ULUSAL ELEKTRONİK VE KRİPTOLOJİ

ARAŞTIRMA ENSTİTÜSÜ

Doküman Kodu: RAPOR-0002

TÜRKİYE BİLGİSAYAR OLAYLARI MÜDAHALE EKİBİ FAALİYET RAPORU 2007 - 2008

SÜRÜM 1.00

10.08.2009

Hazırlayanlar:

Mehmet ERİŞ

Ünal TATAR

P.K. 74, Gebze, 41470 Kocaeli, TÜRKİYE
Tel: (0262) 648 1000
Faks: (0262) 648 1100
http://www.uekae.tubitak.gov.tr
uekae@uekae.tubitak.gov.tr

ÖNSÖZ

Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü (UEKAE)'nün misyonu, "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında Türkiye'nin teknolojik bağımsızlığını sağlamak ve sürdürmek için nitelikli insan gücü ve uluslararası düzeyde kabul görmüş altyapısı ile, bilimsel ve teknolojik çözümler üretmek ve uygulamaktır". Bu ana hedef göz önünde bulundurularak belirlenen "bilgi güvenliği, haberleşme ve ileri elektronik alanlarında yeni teknolojilerin geliştirilmesine öncülük eden uluslararası bilim, teknoloji ve üretim merkezi olmak" vizyonuna ulaşılabilmesi ve ülkenin ihtiyacı olan teknolojilerin geliştirilmesi için Enstitü'nün akredite test ortam ve laboratuarlarında temel ve uygulamalı araştırmalar yapılmakta ve ihtiyaç sahiplerine teknik destek sağlanmaktadır.

Bu doküman, Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) tarafından 2007 – 2008 yıllarında gerçekleştirilen faaliyetleri anlatmaktadır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeği geçen Bilişim Sistemleri Güvenliği Bölümü personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Tolga MATARACIOĞLU'na teşekkürü borç biliriz

İÇİNDEKİLER

1. GİRİŞ

Dünyada ve ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmaktadır. Bilgi ve iletişim sistemleri, hayatımızın hemen her alanının önemli bir parçası haline gelmiştir. Gerek kamu kurumları gerekse özel kuruluşlar, verdikleri hizmetlerin bir çoğunu artık bilgi sistemleri üzerinden vermektedir. Bu şekilde hem hizmet kalitesini arttırmayı hem de iş verimliliğini yükseltmeyi hedeflemektedirler.

Kamu kurumlarının bilgi ve iletişim teknolojisi yatırımları arasında eşgüdüm sağlamak, e-Dönüşüm Türkiye Projesi'nin koordinasyonunu yürütmek, ve bilgi toplumu olma yolunda atılması gereken adımlara ilişkin stratejileri belirlemek üzere 2003 yılında DPT bünyesinde kurulmuş olan Bilgi Toplumu Dairesi tarafından 2006-2010 Bilgi Toplumu Stratejisi hazırlanmıştır.

Tüm bu gelişmelerle, bilgi ve iletişim sistemlerinin güvenliğinin sağlanması da önem arz eden bir konu haline gelmiştir. Bilgi ve iletişim teknolojilerinin güvenliğini sağlamak amacıyla yapılan çalışmalarının en önemlilerinden birisi de DPT Bilgi Toplumu Dairesi tarafından hazırlanan Bilgi Toplumu Stratejisi Eylem Planı'nın 88. maddesinde yer alan Ulusal Bilgi Sistemleri Güvenliği Programı (UBGP)'dır.

Ulusal Bilgi Güvenliği Programı çerçevesinde yapılması gereken faaliyetler **"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."** şeklinde belirtilmiştir. UBGP sorumlusu olarak TÜBİTAK Ulusal Kriptoloji ve Araştırma Enstitüsü (UEKAE), ilgili kurum ve kuruluşlar olarak da üniversiteler ve kamu kuruluşları sıralanmıştır.

