

1511 – ÖNCELİKLİ ALANLAR ARAŞTIRMA TEKNOLOJİ GELİŞTİRME VE YENİLİK PROJELERİ DESTEKLEME PROGRAMI

BİLGİ VE İLETİŞİM TEKNOLOJİLERİ-BİLGİ GÜVENLİĞİ ÇAĞRI DUYURUSU

1. Çağrı Kodu

1511-BIT-BGUV-2016-1

2. Çağrı Başlığı

Yerli Güvenlik Yazılımlarının Geliştirilmesi

3. Çağrı Gerekçeleri ve Amaçlar

Bilgi ve iletişim teknolojilerinin gelişmesi ve yaygınlaşması ile birlikte bilgi güvenliği alanında oluşan risklerde de artış gözlenmiştir. Bu alandaki önlemlere ek olarak, ülkemizde var olan yetkinliğin güçlendirilmesi ve kapasitenin artırılmasına yönelik bilimsel ve teknolojik çalışmalara gereksinim vardır. Söz konusu gereksinim doğrultusunda bu çağrı ile bilgi güvenliği konusunda özgün, yenilikçi, yüksek başarımlı ve kullanılabilirliği yüksek yazılım ve donanım sistemlerini geliştirmeyi hedefleyen projelerin desteklenmesi amaçlanmaktadır.

4. Çağrı Konu ve Kapsamı

Bilişim sistemlerinde güvenlik zafiyetlerini tespit, raporlama ve/veya önleme amacıyla geliştirilecek yazılım ve donanım tabanlı çözümleri hedefleyen projeler bu çağrı kapsamında değerlendirilecektir. Bunun yanı sıra bilgi sistemlerinin güvenliğine ilişkin bilgi birikimi ve farkındalık oluşturmaya yönelik eğitim ve denetim yazılım uygulamaları da aynı şekilde değerlendirmeye alınacaktır. Bu amaca yönelik olarak, proje çıktılarının aşağıdaki belirtilen gereksinimler dahilinde olması hedeflenmektedir.

Hedeflenen Çıktılar ve Teknik Özellikler:

- **Zararlı Yazılım Tespit Araçlarının Geliştirilmesi:**
 - o Zararlı Yazılımların Dinamik Analizi: Zararlı yazılımların dinamik olarak analizini yapacak, sıfırıncı gün saldırılarını (zero-day attacks) tespit edecek altyapı, yöntem ve yazılım araçlarının geliştirilmesi,
 - o Zararlı Yazılım İmza (Signature) Veri Tabanlarının Oluşturulması: Sürdürülebilir bir imza veri tabanının oluşturulması için gerekli altyapının ve yazılım araçlarının geliştirilmesi.
- **İzleme Araçları:** Ağ trafiğini ve sistem aktivitelerini gerçek zamanlı izleyen, anormallikleri tespit eden, raporlayan yazılım araçlarının geliştirilmesi.
- **Dağıtık Hizmet Dışı Bırakma (DDoS) Saldırılarına Tespit ve Etkisiz Bırakma:**
 - o Yüksek bant genişlikli saldırılara karşı koruma sağlayan donanım ve yazılım sistemlerinin geliştirilmesi,
 - o Test amaçlı yüksek bant genişlikli zararlı/normal ağ trafiği yaratan ve değişik test senaryolarını uygulayabilen donanım ve yazılım sistemlerinin geliştirilmesi.
- **Yazılımlardaki Güvenlik Zafiyetlerinin Tespiti ve Raporlanmasına Yönelik Yazılım Araçları:** İşletim sistemi ve uygulama kodlarının sistematik güvenlik testlerini gerçekleştirecek, açıkların bulunmasını ve raporlanmasını sağlayacak yazılım araçlarının geliştirilmesi.
- **Güvenlik Bilgi ve Olay Yönetim Yazılım Araçları:** Bu alanda geliştirilecek ürünlerin aşağıdaki özelliklere sahip olması beklenmektedir.

