ULUSAL SİBER GÜVENLİK TATBİKATI SONUÇ RAPORU

25-28 Ocak 2011

ISBN: 978-605-62506-1-3

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

TÜBİTAK

ULUSAL SİBER GÜVENLİK TATBİKATI • 2011 •

U S G T

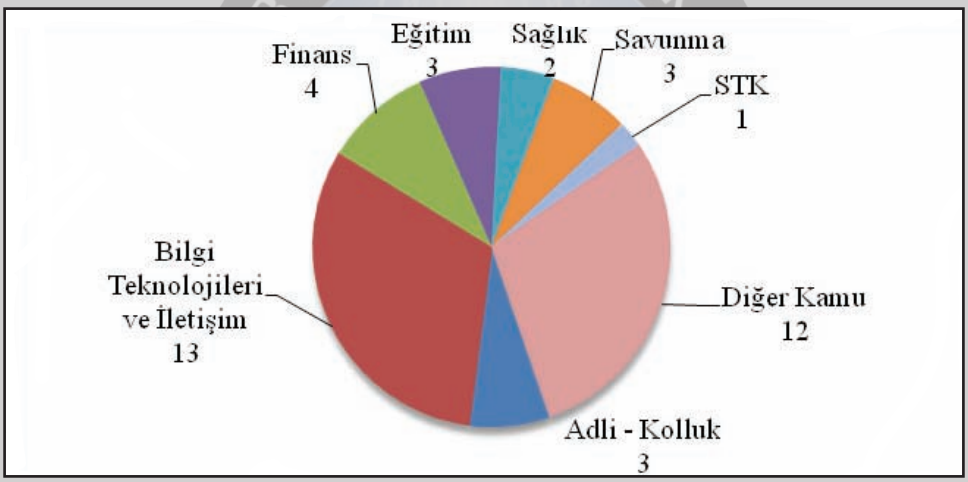
içindekiler

kısaltmalar

APCERT	Asia Pacific Computer Emergency Response Team (Asya Pasifik Bilgisayar Olaylarına Müdahale Ekibi)
BGYS	Bilgi Güvenliği Yönetimi Sistemi
BİLGEM	Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi
BOME	Bilgisayar Olaylarına Müdahale Ekibi
BTK	Bilgi Teknolojileri ve İletişim Kurumu
CERT	Computer Emergency Response Team (Bilgisayar Olaylarına Müdahale Ekibi)
DDoS	Distributed Denial of Service (Dağıtık Servis Dışı Bırakma)
EHK	Elektronik Haberleşme Kanunu
IP	Internet Protocol (İnternet Protokolü)
ITU	International Telecommunication Union (Uluslararası Telekomünikasyon Birliği)
İSS	İnternet Servis Sağlayıcı
NCDEX	NATO Cyber Defence Exercise (NATO Siber Savunma Tatbikatı)
STK	Sivil Toplum Kuruluşu
TOBB	Türkiye Odalar ve Borsalar Birliği
TOBB ETÜ	TOBB Ekonomi ve Teknoloji Üniversitesi
TR-BOME	Türkiye Bilgisayar Olaylarına Müdahale Ekibi
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
UEKAE	Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü
USGT	Ulusal Siber Güvenlik Tatbikatı

YÖNETİCİ ÖZETİ

Ulusal Siber Güvenlik Tatbikatı (USGT) 2011 finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun (STK) katılımıyla **(Şekil 1)** 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir. Söz konusu kurum/kuruluşların altısı tatbikata gözlemci statüsünde katılmıştır. Tatbikatta katılımcı kurum/kuruluşlardan bilgi teknolojileri ve iletişim, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e yakın personel görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmiştir.



Şekil 1. Çalışma Alanlarına Göre Katılımcı Kurum ve Kuruluşların Profili

25-28 Ocak 2011 tarihleri arasında gerçekleştirilen USGT 2011'in ilk iki günlük bölümünde katılımcılar çalışmalara kendi kurumlarından katılmıştır. USGT 2011'in son iki günlük bölümü ise toplu halde Türkiye Odalar ve Borsalar Birliği (TOBB) Ekonomi ve Teknoloji Üniversitesi (ETÜ) Konferans Salonu'nda gerçekleştirilmiştir.

Ülkemizde gerçekleştirilen ikinci ulusal siber güvenlik tatbikatı olan USGT 2011'de katılımcı kurumların teknik kabiliyetlerini tespit etmek ve kurumlara

olası saldırılara karşı müdahalede deneyim kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir.

USGT 2011 kapsamında, hem senaryoların yazılı ortamda gerçekleştirilmesi, hem de gerçek saldırılar sonucunda elde edilen bulgular aşağıda özetlenmiştir. Bulgulara ilişkin daha detaylı bilgi raporun "Tatbikat Bulguları" başlıklı 2. bölümünde yer almaktadır.

Bulgu 1. Bilgi Güvenliği Yönetim Sistemi Eksikliği:

Bazı katılımcılarda Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) bulunmadığı ve katılımcıların yazılı politikalarının, özellikle bilgi güvenliği politikasının, prosedür ve talimatlarının olmadığı, risk analizlerinin yapılmadığı, bir bilgi güvenliği ihlali gerçekleştiğinde bu olayın nasıl yönetileceğine ve böyle bir olayla bir daha karşılaşmamak için gerçekleştirilmesi gereken düzeltici/önleyici faaliyetlerin nasıl belirleneceğine dair yerleşik bir bilgi güvenliği kültürünün bulunmadığı gözlemlenmiştir.

Bulgu 2. Sistem Yöneticilerinin Teknik Yetersizliği:

Bazı katılımcıların sistem yöneticilerinin yeterli teknik bilgi birikimine sahip olmadıkları, sistemde bir problem meydana geldiğinde bu problemle teknik olarak nasıl başa çıkacaklarını bilemedikleri, dolayısıyla problemlerin olması gerekenden daha uzun sürede çözüldüğü tespit edilmiştir.

Bulgu 3. Saldırı Tespit Sistem ve Süreçlerinin Yetersizliği:

Bazı katılımcılarda düzenli olarak gerçekleştirilen saldırılara karşı önlem almak amacıyla saldırı tespit sistemlerinin kullanılmadığı, saldırı tespit sistemlerinin bulunduğu bazı katılımcılarda ise söz konusu sisteme ait uygulamanın ürettiği kayıtların etkin olarak incelenemediği, dolayısıyla saldırıların tespit edilmesi noktasında sıkıntılar yaşandığı gözlemlenmiştir.

Bulgu 4. Sosyal Mühendislik Saldırılarına İlişkin Bilinç Yetersizliği:

Bazı katılımcıların, yaşanan güvenlik olaylarına sadece teknik çözüm arayışında oldukları, güvenlik zincirinin en önemli halkasını oluşturan insan faktörünü göz ardı ettikleri tespit edilmiştir.

Katılımcıların genel olarak çalışanlarına*, sosyal mühendislik saldırılarına karşı düzenli olarak farkındalık eğitimleri vermedikleri, bazı katılımcılarda bu tip saldırıları engellemek amacıyla kullanıcılara düzenli olarak uyarı e-postaları gönderme ve kurum içerisinde belirli yerlere çeşitli bilgi güvenliği uyarıları asma gibi bilgi güvenliğini hatırlatıcı yöntemlerin etkin olarak kullanılmadığı gözlemlenmiştir. Ayrıca bazı katılımcılarda personelin bu tür saldırılara karşı bağışıklığını arttırmak için periyodik olarak sosyal mühendislik testlerinin yapılmadığı gözlemlenmiştir.*

Bulgu 5. Güncel Olmayan Antivirüs Sistemleri:

Bazı katılımcılarda merkezi antivirüs sunucuların imza dosyalarının düzenli olarak güncellenmediği, dolayısıyla merkezi antivirüs sunucusundan güncellemeleri alan uç birimler üzerinde kurulu olan antivirüs yazılımlarının imza dosyalarının da periyodik olarak güncellenmediği tespit edilmiştir.

Bulgu 6. Sistem Yöneticilerinin Güvenlik Boyutunda Yetersizliği:

Bazı katılımcılarda sistem yöneticilerinin bilgi güvenliği konusunda gerekli yetkinliğe sahip olmadıkları, ayrıca katılımcıların özel ilgi grupları*, diğer uzman güvenlik forumları ve STK'lar ile iletişim içinde olmadığı gözlemlenmiştir.*

Bulgu 7. Kurum İçi Koordinasyonun Yetersizliği:

Bazı katılımcılarda kurum içinde birimler arası koordinasyonun yetersiz olduğu, bazı birimlerde personel yedekliliğinin sağlanamadığı, dolayısıyla bir bilgi gü-

venliği olayı gerçekleşmesi durumunda gerekli adımların zamanında atılamadığı ve ilgili mercilerle temasın hiç sağlanamadığı ya da geç sağlanabildiği tespit edilmiştir.

Bulgu 8. Erişim Kontrol Politikasının Bulunmaması:

Bazı katılımcılarda, erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikasının bulunmadığı, bunun bir sonucu olarak personelin kendileriyle ilgili olmayan bilgi ve hizmetlere de erişebildiği tespit edilmiştir.

Bulgu 9. Sistem Tasarımı Aşamasında Güvenliğin Göz Ardı Edilmesi:

Bazı katılımcılarda, sistem tasarım aşamasında güvenliğin bir temel tasarım prensibi olarak ele alınmadığı, bu durumun güvenlik olaylarının yaşanmasını tetiklediği ve yaşanan güvenlik olaylarına etkin müdahaleyi zorlaştırdığı tespit edilmiştir.

Bulgu 10. Kablosuz Ağlardan Kaynaklanan Riskler:

Bazı katılımcılarda, saldırgan tarafından yayıma sunulan kablosuz erişim noktasının tespitinin yapılamadığı ve personelin bu yetkisiz erişim noktası üzerinden hizmet alabilecek durumda oldukları gözlemlenmiştir.

Bulgu 11. İş Sürekliliği Planlarının Bulunmaması:

Bazı katılımcıların, sistem kesintisine yol açan bilgi güvenliği olayı yaşanması durumunda iş faaliyetlerindeki kesintileri önlemek ve önemli iş süreçlerinin devamlılığını sağlamak amacıyla tesis edilmiş bir iş sürekliliği planına sahip olmadıkları tespit edilmiştir.

Bulgu 12. Port Tarama Saldırılarının Algılanmaması:

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerine yapılan "Port Tarama" saldırısını algılayamadıkları tespit edilmiştir.

Bulgu 13. Dağıtık Servis Dışı Bırakma Saldırılarının Olumsuz Sonuçları:

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerine yapılan "Dağıtık Servis Dışı Bırakma" *(DDoS) saldırısı sonucunda kurumların çoğunun hizmetlerinin kesintiye uğradığı, hizmet kesintisi yaşamayanların İnternet Servis Sağlayıcılarından* (İSS) *bu tür saldırılardan korunmak amacıyla hizmet satın aldıkları tespit edilmiştir. Bu durum, bilgi güvenliğinin sağlanmasında kurumlar arası iletişime, işbirliğine ve koordinasyona verilmesi gereken önemi ortaya koymaktadır.*

Bulgu 14. Web Uygulamalarında Bulunan Açıklıklar:

Bazı katılımcıların, İnternet'e bağlı bilgi sistemlerinde çalışmakta olan web uygulamalarında çeşitli açıklıklar bulunduğu tespit edilmiştir. Uygulama geliştirirken güvenliği *temel ihtiyaç olarak göz önünde bulunduran, ek olarak web uygulamalarını bağımsız kurum/kuruluşlara denetlettiren katılımcıların web uygulamalarında nispeten daha az açıklık bulunduğu görülmüştür.*

Bulgu 15. Kayıt Dosyalarının Analizinin Gerçekleştirilememesi:

Bazı katılımcılarda tatbikat kapsamında yapılan saldırılar sırasında oluşturulmuş saldırı kayıt dosyalarını analiz ederek saldırının ne zaman, nasıl, kim tarafından gerçekleştirildiğini belirleyemediği tespit edilmiştir. Özel bir bilgi güvenliği birimine sahip olan katılımcıların nispeten daha başarılı oldukları görülmüştür.

