

# ULAKBİM (Ulusal Akademik Ağ ve Bilgi Merkezi) OLTA Güvenlik Olay Takip Süreci ve İstatistiksel Verileri

Kenan KOÇ<sup>1</sup>, Çağlar GÜLÇEHRE<sup>1</sup>, Aslıhan TÜFEKÇİ<sup>2</sup>

<sup>1</sup> TÜBİTAK-ULAKBİM, Ağ Teknolojileri Birimi, Ankara,

<sup>2</sup> Gazi Üniversitesi, Bilgisayar Eğitimi Bölümü, Ankara,

kenan@ulakbim.gov.tr, caglar@ulakbim.gov.tr, asli@gazi.edu.tr

**Özet:** OLTA, ismi “OLay TAKipçisi” kelimelerinin baş harflerinin kısaltılması ile oluşturulan, Ulusal Akademik Ağa (ULAKNET) veya ULAKNET ağından dış dünyaya yapılan saldırıların sorumlularını tespit etmek, saldırıyla karşılaşan ağın yöneticileriyle düzenli bir şekilde bilgi paylaşımını sağlamak amacıyla geliştirilmiş olan bir uygulamadır. OLTA uygulaması, TÜBİTAK Ulusal Akademik Ağ ve Bilgi Merkezi (ULAKBİM) bünyesinde bulunan ULAK-CSIRT(Computer Security Incident Response Team) tarafından yönetilmektedir. ULAK-CSIRT, dış ağlardan ULAKNET’e yapılabilecek güvenlik ihlallerini önleme, gerçekleşen saldırı ve sorumlularını tespit etme ve aynı şekilde, ULAKNET’ten dış dünyaya yapılan saldırıları önleme, eğer saldırı oluşmuşsa saldırı sorumlusunu tespit ederek saldırıyla karşılaşan ağın yöneticileriyle bilgileri paylaşmakla sorumludur.

OLTA sistemi, ULAK-CSIRT tarafındaki yetkililer ve ULAKNET’i kullanan kurumların bilgi işlem birimlerinde çalışan ağ yöneticilerinin kullanımına açıktır. Sistem sayesinde olay kayıtları üzerinde gerekli takipler ve güncellemeler yapılarak hem olay kaydı sahibinin, hem şikayetçinin, hem de ULAK-CSIRT yetkililerinin bilgilendirilmesi ve karşılaşılan problemlerin çözülmesi sağlanmaktadır.

Bu çalışmada, OLTA sistemi hakkında detaylı bilgi verilecek, OLTA sistemi kullanan kullanıcılar atanan olay kayıtları hakkında detaylı bir şekilde istatistiksel bilgi verilecektir.

**Anahtar Sözcükler:** ULAKNET, Ağ Güvenliği, OLTA(Olay Takipçisi)

## ULAKBİM (Turkish Academic Network and Information Centre)’s OLTA Incident Handling Process and Statistical Data Related to Security Incidents

**Abstract:** OLTA is the acronym of Incident(OLAY) Tracker(TAKİPÇİSİ) and it is a web-based application that is used for detecting, tracking and handling the security incidents or either attacks that are targeted to the Turkish National Academic Network(ULAKNET) or attacks that are from ULAKNET to the other Networks. OLTA is administrated by TÜBİTAK- Turkish Academic Network and Information Centre (ULAKBİM) and the security team that are located in this body which is called ULAK-CSIRT(Computer Security Incident Response Team). The missions of Ulak-CSIRT is to ensure the present and future security of ULAKNET, take the lead on the ULAKNET security policy, coordinate security responses, develop security resources and to maintain leading-edge skills.

OLTA is open for administration by the authorized personel at ULAK-CSIRT team and use by system administrators and NOC(Network Operation Center)s at the computer centers that are directly connected to ULAKNET. OLTA helps the users to easily manage, handle and track the security incidents and it aids the ULAK-CSIRT to apply the certain security policies among the users of ULAKNET. It also helps connecting the ULAK-CSIRT and the other organizations that are connected to ULAKBİM in one central place.

