7/4602
6-K:122

T.C.
ULAŞTIRMA DENİZCİLİK VE HABERLEŞME BAKANLIĞI
Strateji Geliştirme Başkanlığı

27 Haziran 2012

Sayı : B.11.0.SGB.0.01.00.610.01/2014
Konu : Antalya Milletvekili
Sayın Mehmet GÜNAL'ın
yazılı soru önergesi

TÜRKİYE BÜYÜK MİLLET MECLİSİ BAŞKANLIĞINA

İlgi: 07.03.2012 tarihli ve A.01.0.KKB.0.10.00.00-52572 sayılı yazınız.

Antalya Milletvekili Sayın Mehmet GÜNAL'ın 7/4602 esas sayılı yazılı soru önergesinin cevabı hazırlanarak ekte sunulmuştur.

Bilgilerinize arz ederim.

Binali YILDIRIM
Bakan

EK :
1) Cevap formu (5 Sayfa)
2) Bilgi Notu (5 Sayfa)

Hakkı Turaliç Caddesi No:5 06338 Emek / Çankaya / ANKARA
Telefon: 203 13 45 Faks: 203 13 86
E-posta: sgb1@ubak.gov.tr İnternet Adresi: www.ubak.gov.tr
Ayrıntılı bilgi alınacak kişi:
Şakir ÖZDEMİR
Şube Müdürü

ANTALYA MİLLETVEKİLİ SAYIN MEHMET GÜNAL'IN 7/4602 ESAS SAYILI YAZILI SORU ÖNERGESİ VE CEVABI

BTK ve TÜBİTAK tarafından 25-28 ocak 2011'de 41 kurumun katılımıyla Ulusal Siber Güvenlik Tatbikatı uygulanmıştır. Tatbikat gereği kuruluşlara gerçek siber saldırı yapılmış ve 41 kurumun bilgi sistemleri teste tabi tutulmuştur. Tatbikat kapsamında 500'ün üzerinde yazılı enjeksiyon saldırısına ek port taraması, dağıtık servis dışı bırakma saldırıları (DDoS) gibi gerçek saldırılar düzenlenmiştir. Aralarında MSB, MGK, Ankara Başsavcılığı, Merkez Bankası, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) ve SPK gibi Türkiye'nin siyasi, askeri, ekonomik açıdan en önemli kurumlarının da içinde bulunduğu pek çok kurum söz konusu testi geçememiştir. Bu kurumların BGYS'si (Bilgi Güvenliği Yönetim Sistemi) bulunmadığı, saldırı tespit sistem ve süreçlerinde aksaklık olduğu, merkezi antivirüs yazılımlarının güncellenmediği, sistem tasarımı aşamasında güvenliğin gözardı edildiği, internet'e bağlı bilgi sistemlerine yapılan 'Port Tarama' saldırısını algılayamadığı ve Ddos saldırılarına yenik düştüğü gibi pek çok eksiklikler tatbikat sonucunda ortaya çıkmıştır. Ayrıca, Bilgi Teknolojileri ve İletişim Kurumu Basın ile ilişkiler Müdürlüğü'nün tüketici şikayetlerinin hızlı ve etkili bir şekilde çözümü amacıyla kurup 30 Ocak 2012 tarihinde hizmete açılan Online Şikayet Bildirim Sistemi'ne ait "tuketici.btk.gov.tr" sayfasına 12 Şubat 2012 Pazar günü bir saldırı gerçekleştirilmiş ve sayfa çökertilmiştir. Sistem çökünce, online şikayette bulunan vatandaşların e-mailleri, cep telefonları ve adresleri internete yayılmıştır.

Buna göre,

SORULAR:

1-BTK Ulusal Siber Güvenlik Tatbikatına neden gereksinim duymuştur?

2-Ortaya çıkan test sonuçlarından sonra kurumların güvenliğinde tedbir alınmış mıdır, alındıysa ne gibi tedbirler alınmıştır? Bu güvenlik sistemi test edilmiş midir?

3-BTK hali hazırda nasıl bir güvenlik sistemi uygulamaktadır? Bu sistem devletin ve vatandaşların bilgilerini korumakta yeterli midir?

4-BTK ve TÜBİTAK tarafından yapılan bilgi sistemleri testi sonucunda MSB, MGK, Ankara Başsavcılığı, Merkez Bankası, ve SPK gibi kurumlarda ortaya çıkan olumsuz sonuçlar Türkiye'nin siyasi, askeri, ekonomik açıdan risk altında bulunduğumuzu göstermez mi?