Bulgu 16. Yasal Mevzuata İlişkin Bilgi Eksikliği:

Bazı katılımcıların, siber güvenliğe ilişkin ulusal mevzuatımız hakkında yeterli bilgiye sahip olmadıkları, dolayısıyla tatbikatta uygulanan yazılı senaryolarda yer alan yasal mevzuatta bilişim suçu olarak tanınan fiilleri adli mercilere bildirmedikleri tespit edilmiştir.

Elde edilen bulgular genel olarak değerlendirildiğinde ülkemizde siber güvenliğin sağlanması için bilgi güvenliği yönetim sistemleri, iş sürekliliği, insan kaynakları, kurum içi ve kurumlar arası iletişim ve koordinasyon alanlarında çalışmaların yapılması, yapılmakta olan çalışmaların ise etkinliğinin artırılması gerektiği görülmektedir.

1. TATBİKAT İHTİYACI VE İLGİLİ KURUMLAR

Dünya'da Bilgi Toplumu ve Güvenlik

Bilgi toplumuna dönüşüm sürecinde her geçen gün daha fazla insan bilgi sistemlerini kullanmakta ve bu sistemlere daha çok bağımlı hale gelmektedir. Elektrik, gaz, su, iletişim ve ulaşım, kara, demir hava yolları gibi pek çok şebeke bilgi teknolojisi bileşenleri ile yönetilmektedir. Tüm bu gelişmeler bilgi sistemlerini oldukça kritik bir noktaya taşımış ve korunması gereken değerler haline getirmiştir.

Dünya'da ve ülkemizde siber güvenliğe ilişkin birçok çalışma ve düzenleme yapılmaktadır. Bu çalışma ve düzenlemeler siber tehditlerden olabildiğince sakınma ve kullanıcıların korunması temeline dayandırılmaktadır. Uluslararası Telekomünikasyon Birliği (ITU) tarafından düzenlenen ve ilk aşaması Aralık 2003'te Cenevre'de, ikinci aşaması ise Kasım 2005'te Tunus'ta gerçekleştirilen Dünya Bilgi Toplumu Zirvesi sonucunda belirlenen 11 ana faaliyet alanından biri olan "Bilgi ve İletişim Teknolojilerinin Kullanımında Gizlilik ve Güvenliği Tesis Etmek" görevi uluslararası toplum tarafından ITU'ya verilmiştir. ITU 2005 yılından bu yana bu görev doğrultusunda çalışmalar yapmaktadır.

Dünya'da siber güvenliğe ilişkin yapılan çalışmalar içinde ulusal ve uluslararası kapsamda gerçekleştirilen tatbikatların da önemli yer tuttuğu görülmektedir. Bu tatbikatlar aracılığı ile kurumsal siber güvenlik durumunun yanı sıra kurumlar arası / uluslararası koordinasyon kabiliyeti de tespit edilmekte ve elde edilen bulgular ışığında iyileştirme çalışmaları yapılmaktadır.

Türkiye'deki Çalışmalar

10.11.2008 tarihinde yayımlanan 5809 sayılı Elektronik Haberleşme Kanunu (EHK) ile aşağıdaki düzenlemeler yapılmıştır:

1. Yapılacak düzenlemelerde Bilgi güvenliği ve haberleşme gizliliğinin gözetilmesi[1] ilkesinin Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından göz önüne alınması gerekmektedir.

2. BTK, *Elektronik haberleşme sektörüne yönelik olarak,* millî güvenlik, kamu düzeni veya kamu hizmetinin gereği gibi yürütülmesi amacıyla mevzuatın öngördüğü tedbirleri almakla[2] görevlendirilmiş ve yetkilendirilmiştir.

3. Ayrıca BTK'nın işletmecilere getireceği yükümlülükler arasında *kişisel veri ve* gizliliğin korunması[3]*ve izinsiz erişime karşı* şebeke güvenliğinin sağlanması[4] bulunmaktadır.

BTK, gerek 5809 sayılı EHK ile kendisine verilen yetkiye, gerekse Türkiye'nin ITU nezdindeki temsilcisi olmasına binaen, siber güvenlik konusunda çeşitli çalışmalar yürütmektedir.

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 Kurulu 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 Araştırma Kurumu (TÜBİTAK) Ulusal Elektronik ve Kriptoloji Araştırma Enstitüsü'ne (UEKAE)

1 4 üncü madde l bendi
2 6 ncı madde ş bendi
3 12 nci madde d bendi
4 12 nci madde j bendi

1. Siber alemdeki güvenlik tehditlerini sürekli olarak takip edecek, uyarılar yayımlayacak, 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) kurma,

2. Kamu kurumları için gereken asgari güvenlik seviyelerini belirleme, kurumlar tarafından kullanılan sistem, yazılım ve ağların güvenlik seviyelerini tespit etme ve eksiklikleri giderme konularında öneriler geliştirme

görevleri verilmiştir.

Bu çerçevede TÜBİTAK Bilişim ve Bilgi Güvenliği İleri Teknolojiler Araştırma Merkezi (BİLGEM) UEKAE bünyesinde Türkiye Bilgisayar Olaylarına Müdahale Ekibi (TR-BOME) kurulmuş ve TR-BOME çalışmaları kapsamında Ulusal Bilgi Sistemleri Güvenliği Tatbikatı'nın ilki (BOME 2008) 20-21 Kasım 2008 tarihlerinde 8 kamu kurumunun katılımıyla gerçekleştirilmiştir.

5809 sayılı Kanun sonrasında ortaya çıkan durumu da göz önüne alarak; BTK ve TÜBİTAK BİLGEM UEKAE, 2010 yılında, 2008 yılında gerçekleştirilen Ulusal Bilgi Sistemleri Güvenliği Tatbikatı'na nazaran daha geniş kapsamlı ve daha fazla katılımlı bir tatbikat düzenlemek amacıyla işbirliği yaparak Ulusal Siber Güvenlik Tatbikatı - 2011 (USGT) hazırlık çalışmalarını başlatmışlardır.

1.1. Amaç

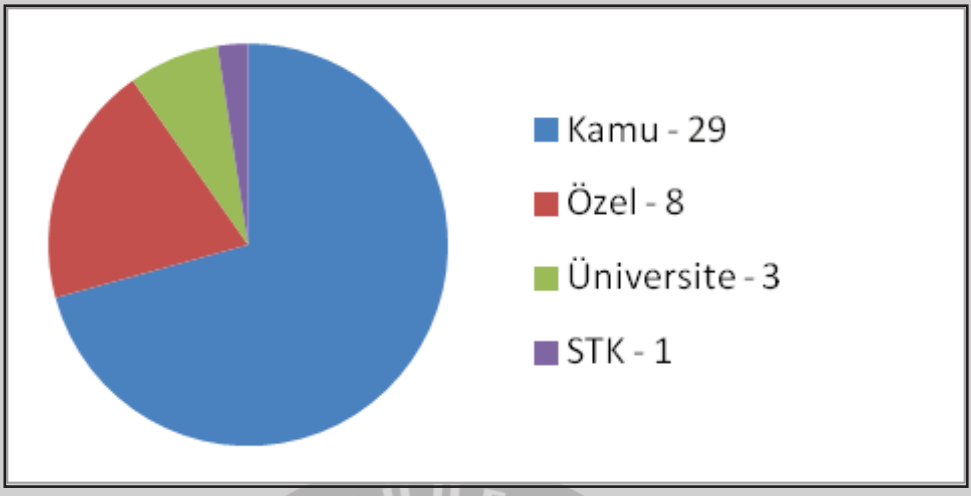
BTK ve TÜBİTAK BİLGEM UEKAE koordinatörlüğünde 25-28 Ocak 2011 tarihleri arasında gerçekleştirilen USGT 2011'in temel amacı; ülkemizde siber güvenlik konusunda idari, teknik ve hukuki kapasitenin geliştirilmesine, kurumlar arasında bilgi ve tecrübe paylaşımına ve başta yönetim seviyesinde olmak üzere tüm kademelerde farkındalık oluşumuna önemli katkılar sağlanması ve kurumların bilgisayar olaylarına müdahale yeteneğinin tespit edilmesidir.

Tatbikatta, kurumların çeşitli siber güvenlik ihlalleri karşısında verdikleri tepkiler, bu tepkiler için kullandıkları kapasite ve kurumlar arası koordinasyon değerlendirilerek tespit edilen mevcut durumun ileride siber güvenlik konusunda yapılacak ulusal ve uluslararası çalışmalara girdi oluşturması da amaçlanmıştır.

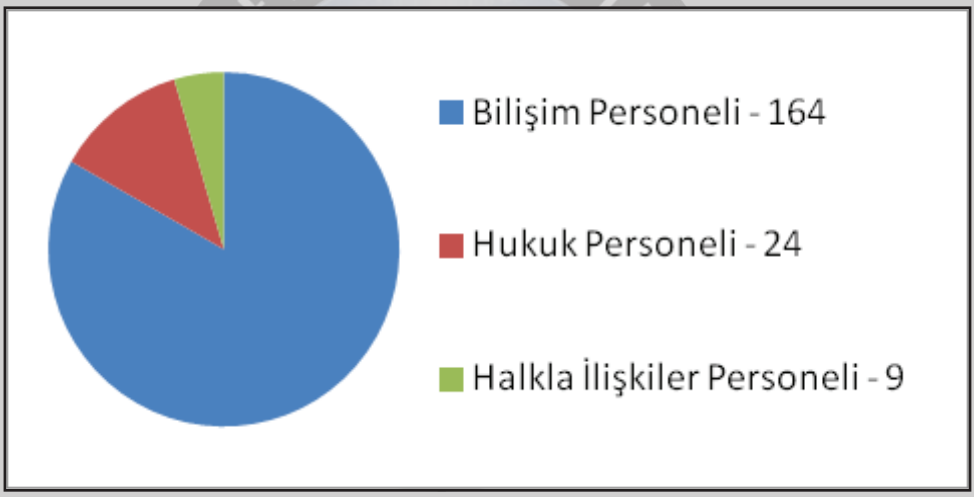
1.2. Kapsam

USGT 2011 finans, bilgi teknolojileri ve iletişim, eğitim, savunma, sağlık sektörlerinin; adli birimlerin, kolluk kuvvetlerinin ve çeşitli bakanlıkların ilgili birimlerinin temsilcilerinden oluşan 41 kamu kurumunun, özel sektör kuruluşunun ve sivil toplum kuruluşunun (STK) katılımıyla gerçekleştirilmiştir. Söz konusu kurum/kuruluşların altısı tatbikata gözlemci statüsünde katılmıştır. Tatbikatta katılımcı kurum/kuruluşlardan bilgi teknolojileri ve iletişim, hukuk ve halkla ilişkiler uzmanı statüsündeki 200'e yakın kişi görev almıştır. Katılımcı kurumların siber saldırı durumunda verecekleri tepkilerin gerçek ortamdaki ve simülasyon ortamındaki saldırılarla ölçülmesiyle, kurumların hem teknik kabiliyetleri hem de kurum içi ve kurumlar arası koordinasyon yetenekleri değerlendirilmiştir.