In this study, we are going to give a detailed overview of OLTA application and present the detailed results of some statistical information gathered from the incidents opened in the OLTA.

**Keywords:** ULAKNET, Network Security, OLTA(Incident Tracker)

## 1-Giriş

ULAKBİM akademik kurumlara ve bunların kullanıcılarına başta bilgisayar ağları olmak üzere, bilgi teknolojisi desteği ile ulusal bilgi ve belge erişim hizmetleri sunmak amacıyla TÜBİTAK tarafından kurulmuş bir teknoloji kolaylık enstitüsüdür. ULAKNET ise ULAKBİM bünyesinde kurulan bir eğitim ve araştırma ağıdır[1].

ULAKNET bünyesinde bilgi güvenliği konusundaki bilincin artırılması, yaşanan bilgisayar güvenlik olaylarının sayısının azaltılması ve ağın kurulduğu tarihten bu yana sürdürülen çalışmaların daha koordineli bir hale getirilmesi için “ULAKNET Bilgisayar Olaylarına Müdahale Birimi”nin kurulmasına karar verilmiştir. Dünyadaki benzerleri ile paralel bir organizasyona sahip bu birim, Ulak-CSIRT (http://csirt.ulakbim.gov.tr) olarak adlandırılmış ve Şubat 2006’da faaliyetlerine başlamıştır[2].

Kurumların ULAKNET’i kullanabilmesi için Kullanım Politikası Sözleşmesini imzalanması gerekmektedir. İmzalayacak kişi rektör seviyesinde olması gerekmektedir. İmzalamayan kurumlar ULAKNET’i kullanamamaktadır. ULAKBİM kabul edilebilir kullanım politikasının 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 ihlalinin engellemekle ve bilgi akışını sağlamakla sorumludur.”

Kabul edilebilir kullanıcı politikası gereği, ULAKNET üzerinde çalışan bir kullanıcı, ağ ve sistem güvenliğini ihlal edemez (İstenmeyen e-posta mesajları, servis kalitesini etkileyerek trafik düzenlemeleri, fikri hakları ihlal edecek materyal dağıtmak vb). TÜBİTAK ULAKBİM, kabul edilebilir kullanıcı politikasında da belirtildiği gibi bir sorun halinde ulusal ve uluslararası bağlantıyı kesmek dahil acil önlemler alabilmektedir[3].

OLTA sistemi, ULAK-CSIRT yetkilileri ve üniversitelerin bilgi işlem birimlerinde çalışan ağ yöneticilerinin kullanımına açıktır. Sistem sayesinde olay kayıtları üzerinde gerekli takipler ve güncellemeler yapılarak hem olay kaydı sahibinin, hem şikayetçinin, hem de ULAK-CSIRT yetkililerinin bilgilendirilmesi ve karşılaşılan problemlerin çözülmesi sağlanmaktadır.

## 2- OLTA Sisteminde Açılan Olay Kayıtları

OLTA sisteminin açılımı Olay Takip Sistemi olarak açıklanmaktadır. OLTA olay kayıtlarının merkezi bir sistemde oluşturulup takip edilmesi için geliştirilmiş bir uygulamayı oluşturmaktadır. OLTA sayesinde olay kayıtları üzerinde gerekli güncellemeler yapılarak hem olay kaydı sahibinin, hem şikayetçinin, hem de Ulak-CSIRT yetkililerinin bilgilendirilmesi sağlanmaktadır[4].

### 2. 1. OLTA Sistemi Şikayet Türleri

OLTA sisteminde açılan olay kayıtları 9 ayrı şikayet türünden oluşmaktadır. Bu şikayet türlerinin kısaca ne oldukları hakkında aşağıda bilgi verilmektedir.