5-BTK Başkanı Dr. Tayfun Acarer 2011'de siber saldırıların yol açtığı zararların yüzde 56 oranında arttığını söylemiştir. Kurum şimdiye kadar kaç kere bu saldırılara maruz kalmıştır ve bu saldırıların maliyeti ne kadardır? Bu saldırılara karşı hangi tedbirler alınmıştır?

6-TÜBİTAK-BİLGEM (Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi) bünyesinde kurulan Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü(UEKAE) ve Bilişim Teknolojileri Enstitüsü (BTE) gibi kurumların kuruluş amacı nedir? TÜBİTAK'a bağlı bu kurumların bu sanal saldırılara karşı kurumları koruma projeleri var mıdır? Varsa uygulanmakta mıdır? Yoksa yapılması planlanmakta mıdır?

CEVAPLAR

10.11.2008 tarihinde yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu uyarınca Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından yapılacak düzenlemelerde bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi, elektronik haberleşme sektörüne yönelik olarak, milli güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirlerin alınması gerekmektedir. Ayrıca yine 5809 sayılı Kanun uyarınca, BTK işletmecilere kişisel veri gizliliğinin korunması ve izinsiz erişime karşı şebeke güvenliğinin sağlanması hususlarında yükümlülük getirme yetkisini haizdir.

Öte yandan, ülkemizin bilgi toplumuna dönüşüm sürecinin koordinasyonu amacıyla yürütülen e-Dönüşüm Türkiye Projesi kapsamında hazırlanan ve 2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı, *2006/38* sayılı Yüksek Planlama Kararı ile onaylanmış ve 28 Temmuz 2006 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe girmiştir. Eylem Planında yer alan "Ulusal Bilgi Sistemleri Güvenlik Programı" başlıklı 88 numaralı eylem ile Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne (UEKAE) kamu kurumları için gereken asgari güvenlik seviyelerini belirleme, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit etme ve eksiklikleri giderme konularında öneriler geliştirme görevleri verilmiştir.

Bilgi ve iletişim teknolojilerinin gelişimi ve internet kullanımının yaygınlaşması ile birlikte, geçmişte geleneksel yöntemlerle yapılagelen bir çok iş ve işlem günümüzde elektronik ortamda online olarak gerçekleştirilmektedir. Söz konusu uygulamalar arasında, internet bankacılığı, internet üzerinden alışveriş (e-ticaret), e-devlet kapısı ve ulusal yargı ağı (UYAP) üzerinden yapılan işlemler gibi birçok e-uygulamalar bulunmaktadır. Giderek yoğun bir şekilde kullanılan ve gelişen siber ortamda kullanıcılar ve kurumları hedef alması muhtemel tehditlere ilişkin kaygılar artmaktadır. Bu noktadan hareketle, siber ortamda bir güvenlik ihtiyacının olduğu gözlemlenmiştir.

Bu çerçevede son yıllarda internetin gelişimine paralel olarak dünyada ve ülkemizde siber güvenliğin sağlanmasına yönelik politika geliştirme çalışmaları ve uygulamalar yoğunlaştırılmıştır. Bu bağlamda, siber güvenlik konusunda idari, teknik ve hukuki kapasitenin geliştirilmesi, kurumlar arasında bilgi ve tecrübe paylaşımına ve başta yönetim seviyesinde olmak üzere tüm kademelerde farkındalık oluşumuna katkı sağlaması amacıyla siber güvenlik tatbikatları gerçekleştirilmesi düşünülmüştür. BTK ve TÜBİTAK tarafından 2011 yılında gerçekleştirilen ulusal siber güvenlik tatbikatı da bu kapsamda değerlendirilmektedir.

25-28 Ocak 2011 tarihinde gerçekleştirilen Ulusal Siber Güvenlik Tatbikatı'ndan (USGT) sonra web taraması ve dağıtık servis dışı bırakma saldırısına katılan kurumlara, sadece kurumun sistemlerinde tespit edilen açıklıkların ve bu açıklıkların nasıl kapatılacağı bilgisinin bulunduğu raporlar iletilmiştir. Daha sonra alınacak önlemler tatbikat katılımcısı kurumun sorumluluğundadır.

