*

PC Yönlendirici Ç.G. Faliyetleri

Üretilen belgeler

- PC Yönlendirici Genel Bilgiler: 11 adet
- PC Yönlendirici Linux Tabanlı : 11 adet
- PC Yönlendirici BSD Tabanlı: 3 adet
- İşletim Sistemleri - Debian: 1 adet
- İşletim Sistemleri - FreeBSD: 3 adet
- İşletim Sistemleri - Genel: 3 adet
- İşletim Sistemleri - Linux: 12 adet
- İşletim Sistemleri - Unix: 1 adet
- İşletim Sistemleri - Microsoft: 2 adet

Sunumlar

Gökova Çalışmayı 2007:

- Pc Yönlendirici ve Güvenlik Merkezi Çalışma Grubu (pdf) "Gökhan Eryol - ULAKBİM"
- Özgür Yazılım Çözümleri Ağ Yönlendirici Cihazı (pdf) "Hüsnü Demir- O.D.T.Ü"
- Linux ile Ağ Yönetimi (pdf) "Can Uğur Ayfer, Yavuz Selim Kömür - Bilkent Üniversitesi"
- Pc Yönlendirici ve Güvenlik Merkezi Çalışma Grubu (pdf) "Sertaç Selim Sarıca - Süleyman Demirel Üniversitesi"

Konya Çalışmayı 2008:

- Metro Ethernet Teknolojileri (pdf) - Gökhan Eryol TÜBİTAK ULAKBİM
 - OpenPGP ve Web of Trust (pdf) - Gökhan Eryol TÜBİTAK ULAKBİM
 - PC Yönlendirici ve Temel Ayarlar (pdf) - Gökhan Eryol TÜBİTAK ULAKBİM
 - Güvenlik Merkezi (pdf) - Hüsnü Demir ODTÜ
3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009

Web Güvenliđ Ç.G. Faaliyetleri



1. Tercüme OWASP ilk 10 - En Kritik 10 Web Uygulaması Güvenlik Zayıflıkları ? 2007

http://csirt.ulakbim.gov.tr/dokumanlar/Ceviri_OWASP_ilk10_2007.pdf

Katılanlar:

Enis Karaarslan, Ege Üniversitesi

Murat Sürücü, Karaelmas Üniversitesi

Nazım Karadağ, Ondokuz Mayıs Üniversitesi

Oğuzhan Yalçın, Gazi Üniversitesi

Vedat Fetah, Ege Üniversitesi

2. Web Güvenliđi Günleri -2007

<http://agguvenligi.blogspot.com/2007/12/web-gvenlii-gnleri-izmir-ardndan.html>

Katılanlar:

Bünyamin Demir - Web Güvenlik Topluluđu

Bedirhan Urgan - Web Güvenlik Topluluđu

Oğuzhan Yalçın - ULAK-CSIRT

Enis Karaarslan - ULAK-CSIRT

Tahsin Türköz - UEKAE-TÜBİTAK

3. "Kurumsal Web Güvenliđi Yapısı" Bildirisi

http://csirt.ulakbim.gov.tr/dokumanlar/Karaarslan_KurumsalWebGuvenligi2008.pdf

Akademik Bilişim 2008 'de sunuldu

4. "Kurumsal Web Güvenliđi Yapısı" Gökova'da sunuldu

5. Zayıflık Tarama sistemi kuruldu - Çalıştayda sunuldu-Gökova 2008

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009



Balküpu ve Karadelik Ç.G. Faaliyetleri



Grubun çalışması sürecinde oluşturulan çıktılar şu şekildedir:

- ULAKNET Balküpu Sistemi
- Balküpu İstatistikleri Servisi
- Balküpu & OLTA entegrasyonu
- AB 2007, AB 2008 Çalışma Grubu sunumları
- I.ULAKNET Eğitim ve Çalıştayı "Balküpu Test Yatağı Sunumu"
- I.ULAKNET Eğitim ve Çalıştayı "Honeyd Kurulumu Sunumu"
- II.ULAKNET Eğitim ve Çalıştayı "ULAKNET Balküpu Sistemi Sunumu"
- Ulak-CSIRT "Honeyd Kurulumu Belgesi"
- Ulak-CSIRT "Honeywall Kurulumu Belgesi"
- Soysal, M., Bektas O., Analysis of Attacks Towards Turkish Academic Network, ISCTURKEY'08, pp. 126-131, 25-27 December 2008, Ankara, Turkey

Sunum ve belgelere <http://www.ulakbim.gov.tr/ulaknet/dokuman> sayfasından ulaşabilirsiniz.