#### 2.1.1 Spam (İstenmeyen E-posta)

İnternet üzerinde aynı mesajın yüksek sayıdaki kopyasının, bu tip bir mesajı alma talebinde bulunmamış kişilere, zorlayıcı nitelikte gönderilmesi spam olarak adlandırılmaktadır. Spam çoğunlukla ticari reklam niteliğinde olup, bu reklamlar sıklıkla

güvenilmeyen ürünlerin, çabuk zengin olma kampanyalarının, yarı yasal servislerin duyurulması amacıyla yönelik olmaktadır. Spam gönderici açısından çok küçük bir harcama ile gerçekleştirilebilirken, mali yükü büyük ölçüde mesajın alıcıları veya taşıyıcı servis sağlayıcı kurumlar tarafından karşılanmaktadır[5].

Elektronik mesaj aracılığıyla gönderilen spam, doğrudan gönderilen mesajlarla bireysel kullanıcıları hedef almaktadır. Spam listeleri genellikle tartışma gruplarının üye listelerinin çalınması veya ağ üzerinden adres aramalarıyla oluşturulmaktadır. Spam gönderileri tipik olarak alan kullanıcının hem para (bağlantı ücreti) hem de zaman bakımından masraf yapmasına sebep olmaktadır. Bunun ötesinde, bu mesajlar internet üzerindeki trafiği artırarak başta servis sağlayıcılar olmak üzere birçok internet servisi üzerinde gereksiz yük oluşturmaktadırlar. Bu mesajların içeriği ticari olabileceği gibi, politik bir görüşü savunan mesajlar da olabilmektedir [6].

#### **2.1.2 Honeypot (Balküpü)**

Bilgi ve ağ güvenliğine yönelik yapılan saldırıların farkına varmak, saldırganların yöntemlerini izlemek, metodlarını belirlemek, yeni geliştirilen saldırı sistemlerinden önceden haberdar olmak için özel olarak tasarlanmış yazılım veya sistemlerdir. Bilişim sistemlerine karşı gerçekleşen saldırıların tespit edilmesi için kurulmuş olan tuzaklardır[7]. ULAKNET’te Balküpü Servisi bulunmaktadır. Bu servisten gelen uyarıları balküpü şikayeti olarak sınıflandırılmaktadır.

#### **2.1.3 Copyright (Telif Hakkı)**

Herhangi bir bilgi veya düşünce ürününün kullanılması ve yayılması ile ilgili hakların, yasalarla belirli kişilere verilmesidir. Kısaca, orijinal bir yaratının kopyalanmasına veya kullanılmasına izin verme hakkıdır. Orijinal bir yaratının izinsiz bir şekilde kopyalanıp kullanılması sonucunda gelen şikayetlerdir. Bilgisayar kaynaklarının paylaşımı P2P’in

(Peer to Peer) yaygınlaşmasıyla birlikte izinsiz kopyalanmalar da yaygınlaşmaktadır [8].

#### **2.1.4 Phishing(Olta Atma)**

Sosyal mühendislik teknikleri kullanılarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenlik isteyen bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanabilir. Phishing kelimesi İngilizce fishing (balık tutma) kelimesinden türetilmiş bir kelimedir. Bu anlamda kurbanlara phish (fish – balık) denilmektedir [9].