Ülkemizde 2011 yılında yapılan ulusal siber güvenlik tatbikatına 41 kurum ve kuruluş katılmıştır. Bunlardan 6 tanesi sadece gözlemci statüsünde olup, 27 tanesine port tarama testi, 20 tanesine DDOS saldırısı testi, 25 tanesine web sayfası güvenlik denetimi, 26 tanesine kayıt dosyası analizi testi uygulanmıştır. Tatbikat kapsamında bu testler sonucunda her bir kuruma ilişkin elde edilen bulgular sadece söz konusu kurum ile paylaşılmış olup muhtemel güvenlik açıklarına karşı mahremiyete özen gösterilmiştir. Bununla birlikte tatbikat sonucu elde edilen genel bulgular Ulusal Siber Güvenlik Tatbikatı Sonuç Raporu olarak hazırlanmış ve internet sitesi üzerinden kamuoyu ile paylaşılmıştır.

Ulusal siber güvenlik tatbikatının temel amacı, katılımcı kurum ve kuruluşların siber güvenlik alanındaki muhtemel açıklarının ve eksiklerinin tespit edilmesi ve ihtiyaçların vurgulanmasıdır. Tatbikat sonucunda elde edilen bulgular ilgili kurumlarla paylaşılmış olup, ortaya çıkan ihtiyaçlara yönelik alınacak tedbirler ile ilgili değerlendirmeler söz konusu kurum ve kuruluşlar tarafından yapılmak durumundadır. Bununla birlikte, 2012 ve 2013 yıllarında yapılacak olan tatbikatların ihtiyaçlar ve tehditlere yönelik farkındalığın artırılmasına ve teknik ve idari kapasitelerin giderek geliştirilmesine katkı sağlayacağı değerlendirilmektedir.

Kurumların tatbikat sonrasında aldıkları önlemlerden TÜBİTAK işbirliği ile gerçekleştirilenler olmuştur. Bankacılık Düzenleme ve Denetleme Kurumu ülkemizde faaliyet gösteren tüm bankalara 2011 yılı sonuna kadar TÜBİTAK'a sızma testi yaptırma ve sonraki yıllar için ise kendi belirleyecekleri bağımsız bir kuruluşa sızma testi yaptırma zorunluluğu getirilmiştir. Bu karar finans sektörünün güvenliğinin sağlanması için önemli bir adımdır. TÜBİTAK 2011 sonuna kadar 31 bankanın sistemini test etmiştir. Test edilen bankalar sahip oldukları aktifler bakımından sektörün %97'sini oluşturmaktadır.

Ayrıca, E-devlet altyapısının işletiminden sorumlu olan TÜRKSAT da Ulusal Siber Güvenlik Tatbikatı'ndan (USGT) sonra sistemlerini TÜBİTAK test ettirmiş ve sistemlerinin güvenliğinin sağlanması için gerekli önlemleri almaya çalışmıştır.

Öte yandan; NATO Terörle Mücadele Mükemmeliyet Merkezi (Ankara) düzenleyeceği Siber Terör konulu eğitimde Türkiye'deki çalışmaların ve Ulusal Siber Güvenlik Tatbikatı'nın anlatılması amacıyla TÜBİTAK BİLGEM'den talepte bulunmuştur. Bu eğitime büyük kısmı yurt dışından olmak üzere 100 civarında üst düzey personel katılmıştır.

Milli Güvenlik Akademisi General/Amiral seviyesindeki katılımcılardan oluşan üst düzey yönetici sertifika programına Siber Güvenlik konusunu almış olup bu konuda eğitim verilmesi için TÜBİTAK BİLGEM'den eğitmen görevlendirmiştir.

Bilindiği üzere teknik olarak bilişim sistemlerine yapılan saldırılar çok geniş bir yelpazede gerçekleştirilmektedir. Bu nedenle herhangi bir bilişim sistemini korumak için tek bir güvenlik sistemi yeterli olamamaktadır. Bu nedenle Bilgi Teknolojileri ve İletişim Kurumunun da bilgi güvenliğini sağlamak amacıyla birden fazla güvenlik sistemi kullanılmakta, sahip olduğu ISO 27001 standardı kapsamında gerekli çalışmalar gerçekleştirilmektedir.