Ulusal Bilgi Güvenliği Programı'nın süresi 24 ay olarak belirlenmiştir. Fakat daha sonra yapılan değerlendirmeler sonucunda toplam süre 48 ay olacak şekilde 2010 yılı Aralık ayına kadar uzatılmıştır. UBGP çerçevesinde başta kamu kurum ve kuruluşları olmak üzere ülkemizin bilgi sistem güvenliği ile ilgili bilgi ihtiyacını karşılamak ve kamu bilgi sistemlerinin güvenliğinin sağlanması ile ilgili etkin önlemler alınmasına ön ayak olmak amacıyla Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi (TR-BOME) kurulmuştur.

1.1 Amaç ve Kapsam

Bu dokümanın amacı Türkiye Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi tarafından verilen hizmetler ve gerçekleştirilen faaliyetler hakkında bilgilendirmede bulunmaktır.

Dokümanda TR-BOME tarafından 2007 – 2008 yıllarında gerçekleştirilen faaliyetler kapsanmaktadır.

1.2 Kısaltmalar ve Tanımlar

TR- BOME	**:**	Türkiye Bilgisayar Olaylarına Müdahale Ekibi
UBGP	**:**	Ulusal Bilgi Sistemleri Güvenliği Programı
UEKAE	**:**	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
ULAKBİM	**:**	Ulusal Akademik Ağ ve Bilgi Merkezi
ULAK-CSIRT	**:**	ULAKBİM Computer Security Incident Response Team
Güvenlik olayı	**:**	Kanunlarda veya güvenlik politikalarında açıkça veya dolaylı olarak belirtilen bir kuralın ihlali
NATO	**:**	North Atlantic Treaty Organization
NCIRC	**:**	NATO Computer Incident Response Capability
EGC	**:**	European Government CERTs

2. TÜRKİYE BİLGİSAYAR OLAYLARI MÜDAHALE EKİBİ

Bilgisayar olaylarına müdahale ekipleri belirli bir sorumluluk alanı dâhilinde faaliyet gösteren, bu sorumluluk alanında bilgi sistemleri güvenlik olaylarına müdahale hizmeti ve bilgi sistem güvenliği ile ilgili diğer önleyici veya düzeltici hizmetleri veren ekiplerdir.

BOME'ler, amaçlarına ve sorumluluk alanlarına göre farklılık gösterebilir. BOME'ler personel sayısı, teknik kabiliyetler gibi kısıtları göz önünde bulundurarak Tablo 1'de verilen servislerden uygun gördüklerini verebilir. Örnek verecek olursak:

- Kurum BOME'si: Bir kurum içindeki bilgi sistem güvenlik olaylarına müdahale amacıyla kurulan kurum BOME'sinin sorumluluk alanı o kurumun bilgi sistemleri ve bu sistemlerin kullanıcılarıdır.
- Ulusal BOME'ler: Kurum BOME'si dışında, üreticilerin müşterilerine sattıkları ürünlerle ilgili güvenlik desteği verebilecekleri BOME'ler ya da ülke içindeki olay müdahale koordinasyonunu gerçekleştirmeyi amaçlayan Ulusal BOME'ler diğer BOME örnekleridir.
- Servis Sağlayıcılar: Bunların dışında İnternet hizmet sağlayıcılar da BOME kurabilirler. Bir İnternet hizmet sağlayıcı olan ULAKBİM bünyesinde kurulmuş olan ULAK-CSIRT bunun ülkemizdeki bir örneğidir.