#### **2.1.5 Port Taraması (Port Scan)**

Günümüz dünyasında birçok işletim sistemi birden fazla programın aynı anda çalışmasına izin vermektedir. Bu programlardan bazıları dışarıdan gelen istekleri (istemci-client/request) kabul etmekte ve uygun gördüklerine cevap (sunucu-server/response) vermektedir. Sunucu programları çalışan bilgisayarlara birer adres verilmektedir (IP adresleri) ve bu adresler kullanılarak istenilen bilgisayarlara ulaşılmaktadır. Ulaşılan bu bilgisayar üzerindeki hangi sunucu programdan hizmet almak istendiği belirlemek ise port’lar sayesinde sağlanmaktadır. Bunun için bilgisayarlar üzerinde birtakım soyut bağlantı noktaları tanımlanmaktadır ve her birine adresleyebilmek amacıyla pozitif bir sayı verilmektedir (port numarası). Bazı sunucu programları, daha önce herkes tarafından bilinen portlardan hizmet verirken (örn: telnet->23. port) bazıları da sunucu programını çalıştıran kişinin türüne ve isteğine göre değişik portlardan hizmet vermektedir. Dolayısıyla, ağ üzerindeki herhangi bir sunucu programa bağlanmak istenildiğinde, programın çalıştığı bilgisayarın adresinin yanında istekleri kabul ettiği port numarasını da vermek gerekmektedir. Port numarası genellikle 2 byte olarak tutulmaktadır. Bu nedenle 65536 adet port numaralamak mümkündür. Genellikle 1024’ten küçük olan port

numaraları özel hakları olan kullanıcılar (root) tarafından kullanılırken, büyük olanlar genel kullanıma açık olmaktadır.

Port Scanner'ler (tarayıcı) ise varolan bu portları otomatik olarak tarayan yazılımlardır[10].

### 2.1.6 Unauthorized Access (İzinsiz Giriş)

Sunucu veya kullanıcının izni olmaksızın güvenlik açıklıklarından faydalanıp yetkisi olmadığı halde sisteme giriş yapılmasına denilmektedir.

### 2.1.7 DoS(Servis Dışı Bırakma)

Denial-of-Service yada kısaca DoS olarak adlandırılan saldırı yöntemi yazılımlardaki hataları kullanarak ya da sunucu veya ağ kaynaklarını tüketme yoluyla, normal kullanıcıların erişimlerini engelleyecek şekilde bilgisayar sistemlerini ulaşılamaz hale getirme amacıyla yapılmaktadır. Bu tip saldırılar yapılış tarzına bağlı olarak sistemi veya sistemin sunduğu hizmet yada hizmetleri tamamıyla devre dışı bırakabilir. DoS tipindeki saldırıları tehlikeli kılan bir başka yön ise çok eski tip makineler ve modemler ile çok karmaşık ve sofistike sistemlerin devre dışı bırakabilme olanağıdır. DoS tipindeki saldırılar sistemler ve sistemlerin sunduğu servislerin çeşitliliği göz önüne alındığı zaman çok fazla çeşide sahip olması sonucu ortaya çıkar[10].

### 2.1.8 Virus (Virüs)

Programlandığı görevi yerine getirmek için başka bir programa ihtiyaç duyan yazılımları oluşturmaktadır. E-posta, sisteme eklenen depolama aletleri, internetten indirilen ya da depolama aletlerinden alınan yazılımlar ve ya işletim sistemi açıklıklarını kullanarak ağ yoluyla da virüsler bulaşabilmektedirler[11].

### 2.1.9 Diğer

OLTA sisteminde 8 adet şikayet türüne uymayan şikayetlere diğer şikayeti olarak olay kaydı açılmaktadır.

## 3. OLTA Sistemi İhtiyaç Analizi

Bu bölümde OLTA sisteminin neden kurulma ihtiyacı olduğunu ve OLTA sisteminin kullanımı hakkında detaylı bilgiler verilmektedir.

OLTA sistemini ULAKNET uç sorumlularını ULAKNET ağ güvenliği konusunda bilinçlendirmek amacıyla kurulmuştur.