Katılımcı kurum ve kuruluşların sektör bazında profili Şekil 2'de, bunların temsilcilerinin uzmanlık bazında profili Şekil 3'te görülmektedir. Katılımcı kurum ve kuruluşların listesi Ek-1'de sunulmaktadır.



Şekil 2. Sektör Bazında Katılımcı Kurum ve Kuruluşların Profili



Şekil 3. Kurum Temsilcilerinin Uzmanlık Bazında Profili

USGT 2011'de Avrupa Birliği (AB) ülkeleri ve Amerika Birleşik Devletleri başta olmak üzere gelişmiş ve gelişmekte olan ülkelerin bir çoğunda öncelikli olarak korunması gereken sektörler olarak tanımlanan kritik sektörlerden katılım sağlanması hususuna özen gösterilmiştir. Ayrıca, 20-21 Kasım 2008 tarihleri arasında düzenlenen BOME-2008'in katılımcıları incelendiğinde USGT 2011'in kapsamının ne kadar büyüdüğü daha net ortaya çıkmaktadır. Öte yandan, diğer kritik sektörler olarak nitelenen enerji,

gıda, tarım gibi sektörlerin de gelecek yıllarda düzenlenmesi planlanan siber güvenlik tatbikatlarında yer alması yönünde çalışmalar yapılacaktır.

1.3. Hedefler

USGT 2011 gerçekleştirilirken; gün geçtikçe daha somut bir tehlike haline gelen siber tehditlere karşı hazırlıklı olunması, kurumların bilgi sistemi güvenliği olaylarına müdahale ve kurumlar arası koordinasyon yeteneklerinin tespit edilmesi, kurumlar arası iletişimin arttırılması, bilgi ve tecrübe paylaşımının ve ulusal siber güvenlik bilincinin arttırılması hedeflenmiş ve bu doğrultuda gerekli adımlar atılmıştır.

1.4. Planlama Süreci

2006-2010 dönemini kapsayan Bilgi Toplumu Stratejisi ve Ek'i Eylem Planı kapsamında BTK ve TÜBİTAK BİLGEM koordinasyonunda gerçekleştirilen Siber Güvenlik Tatbikatı 2011 hazırlık çalışmaları TÜBİTAK ve BTK arasındaki yazışmalar sonucunda 2010 yılı Şubat ayında başlamıştır. Siber Güvenlik Tatbikatı'nın planlanma süreci yaklaşık bir yıl sürmüştür. Bu süreçte tatbikata katılacak taraflar davet edilmiş, ilgili taraflarla görüş alışverişinde bulunulmuş ve tatbikatın düzenleneceği yerin belirlenmesiyle lojistik ihtiyaçların karşılanması için çalışmalar yapılmıştır. Bu çalışmalara paralel olarak gerçekleştirilecek gerçek saldırıların ve yazılı enjeksiyonların planlaması yapılmıştır.

Hazırlık Toplantıları

Tatbikata ilişkin planlamanın en önemli aşamalarından birisini katılımcılarla yapılan hazırlık toplantıları oluşturmuştur. Bu toplantılarda hem katılımcılar bilgilendirilmiş hem de katılımcılarla görüş alışverişi yapılarak süreç şekillendirilmiştir.

29 Nisan 2010 tarihinde BTK'da yapılan ilk hazırlık toplantısına 23 farklı kamu ve

özel sektör kuruluşundan 60'a yakın yetkili katılmıştır. Toplantıda, katılımcılara 2008 yılında yapılan tatbikat ve USGT 2011 hakkında bilgi verilmiş ve konu ile ilgili görüş alışverişinde bulunulmuştur. Toplantı sonucunda katılımcılardan tatbikata katılımları konusunda kararlarını bildirmeleri istenmiştir.

İkinci toplantı, 13 Temmuz 2010 tarihinde USGT 2011 katılımcıları ile BTK'da yapılmıştır. Bu toplantıda, uygulanacak senaryolar üzerinde durulmuş ve katılımcıların tatbikat sırasında kullanılacak enjeksiyonlara katkı sağlamaları istenmiştir.

Yapılan ilk iki toplantının ardından katılacak kurum ve kuruluşlar belirlenmiş ve kurum/kuruluşlara tatbikatın nasıl olacağına dair genel hatlarıyla bilgi verilmiştir. Bu toplantılardan sonra katılımcılar sektörlerine göre gruplandırılmışlardır. Bu gruplar,

- ✓ Adli birimler ve kolluk kuvveti,
- ✓ Finans sektörü,
- ✓ Üniversiteler,
- ✓ İSS'ler de dahil olmak üzere telekomünikasyon sektörü,
- ✓ Savunma sektörü,
- ✓ Diğer bakanlıklar

şeklinde olmuştur. Her bir grupla odak grup toplantıları adı altında her sektöre özel enjeksiyon geliştirmek ve sektörlerin kendilerine has bilgi sistemlerini yakından dinlemek amacıyla toplantılar yapılmıştır. Ağustos-Eylül 2010 tarihlerinde bu kapsamda on toplantı gerçekleştirilmiştir.

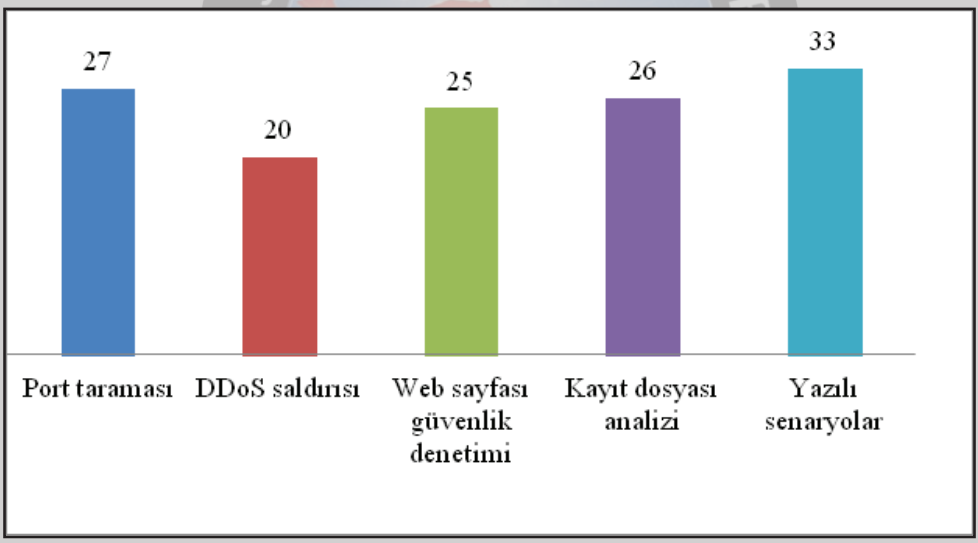
Tatbikat öncesi son hazırlık toplantısı üç grup halinde 11-13 Ocak 2011 tarihleri arasında BTK'da gerçekleştirilmiştir. Bu toplantılarda katılımcılara kullanılacak mesajlaşma platformu ve kablosuz ağ altyapısı ile ilgili bilgi verilmiş, yazılı enjeksiyonların ne şekilde olacağı ve nasıl karşılık beklendiği açıklanmıştır.

1.5. Senaryolar

25-28 Ocak 2011 tarihleri arasında gerçekleştirilen USGT 2011'in ilk iki günlük bölümünde katılımcılar kendi kurumlarında yer almışlardır. USGT 2011'in son iki günlük bölümü ise toplu halde TOBB ETÜ Konferans Salonu'nda gerçekleştirilmiştir.

Ülkemizde gerçekleştirilen ikinci ulusal siber güvenlik tatbikatı olan USGT 2011'de katılımcı kurumların teknik kabiliyetlerini tespit etmek ve kurumlara olası saldırılara karşı müdahale deneyimi kazandırmak amacıyla hem gerçek saldırılar hem de yazılı ortamda senaryolar gerçekleştirilmiştir.

USGT 2011'de gönüllülük esasına göre uygulanan gerçek saldırılar ile yazılı senaryoların uygulandığı kurum/kuruluş sayıları Şekil 4'te verilmektedir.



Şekil 4. Gerçek Saldırı ve Yazılı Senaryoların Uygulandığı Katılımcı Sayısı

1.5.1. Gerçek Saldırılar

Tatbikatın ilk iki gününde gönüllülük esasına göre düzenlenen gerçek saldırılar kapsamında;

1. Port Taraması,
2. Dağıtık Servis Dışı Bırakma (DDoS) saldırısı,
3. Web sayfası güvenlik denetimi
4. Kayıt dosyası (log) analizi

olmak üzere dört farklı faaliyet gerçekleştirilmiştir. Bu faaliyetlerle ilgili daha detaylı açıklama, faaliyetlere ilişkin bulgularla birlikte "2. Tatbikat Bulguları" bölümünde yer almaktadır.

1.5.2. Yazılı Senaryolar

Tatbikatın son iki günündeki toplu oturumda katılımcı kurum ve kuruluşların her birine yaklaşık birer saat arayla, 14 farklı yazılı senaryo (enjeksiyon) gönderilmiş ve gerçek hayatta bu senaryolar ile karşılaşmaları durumunda verecekleri tepkileri yaklaşık bir saat içinde yazılı olarak iletmeleri istenmiştir.

Katılımcılara gönderilen yazılı senaryoların kapsamı şöyledir:

1. Kurumun resmi web sayfasının içeriğinin yetkisiz kişilerce değiştirilmesi
2. Kuruma ait bir IP adresinden başka bir kurum/kuruluşa DDoS saldırısı yapıldığının tespit edilmesi
3. Kuruma ait bir IP adresinden başka bir kurum/kuruluşa istek dışı elektronik posta mesajları gönderildiğinin tespit edilmesi
4. Kuruma başka bir kaynaktan DDoS saldırısı yapılması

5. Kurumdan ayrılan kötü niyetli bir personelin ayrılmadan önce veritabanına zarar vermesi

6. Kuruma ait sistemlere İnternet üzerinden yayılan bir solucanın bulaşması

7. Telefon yoluyla kurumda çalışan personelden bilgi çalma girişimi

8. Elektronik posta yoluyla kurumda çalışan personelden bilgi çalma girişimi

9. Kurum çalışanlarından biri tarafından 5651 sayılı kanun kapsamında erişimi engellenen bir siteye giriş yapıldığının tespit edilmesi

10. Kuruma aitmiş gibi görünen sahte bir web sitesinden istek dışı elektronik posta mesajları gönderildiğinin tespit edilmesi

11. İzinsiz yapılan bir kazı neticesinde kurumun İnternet bağlantısını sağlayan fiber hattının kopartılması

12. Sistem odasında bulunan soğutma sisteminin mesai saati dışında bir saatte arızalanması

13. Kurumun bulunduğu bölgede elektrik kesintisi yaşanmasına rağmen jeneratör sisteminin devreye girmemesi

14. Kurum içinde ismi kolaylıkla tahmin edilerek bağlanılabilen bir kablosuz ağ erişim noktasının tespit edilmesi

Tatbikatın bu kısmında, katılımcı kurum ve kuruluşların, söz konusu yazılı senaryolar ile karşılaştıklarında;

- ✓ Kurum içinde ne tür tedbirler aldıkları,
- ✓ Birimler arasındaki koordinasyonu nasıl sağladıkları,
- ✓ Olayın kurum dışına olumsuz yansımaması için ne tür çalışmalar yaptıkları,
- ✓ Gereken durumlarda adli makamlar ile iletişime geçip geçmedikleri

hususları değerlendirilmiştir.