Tepki Servisleri	Önleyici Servisler	Güvenlik Kalite Yönetim Servisleri
• Alarm ve Uyarılar	• Duyuru	• Risk Analizi
• Olay Müdahale	• Teknoloji Takibi	• İş Sürekliliği ve Felaket Kurtarma
o Olay Analizi	• Güvenlik Denetleme ve Değerlendirme	
o Olay Yerinde Müdahale		• Güvenlik Danışmanlığı
o Olay Müdahale Destek	• Güvenlik Araçlarının, Uygulamalarının ve Altyapısının Yapılandırılması ve Bakımı	• Bilinçlendirme
• Açıklık Müdahale		• Eğitim
o Açıklık Analizi		• Ürün Değerlendirme ve Sertifikasyonu
o Açıklık Müdahale		
o Açıklık Müdahale Koordinasyonu	• Güvenlik Araçlarının Geliştirilmesi	
• Saldırı Araçları Müdahale	• Saldırı Tespit Servisleri	
o Saldırı Araçları Analizi	• Güvenlik ile İlgili Bilgi Yayınlanması	
o Saldırı Araçları Müdahale		
o Saldırı Araçları Müdahale Koordinasyonu		

Tablo 1[1] : BOME tarafından verilebilecek hizmetler

[1] www.cert.org

Olay Koordinasyon:

Bilgi ve iletişim sistemleri üzerinde gerçekleşen güvenlik olayları çoğu zaman farklı kurumlar arasında, hatta farklı ülkelerde bulunan taraflar arasında cereyan etmektedir. Bu durum, olaylara etkin bir şekilde müdahale edilebilmesi için koordinasyonu sağlayacak ve tek bir temas noktası olma özelliğine sahip olan bir birimin oluşturulmasını gerekli kılmaktadır. Bu amaçla bilgisayar olaylarına müdahale ekibi koordinasyon merkezleri kurulmuştur. Bilgisayar olaylarına müdahale ekibi koordinasyon merkezleri, sorumluluk alanındaki kurum ve kuruluşlar arasında bir güven ağı oluşturmayı hedefler ve farklı kurum ve kuruluşlar arasında meydana gelen olaylarda güvenli bir nokta olarak kurumlar arası iletişimde ve olay bilgisi paylaşımında rol alan güvenli bir nokta olarak hizmet sunmayı amaçlar.

Ulusal bir BOME olan ve koordinasyon merkezi olarak görev yapan TR-BOME, BOME kurulum danışmanlığı, olay müdahale koordinasyonu ve alarm-uyarılar hizmetlerini vermektedir.

2.1 TR-BOME Tarafından Verilen Hizmetler

TR-BOME tarafından verilen hizmetler aşağıda anlatılmıştır.

2.1.1 BOME Kurulum Danışmanlığı

Bilgisayar güvenlik olayı yaşayan her bir kuruma ayrı ayrı yerinde müdahalede bulunmak sınırlı kaynaklarla mümkün olamamaktadır. Bu sorunun çözümü olay müdahale yeteneğini her bir kuruma kazandırmakla mümkün olacaktır.

Bir kurumun karşılaştığı bir bilgi güvenliği olayını tespit edebilmesi ve bu olaya etkin bir şekilde müdahale edebilmesi için bünyesinde teknik yeterliliğe sahip personel/ekip bulundurması, olay müdahale esnasında uyulması gereken genel prensipleri içeren politika ve prosedürlere sahip olması gerekmektedir.

TR-BOME verdiği danışmanlık hizmetiyle kurumların olay müdahale sorumluluğu bulunan çalışanlarının eğitilmesi, kurumda verilecek hizmetlerin belirlenmesi, bu hizmetlerin verilebilmesi için gerekli altyapının sağlanması ve olay müdahalede kullanılacak politika ve prosedürlerin belirlenmesi gerçekleştirilmektedir.

2.1.2 Olay Müdahale Koordinasyon Hizmeti

Bilgi sistemleri üzerinde gerçekleşen güvenlik olayları farklı kurumlar arasında hatta farklı ülkeler arasında gelişebilmektedir. Farklı kurumlar veya ülkeler arasında gelişen güvenlik olaylarına hızlı ve etkin müdahalede bulunabilmek, ülke çapındaki büyük resmi görebilmek, elde edilen bulguların paylaşılmasını sağlamak için koordinasyondan sorumlu bir birime ihtiyaç bulunmaktadır.