Ulusal Siber Güvenlik Tatbikatı'na katılan kurumlardan MSB, MGK gözlemci statüsündeki kurumlardır ve bu kurumların bilgi sistemlerindeki açıklıkların bulunması için herhangi bir çalışma yapılmamış, olumsuz bir durum raporlanmamıştır. Ankara Cumhuriyet Başsavcılığı Ulusal Siber Güvenlik Tatbikatı'na siber güvenliğin hukuki boyutuyla ilgili katkı sağlamak amacıyla katılmıştır. Ankara Cumhuriyet Başsavcılığı'nın sahip olduğu bilgi sistemlerine yönelik herhangi bir test gerçekleştirilmemiş ve olumsuz bir durum raporlanmamıştır.

Merkez Bankası ve SPK bilgi sistemlerine yönelik olan gerçekleştirilen testlerde ise bulunan açıklıklar bu kurumlara hazırlanan özel raporlarla iletilmiştir. Kurumların tespit edilen açıklıkların kapatılması için destek sağlanmıştır.

Ulusal Siber Güvenlik Tatbikatı'nda tespit edilen bulgular ülkemizin siber güvenlik durumunun tespiti için önemlidir. Unutulmamalıdır ki yüzde yüz güvenlik ulaşılması mümkün olmayan bir hedeftir. Kurumların ve ülkelerin yapması gereken ise risk analizi çerçevesinde sahip olunan riskleri belirleyip bu risklerin ortadan kaldırılması için gerekli tedbirleri almaktır. Ulusal Siber Güvenlik Tatbikatı'nda elde edilen bulgular çerçevesinde ülkemizin sahip olduğu siber alandaki risklerin tespiti için bir adım atılmış olup katılımcı kurumların bu risklerden kurtulmaları için önemli bir başlangıç olmuştur.

Ülkelerin gerçek hayatta maruz kaldıkları tehditler, bilgi ve iletişim teknolojilerinin gelişimi ile birlikte siber ortamda da hissedilmektedir. Söz konusu tehditlerin ve risklerin varlığı son yıllarda uluslararası alanda da siber güvenlik tatbikatlarının yoğunlaşmasının gerekçeleri arasındadır. Bu kapsamda, örneğin ABD ve bölge ülkelerinde 2006, 2008 ve 2010 yıllarında düzenlenen Cyber Stonn tatbikatları, NATO bünyesinde 2008, 2009 ve 2010 yıllarında düzenlenen Cyber Coalition tatbikatları, Avrupa Birliği bünyesinde 2010 yılında düzenlenen Cyber Europe tatbikatları sayılabilir.

İster bilişim alanında, ister diğer alanlarda herhangi bir güvenlik sisteminin yüzde yüz güvenlik sağlayabileceğini, alınan güvenlik tedbirlerinin bilgileri korumakta yeterli olduğunu düşünerek sistem işletmenin güvenlik alanında en büyük yanlışlardan birisi olacağı değerlendirilmelidir. Bu çerçevede Bilgi Teknolojileri ve İletişim Kurumu da bilgi güvenliği tedbirlerini hassasiyetle sürekli gözden geçirmekte, güncel tehditleri takip ederek gereğini yapmaktadır.

Türkiye Bilimsel ve Teknolojik Araştırmalar Kurumundan (TÜBİTAK) alınan UEKAE bünyesinde faaliyet gösteren Bilişim Sistemleri Güvenliği Grubu kurumların sanal saldırılara karşı korunması için 1999 yılından bu yana gerçekleştirilen projeler ile ilgili detaylar (EK 1) bilgi notunda sunulmaktadır.

Türkiye Bilimsel ve Teknolojik Araştırmalar kurumundan alınan UEKAE bünyesinde faaliyet gösteren bilişim sistemleri güvenliği grubu kurumların sanal saldırılara karşı korunması için 1999 senesinde bu yana gerçekleştirilen projeler bu projeler ile ilgili detaylar