1.6. Tatbikatla İlgili Diğer Hususlar

Güvenlik ve Gizlilik

Tatbikat öncesinde ve sonrasında katılımcılarla ve tatbikatla ilgili bilgilerin güvenliğinin sağlanması konusunda azami dikkat gösterilmiştir. Yapılan toplantılarda katılımcıların sistemleri hakkında elde edilen bilgiler ve gerçek saldırılarda

bulunan açıklıklar hakkında üçüncü tarafların bilgi edinmesinin önüne geçilmiştir. Web uygulama denetimi yapılan katılımcı kurumlar ile ilgili hazırlanacak özel raporlar sadece ilgili kurumlarla paylaşılmıştır.

Tatbikata katılacak kurumlara ve tatbikatın düzenleyicilerine yapılabilecek saldırılara karşı önlemler alınmış ve yaşanabilecek problemlerin tatbikatın gidişatına engel olmasının önüne geçmek amacıyla alternatif haberleşme yöntemleri belirlenmiştir. Tatbikatın yazılı enjeksiyonlarının gerçekleştirildiği son iki gününde de gereken güvenlik önlemleri alınmıştır.

Kamuoyu ile İlişkiler

Tatbikatın kamuoyunda bilinirliğinin arttırılması için çeşitli çalışmalar yapılmıştır. Tatbikattan önce sektör dergilerinde makaleler yayımlanarak farkındalık arttırılırken BTK'nın ve TÜBİTAK'ın sitelerinde konuyla ilgili bilgilendirmeler yayımlanmıştır. Gerek tatbikat öncesinde gerekse tatbikatın açılışı sırasında basının ilgisi büyük olmuş, ulusal televizyon kanallarında ve gazetelerde tatbikatla ilgili haberler yer almıştır.

Tatbikatın resmi açılışı 27 Ocak 2011 günü Devlet Bakanı ve Başbakan Yardımcısı Sayın Bülent ARINÇ, Devlet Bakanı Sayın Prof. Dr. Mehmet AYDIN, Ulaştırma Bakanı Sayın Binali YILDIRIM, BTK Başkanı Sayın Dr. Tayfun ACARER, TÜBİTAK Başkanı Sayın Prof. Dr. Nüket YETİŞ, katılımcı kurum ve kuruluşlar ile BTK ve TÜBİTAK BİLGEM yetkililerinin katılımıyla gerçekleştirilmiştir.

2. TATBİKAT BULGULARI

Ulusal Siber Güvenlik Tatbikatı'nda hem gerçek saldırılar hem de yazılı ortamda gerçekleştirilen senaryolar sonucunda toplam 16 bulgu elde edilmiştir. Bu bulgular, çözüm önerileriyle birlikte bu bölümde açıklanmaktadır.

Bulgu 1. BGYS Eksikliği:

Bazı katılımcılarda BGYS bulunmadığı ve yazılı politikaların, özellikle bilgi güvenliği politikaları, prosedür ve talimatlarının olmadığı, risk analizlerinin yapılmadığı, bir bilgi güvenliği ihlali gerçekleştiğinde bu olayın nasıl yönetileceğine ve böyle bir olayla bir daha karşılaşmamak için gerçekleştirilmesi gereken düzeltici/önleyici faaliyetlerin nasıl belirleneceğine dair yerleşik bir bilgi güvenliği kültürünün bulunmadığı gözlemlenmiştir.

Açıklama:

Kurumlarda bir bilgi güvenliği olayı gerçekleştiğinde, olayın ortaya çıkmasından sona ermesine kadar yönetilmesi ve bir daha yaşanmaması için önlemler alınması BGYS aracılığı ile gerçekleştirilmektedir. Bu tip sistemlerin içerisinde barındırdığı süreçler sayesinde faaliyetler öncelikle planlanır, daha sonra uygulanır, kontrol edilir ve son aşamada ise tespit edilen eksikleri gidermek için düzeltici faaliyetler gerçekleştirilir. Bu sürecin devamlı çalıştırılması ile BGYS kurumda tesis edilmiş olur. BGYS kapsamında kurumlarda varlıklar, varlıkların açıklıkları ve bu varlıklar üzerine etki edebilecek tehditler listelenir ve kurumun risk değerlendirmesi gerçekleştirilmiş olur. Risk değerlendirme dokümanı kurumda alınması gereken önlemleri belirleme sürecine girdi oluşturmaktadır.

Çözüm Önerileri:

Kurumlarda Bilgi Güvenliği Yönetim Sistemleri kurulmalıdır. Kurumun politika, prosedür ve talimatları yazılı olarak muhafaza edilmelidir. Kurumlarda bilgi varlıklarının gizlilik, bütünlük ve erişilebilirlik değerleri göz önüne alınarak envanterleri çıkartılmalıdır. Kurumdaki bilgi varlıklarına etki edebilecek tehditler belirlenmeli ve kurumda risk analizi yapılmalıdır. Risk analizi sonucunda alınması gereken önlemler belirlenmeli ve bu önlemler hayata geçirilmelidir. Kurumda periyodik olarak denetimler yapılmalı ve denetimlerde belirlenen açıklıkların ve uygunsuzlukların giderilmesi için düzeltici/önleyici faaliyetler gerçekleştirilmelidir.

Bulgu 2. Sistem Yöneticilerinin Teknik Yetersizliği:

Bazı katılımcılarda, sistem yöneticilerinin yeterli teknik bilgi birikimine sahip olmadıkları, sistemde bir problem meydana geldiğinde bu problemle teknik olarak nasıl başa çıkacaklarını bilemedikleri, dolayısıyla problemlerin olması gerekenden daha uzun sürede çözüldüğü tespit edilmiştir.

Açıklama:

Sistem yöneticilerinin öncelikli olarak kurumda sorumlu oldukları sistemlerle ilgili bilgi birikiminin yeterli düzeyde olması beklenir. Bu beklentiyi karşılamak için ilk atılması gereken adım, ilgili eğitimlerin sistem yöneticileri tarafından alınmasını sağlamaktır. Bilgi güvenliği olaylarının yönetilmesinde tutarlı ve etkili bir yaklaşımın uygulanması ve yaşanan bilgi güvenliği olayı çözüme kavuşturulduktan sonra elde edilen bilginin kurumsal bilgi birikimine dönüştürülmesi gerekir.

Çözüm Önerileri:

Sistem yöneticileri sorumlu oldukları sistemlerle ilgili teknik eğitimleri almalıdır. Eğitimin etkinliğinin ölçülmesi için, sistem yöneticileri, uluslararası alanda o

konuyla ilgili olarak tanınan sertifikaları almak üzere, düzenlenen sınavlara girmelidir. Kurumda eğer sadece bir sistem yöneticisi varsa, bu sistem yöneticisinin sınır güvenliği sistemleri, veritabanı sistemleri, işletim sistemleri, ve web uygulamaları gibi çok sayıda konuda uzmanlığa sahip olması gerekecektir ki bu durum da sistem yöneticisinin kurumda kritik personel haline gelmesine neden olur. Bu durumdan kaçınmak amacıyla birden fazla sistem yöneticisi kurum bünyesinde görevlendirilebilir ve kurumsal bilgi sistemleri sistem yöneticileri arasında paylaştırılabilir. Bazı kritik konuların sorumluluğu ise birden fazla sistem yöneticisine atanarak bu sistem yöneticilerinin birbirini yedeklemesi sağlanabilir. Alınması gereken eğitimler de bu yöntem doğrultusunda planlanmalıdır. Sistem yöneticileri, teknik eğitimlerin yanı sıra sorumlu oldukları sistemlerle ilgili bilgi güvenliği eğitimlerini de almalıdır. Bilgi güvenliği olaylarının yönetiminde tutarlı ve etkili bir yaklaşımın uygulanması ve yaşanan bilgi güvenliği olayı çözüme kavuşturulduktan sonra elde edilen bilginin kurumsal bilgi birikimine dönüştürülmesi için bilgi güvenliği olaylarının türlerinin, yaşanma sıklığının ve neden olduğu hasarın ölçülüp izlenmesini sağlayan politika ve prosedürler tanımlanmalıdır.

Bulgu 3. Saldırı Tespit Sistem ve Süreçlerinin Yetersizliği:

Bazı katılımcılarda, düzenli olarak gerçekleştirilen saldırılara karşı önlem almak amacıyla saldırı tespit sistemlerinin kullanılmadığı, saldırı tespit sistemlerinin bulunduğu bazı katılımcılarda ise söz konusu sisteme ait uygulamanın ürettiği kayıtların etkin olarak incelenemediği, dolayısıyla saldırıların tespit edilmesi noktasında sıkıntılar yaşandığı gözlemlenmiştir.

Açıklama:

Saldırı tespit sistemleri kendilerine ulaşan veri paketlerini inceleyip, belirlenmiş imzalar aracılığıyla saldırı ve bilgi toplama faaliyetlerinin kayıtlarının tutulmasını sağlamaktadır. Saldırı tespit sistemleri, küçük ve orta boy ağlarda güvenlik duvarının önüne ve arkasına olmak üzere iki noktada konumlandırılmaktadır. Bü-

yük ağlarda ise, sistemin yapısına göre, gerek görülen her noktaya, hatta önemli olduğu değerlendirilen sunucuların üzerine saldırı tespit sistemi sensörleri konulabilmektedir.

Saldırı tespit sistemleri, birçok güvenlik yazılımı/donanımı gibi tak çalıştır cihazlar değildir. Bir saldırı tespit sisteminin etkili bir şekilde kullanılabilmesi, sistemin kurulmasının ardından belirlenecek güvenlik gereksinimlerine göre yapılandırılmasına ve sistemin ürettiği kayıtların düzenli olarak incelenmesine bağlıdır.

Çözüm Önerileri:

Saldırı tespit sistemi olmayan kurumlar bu sistemleri edinmeli ve kurum ağının karmaşıklığını göz önünde bulundurarak konumlandırmalıdır. Ayrıca sistem yöneticileri bu sistemlerle ilgili eğitimleri almalı ve her eğitimin sonunda, eğer mümkünse, sınavına girmeli ve sertifikasını edinmelidir. Sistem yöneticileri, sorumlu oldukları sistemlerin güvenlik gereksinimlerini göz önünde bulundurarak saldırı tespit sistemlerinin yapılandırılmasını doğru olarak yapmalı, bu sistemlerin oluşturacağı kayıtları düzenli olarak incelemeli ve rapor etmelidir. Uygulamada bu sistemlerin etkinliği anlık olarak takip edilmediği için günlük, haftalık, aylık raporlar üretilerek sistemin etkin kullanımını sağlayacak politika ve prosedürler tanımlanmalıdır.

Bulgu 4. Sosyal Mühendislik Saldırılarına İlişkin Bilinç Yetersizliği:

Bazı katılımcıların yaşanan güvenlik olaylarına sadece teknik çözüm arayışında oldukları, güvenlik zincirinin en önemli halkasını oluşturan insan faktörünü göz ardı ettikleri tespit edilmiştir.