Dışişleri Bakanlığı'nın koordinasyonunda NATO'ya karşı bilgisayar güvenlik olayları ile ilgili ulusal temas noktası olarak TR-BOME belirlenmiştir. TR-BOME, web sayfası üzerinden, e-posta ile ve telefonla ihbar kabul etmektedir. Kendisine gelen ihbarları değerlendirip tesis edilmiş olan güven ağı çerçevesinde, gönüllülük esasıyla bu olayların çözümünü sağlamaya çalışmaktadır.

2.1.3 Alarm ve Uyarılar Hizmeti

Bilgi sistemlerine yönelik yapılan saldırıların büyük kısmı yazılım ve donanımlarda ortaya çıkan açıklıkların kullanılmasıyla gerçekleştirilmektedir. Bu saldırılardan etkilenmemek için alınacak en temel önlem var olan açıklıklarla ilgili yayınlanmış olan güncellemelerin uygulanmasıdır.

Ülkemizde yaygın olarak kullanılan bilgi sistemi yazılım ve donanımlarında ortaya çıkan güvenlik açıklıkları takip edilip, özellikle yüksek, acil ve kritik önem derecesine sahip açıklıklara ve bu açıklıkların kapatılmasına ilişkin bilgi web sayfasından yayınlanmaktadır. Ayrıca e-posta listeleriyle de açıklıklar hakkında uyarıda bulunulmaktadır.

Yaygın etkisi görülen açıklıklarla ilgili detaylı teknik incelemenin yapıldığı makaleler hazırlanıp yayınlanmaktadır. Ayrıca önem derecesine göre açıklılar hakkında basın duyurusu hazırlanıp, ulusal basın aracılığıyla vatandaşların konudan haberdar edilmesi sağlanmaktadır.

3. 2007 – 2008 YILLARINDA GERÇEKLEŞTİRİLEN FAALİYETLER

3.1 TR-BOME Hizmetleri Kapsamında Gerçekleştirilen Faaliyetler

TR-BOME tarafından verilen BOME kurulum danışmanlığı, Olay Müdahale Koordinasyon ve alarm-uyarılar hizmetleri kapsamında gerçekleştirilen faaliyetler aşağıda anlatılmıştır.

3.1.1 BOME Danışmanlığı Kapsamındaki Faaliyetler

Bir kurumun karşılaştığı bilgi güvenliği olaylarını tespit edebilmesi ve etkin bir şekilde müdahale edebilmesi için bünyesinde teknik yeterliliğe sahip personel bulundurması, olay müdahale esnasında uyulması gereken genel prensipleri içeren politika ve prosedürlere sahip olması gerekmektedir. Kurumlara, karşılaşacakları güvenlik olaylarına müdahale yeteneği kazandırmak amacıyla iki eğitim hazırlanmıştır. Bu eğitimlerden BOME Kurulum ve Yönetim Eğitimi (2 gün süreli) “BOME birimi nasıl kurulur?”, “Hangi servisleri verebilir ve nasıl yönetilir?” sorularının cevaplarını içermektedir. BOME biriminde çalışacak olan personele teknik kabiliyet kazandırmayı amaçlayan Olay Müdahale ve Sistem Analizi Eğitimi’nde (3 gün süreli) ise bilgisayar güvenlik olayı yaşandığında nasıl müdahalede bulunulacağı, hangi kayıt dosyalarına bakılacağı Linux ve Windows işletim sistemleri için anlatılmaktadır.