### 3.1 OLTA Sisteminin Geliştirilmesi

OLTA sistemi kurulumunda açık kaynak kodlu bir yazılım olan RTIR kullanılmaktadır. RTIR yazılımı, açılan olay kayıtlarını takip etmek amacıyla yazılmıştır. Bu açık kaynak kodlu yazılımı birçok alanda özelleştirilerek kullanılabilir. RTIR,görevler oluşturmak, bunları ilgili kişilere atamak ve bu görev ile ilgili yapılanları takip etmek, en sonunda ise verilen görev yerine getirildiğinde görevi kapatmak amacıyla kullanılmaktadır.RTIR programında OLTA sistemi oluşturulurken bir çok değişiklikler yapılmıştır. İlk olarak tüm ULAKNET kullanıcılarının bilgileri sisteme girilmektedir. ULAKNET ağını kullanan üniversitelerden [abuse@uc\\_domain](mailto:abuse@uc_domain) adresi (Örneğin [abuse@gazi.edu.tr](mailto:abuse@gazi.edu.tr)) açmaları istenmiştir ve bu açılan mail adresi kullanıcı adı olarak atanmıştır. Ayrıca bu mail adresine olay kayıtları ile ilgili yapılan tüm güncellemeler ve bilgiler gönderilmektedir. ULAKNET Olay Kaydı Politikası [12] kuralları OLTA sitemine girilmiştir. Şikayete konu IP'yi kullanan ULAKNET ucu ve o ucun sorumlusu ile ilgili bilgilerin veri tabanından çekilmesi için modüller eklenmiştir. Daha sonra şifre hatırlatma modülü eklenmiştir. Tüm gerekli bilgiler OLTA sistemine eklenince sistem aktif olarak kullanılmaya başlanmıştır.

### 3.2 OLTA Sisteminin Kullanımı

OLTA sistemi nasıl kullanılır kısmına geçmeden önce OLTA sisteminde kısaca nasıl olay kaydı oluşturulduğunu anlatmakta fayda görülmektedir.

a-csirt/abuse/olta@ulakbim.gov.tr adresine gelen saldırı şikayeti e-postaları,

b-http://csirt.ulakbim.gov.tr/ adresinde linki bulunan <https://olta.ulakbim.gov.tr/trouble/index.php> adresinden yapılan şikayetleri

c- Balküpi Servisinden gelen bildirimleri,

d- Diğer yollarla gelen şikayetleri,

değerlendirilmekte ve geçerli bulunanlar hakkında olay kaydı açılmaktadır. Açılan bu olay kayıtları ilgili kurumlara atanmaktadır.

ULAKNET ağını kullanan uca ait IP'lerden birisiyle ilgili olay kaydı açıldığında abuse@uc\_domain adresine bir bilgilendirme e-postası atılmaktadır. Gelen e-postayı okuyan uç sorumlusu OLTA sistemine giriş yaptığında "Benim Açık Biletim" başlığı altında o uca ait henüz kapatılmamış olayları görebilmektedir. Olayın konu başlığına tıklayarak ilgili olay kaydı detaylarını inceleyebilmektedir.

Uç yöneticileri kendilerine atanan olay kayıtlarını belirli süreler içinde müdahale etmelidir. Olay kaydı politikasında iki adet zaman kısıtı vardır:

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

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

Bu açıklamalar doğrultusunda uç sorumlusu yeni bir olay bildirimini aldığı anda, olayın detaylarını incelemeli ve OLTA sisteminde "Cevapla" fonksiyonunu kullanarak olay araştırmasının başladığını belirtmelidir (İlk Tepki Süresi Sonuna kadar). Daha sonra olay hakkında yeni bilgiler edindikçe yine aynı şekilde OLTA sisteminde "Cevapla" fonksiyonu kullanılarak olay güncellenmelidir. Ulak-CSIRT üyeleri güncellemeler sonucu olayın çözüldüğüne karar verilerse ilgili olayı kapatmaktadır.

### 4- OLTA Sisteminde Açılan Olay Kayıtları İstatistikleri

OLTA sistemine Ekim 2008'de olay kaydı girilmeye başlanmıştır. Bu tarihten itibaren sisteme girilen veriler 08 Ocak 2010 tarihinde sistemden alınmıştır. Bu süre içerisinde toplam 3682 adet olay kaydı oluşturulmuş olup, bu olay kayıtları Çizelge 1'de detaylı olarak verilmektedir.