Bazı katılımcı kurumların/kuruluşların çalışanlarına sosyal mühendislik saldırılarına karşı düzenli olarak farkındalık eğitimleri vermedikleri, bazı

katılımcılarda bu tip saldırıları engellemek amacıyla kullanıcılara düzenli olarak uyarı e-postaları gönderme ve kurum içerisinde belirli yerlere çeşitli bilgi güvenliği uyarıları asma gibi bilgi güvenliğini hatırlatıcı yöntemlerin etkin olarak kullanılmadığı gözlemlenmiştir. Ayrıca bazı katılımcılarda personelin bu tür saldırılara karşı bağışıklığını arttırmak için periyodik olarak sosyal mühendislik testlerinin yapılmadığı gözlemlenmiştir.

Açıklama:

Sosyal mühendislik insanların normalde tanımadıkları biri için yapmayacakları şeyleri yapmalarını sağlama sanatı olarak tanımlanabilir. Sosyal mühendislik saldırısı düzenleyenler teknolojiyi kullanarak ya da kullanmadan bilgi edinmek için insanlardan faydalanır, en çok da etkileme ve ikna yöntemlerini kullanır. Sosyal mühendislik saldırıları hiç tahmin edilmeyen bir anda hiç beklenmeyen bir yerden gelebilmekte olup, kurum içinden ya da kurum dışından gerçekleştirilebilmektedir. Bu tür saldırılarda tek bir kullanıcının zafiyetinden kaynaklanan bir bilgi paylaşımı bile tüm kurumu derinden etkileyecek yaraların açılmasına, maddi ve manevi hasarlar oluşmasına, kurumun itibarının zedelenmesine neden olabilmektedir.

Çözüm Önerileri:

Kurum çalışanlarının tanımadıkları kişilerden gelen isteklere karşı temkinli davranmaları ve kullanıcı şifresi gibi kişiye özel bilgilerini sistem yöneticisi, mesai arkadaşı, hatta yöneticileri dâhil, kimseyle paylaşmamaları gerekmektedir. Kurumdaki tüm personele periyodik olarak bilgi güvenliği bilinçlendirme eğitimleri verilmeli ve eğitim sonunda etkinlik ölçümleri yapılmalıdır. Ayrıca kurumda periyodik olarak, sosyal mühendislik saldırı testini de içeren, bilgi güvenliği testleri gerçekleştirilmelidir. Kullanıcılara düzenli olarak uyarı e-postaları gönderme ve kurum içerisinde belirli yerlere çeşitli bilgi güvenliği uyarıları yerleştirme gibi çeşitli bilgi güvenliğini hatırlatıcı yöntemler belirlenmeli ve uygulanmalıdır.

Bulgu 5. Güncel Olmayan Antivirüs Sistemleri:

Bazı katılımcılarda merkezi antivirüs sunucuların imza dosyalarının düzenli olarak güncellenmediği, dolayısıyla merkezi antivirüs sunucusundan güncellemeleri alan uç birimler üzerinde kurulu olan antivirüs yazılımlarının imza dosyalarının da periyodik olarak güncellenmediği tespit edilmiştir.

Açıklama:

Bilgisayar virüsleri, kendini diğer dosyaların içerisinde gizlemeye çalışan ve kullanıcının izni ya da bilgisi haricinde bilgisayarın çalışma şeklini değiştiren bilgisayar programıdır ve gerçek bir virüs, bulaştığı ortamda kendini çoğaltma ve çalıştırma işlevlerini gerçekleştirme kabiliyetine sahiptir. Bu tür zararlı kodlardan korunmak amacıyla antivirüs yazılımları geliştirilmekte ve kullanılmaktadır.

Kullanılan antivirüs programının yeni virüsleri tespit edebilmesi için virüsleri tanırken kullandığı imza dosyalarının düzenli olarak güncellenmesi önem taşımaktadır.

Çözüm Önerileri:

Bir antivirüs yazılımının kurumda etkin olarak kullanılabilmesi için tüm bilgisayarlar merkezi bir antivirüs sunucu üzerinden güncellenmeli, imza dosyası güncel tutulmalı, tüm bilgisayarlarda otomatik koruma özelliği aktif hale getirilmeli ve mümkünse farklı hizmetleri sunan sunuculara farklı antivirüs yazılımları kurulmalıdır. Örneğin dosya sunucusu üzerine bir antivirüs yazılımı kurulurken e-posta sunucusuna farklı, son kullanıcı bilgisayarlarına farklı üretici tarafından geliştirilmiş antivirüs yazılımları kurulabilir; çünkü bir antivirüs yazılımının tespit edemediği zararlı programı başka bir antivirüs yazılımı tespit edebilir ve bu şekilde kurum içerisinde zararlı kod tespit etme yeteneği arttırılmış olur.

Bulgu 6. Sistem Yöneticilerinin Güvenlik Boyutunda Yetersizliği:

Bazı katılımcılarda sistem yöneticilerinin bilgi güvenliği konusunda gerekli yetkinliğe sahip olmadıkları, ayrıca katılımcıların özel ilgi grupları, diğer uzman güvenlik forumları ve STKlarile iletişim içinde olmadıkları gözlemlenmiştir.

Açıklama:

Bilgi güvenliği bilginin gizliliği, bütünlüğü ve erişilebilirliğinin korunmasına ek olarak doğruluk, açıklanabilirlik, inkâr edilemezlik ve güvenilirlik gibi diğer özellikleri de kapsamaktadır. Bilgi güvenliğinin sistem yöneticilerinin görev aldığı bilgi işlem birimi haricinde bilgi güvenliği adı altında ayrı bir birim tarafından gerçekleştirilmesi, bilgi güvenliği ihlallerine etkin olarak müdahale etmek adına alınması gereken temel önlemlerin çatısını oluşturmaktadır.

Çözüm Önerileri:

Bilgi güvenliği ihlallerine etkin olarak müdahale etmek adına kurumlarda bilgi güvenliği birimleri oluşturulabilir ve sistem yöneticilerinden farklı olarak bu birim altında görevi sadece bilgi güvenliğinden sorumlu olacak personel görevlendirilebilir. Bu personel sınır güvenliği, veritabanı güvenliği, işletim sistemleri güvenliği ve web uygulamaları güvenliği gibi teknik konuların güvenliği konusunda eğitim alabileceği gibi BGYS kurulumu ve denetimiyle iş sürekliliği kurulumu ve denetimi gibi bilgi güvenliğinin idari boyutu ile ilgili eğitimler de almalı ve uygulama yapmalıdır. Ayrıca bu birim, özel ilgi grupları veya diğer uzman güvenlik forumları ve STK'lar ile iletişim içinde olmalıdır.

Bulgu 7. Kurum İçi Koordinasyonun Yetersizliği:

Bazı katılımcılarda birimler arası koordinasyonun yetersiz olduğu, bazı birimlerde personel yedekliliğinin sağlanamadığı, dolayısıyla bir bilgi güvenli-

ği olayı gerçekleşmesi durumunda gerekli adımların zamanında atılamadığı ve ilgili mercilerle temasın hiç sağlanamadığı ya da geç sağlanabildiği tespit edilmiştir.

Açıklama:

Bilgi işlem, bilgi güvenliği, hukuk ve halkla ilişkilerden sorumlu kurum içi kritik birimler, bir bilgi güvenliği ihlali esnasında hızlı ve doğru tepkiyi göstermek amacıyla birbirleri arasında gerekli koordinasyonu sağlamak zorundadırlar. Sadece bir personelin görev aldığı kritik birimlerde iş sürekliliği adına personel yedekliliğinin sağlanması gerekir. Ayrıca kurumlar arası koordinasyonun da zamanında sağlanması, bilgi güvenliği ihlallerine zamanında müdahale edilebilmesini teminen hayati öneme sahiptir.

Çözüm Önerileri:

Bilgi işlem, bilgi güvenliği, hukuk ve halkla ilişkilerdensorumlu kurum içi kritik birimlerin, bir bilgi güvenliği ihlali esnasında hızlı ve doğru tepkiyi göstermek amacıyla birbirleri arasında gerekli koordinasyonu sağlamalarının en etkin yollarından bir tanesi, kurum içerisinde periyodik olarak yazılı ve uygulamalı tatbikatlar düzenlemektir. Ayrıca ilgili mercilerle temasın vakit kaybetmeden yapılabilmesi amacıyla periyodik olarak gözden geçirilen ve güncellenen iletişim listeleri oluşturulmalı ve ilgili kişilerin bu listelere kolayca erişimi sağlanmalıdır. Ayrıca sadece bir personelin görev aldığı kritik birimlerde iş sürekliliği adına personel yedekliliğinin sağlanması gerekmektedir. Bu yedeklilik ya yeni personel istihdamıyla ya da kurum içerisinde farklı göreve sahip personelin ilgili alanda da faaliyet gösterebilecek bilgi birikimini kazanmasıyla sağlanabilecektir.

Bulgu 8. Erişim Kontrol Politikasının Bulunmaması:

Bazı katılımcılarda erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikasının bulunmadığı, bunun bir sonucu olarak personelin kendileriyle ilgili olmayan bilgi ve hizmetlere de erişebildiği tespit edilmiştir.

Açıklama:

Erişim kontrolü, en basit tanımıyla, belli bir varlığa sadece yetkili kişi veya grupların kendilerine tanınan yetkiler dâhilinde, tanımlanan zaman aralıklarında erişebilmelerini sağlama amacıyla uygulanır. Bu erişim fiziksel olabileceği gibi mantıksal da olabilir. En genel haliyle mantıksal erişim, bir bilgi varlığına bilgisayar aracılığıyla yapılan erişimi ifade eder.

Çözüm Önerileri:

Kurumlarda erişim için iş ve güvenlik gereksinimlerini temel alan bir erişim kontrol politikasının oluşturulması, politikanın belgelendirilmesi ve düzenli olarak gözden geçirilmesi gerekmektedir. Tüm kullanıcı gruplarının erişim hakları belirlenmeli ve politika dokümanında açıkça belirtilmelidir. Politika dokümanı mantıksal erişimin yanı sıra fiziksel erişime ilişkin esasları da düzenlemelidir. Erişim hakları belirlenirken *"Yasaklanmadığı sürece her şey serbesttir"* yaklaşımından daha sıkı olan *"İzin verilmediği sürece her şey yasaktır"* prensibinin benimsenmesi gerekir. Erişim hakkının talep edilmesi, talebin onaylanması ve bilgi sistemine uygulanması farklı makamlar tarafından gerçekleştirilmelidir. Kurumdan ayrılan veya görev yeri değişen personelin erişim haklarının kaldırılması da erişim kontrolünün önemli bileşenlerindendir. Ayrıca bilgi sisteminde aktif durumdaki erişim haklarının düzenli olarak gözden geçirilmesi gerekir. Tüm bu konulara ilişkin tanımları yapan Erişim Kontrol Politikası belgesinin oluşturulması, tüm kurum çalışanları tarafından anlaşılması ve benimsenmesi, bilgi güvenliğinin

en önemli bileşenlerinden olan erişim kontrolünün kurumda sağlıklı bir biçimde uygulanmasını sağlayacaktır.

Bulgu 9. Sistem Tasarımı Aşamasında Güvenliğin Göz Ardı Edilmesi:

Bazı katılımcılarda sistem tasarım aşamasında güvenliğin bir temel tasarım prensibi olarak ele alınmadığı, bu durumun güvenlik olaylarının yaşanmasını tetiklediği ve yaşanan güvenlik olaylarına etkin müdahaleyi zorlaştırdığı tespit edilmiştir.

