



Ağ Güvenliği Akademisi #20

Ulusal Güvenlik ve ULAK-CSIRT

Bu bölümde ulusal güvenlik ihtiyacından yola çıkarak, güvenlik ve acil durum merkezleri hakkında bilgi vermeye çalışacağım. ULAK-CSIRT oluşumu hakkında Ulakbim'den Murat Soysal bizi bilgilendirecek. Bu yazı dizisi boyunca çeşitli güvenlik açıklarından ve güvenlik önlemlerinden söz ettik. Ağ güvenliği söz konusu olunca, biz güvenlik konusunda çalışan kişiler bile her geçen gün yeni birşeyler öğreniyoruz. Güvenlik açıklarını sürekli takip etmek, karşı önlemleri öğrenmek gerekmektedir. Güvenli ağlar için bilinçli kullanıcılar ve en önemlisi bilinçli/bilgili sistem yöneticileri gerekmektedir.

Özellikle e-devlet kavramı ile ulusal bilgi kaynaklarının güvenliğinin sağlanması çok daha önemli hale gelmektedir. Siber savaşlar ve siber terörizm de ulusal güvenlik kavramına yeni boyutlar getirmektedir. Ulusal güvenlik tehditlerinin analiz edilmesi ve güvenlik politikalarının oluşturularak uygulanması gerekmektedir. Ulusal güvenliğin sağlanması için, öncelikle güvenlik birimlerinin oluşturulması gerekiyor. Bunlar dünya çapında "Computer Emergency Response Team" (CERT - <http://www.cert.org/>) ve "Computer Security Incident Response Team" (CSIRT) adlarıyla tanımlanmaktadır. Dünyadaki bu tür organizasyonların belirli standartları sağlaması gerekmektedir ve bu standartları sağlayan organizasyonlar birbirleriyle devamlı iletişim halindedir.

Kurucu ekibinde yer almaktan onur duyduğum Ulak-CSIRT (Bilgisayar Olaylarına Müdahale Birimi) oluşumu hakkında Ulakbim'den Murat Soysal'a bazı sorular yönelttim:

Ulakbim ve akademik ağ hakkında kısa bir bilgi verebilir misiniz?

Türkiye'deki üniversiteler ve araştırma kurumlarını birbir-

lerine bağlayan Ulusal Akademik Ağ (UlakNet) altyapısını Ocak 1997'de tamamlamış ve küresel internete bağlanmıştır. TÜBİTAK'ın bir enstitüsü olan ULAKBİM (<http://www.ulakbim.gov.tr>) tarafından işletilen bu ağa şu an halen 75 üniversite ve bunların fakülte, meslek yüksek okulları ve diğer altbirimleri, TÜBİTAK birimleri, Askeri Okullar ve Harp Akademisi, Polis Akademileri, Süleymaniye Kütüphanesi, Türk Tarih Kurumu, Milli Kütüphane, YÖK, ÖSYM, Türkiye Atom Enerjisi Kurumu ve Türk Silahlı Kuvvetleri Ar-Ge birimlerinden oluşan pek çok kuruluşa toplam 650 kiralık hat, frame relay ve ATM devresi üzerinden ücretsiz olarak hizmet sağlanmaktadır. Şu an ağda yaklaşık olarak 2 milyon üzerinde kullanıcı ve 200.000 bilgisayar bulunmaktadır.

UlakNet Avrupa Akademik ağı olan Geant'a olan bağlantı kapasitesi 622 Mbps'dir. Akademik ağın global Internet çıkışları Ankara PoP noktasından 1 Gbps, İstanbul PoP noktasından 700 Mbps olmak üzere toplam 1,7 Gbpsdir.

ULAK-CSIRT nedir?

Ulak-CSIRT (<http://csirt.ulakbim.gov.tr>) Ulusal Akademik Ağ kapsamında kurulmuş bir güvenlik birimidir. Dağıtık sorumluluk paylaşımı ilkesiyle kurulan birim, UlakNet'e bağlı uçlar bünyesinde çalışan, güvenlik konusunda bilgi ve tecrübe sahibi ağ uzmanlarından oluşmaktadır. ULAKBİM Teknik Müdür Yardımcısı Serkan Orcan koordinasyonunda kurulan birimin üyeleri Murat Soysal (ULAKBİM), Enis Karaarslan (Ege Üniversitesi), Gökhan Eryol (O.D.T.Ü) ve Hüseyin Yüce (Marmara Üniversitesi)dir.

Neden böyle bir oluşuma gerek duyuldu?

Bilgi teknolojilerindeki hızlı gelişime ayak uydurmada özellikle teknik eleman konusunda zorluk çekilen ülkemizde

“Bilgi Güvenliği” alanında da sıkıntılar yaşanmaktadır. Ayrıca tüm dünyada bilgi teknolojilerinin yaygın kullanımına rağmen genel bir eksiklik olan bilgi güvenliği alanındaki bilinç eksikliği Ulusal Akademik Ağ bileşenlerinde de gözlemlenmiştir. Bu birimin kurulmasındaki temel neden bu eksikliklerin giderilmesidir.