Hazırlanan bu eğitimlerle beraber iki pilot çalışma grubu oluşturulmuştur. İlk çalışma grubunda Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Sermaye Piyasası Kurulu ve Maliye Muhasebat Genel Müdürlüğü yer almıştır. İkinci çalışma grubunda ise Merkez Bankası, Hazine Müsteşarlığı, Dış Ticaret Müsteşarlığı ve Tapu Kadastro Genel Müdürlüğü yer almıştır. Verilen eğitimler ve yapılan periyodik toplantılarla bu kurumlarda bilgisayar olaylarına müdahale ile ilgili politika ve prosedürler hazırlanmış olup kurumlara güvenlik olaylarına müdahale yeteneği kazandırılmıştır.

3.1.2 *BOME 2008 Tatbikatı*

Kurumların güvenlik olaylarını tespit ve müdahaledeki yetenekleri belirlemek amacıyla ülkemizde ilk defa düzenlenen Bilgi Sistem Güvenliği Tatbikatı olan BOME2008 tatbikatı 8 kamu kurumunun katılımıyla 20-21 Kasım 2008 tarihinde icra edilmiştir. Cumhurbaşkanlığı, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu ve Tapu Kadastro Genel Müdürlüğü'nün katılımıyla gerçekleştirilen tatbikatın sonuç raporu Ulusal Bilgi Güvenliği Kapısı olan www.bilgiguvenligi.gov.tr web sayfasında yayınlanmıştır.

3.1.3 Olay Müdahale Koordinasyon Hizmeti Kapsamındaki Faaliyetler

TR-BOME, web sayfası üzerinden, e-postayla ve telefon yoluyla ihbar almaktadır. Bu ihbarları değerlendirip gerekli müdahalenin zamanında yapılabilmesini sağlamak ve olay müdahale esnasında yürütülen faaliyetleri kayıt altına almak için RTIR isimli yazılımın kurulumu gerçekleştirilmiştir. 2008 yılında başlayan çalışmalar sonucunda sistem 2009 yılı itibariyle hizmet vermeye başlamıştır.

TR-BOME'ye 2009 yılı içerisinde 1 Ocak – 31 Mayıs tarihleri arasında yurt dışından 258, yurt içinden 15 olmak üzere toplam 273 ihbar gelmiştir. Gelen ihbarların çok büyük kısmı bankaların İnternet bankacılığı sitelerinin kopyalanması suretiyle kullanıcıların hesap bilgisi ve şifresi gibi özel bilgilerini ele geçirmeyi amaçlayan yemleme (phishing) siteleri ile ilgili ihbarlardır. Bu ihbarlara ilgili taraflarla temasa geçilip müdahale edilmeye çalışılmıştır. Ülkemizde hizmet veren bankaların kullanıcılarını hedef alan 15 web sitesinden 14'ünde zararlı içeriğin kapatılması sağlanmıştır.

Sanal ortamda sınırlar kalktığı için ulusal olarak sorumluluğu bulunan BOME birimlerinin etkinlikleri, uluslar arası organizasyonlarla olan ilişkileriyle yakından ilgilidir. TR-BOME yurt dışındaki ilgili kuruluşlarla yakın temas içerisinde olmayı amaçlamaktadır. Bu kapsamda NATO bünyesinde siber savunmadan sorumlu olan NCIRC birimiyle 2007 yılında imzalanan mutabakat zaptı çerçevesinde bilgi birikiminin paylaşılmasından yaşanan bir bilgi güvenliği olayına ortak olarak müdahalede bulunmaya kadar geniş bir alanda işbirliğini hedeflenmiştir. Yine bu mutabakat zaptı çerçevesinde 2009 Kasım'da gerçekleştirilecek olan ve 10 ülkenin oyuncu, 8 ülkenin gözlemci olarak katılacağı bilgi sistem güvenliği tatbikatında aktif rol alacaktır. TR-BOME, Avrupa çağında faaliyet gösteren BOME'ler arasındaki ilişkileri geliştirmeyi, bağları kuvvetlendirmeyi amaçlayan TF-CSIRT kuruluşuna 2008 yılında üye olmuştur. Avrupa'da ülkeleri temsil eden BOME'lerin bir araya geldiği bir organizasyon olan EGC (European Government CERTs) için üyelik başvurusunda bulunmuş olup, sürecin sonuçlanmasını beklenmektedir.