Açıklama:

Kurumsal bir bilgi sistemi kurulurken yapılacak tasarım, topoloji tasarımı, IP adreslerinin dağılımı, bilgisayar isimlendirme, kullanıcı hesapları ve ölçeklenebilirlik gibi alt başlıklardan oluşmaktadır. Yaşanan bir bilgi sistemi olayında olaydan etkilenen bilgi sistem bileşenlerinin tespit edilebilmesi, bu sistemlerin gerektiğinde karantinaya alınıp kurum bilgi sisteminden izole edilebilmesi ve gerçekleşen bir saldırının kaynağının hızlı bir şekilde bulunabilmesi için sistem tasarımı önem taşımaktadır.

Tasarımı bilgi güvenliği prensipleri de göz önünde bulundurularak yapılmış bir sistem daha yönetilebilir hale gelmektedir. Daha yönetilebilir olan bu sistem ile bilgi güvenliği olaylarına müdahale ne kadar kolay ve etkin olarak gerçekleştiriliyorsa bilgi güvenliği prensiplerine göre tasarlanmamış olan, dolayısıyla iyi yönetilemeyen bir sistemde bilgi güvenliği olaylarına müdahale de o derece zor olmaktadır.

Çözüm Önerileri:

Bilgi güvenliği olaylarına etkin bir şekilde müdahale edilebilmesi için işletilen sistemin mümkün olduğunca güvenlik prensibine dayanılarak ele alınıp yeniden

tasarlanması gerekmektedir. Sistemin yeniden tasarımının kısa vadede uygulanabilir olmadığı durumlarda aşamalı olarak planlama yapılıp çeşitli düzenlemeler zamana yayılabilir. Sistem tasarımında en önemli başlıklardan biri sistem topolojisidir. Sistem topolojisinin sistemin devreye alınmasından sonra değiştirilmesi zor olduğundan ilk aşamada uzmanlardan destek alınabilir. IP adreslerinin dağılımı, bilgisayar isimlendirme, kullanıcı hesaplarının oluşturulması, ortak hesapların kullanımdan kaldırılması ve görevler ayrılığı prensibinin uygulanması da bu kapsamda değerlendirilebilir.

Bulgu 10. Kablosuz Ağlardan Kaynaklanan Riskler:

Bazı katılımcılarda saldırgan tarafından yayıma sunulan kablosuz erişim noktasının tespitinin yapılamadığı ve personelin bu yetkisiz erişim noktası üzerinden hizmet alabilecek durumda oldukları gözlemlenmiştir.

Açıklama:

Kablosuz ağlar, kablosuz haberleşme yeteneğine sahip (802.11, Bluetooth, IR(infrared), GSM vb.) cihazların herhangi bir fiziksel bağlantı olmaksızın birbirleriyle bağlantı kurmalarını sağlayan ağ yapılarıdır. Kablosuz ağların taşıdıkları riskler, kablolu ağa sızma, trafiğin dinlenip verinin çözülmesi, ağ topolojisinin ortaya çıkartılması, istemcilerin yetkisiz erişim noktalarına bağlanması, servis dışı bırakma ve istenmeyen yerlere hizmet verme olarak sıralanabilir.

Çözüm Önerileri:

Yapılacak risk analizi sonuçlarına göre kablosuz erişimin gerçekleştiği ortamı sürekli izleyen, bilinen saldırı çeşitlerinin gerçekleşmesi durumunda alarm veren, yetkisiz erişim noktalarını ve istemcileri tespit eden bir gerçek zamanlı saldırı tespit sistemi kurum bünyesinde hizmet verebilir. Kullanıcıların güvenlik önlem-

leri konusunda bilgilendirilerek belli güvenlik önlemlerini yanlışlıkla pasif hale getirmeleri önlenmelidir. Kullanıcı bilgisayarlarında kablosuz bağlantı sırasında, Ethernet ara yüzünden kablolu ağa bağlanılmamalıdır. Aksi takdirde kullanıcı bilgisayarı kablosuz ağ ile kablolu ağ arasında köprü işlevi görebilir. Ayrıca erişim noktaları, kablosuz köprü cihazları hırsızlık veya diğer müdahalelere olanak tanımayacak şekilde yerleştirilmelidir. Bina yakınlarında güçlü antenler kullanılarak kablosuz ağın dinlenilmesi mümkün olabilir, bu sebeple tesis güvenliğinden sorumlu personelin bu hususta bilgilendirilmesi gerekmektedir.

Bulgu 11. İş Sürekliliği Planlarının Bulunmaması:

Bazı katılımcıların sistem kesintisine yol açan bilgi güvenliği olayı yaşanması durumunda iş faaliyetlerindeki kesintileri önlemek ve önemli iş süreçlerinin devamlılığını sağlamak amacıyla tesis edilmiş bir iş sürekliliği planına sahip olmadıkları tespit edilmiştir.

Açıklama:

İş sürekliliği, kurumun kritik iş süreçlerinin devamlılığını sağlamak, sağlanamadığı durumlarda ise söz konusu süreçleri ön görülen kesinti süreleri içerisinde yeniden çalışır hale getirmek için gerçekleştirilen çalışmaları kapsamaktadır. Kritik iş süreçlerinin her zaman çalışır vaziyette bulunması arzu edilen durumdur. Fakat zaman içerisinde yaşanan olaylar nedeni ile süreçlerin kesintiye uğraması kaçınılmazdır. İş süreçlerinde kesintiye neden olan olaylar küçük ve kısa zamanda telafi edilebilir olaylar olabileceği gibi, ciddi felaketler de olabilir.

Çözüm Önerileri:

Kurumlarda yaşanabilecek hizmet kesintilerinden asgari düzeyde etkilenmek için iş sürekliliği çalışması yapılması gerekmektedir. Bu kapsamda öncelikle kurumun

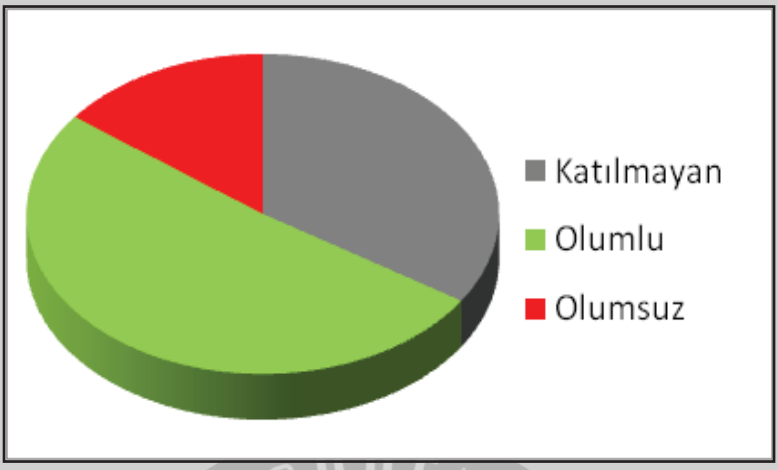
kritik iş süreçlerinin yer aldığı ve bu süreçlerden her biri için kabul edilebilir azami kesinti süresinin yer aldığı iş etki analizinin yapılması gerekmektedir. İş etki analizi sonrasında taktik anlamda olay yönetim planları ve stratejik anlamda iş sürekliliği planlamaları oluşturulmalıdır. Bu planların periyodik olarak tatbikatlarla denenmesi gerekmektedir. Bu çalışma sonrasında ilgili tüm kişilerin erişebileceği güncel bir iletişim listesi oluşturulmalıdır. Yedek sistemlerin tesis edilmesi, personel bağımlı olmayan otomatik uyarı sistemlerinin kurulması, paydaşlarla ilişkilerin iş sürekliliği çerçevesinde koordine edilmesi ve yapılan analizler sonucunda gerekirse felaket kurtarma merkezinin kurulması atılabilecek adımlardandır.

Bulgu 12. Port Tarama Saldırılarının Algılanmaması:

Bazı katılımcıların İnternet'e bağlı bilgi sistemlerine yapılan "Port Tarama" saldırısını algılayamadıkları tespit edilmiştir.

Açıklama:

Saldırganların bir saldırıya başlamadan önce ilk olarak gerçekleştirdikleri eylemlerden olan port taraması, sistem üzerinde açık durumda bulunan portları tespit etmeyi amaçlamaktadır. Kullanıcı bilgisayarını dış dünya ile bağlayan kapılar olarak ifade edilebilen portların taranması bir nevi saldırganların saldırı öncesi sistem açıklıklarını keşif çalışmalarıdır. Port taramaları, sistemlerin çalışmasına zarar vermez ve işlenen bilginin gizliliğini tehlikeye atmaz. Tatbikat esnasında yapılan port taramalarıyla, kurumların kendi sistemlerine dışarıdan yapılan bir taramayı tespit etme yetenekleri görülmüştür.



Şekil 5. Port Tarama Saldırısının Sonuçları

Tatbikat katılımcısı kurum/kuruluşlardan 27'si bu saldırının tatbikat esnasında kendi sistemlerine yönelik olarak gerçekleştirilmesi için gönüllü olmuşlar ve bu saldırıyı tespit için gerekli sistemlere sahip olduklarını tatbikat öncesi hazırlık toplantılarında beyan etmişlerdir. Yapılan saldırı sonucunda 21 katılımcı saldırıyı başarıyla tespit ederken altı katılımcı saldırıyı tespit edememiştir (Şekil 5).

Çözüm Önerileri:

Kurumlarda bulunan Güvenlik Duvarı, Saldırı Tespit Sistemi ve benzeri sınır güvenlik sistemlerinin doğru yapılandırılması sonucunda "Port Tarama" saldırısının kurum tarafından algılanması için teknolojik altyapı hazırlanmış olacaktır. Bu altyapıya ilave olarak bu sistemlerden sorumlu sistem yöneticilerinin bulunması ve sistem yöneticilerinin sistemler tarafından üretilen kayıt, alarm ve benzeri verileri düzenli olarak izlemesi gerekmektedir.

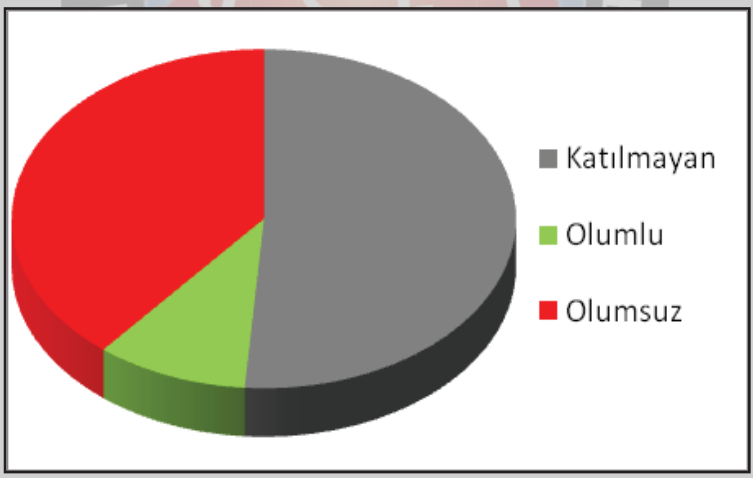
Bulgu 13. Dağıtık Servis Dışı Bırakma Saldırılarının Olumsuz Sonuçları:

Bazı katılımcıların internete bağlı bilgi sistemlerine yapılan DDoS saldırısı sonucunda kurumların çoğunun hizmetlerinin kesintiye uğradığı, hizmet kesintisi yaşamayanların İSS'lerinden bu tür saldırılardan korunmak amacıyla

hizmet satın aldıkları tespit edilmiştir. Bu durum, bilgi güvenliğinin sağlanmasında kurumlar arası iletişim, işbirliği ve koordinasyona verilmesi gereken önemi ortaya koymaktadır.