UEKAE ve BTE, bilişim, bilgi güvenliği ve ileri elektronik teknolojileri alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak amacıyla faaliyetlerde bulunur ve bu alanlarda ulusal ve uluslararası düzeyde temel bir çözüm ve bilim yeri olmak hedefini göz önünde bulundurur. Türkiye'nin savunma gücüne katkıda bulunmak, ulusal sistem içinde sivil ve askeri sektörün ihtiyacı olan her türlü bilişim, bilgi güvenliği ve ileri elektronik teknolojileri konularında araştırmalar yapmak, sözleşmeli projeler yolu ile bilişim, bilgi güvenliği ve ileri elektronik teknolojileri konusundaki sorunları ortaya koymak, çözmek ve/veya çözülmesine yardımcı olmak ve bu çözümlerin uygulanmasını sağlamak, üniversite, kamu ve özel sektör arasında köprü görevi üstlenerek işbirliklerini geliştirmek ve bu kesimlerin teknolojik birikimlerini arttırmak amacıyla kurulmuş bir araştırma, teknoloji geliştirme ve uygulama kuruluşudur. Amacı, Türkiye'de sivil ve askeri sektörün ihtiyacı olan her türlü elektronik ve elektro-optik cihaz ile bilişim sistemlerine ilişkin donanım ve yazılım ile tüm devreleri, dünyadaki gelişen teknolojiye uygun biçimde, ulusal olarak ve ulusal kalkınma hedeflerine erişilmesine katkıda bulunacak şekilde araştırmak ve geliştirmek, sivil ve askeri amaçlar için ortak hizmet verebilecek güvenlik ve test merkezleri kurmak, bu merkezlerde TSK ve diğer kamu kurum ve kuruluşlarının envanterinde bulunan veya envanterine girecek kripto ve haberleşme cihazları ile bilişim ve bilgi güvenliği konularını içeren her türlü donanım ve yazılım ile silah sistemlerinin testini yapmak, bu konulara ilişkin standartları koymak ve geliştirmektir. Çalışmalarında TÜBİTAK'ın diğer organları ile ve gerektiğinde ulusal ve uluslararası kuruluşlarla işbirliği yapar, kendi bünyesindeki araştırıcı ve teknik personel ile talep eden ilgili kuruluşların bilişim, bilgi güvenliği ve ileri elektronik teknolojileri alanındaki teknik personelini eğitme ilkelerini göz önünde tutar.

Ulusal Bilgi Sistemleri Güvenlik Programı: Kalkınma Bakanlığı (Devlet Planlama Teşkilatı) Bilgi Toplumu Dairesi tarafından hazırlanan Bilgi Toplumu Stratejisi Eylem Planı 2006 - 2010 belgesinin 88 numaralı maddesinde tanımlanan "Ulusal Bilgi Sistemleri Güvenlik Programı" isimli projede sorumlu olarak TÜBİTAK-UEKAE belirlenmiştir. Bu projenin kapsamı "Siber alemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayınlayacak, bu risklere karşı ne şekilde tedbir alınabileceğine dair bilgilendirme yapacak, risklerin ortaya çıkması durumunda karşı tedbirleri koordine edebilecek bir "bilgisayar olaylarına acil müdahale merkezi (CERT)" kurulacaktır. Kamu kurumları için gerekli minimum güvenlik seviyeleri kurum ve yapılan işlem bazında tanımlanacak, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyeleri tespit edilecek ve eksikliklerin giderilmesi yönünde öneriler oluşturulacaktır." ifadesi tanımlanmıştır. Bu proje 2006 - 2010 yılları arasında yürütülmüştür. Program kapsamında gerçekleştirilen çalışmalar aşağıda özetlenmiştir:

- Ulusal Bilgi Güvenliği Kapısı www.bilgiguvenligi.gov.tr adresinden hizmet vermeye başlamıştır. Halihazırda üçbinin üzerinde üye ve 135 adet yazar yer almaktadır. Yazarların %40'ı TÜBİTAK dışıdır.
- Yirmi kamu kurumundan 131 personele 21 farklı alanda bilgi güvenliği eğitimleri verilmiştir.
- 71 üniversiteden 93 bilgi işlem personeline bilgi güvenliği eğitimleri verilmiştir.
- Dokuz adet kamu kurumuna, BOME (Bilgisayar Olaylarına Müdahale Ekibi) kurma danışmanlığı verilmiştir. BOME kurulum danışmanlığının bitmesine müteakip bu kurumlar ile birlikte Kasım 2008'de BOME-2008 Siber Güvenlik Tatbikatı yapılmıştır.
- Dört kamu kurumuna ISO 27001 tabanlı Bilgi Güvenliği Yönetim Sistemi (BGYS) kurulum danışmanlığı verilmiştir. Beş kamu kurumuna sızma testi yapılmıştır.