3.1.4 Alarm ve Uyarılar Hizmeti Kapsamındaki Faaliyetler

Ülkemizdeki bilgi sistemlerinde yaygın olarak kullanılan yazılım ve donanımlarda bulunan açıklıklar ve bu açıklıkların nasıl kapatılacağı bilgisi Ulusal Bilgi Güvenliği Kapısı olan www.bilgiguvenligi.gov.tr web sayfasında yayınlanmaktadır. Bu kapsamda 2007 – 2008 yıllarında 94 tane acil, 77 tane yüksek olmak üzere toplam 185 adet açıklık için duyuru yayınlanmıştır.

Ayrıca bu açıklıklarda önem derecesi ve yaygın etkisinden dolayı

- Sertifikasyon Makamları'nın(CA) Güvenilirliği
- Internet Explorer XML Databinding Açıklığı

- Windows Server Servisinde Bulunan Kritik Açıklık (MS08-067)
- DNS Önbellek Zehirlenmesi: Açıklık ve Kapanması

açıklıklarının detaylı analizlerinin yapıldığı teknik makaleler aynı sitede yayınlanmıştır.

Dünya üzerindeki birçok sistemi etkileyen ve ülkemizde de etkisi görülen *DNS Önbellek Zehirlenmesi* açıklığı için ulusal basında duyuru yayınlatılmıştır.

3.2 Ulusal Bilgi Güvenliği Programı Kapsamında Gerçekleştirilen Faaliyetler

UBGP kapsamında TR-BOME tarafından gerçekleştirilen faaliyetler eğitim, Ulusal Bilgi Güvenliği Kapısı, teknik güvenlik testleri ve AR-GE başlıkları altında aşağıda açıklanmıştır.

3.2.1 Eğitim Faaliyetleri

Kamu kurum ve kuruluşlarında çalışan bilgi sistem uzmanlarının bilgi sistem güvenliğinin değişik alanları ile ilgili bilgi eksikliğini gidermek amacıyla program kapsamında eğitimler düzenlenmiştir. Bu eğitimler, 20 kişilik laboratuar ortamına sahip sınıflarda uygulamalı olarak gerçekleştirilmiştir. Eğitimlere katılanlar, öğrendikleri konuların uygulamalarını sınıfta gerçekleştirme imkanı bulmuşlardır.

Bilgi sistem güvenliği, 13 farklı eğitim alanında ele alınmaktadır. Her bir eğitim bir ile altı gün arasında değişen sürelere sahiptir.

•ISO 27001 Uygulama ve Denetim Eğitimi

•Sistem Güvenlik Denetleme Eğitimi

•Windows Güvenliği Eğitimi

•Microsoft Sistemleri Güvenliği Eğitimi

•Unix/Linux Güvenliği Eğitimi

•Sınır Güvenliği Eğitimi

•Veritabanı Güvenliği Eğitimi

•Web Uygulamaları Güvenliği Eğitimi

•BOME Kurulum ve Yönetim Eğitimi

•Olay Müdahale ve Sayısal Adli Analiz Eğitimi

•Kablosuz Ağ Güvenliği Eğitimi

•İş Sürekliliği /Felaket Kurtarım Planlaması Eğitimi

•Bilgi Sistemleri Denetimi Eğitimi

Tüm eğitimler yaklaşık olarak 40 gün sürmektedir. Şu ana kadar eğitimlerin her birisi program kapsamında altışar kez verilmiştir. Tamamı ücretsiz olan bu eğitimlere olarak 91 kamu kurumundan 224 personel katılmıştır.