- Bilgisayar sistemlerinde hâlihazırda tutulan günlük (log) verilerinin etkin bir şekilde toplanması, birleştirilmesi, analizlerinin gerçekleştirilmesi ve raporlanması,
- Toplanan verilerin büyük veri sistemi içerisinde saklanması ve işlenmesi,
- Toplanan verilerin görselleştirilmesi.
- **Adli Bilişim Yazılım Araçları:** Bilişim suçlarının tespiti amacıyla aşağıda yer alan konulara yönelik sistemlerin geliştirilmesi;
 - Sabit disk ve hafıza imajı alma araçları,
 - İmaj dosyaları üzerinde etkin adli analiz yapma araçları,
 - Veri kurtarma araçları.
- **Güvenlik Eğitim Uygulamaları:** Bilgi güvenliği alanında çalışan personelin yetkinliğini geliştirmek ve ölçmek amacıyla kullanılacak, aşağıda muhtemel özellikleri listelenen eğitim yazılım araçlarının geliştirilmesi;
 - Mevcut senaryoları olan ve yeni senaryoların dinamik olarak eklenebilen,
 - Multimedya içerikle desteklenebilen,
 - Uzaktan öğrenimi destekleyen,
 - Etkileşimli çalışan.
- **Bilgi Güvenliği Denetleme Yazılım Araçları:** Bilgi güvenliği yönetim süreçlerinin denetimlerinin planlanması, denetlenmesi, raporlanması ve izlenmesi hususunda yazılımların geliştirilmesi.

5. Çağrı Takvimi

Çağrı Açılış Tarihi	22 Haziran 2016
Çağrı Kapanış Tarihi	2 Eylül 2016
Ön Kayıt Son Tarihi*	26 Ağustos 2016 Saat 17:30
Proje Öneri Başvuru Tarihleri	22 Temmuz 2016 - 2 Eylül 2016 Saat 17:30

*: Proje başvuruları yapabilmek için proje öneri başlığınız ve kuruluşunuz durumu ile ilgili belgeleri TÜBİTAK'a sunarak ön kayıt onayı almanız gerekmektedir. Burada belirtilen tarih bu evrakların TÜBİTAK'a evrak girişinin yapılabileceği en son tarihi ifade etmektedir. Bu tarihe kadar ön kayıt evraklarını TÜBİTAK'a ulaştıramayanlar proje başvurusu yapamayacaktır.

6. Çağrıya Özel Şartlar

Proje Süresi Üst Sınırı: 24 Ay

Proje Bütçesi Üst Sınırı: 2.000.000 TL

Ortaklı Proje Bütçesi Üst Sınırı: 3.000.000 TL

İşbirliği Yapısı: Kısıt Yok

7. İrtibat Noktası

Çağrı Sorumlusu	<i>Yunus Emre SEYYAR</i>	<i>0 312 468 5300/1836 yunusemre.seyyar@tubitak.gov.tr</i>
Ön Kayıt Sorumluları	<i>Fatih M. ŞAHİN</i>	<i>0 312 468 5300/1765 fatih.sahin@tubitak.gov.tr</i>
1511 Program Sorumlusu	<i>Halil Emre POLAT</i>	<i>0 312 468 5300/1846 halil.polat@tubitak.gov.tr</i>
Ayrıntılı bilgi için: www.tubitak.gov.tr/1511 E-mail: 1511@tubitak.gov.tr		

8. İlgili Belgeler

- 1511 Öncelikli Alanlar Araştırma Teknoloji Geliştirme ve Yenilik Projeleri Destekleme Programı Uygulama Esasları
- 1511 Proje Öneri Başvuru Formu (AGY111-02)

9. Ek Bilgi

- Proje başvuru tarihi itibari ile proje ekibinde proje konusu ile ilgili en az lisans düzeyinde **firma çalışanı** personel istihdam edilmeyen projeler hakem ataması yapılmadan ön incelemede reddedilir.
- Bu çağrı duyurusu TÜBİTAK 1511 kodlu “Öncelikli Alanlarda Araştırma Teknoloji Geliştirme ve Yenilik Projeleri Destekleme Programı” uygulama esasları çerçevesinde yapılmış olup, burada belirtilmeyen hususlar için uygulama esaslarında yer alan hükümler geçerlidir.