Ağ Kimlik Denetimi Çalışma Grubu



(Gökhan AKIN – İTÜ / Hüseyin YÜCE - Marmara Üni. / Hüsnü DEMİR - ODTÜ)

Çalışma Grubu dahilinde hazırlanmış ve 2008 Konya Çalıştay'ında sunumları gerçekleştirilmiş olan Kimlik Denetim Klavuzu ve detaylarını gösteren çeşitli sunumlar şu şekilde :

1. **FreeRADIUS - LDAP ile Kimlik Denetimi Klavuzu** ([pdf](#)) - Sunumu ([pdf](#))

2. **Free Radius Kurulum Detayları Sunumu** ([pdf](#))

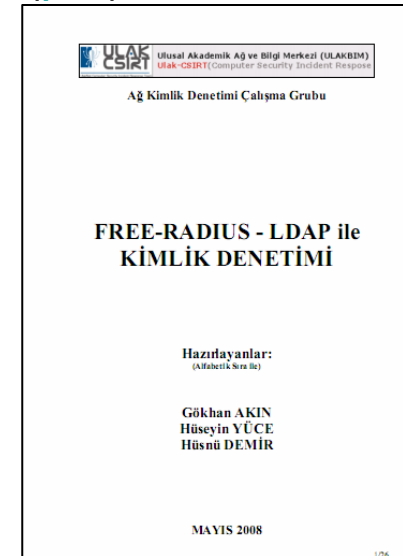
3. **FreeRADIUS ve LDAP ile 802.1x Ağ Kimlik Denetimi Sunumu** ([pdf](#))

3. **Ağ Erişim Kontrolü Sunumu(NAC)** ([pdf](#))

4. **ACS Kimlik Denetimi Sunucusunda PEAP yapılandırması ve Active Directory Entegrasyonu Sunumu** ([pdf](#))
(Ahmet UNCU – İTÜ / Gökhan AKIN – İTÜ)

Sunum ve belgelere <http://www.ulakbim.gov.tr/ulaknet/dokuman> sayfasından ulaşabilirsiniz.

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009



Zararlı Yazılımlar ile Mücadele

Korsan Grubu 😊



Enis Karaarslan – Ege Üniversitesi / Gökhan AKIN – İTÜ

Çalışma Grubu dahilinde Akademik Bilişim 2008 ve Ulaknet Konya Çalıştay'ında sunumlar gerçekleştirilmiş tir. Çalışma sonucunda oluşturulmuş Kurumsal Aglarda Zararlı Yazılımla Mücadele Klavuzu ve sunumları şu şekildedir:

ULAKNET Çalıştayı 2008 (Konya)

Kurumsal Aglarda Zararlı Yazılımla Mücadele Klavuzu ([pdf](#))- Sunumu: ([pdf](#))

Akademik Bilişim 2008(Çanakkale)

Kurumsal Aglarda Zararlı Yazılımla Savaş Bildirisi ([pdf](#)) Sunumumu: ([pps](#))

Sunum ve belgelere <http://www.ulakbim.gov.tr/ulaknet/dokuman> sayfasından ulaşabilirsiniz.

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009



Amaçlar (Mayıs 2009 - Mayıs 2010) Yarın

Ulak-CSIRT Çalışma Grupları (2007)

**ULAKNET Servisleri
(Balküpe, PC Yönledirici)
(2009)**

**ULAKNET
Ağ Araştırmaları Ç.G.
(2009)**

- Web güvenliği(Eski Ç.G.)
- 802.1x uygulamaları(Eski Ç.G)
- Kullanıcı tespit yöntemleri (5651)
- Yeni Öneriler???

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

3. ULAKNET ÇALIŞTAY ve EĞİTİMİ – Didim 02.06.2009