#### 4.1. Şikayet Türüne Göre Olay Kayıtları İstatistikleri

Çizelge 1'de bugüne kadar oluşturulan tüm olay kayıtları şikayet türüne göre verilmektedir. En çok oluşturulan şikayet türü spam, şikayeti olmuştur. Şikayet türlerini olay kayıt politikası gereği önem derecesine göre incelediğimizde ters orantılı bir durum söz konusu olmaktadır. Oluşturulan şikayetin derecesi arttıkça oluşan şikayet sayısı da azalmaktadır. Phishing, port tarama, izinsiz giriş ve DoS şikayetleri sayıca az olmasına rağmen ağa veya kişisel verilere verebilecekleri zararlar bunlar dışındaki şikayetlerden çok daha fazla olabilmektedir. Bu durum örneklerle açıklanabilmektedir. DoS saldırısı yazılımlardaki hataları kullanarak ya da sunucu veya ağ kaynaklarını tüketme yoluyla, normal kullanıcıların erişimlerini engelleyecek şekilde bilgisayar sistemlerini ulaşılamaz hale getirme amacıyla yapılmaktadır. DoS saldırısına uğrayan bir kurumda normal kullanıcıları ağı kullanamaz duruma gelebilmekteledir. Eğer DoS saldırısı yapılan ağın çok fazla kullanıcısı var ise, bu durum çok büyük bir prestij kaybına da neden olabilmektedir.

Şikayet Türüne Göre Olay Kayıtları										
Durumu	Spam	Balküpü	Copyright	Phishing	Port	Giriş	Dos	Virüs	Diğer	Genel Toplam
Çözülmüş	1107	638	162	33	35	16	13	7	10	2021
Açık	677	787	171	6	3	5	1	4	7	1661
<b>Toplam</b>	<b>1784</b>	<b>1425</b>	<b>333</b>	<b>39</b>	<b>38</b>	<b>21</b>	<b>14</b>	<b>11</b>	<b>17</b>	<b>3682</b>

**Çizelge1:** Şikayet Türüne Göre olay Kayıtları

Phishing sosyal mühendislik teknikleri kullanılarak, kurbanın şifreleri, banka hesap numaraları, kredi kartı bilgileri gibi özel ve yüksek güvenlik isteyen bilgilerini, kurbanı aldatarak elde etme yöntemi olarak tanımlanmaktadır.

Phishing saldırısı yapılarak kurbanın kişisel bilgilerini, banka hesap numarasını, kredi kartı bilgileri ve şifrelerini alılabilmektedir. Phishing saldırısı yaparak bu bilgilere sahip olan kişi, kurbanın banka hesabında bulunan paraları istediği hesap numarasına veya kişiye aktarabilmektedir. Kurbanın kredi kartını kendi çıkarları için kullanabilmektedir.

Çizelge 1'in 1. satırında 08 Ocak 2010 tarihine kadar toplam 2021 adet olay kaydının çözüldüğü görülmektedir. Olay kayıtlarının çözülebilmesi için, uç tarafındaki sorumlu kişilerin ilgili olay kaydında bulunan "cevapla" fonksiyonunu kullanarak olay kaydı için aldığı önlemleri yazmalıdır. Alınan önlemlerin yeterli görüldüğü takdirde CSIRT yetkilileri tarafından ilgili olay kaydı çözülmektedir.

Çizelge 1'in 2. satırında ise 08 Ocak 2010 tarihine kadar toplam 1661 adet olay kaydının açık olduğu görülmektedir. Bu olay kayıtlarının hala sorumlu kişiler tarafından cevaplanmadığı gözlenmektedir. Olay kayıtlarının kapatılmamış olması istenen bir durum olmamakla birlikte, sorumluları tarafından bir an önce ilgilenilmesi gerekmektedir. Olay kayıtlarından phishing, port tarama , izinsiz giriş ve DoS şikayetleri için olay kayıt politikası gereği gerekli işlemler yapılmaktadır.