Bu oluşumla amaçlananlar nelerdir?

Özelde UlakNet, genelde ise ülkemizde Bilgi Güvenliği bilinç ve uygulamaları konusunda temel eksiklikler olduğunu düşünüyoruz. Daha detaylı incelemeler yapıldığında bu olumsuzluk, uçlardaki kısıtlı eleman sayısı, yabancı dil yetersizliği ve bilgi eksikliğinden kaynaklanmaktadır. Ulak-CSIRT, dış ağlardan UlakNet’e yapılabilecek güvenlik ihlalleri ve UlakNet’ten dış dünyaya yapılan saldırılar konularında ağ genelinde hissedilen ihtiyacı karşılamayı ve uzun vadede ağa güvenlik bilicini yaymayı amaçlamaktadır.

Bu amacı daha da netleştirsek:

- Ağ genelinde bilgi güvenliği bilincini artırmak,
- Akademik ağa yapılan bilgisayar güvenliğini tehdit edici saldırı sayısını azaltmak,
- Güvenlik ihlali sorumlularını tespit etme aşamasının koordinasyonunu sağlamak,
- Güncel açıkları ve çözümleri hakkında ağa bağlı uçların yöneticilerini bilgilendirmek,
- Bağlı uç yöneticilerine bilgi güvenliği hakkında eğitim vermek
- Bilgi güvenliğini sağlamak için kullanılacak yöntemler hakkında Türkçe döküman sağlamak

Bu oluşumda ne tür güvenlik hizmetlerinin verilmesi hedefleniyor?

Daha öncede belirttiğim gibi, bu birimi oluştururken dağıtık sorumluluk paylaşımı ilkesini benimsedik. Böylece kısa vadede ağ ve bilgi güvenliği konusunda deneyimli uzmanları bir araya getirerek UlakNet’i dış ağlardan gelen saldırılara karşı güvenli hale getirmeyi, bununla birlikte dış ağlara yapılan saldırılarda sorumlu tespit aşamasını koordine ederek UlakNet’in dış dünyadaki prestijini artırmayı planlamaktayız. Bu amaçlara yönelik hedeflediğimiz çalışmalarını şöyle sıralayabiliriz:

- Güvenlik Olaylarına müdahale
- Güncel açıklar ve tehditler hakkında Türkçe uyarılar sağlanması
- Güvenlik uygulamaları konfigürasyonu ve çalıştırılması (Türkçe Dokümantasyon)
- Eğitim-Çalıştay
- Olay bildirim formu işletimi (trouble ticket)
- Hukuki konularda takip ve bilgilendirme
- Ulakbim ve uçların hukuki sorumlulukları

UlakNet’in dış dünyadaki prestijinden söz ettiniz. Ulak-CSIRT benzeri diğer oluşumlardan bahsedebilir misiniz?

CERT-CSIRT benzeri oluşumlar iyi yönetilen bir çok ağda yer almaktadır. Bilgi teknolojilerinin doğası gereği güvenlik tüm İnternet için bir bütün teşkil etmektedir. Bu da CSIRT birimlerinin tam koordinasyonunu gerektirmektedir. Bu amaçla kurulmuş olan FIRST (The Forum of Incident Response and Security Teams) ve TI (Trusted Introducer) organizasyonları ile kurduğumuz sürekli iletişimi, en kısa sürede akredite olarak resmi bir platforma taşımayı amaçlamaktayız. Bu akreditasyonun tamamlanması Ulak-CSIRT’i ve dolayısıyla UlakNet’i güvenlik konusunda daha prestijli bir nok-

taya taşıyacaktır. Tabi ki prestijden daha önemlisi, diğer birimlerle paylaşımdan sağlanacak birikimlerle “UlakNet Bilgi Güvenliği” en üst düzeye taşınacaktır.

taya taşıyacaktır. Tabi ki prestijden daha önemlisi, diğer birimlerle paylaşımdan sağlanacak birikimlerle “UlakNet Bilgi Güvenliği” en üst düzeye taşınacaktır.

Ekleme istediğiniz bir şey var mı?

Son olarak World Wide Web (www) ve süper bilgisayar örneklerinden yola çıktığımızda görüyoruz ki bilgi teknolojileri konusunda dünyada her alanda önderliği akademik kurumlar yapmıştır. Bu ekseni ülkemize uyarladığımızda; Ulusal Akademik Ağ Güvenlik Birimi olarak uzun vadedeki en büyük amacımız akademik ağda oluşacak güvenlik bilinci, Türkçe dokümantasyon ve iyi yetişmiş teknik eleman altyapısını ülke geneline yayarak, gerek hızla gelişen devlet uygulamaları ile elektronik ortama taşınan kişisel bilgilerin korunmasına gerekse siber terorizm tanımı altına giren suçlar konusunda ülkemiz güvenliğine katkıda bulunmayı planlamaktayız.

Bu bölümde “Ulusal Güvenlik” kavramını ve ULAK-CSIRT oluşumunu özetlemeye çalıştık. Her türlü öneriniz için bana e-posta ile ulaşabilirsiniz.