Açıklama:

Günümüzde sistemlerin çalışmasını önlemeye yönelik olarak gerçekleştirilen saldırıların ilk sıralarında DDoS saldırıları bulunmaktadır. Bu saldırılarda, çalışması engellenmek istenen sisteme farklı kaynaklardan yoğun olarak paket (ağ trafiği) gönderilmesiyle sisteme normalde erişmesi gereken kullanıcıların bağlantı yapması engellenmektedir. Tatbikat çerçevesinde, sadece belli zaman aralıklarında katılımcı kurumların sahip oldukları sistemlerin bu tür saldırılara ne kadar dayanıklı olduklarını tespit etmek ve kurumların olası benzer bir saldırı esnasında müdahale yeteneklerini geliştirmek amacıyla DDoS saldırıları gerçekleştirilmiştir.



Şekil 6. Dağıtık Servis Dışı Bırakma Saldırısının Sonuçları

Bu saldırı için gönüllü olan 20 kuruma mesai saatleri dışında önceden bildirilen ikişer saatlik zaman diliminde saldırıda bulunulmuştur. Katılımcılardan 16 tanesi saldırı esnasında hizmet kesintisi yaşarken dört katılımcı kurum ve kuruluşta hizmet kesintisi meydana gelmemiştir (Şekil 6). Hizmet kesintisi yaşamayan katılım-

cıların İSSler ile bu tür saldırılardan korunmak amacıyla hizmet satın aldıkları görülmüştür. Bu durum, bilgi güvenliğinin sağlanmasında kurum ve kuruluşlar arası iletişim, işbirliği ve koordinasyona verilmesi gereken önemi ortaya koymaktadır.

Çözüm Önerileri:

Dağıtık Servis Dışı Bırakma saldırılarının bertaraf edilmesi ile ilgili olarak kesin bir çözüm bulunmamakla birlikte aşağıdaki tedbirlerin hayata geçirilmesi ile olumlu sonuçlar alınabilmektedir.

- Servis veren sunucu cihazlarında açık kaynak kodlu işletim sistemlerinin kullanılması, bu işletim sistemleri üstünde "SynCookie" vb. önlemlerin alınması.

- Saldırıya uğrayan sunucunun bulunduğu ağda yer alan sınır gözetleme sistemlerinin izleme için devamlı olarak kullanılması, saldırı başladığında saldırıda kullanılan paketlerin ortak özelliklerinin belirlenmesi ve bu paketlerin Güvenlik Duvarı vb. sistemlerle süzülmesi.

- Ülke genelinde İSS konumundaki kurum ve kuruluşların sorumlu oldukları ağların çıkış noktalarında saldırı paketlerini süzecek politikaları uygulamaları.

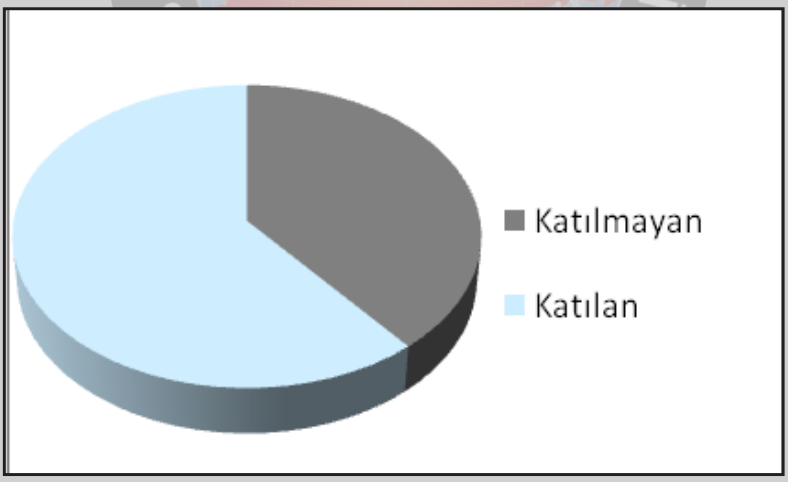
Sayılan önlemlerin uygulanabilmesi için kurum bilgi işlem çalışanlarının DDoS gibi güncel saldırı türleriyle ilgili bilgi birikimine sahip olmalı, bu konularda eğitim almış olmalıdır. Bu sayede kurumlarına/kuruluşlarına yönelik bir saldırıyı zamanında doğru şekilde tespit edebilir ve önleme amacıyla hem gerekli çabayı gösterebilirler hem de ilgili kurum/kuruluşlarla temasa geçebilirler. Kurumlar/kuruluşlar, hizmet aldıkları İnternet Servis Sağlayıcılardan Dağıtık Servis Dışı Bırakma saldırılarını önlemeye yönelik hizmeti satın alabilir. Ayrıca bu tip saldırılar esnasında İSS ile gerekli ve yeterli koordinasyonun sağlanması gerekmektedir. İSS'nin sağlaması gereken hizmetler ve bu hizmetlerin seviyeleri konusunda kurumlar/kuruluşlar arasında imzalanan anlaşmalar gözden geçirilmeli, bir olayın meydana gelmesi durumunda İSS'den kimlerle temasa geçileceği açık ve net olarak tanımlanmalıdır. Bir saldırı durumundan önce bu kanalların işlevselliği düzenli olarak kontrol edilmelidir.

Bulgu 14. Web Uygulamalarında Bulunan Açıklıklar:

Bazı katılımcıların İnternet'e bağlı bilgi sistemlerinde çalışmakta olan web uygulamalarında çeşitli açıklıklar bulunduğu tespit edilmiştir. Uygulama geliştirirken güvenliği temel ihtiyaç olarak göz önünde bulunduran, buna ilaveten web uygulamalarını bağımsız kurum/kuruluşlara denetlettiren katılımcıların web uygulamalarında nispeten daha az açıklık bulunduğu görülmüştür.

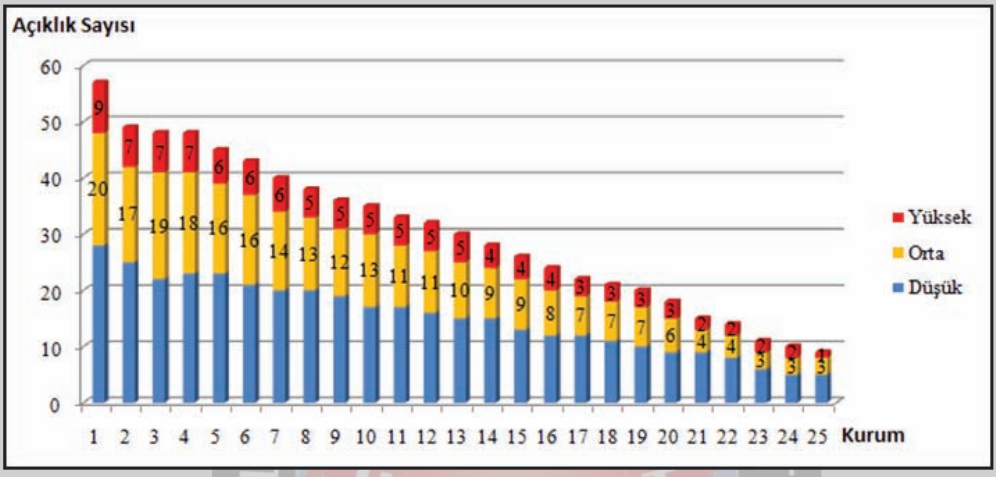
Açıklama:

Kurumların/kuruluşların web sayfaları özellikle kurum/kuruluş imajına zarar vermek isteyen saldırganların hedefi olmaktadır. Dünya tarihine ilk siber savaş örnekleri olarak geçen 2007 ve 2008 yıllarında Estonya ve Gürcistan'a karşı yapılan saldırılarda kamu kurumlarının web sayfalarının ele geçirilmesi ve içeriğinin değiştirilmesi en yaygın olarak görülen saldırı yöntemlerinden biri olarak dikkat çekmiştir. Tatbikat esnasında, katılımcıların web sayfalarının güvenliği, bir saldırganın bakış açısıyla denetlenmiştir.



Şekil 7. Web Uygulamaları Analizi Çalışmasına Katılım

Bu saldırı için 25 katılımcı gönüllü olmuştur (Şekil 7). Söz konusu katılımcılar tarafından bildirilen toplam 66 uygulama denetlenmiş ve tespit edilen açıklıkların Yüksek, Orta ve Düşük dereceli olarak sınıflandırıldığı grafik **Şekil 8'de sunulmuş**tur. Bu grafikte, gizlilik prensibi uyarınca, kurum/kuruluş adları sayılarla ifade edilmiştir. Web uygulaması denetimine katılan her bir kurum/kuruluş için özel



Şekil 8. Kurumlarda/Kuruluşlarda Tespit Edilen Web Açıklıklarının Sayıları

rapor üretilmiş ve ilgili kurumlara iletilmiştir. Uygulama geliştirirken güvenliği bir tasarım ihtiyacı olarak göz önünde bulunduran ve uygulamalarını bağımsız kurum/kuruluşlara denetlettiren katılımcıların nispeten daha az zafiyete sahip oldukları görülmüştür.

Çözüm Önerileri:

Açıklama bölümünün sonunda da belirtildiği gibi, web uygulamalarının tasarlanma ve gerçekleştirme aşamalarında kurumun kendisince veya yazılımı geliştiren üçüncü taraflarca "güvenli yazılım geliştirme" teamülleri uygulanmalıdır. Bu teamüllerin uygulanması kurumun/kuruluşun kendisine veya yazılımı geliştiren üçüncü taraflara düşebilmektedir. Her iki halde yazılım geliştirmenin hem idari, hem teknik boyutlarını ele alan kurumsal bir iş sürecinin tanımlanması gerekmektedir.

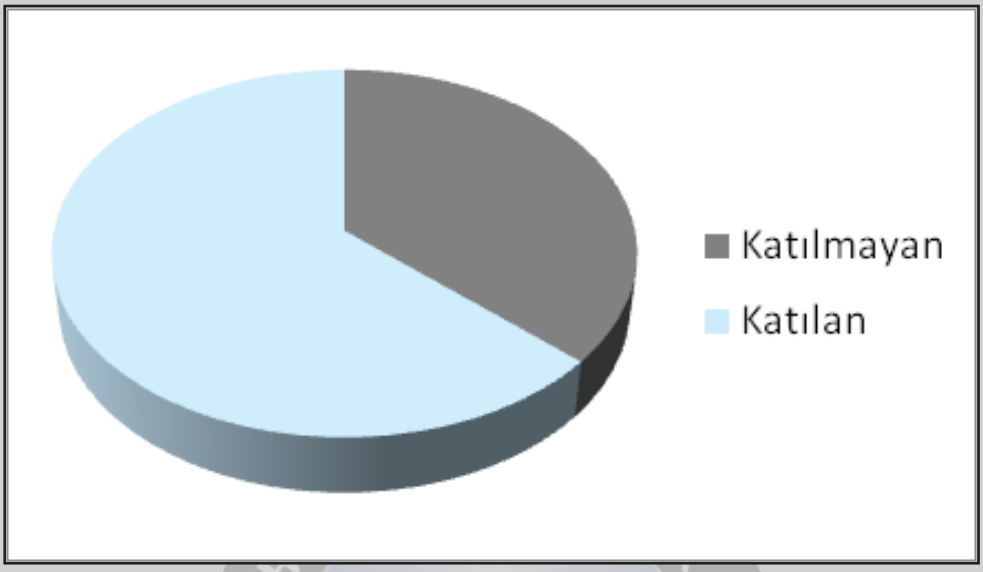
Geliştirilen yazılımların bağımsız olarak test edilmesinin de son derece önemli bir ihtiyaç olduğu bilinmekte, bu ihtiyacın nasıl karşılanacağı konusunun da yazılım geliştirme süreci kapsamında tanımlanması gerektiği değerlendirilmektedir.