- Bilgisayar kullanıcılarına yönelik hazırlanmış, multimedya içerikli, interaktif bölümlerin olduğu bilgi güvenliği bilincinin artırılmasına yönelik portal www.bilgimikoruyorum.org.tr adresinden yayına başlamıştır.
- Ulusal Siber Güvenlik Tatbikatı 2011, yaklaşık bir yıl süren hazırlık sürecinin ardından 25-28 Ocak tarihlerinde 39 kurum/kuruluşun katılımıyla gerçekleşmiştir. Tatbikat organizasyonunu BTK ve TÜBİTAK yapmıştır. USGT 2011 kapsamında 500'ün üzerinde yazılı enjeksiyona ilave olarak port taraması, dağıtık servis dışı bırakma saldırıları, web uygulamalarının denetimi ve kayıt dosyası (log) analizinden oluşan gerçek saldırılar yapılmıştır. Kurumlara özel tarama ve analiz raporları resmi olarak iletilmiştir. Kurumlara özel olmayan tatbikat sonuç raporu hazırlanmıştır.

2012 Yatırım Programı Projeleri: 2012 Yatırım Programı'nda "Kamu Bilgi Güvenliği Programı" ve "Kritik Altyapılarda Bilgi Güvenliği Yönetimi – Tespit, Analiz, Önlemler" isimli iki adet siber güvenlik projesi yer almaktadır. Her iki proje de Kalkınma Bakanlığı Bilgi Toplumu Dairesi ile birlikte bir seneye yakın bir sürede yapılan değerlendirmeler sonucunda oluşturulmuştur. Her iki projenin temel ilkesi, siber güvenlik konusunda kurumsal kapasite geliştirmek olarak benimsenmiştir.

TÜBİTAK UEKAE Bilişim Sistemleri Güvenliği Grubu deneyimlerinden ve Ulusal Siber Güvenlik Tatbikatı 2011'in sonuçları incelendiğinde siber güvenlik açısından ülkemizdeki problemin en genel ifadeyle yetenek eksikliği olduğu görülmektedir. Kamu kurumlarında çalışan bilgisayar mühendisleri ve bilişim uzmanlarında siber güvenlik bilinci ve bilgisinde görülen eksikliği gidermek ve kamu kurumlarında çalışan mühendis ve uzmanları siber güvenlik konusunda kurumsal ihtiyaçları karşılayacak seviyeye getirmek amacıyla Kamu Bilgi Güvenliği Programı hazırlanmıştır. Kamu Bilgi Güvenliği Programı, Eğitim, Bilgi Bankası Oluşturulması ve Risk Analizi olmak üzere üç projeden oluşmaktadır.

- Eğitim projesi kapsamında halihazırdaki eğitimler geliştirilecek, yeni siber güvenlik eğitimleri hazırlanacak ve bu eğitimlerin verilmesi suretiyle kapasite artırımı sağlanacaktır.
- Bilgi Bankası Oluşturulması Projesi kapsamında kamu kurumlarının ihtiyacı olan bilgi birikimi, kılavuzlar, teknik kontrol listeleri, saldırılardan korunma ve saldırılarla mücadele el kitapları hazırlanarak artırılacaktır.
- Risk Analizi Projesi kapsamında, kamu kurumlarının sahip olduğu bilgi güvenliği risklerinin 6 ayda bir yapılacak testlerle tespit edilmesi ve önceki sonuçlarla karşılaştırılarak hem kurumun gelişiminin hem de ihtiyaçlarının tespitinin yapılması amaçlanmaktadır. Eğitim ve Bilgi Bankası Oluşturulma Projelerinin etkinliğinin ölçülmesi de bu projeyle sağlanacaktır.

Kritik altyapılar devlet düzeninin ve toplumsal düzenin sağlıklı bir şekilde işlemesi için gerekli olan ve birbirleri arasında bağımlılıkları olan fiziksel ve sayısal sistemlerdir. Enerji üretim ve dağıtım sistemleri, telekomünikasyon altyapısı, finansal servisler, su ve kanalizasyon sistemleri, güvenlik servisleri, sağlık servisleri ve ulaştırma servisleri en başta gelen kritik altyapılar olarak sıralanabilir. OECD üyesi ülkeler, Avrupa Birliği, ABD, Kanada gibi gelişmiş ülkeler kritik altyapıların korunması ile ilgili çalışmalara başlamışlar ve ciddi yol almışlardır. Bütün kritik altyapılar içerisinde bilgi teknolojileri yoğun olarak kullanılmaktadır. Bu durum ise, kritik altyapıları siber tehditlere karşı açık hale getirmektedir. Bu proje eğer kapsamında, kritik altyapıların tespiti ve analizi amacıyla ülkemizde gerçekleştirilen ilk çalışma olacaktır. Proje kapsamında, Türkiye'nin kritik altyapılarının tespiti yapılacak ve bilgi teknolojilerinden kaynaklanan açıklıkların kritik altyapılara etkisi analiz edilecektir. Sektör bazlı pilot çalışma gerçekleştirilecektir. Proje kapsamında kritik altyapılarda kullanılan SCADA bilgi sistemleri için simülasyon ortamı oluşturulacaktır. Proje sonucunda toplam 10 adet doküman hazırlanmış olacaktır. Bu dokümanların en önemlileri Türkiye'de kritik altyapılar ve kritik altyapıların BT güvenlik durumu dokümanı ve diğer kritik altyapılara yaygınlaştırılma için yol haritası dokümanıdır.