3.2.2 Ulusal Bilgi Güvenliği Kapısı

Ulusal Bilgi Sistemleri Güvenlik Programı'nın en önemli unsurlarından birisi de Ulusal Bilgi Güvenliği Kapısı Projesi'dir. Ülkemizde bilgi güvenliği konusunda web üzerinden bilgi paylaşım ortamı sağlamayı amaçlayan site www.bilgiguvenligi.gov.tr adresinden yayın yapmaktadır.

Sitede, bilgi güvenliğiyle ilgili özel konularda okuyucu bilgilendirmeyi amaçlayan teknik yazılar, bilgi güvenliği ile ilgili kılavuzlar, ülkemizde yapılan etkinlik, toplantı, sempozyum vs. gibi organizasyonların duyuruları, önemli açıklıklarla ilgili güvenlik bildirisi sayfası bulunmaktadır. Ulusal Bilgi Güvenliği Kapısı'nın, şu anda iki binin üzerinde kayıtlı kullanıcısı, yirmi altısı kurum dışından olmak üzere altmış yedi yazarı, yayınlanmış yetmiş iki makalesi, otuz kılavuzu ve üç yüzün üzerinde güvenlik bildirisi mevcuttur.

Bilgi birikimine katkının sadece TR-BOME tarafından değil, ülkemizde bilgi güvenliği alanında yetkinliğe sahip her türlü kurum veya kişi tarafından yapılmasına imkan sağlanmaktadır. Kişilerin siteye kayıt olduktan sonra, bilgi güvenliği konularında oluşturduğu rehber, doküman veya makale, oluşturulacak değerlendirme komitesinin gözden geçirmesini takiben web kapısında yayınlanmaktadır.

3.2.3 Teknik Testler

Kurumların karşı karşıya oldukları riskin tespit edilmesi ve bilgi sistemlerinde bulunan açıklıkların raporlanması amacıyla Başbakanlık, Adalet Bakanlığı, Milli Eğitim Bakanlığı, Sayıştay Başkanlığı ve Maliye Muhasebat Genel Müdürlüğü'ne testler yapılmış olup sistemlerde bulunan açıklıklar, bunların risk değeri ve düzeltme yolları hazırlanan raporlarla ilgili kurumlara teslim edilmiştir.

3.2.4 Ar-Ge Çalışmaları

Virüs, solucan gibi zararlı kodların incelenmesi için laboratuar ortamında çalışmalar yapılmaktadır. Ayrıca, prototip olarak geliştirilmiş olan ve tamamen açık kaynak kodlu yazılımlardan oluşan Ulusal Sanal Ortam Savunma Merkezi, kamu kurumlarına ait kritik bilgi sistemlerini hedef alan tehditleri tespit etmeyi amaçlamaktadır. Bu sistem, birden fazla kamu kurumunu hedef alan koordineli saldırıları tespit edebileceği gibi bir kamu kurumunu hedef alan çok ciddi saldırıları da fark edebilecek yapıda oluşturulmuştur. Farklı bilgi kaynaklarını ilişkilendirerek saldırı tespiti yapabilen teknoloji, sistemin temelini oluşturmaktadır. Bu sisteme ilave olarak dağıtık yapıda bir balküpü (honeypot) sistemi kurularak, saldırganların faaliyetlerini ne şekilde gerçekleştirdikleri ile ilgili analizler yapılabilmektedir.

4. SONUÇ

DPT Bilgi Toplumu Dairesi'nce hazırlanan Bilgi Toplumu Stratejisi Eylem Planı'nın 88. maddesi ile Ulusal Bilgi Sistemleri Güvenliği Programı çerçevesinde kurulmuş olan Türkiye Bilgisayar Olayları Müdahale Ekibi (TR-BOME) ülkemizin daha güvenli bilgi ve iletişim sistemlerine sahip olabilmesi için çalışmalar yürütmektedir.

2007 – 2008 yıllarında raporda anlatılan çalışmalar gerçekleştirilmiş olup planlanan yeni faaliyetlerin gerçekleştirilmesiyle de etkinliğini artıracaktır.