Çizelge 1'in 3. satırında ise 08 Ocak 2010 tarihine kadar toplam 3682 olay kaydı

bulunmaktadır. Bu olay kayıtları, hem çözülmüş olay kayıtlarını hem de açık olay kayıtlarını toplamını oluşturmaktadır. OLTA sisteminde açık olay kaydının bulunmaması gerekmektedir. Olay kayıtlarına zamanında müdahale edip önlemler almak gerekmektedir.

## 5 Sonuç

Bu çalışmada OLTA sisteminde açılan olay kayıt türlerinin neler olduğu OLTA sisteminin geliştirilmesi, OLTA sisteminin kullanımı ve OLTA sisteminde açılan olay kayıt istatistikleri hakkında bilgi vermektedir.

OLTA sistemi olay takibini kolaylaştırmak için kurulmuştur. ULAKBİM Olay Kaydı Politikasında bahsedildiği gibi OLTA Sistemi 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 paylaşılmasını sağlamaktadır. Kullanıcı kuruluşlar, ULAK-CSIRT tarafından önem seviyesine göre belirlenerek talep edilen süre içerisinde istenilen bilgileri sağlamakla, gerekli önlemleri alarak güvenlik ihlalinin engellemekle ve bilgi akışını sağlamakla sorumlu olmaktadır.

OLTA sisteminin en temel özelliği ULAKNET uç sorumlularını ULAKNET ağ güvenliği konusunda bilinçlendirmek amacıyla kurulmuştur. OLTA sistemi hakkında kullanıcılara bilgi vermek amacıyla 1 Haziran 2009 tarihinde Aydın'da Ulaknetçe Eğitim ve Çalıştayı'nda sunum yapılmıştır.

OLTA sistemi ULAKNET'in güvenlik olay takip sürecinin vazgeçilmez bir parçasıdır. Bu sistem sayesinde ULAKNET'i kullanan kurumlara yapılan saldırılar olay kaydı haline dönüştürülüp anında ilgili kurumlara mail yoluyla bildirilmektedir. Yapılan saldırılardan haberdar olan kurumlar da gerekli önlemleri alabilmektedirler.

#### KAYNAKÇA

1. ULAKBİM Yönetmeliği., 17.10.2001 tarih ve 24556 sayılı Resmi Gazete'de yayımlanmıştır.
2. SOYSAL Murat, Ulak-CSIRT Dünü, Bugünü Yarını, 3.ULAKNET Çalıştay ve Eğitimi., 2009
3. KONUSUŞ Kürşad Yusuf, SOYSAL Murat, TEMİZSOYLU Onur., "ULAKNET 2003" ULAKNET Sistem Yönetimi Konferansı Ekim 2003, Ankara
4. GÜLÇEHRE Çağlar, KOÇ Kenan., OLTA Sistemi Sunumu., 3. ULAKNET Çalıştay ve Eğitimi., 2009
5. Spam Nedir?, <http://www.spam.org.tr/nedir.html>, 15 .01.2010
6. GÜNGÖR Tunga, GÜRGEN Fikret, ÖZGÜR Levent., Uyarlamalı Türkçe Spam-Önler Filtrelemesi, Boğaziçi Üniversitesi
7. BEKTAŞ Onur, SOYSAL Murat, Ulak-CSIRT Balküpe Çalışma Grubu, 2008
8. AKIN Gökhan, FETAH Vedat, SOYSAL Murat., P2P ile Yaşamak., AB 2006
9. ALATAŞ Şükrü, ATAN Murat PHISHING: İnternet Denizinin Popüler Avlanma Yöntemi,AB 2007
10. Ahmet BERKAY, Hack Teknikleri, Gebze Yüksek Teknoloji Enstitüsü
11. KONUSUŞ Kürşad Yusuf; SOYSAL Murat; TEMİZSOYLU Onur., İstenmeyen Trafik., AB 2005.
12. ULAKBİM, Ulak-CSIRT Olay Kaydı Politikası, <http://csirt.ulakbim.gov.tr/politika/> , 15.01.2010