Türkiye Bankacılık Sektörü Sızma Testleri: Bankacılık Düzenleme ve Denetleme Kurumunun Şubat 2011'de yaptığı düzenleme ve TÜBİTAK'a yaptığı talep sonucunda Türkiye'de faaliyet gösteren 31 bankanın (sahip oldukları aktifler açısında Türkiye'nin %96'sına sahip) bilgi sistemlerine sızma testi yapılmıştır. BDDK'nın talebi doğrultusunda Türkiye Bankacılık Sektörü Siber Güvenlik Analiz Raporu hazırlanmış ve BDDK'ya teslim edilmiştir.

Ulusal Sanal Ortam Güvenlik Politikası Hazırlanmasında Koordinatörlük: 2007 senesinin Nisan ve Mayıs aylarında Estonya'nın bilgi ve iletişim teknolojilerini hedef alan koordine atakların ardından NATO bazı önemli adımlar atmıştır. Öncelikle, Brüksel'de NATO Sayısal Ortam Savunma Otoritesi kurulmuş ve faal duruma gelmiştir. NATO, kendi bilgi sistemlerini kapsam içine alan, Sayısal Ortam Savunma Konsepti hazırlanmıştır. Hazırlanan bu konsepte göre olası bir sayısal savaşta koordinasyonun kurulması amacıyla üye ülkeler NATO'ya ulusal temas noktalarını bildirmişlerdir. Aynı konseptin bir gereği olarak, üye ülkelerden ulusal bilgi sistemlerini kapsam içine alan sayısal ortam güvenlik politikalarını hazırlamaları talep edilmiştir.

Ülkemizde, TÜBİTAK'a bağlı olarak faaliyet gösteren UEKAE (Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü) ulusal temas noktası olarak NATO'ya bildirilmiştir. NATO'nun sayısal ortam güvenlik politikası hazırlanması talebi Dışişleri Bakanlığı tarafından Başbakanlık'a iletilmiş, Başbakanlık Mayıs 2008'te söz konusu politikanın UEKAE koordinasyonunda hazırlanmasını resmen talep etmiştir. Politika dokümanı 19 adet kamu kurumunun katılımı ile hazırlanmıştır. Kurum listesi, Başbakanlık tarafından koordinatör kuruma bildirilmiştir. Politika dokümanı, Temmuz 2008 – Kasım 2008 ayları arasında hazırlanmış; bu sürede tüm kurumların katıldığı üç adet toplantı gerçekleştirilmiştir. Hazırlanan politika dokümanı beş sayfadan oluşmaktadır. Üçüncü toplantının ardından, politika belgesinde son düzenlemeler yapılmış, katılımcı kamu kurumlarının çoğunluğunun onayı ile belge Ocak 2009'da Başbakanlık'a resmi olarak teslim edilmiştir.

Kurum Bazlı Siber Güvenlik Kapasite Geliştirme Çalışmaları: Ziraat Bankası bilgi işlem personeli kapasite geliştirme çalışmaları kapsamında bilgi güvenliği eğitimleri yapılmış ve Ziraat Bankası bilgi sistemleri birlikte denetlenmiştir. Sayıştay Başkanlığı bilgi sistem denetim personeli için kapasite geliştirme çalışmaları gerçekleştirilmiştir. Bu çalışmalar kapsamında 40 iş günlük bilgi güvenliği eğitimi verilmiştir. Eğitimlerinde tamamlanmasına müteakip Sayıştay personeli tarafından hazırlanmış olan denetim rehberi güncelleme çalışması yapılmıştır. Sayıştay'ın gerçekleştirmiş olduğu 3 adet denetimde teknik destek verilmiştir. Bu denetimler kapsamında gerçekleştirilen teknik bilgi güvenliği denetimlerinin sonucu raporlanmıştır. Bankacılık Düzenleme ve Denetleme Kurumu bilgi işlem personeli kapasite geliştirme çalışmaları kapsamında 40 iş günlük bilgi güvenliği eğitimleri verilmiştir.

Etkinlik ve Konferans Düzenleme: 2006 senesinden bu yana her sene Haziran ayında Ankara'da Kamu Kurumları Bilgi Güvenliği Konferansı düzenlenmektedir. Ayrıca, 2007-2010 seneleri arasında 4 kez İstanbul'da Özel Sektör Bilgi Güvenliği Konferansı düzenlenmiştir. 2009 ve 2010 senelerinde özel sektör tarafından düzenlenen Ankasec isimli siber güvenli konferanslarına sponsor olunmuş ve içerik sağlanmıştır. 2009 senesinde Ankara'da düzenlenen SASAD Sayısal Ortam Savaş Sempozyumu'nda koordinatörlük yapılmış ve konferansa içerik sağlanmıştır. 2011 senesinde İstanbul'da düzenlenen TSK Siber Savunma Sempozyumu koordinatörlük yapılmış ve sempozyuma içerik sağlanmıştır.

Ar-Ge Projeleri: "SysSec : A European Network of Excellence in Managing Threats and Vulnerabilities in the Future Internet: Europe for the World" isimli FP7 Avrupa Birliği projesi kapsamında çalışılmaktadır. Proje Ortakları, Avrupa Birliğinden sekiz adet kurumdur. (Yunanistan, İtalya, Fransa, Hollanda, Bulgaristan, Avusturya, İsveç) Proje 2010 başlamış olup 2014 senesi sonunda tamamlanacaktır. Sorumlu olduğumuz iş paketi Türkiye'deki kötücül yazılım haritasının çıkartılması olarak tanımlanabilir. Diğer bir Ar-Ge projesi Bilgisayar Destekli Denetim isimli TÜBİTAK 1007 destekli projedir. Sayıştay Başkanlığı için yürütülen proje 2013'de tamamlanacaktır. Dışişleri Bakanlığı için gerçekleştirilecek olan üçüncü bir Ar-Ge projesi Veri Kaçağı Önleme Sistemi projesidir. Proje imza aşamasındadır.

Kurumsal Projeler: Birçok kamu kurumu, Türk Silahlı Kuvvetleri ve özel sektör için siber güvenlik projeleri gerçekleştirilmiştir. Bu projeler kapsamında, güvenli sistem kurulumu, bilgi güvenliği yönetim sistemi kurulum danışmanlığı, sızma testleri, bilgi güvenliği eğitimleri, yazılım testleri, sistem konfigürasyon testleri, ortak kriter testleri, COMSEC testleri gibi faaliyetler gerçekleştirilmiştir. Proje gerçekleştirilen bazı kurumlar aşağıda listelenmiştir:

- Genelkurmay Başkanlığı
- Deniz Kuvvetleri Komutanlığı
- Deniz Kuvvetleri Komutanlığı Bağlıları
- Sahil Güvenlik Komutanlığı
- Harp Akademileri Komutanlığı
- GES Komutanlığı
- Özel Kuvvetler Komutanlığı
- Muhabere Bilgi Destek Komutanlığı
- ATASE Başkanlığı
- Dış Ticaret Müsteşarlığı
- Radyo Televizyon Üst Kurulu
- Hazine Müsteşarlığı Merkezi Finans ve İhale Birimi
- PTT
- YÖK
- ÖSYM
- Turkcell
- Avea
- Vodafone
- 31 adet banka
- Aselsan
- Hazine Müsteşarlığı
- İGDAŞ
- Türksat
- Sermaye Piyasası Kurumu
- STM
- TTNET
- Tapu Kadastro Gn. Md.

- EPDK
- İstanbul Büyükşehir Belediyesi
- Kredi Yurtlar Kurumu
- Gazi Üniversitesi Hastanesi
- TAV
- RTÜK
- PTT
- TAEK
- Pakistan Savunma Bakanlığı
- EGA
- TÜBİTAK SAGE
- DMO
- Havelsan
- Labris