Bulgu 15. Kayıt Dosyalarının Analizinin Gerçekleştirilememesi:

Bazı katılımcıların tatbikat kapsamında yapılan saldırılar sırasında oluşturulmuş saldırı kayıt dosyalarını analiz ederek saldırının ne zaman, nasıl, kim tarafından gerçekleştirildiğini belirleyemedikleri tespit edilmiştir. Özel bir bilgi güvenliği birimine sahip olan katılımcıların nispeten daha başarılı oldukları görülmüştür.

Açıklama:

Olası bir saldırı sonrası ortaya çıkan kayıt (log) dosyalarının analiz edilmesi, saldırının kim tarafından, ne zaman ve nasıl gerçekleştirildiğinin anlaşılmasını sağlamaktadır. Tatbikat esnasında, test ortamında yapılan saldırılar ile oluşturulmuş saldırı kayıtları katılımcılara gönderilmiş ve katılımcıların bu kayıt dosyalarını analiz ederek saldırının ne zaman, nasıl, kim tarafından gerçekleştiğini tespit etmeleri istenmiştir. USGT 2011'de kayıt dosyası analizi ile hem katılımcılara olay analizi deneyimi kazandırılması hem de var olan yeteneklerin tespit edilmesi hedeflenmiştir.



Şekil 9. Kayıt Dosyası Analizi Çalışmasına Katılım

Kayıt dosyası analizi için 26 katılımcı gönüllü olmuştur (Şekil 9). Bu katılımcılara hazırlanmış olan beş farklı kayıt dosyası her katılımcının sahip olduğu sistemlerle uyumlu olacak şekilde seçilerek sorular yöneltilmiştir. Kurum/kuruluş içinde özel bir bilgi güvenliği birimine sahip olan katılımcıların nispeten daha başarılı oldukları görülmüştür.

Çözüm Önerileri:

Kayıt dosyası analizi çalışmasının amacı olan kurumlara/kuruluşlara, deneyim kazandırma hedefine ulaşabilmek için tatbikat sonrasında düzenlenen bir atölye çalışmasıyla çözümler uygulamalı olarak tartışılmıştır.

Bulgu 16. Yasal Mevzuata İlişkin Bilgi Eksikliği:

Bazı katılımcıların siber güvenliğe ilişkin ulusal mevzuatımız hakkında yeterli bilgiye sahip olmadıkları, dolayısıyla tatbikatta uygulanan yazılı senaryolarda yer alan yasal mevzuatta bilişim suçu olarak tanınan fiilleri adli mercilere bildirmedikleri tespit edilmiştir.

Açıklama:

Ülkemizde, siber güvenliğe ilişkin yasal mevzuatta çeşitli eksiklikler bulunsa da; hâlihazırda gerek bazı siber güvenlik ihlallerinin önlenmesine, gerekse ihlal sonrasında uygulanabilecek cezai yaptırımlara yönelik çeşitli düzenlemeler bulunmaktadır.

Örneğin; 5237 sayılı Türk Ceza Kanununun "Bilişim Alanında Suçlar" başlıklı onuncu bölümünde yer alan hükümler ile bu kanunun çeşitli maddelerinde ele alınan "fiilin bilişim sistemlerinin kullanılması suretiyle işlenmesi" halinde uygulanacak hükümler bunlardandır.

Ayrıca, 5651 sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun ile aynı zamanda Telekomünikasyon İletişim Başkanlığı'na (TİB) internet ortamında yapılan yayınların içerik denetimi ve belli suçları oluşturduğu hususunda yeterli şüphe sebebi bulunan yayınlarla ilgili olarak uyarı yapma ve bu yayınlara erişimi engelleme yetkisi verilmektedir.

Son olarak, 10 Kasım 2010 tarihinde Dışişleri Bakanlığı düzeyinde imzalanan Avrupa Konseyi Siber Suç Sözleşmesi'nin önümüzdeki günlerde Türkiye Büyük Millet Meclisi tarafından onaylanması beklenmektedir. Uluslararası bir sözleşme olarak tüm kanunların üzerinde işlem görecek olan 48 maddeden oluşan bu belgede; özellikle telif hakları ihlalleri, yetkisiz erişim, bilgisayarlarla ilişkili sahtecilik eylemleri ve çocuk pornografisine ilişkin suçlar tanımlanmakta, cezai soruşturma ve kovuşturma yöntemleri belirlenmektedir.

Çözüm Önerileri:

Kurumların gerek bilgi işlem, gerekse hukuk personelinin bilişim hukuku ve ülkemizdeki ilgili mevzuat hakkında gerekli eğitimleri almaları ve herhangi bir bilgi güvenliği ihlali durumunda hangi mercilere ne şekilde başvurmaları konusunda bilgilendirilmeleri gerekmektedir. Ayrıca, yazılı ve görsel basın organlarının da bu konuda farkındalığın arttırılması hususunda üzerilerine düşen görevi yerine getirmeleri beklenmektedir.

3. SONUÇ VE ÖNERİLER

USGT 2011, yaklaşık bir yıl süren hazırlık sürecinin ardından 25-28 Ocak tarihlerinde 41 kurum/kuruluşun katılımıyla başarıyla tamamlanmıştır. USGT 2011 kapsamında 500'ün üzerinde yazılı enjeksiyona ilave olarak port taraması, dağıtık servis dışı bırakma saldırıları (DDoS), web uygulamalarının denetimi ve kayıt dosyası analizinden oluşan gerçek saldırılar yapılmıştır.

Bulgular ve Genel Durum

Yapılan çalışmalar, tatbikata katılan kurum ve kuruluşlarda bilgi güvenliği açısından azımsanmayacak miktarda açıklık olduğu sonucunu gözler önüne sermektedir.

Açıklıkların kapatılması konusunda, bilgi teknolojilerine yapılacak donanım-yazılım satın alımı ve benzeri yatırımların yeterli olmayacağına, başta kurum/kuruluş yöneticileri olmak üzere kurum/kuruluş çalışanlarının tamamının bilgi güvenliği konusunda eğitilmesi, ilave olarak bilgi güvenliğine ilişkin kurumsal iş süreçlerinin hayata geçirilmesi gerekmektedir.

Elde edilen bulgular genel olarak değerlendirildiğinde ülkemizde siber güvenliğin sağlanması için **özetle bilgi güvenliği yönetim sistemi, iş sürekliliği, insan kaynakları**, kurum içi ve kurumlar arası iletişim ve koordinasyon alanlarında çalışma yapılması gerektiği görülmektedir.

Bilgi Güvenliğine Kurumsal Yaklaşım için BGYS

Kurumsal olarak siber güvenliğin sağlanmasına çalışılırken gerçekleştirilecek faaliyetlerin çalışanların kişisel bilgi ve yeteneklerine bağımlılığını azaltacak, ölçüm, denetim ve sürekli iyileştirme anlayışını kuruma yerleştirecek Bilgi Güvenliği Yönetim Sistemleri (BGYS) önem arz etmektedir. Tatbikat kapsamında gerçekleştirilen senaryolarda bilgi güvenliği olaylarına müdahale aşamalarında BGYS'ye sahip kurumların daha sistematik olarak sorunları çözmeye çalıştıkları görülmüştür.

İş Sürekliliği

Hizmet kesintilerini önlemek, bir kesinti durumunda ise kısa zamanda sistemin çalışır hale gelmesini sağlamak için iş sürekliliği çalışmaları önem taşımaktadır. Yapılacak analizlere göre kurumlar öncelikle iş sürekliliği planlarını oluşturmalıdır. Daha önce iş sürekliliği konusunda çalışma yapmış olan kurumların/kuruluşların tatbikat esnasındaki senaryolarda hizmet kesintileriyle daha etkin mücadele edebildiği ve daha kısa zamanda sistemlerini çalışır hale getirdikleri görülmüştür.

İnsan Kaynakları Güvenliği

Siber güvenliğin sağlanması için gerçekleştirilecek insan kaynakları çalışmalarında personel istihdamı ve eğitim önemli yer tutmaktadır. Bu kapsamda, öncelikle yedekliliği sağlayacak şekilde yetişmiş personel istihdam edilmeli, sistem yöneticilerine işlettikleri sisteme hâkim olmalarını sağlayacak eğitimler planlanmalı, devamında ise bilgi güvenliği konusunda çalışacak uzman personel (mümkünse ayrı bir birim olacak şekilde) için bilgi güvenliği uzmanlık eğitimleri planlanmalıdır. İnsan kaynakları, çalışmaları siber güvenliği sadece teknik bir olgu olarak görmemeli, siber güvenlik için gerçekleştirilecek eğitimlerde tüm bilgi sistemi kullanıcıları için düzenli bilinçlendirme çalışmaları yapmalıdır.

Kurum İçi ve Kurumlar Arası Koordinasyon

Son olarak, yaşanan bilgi güvenliği olaylarının çoğuna kurumların/kuruluşların tek başına müdahale etmesi ya da kurum/kuruluş içindeki bilgi işlem biriminin tek başına çözüm üretmesi mümkün olmamaktadır. Siber güvenlik tehditleriyle mücadele edebilmek için gerek kurum/kuruluş içi (bilgi işlem birimi, hukuk birimi, iletişim birimi vs.) gerekse kurum/kuruluş dışı paydaşlarla iletişim arttırılmalı ve gerekli koordinasyon sağlanmalıdır.

EK1 : USGT 2011'E KATILAN KURUM VE KURULUŞLAR

Kamu	Özel	Üniversite	STK
Adalet Bakanlığı	Avea	Ankara Üniversitesi	Bilgi Güvenliği Derneği
Ankara Cumhuriyet Başsavcılığı	Microsoft Türkiye	ODTÜ	
Bankacılık Düzenleme ve Denetleme Kurumu	TTNET	TOBB ETÜ	
Başbakanlık	Turkcell		
BTK	Türksat		
BTK Telekomünkasyon İletişim Başkanlığı	Türk Telekom		
Devlet Planlama Teşkilatı Müsteşarlığı	Vakıfbank		
Dış Ticaret Müsteşarlığı	Vodafone		
Dışişleri Bakanlığı			
Emniyet Genel Müdürlüğü			
Genelkurmay Başkanlığı			
Hazine Müsteşarlığı			
İçişleri Bakanlığı			
Maliye Muhasebat Genel Müdürlüğü			
Merkez Bankası			
Milli Güvenlik Kurulu Genel Sekreterliği			
Milli Savunma Bakanlığı			
Nüfus ve Vatandaşlık İşleri Genel Müdürlüğü			
Posta Telgraf Teşkilatı Genel Müdürlüğü			
Savunma Sanayi Müsteşarlığı			
Sayıştay Başkanlığı			
Sermaye Piyasası Kurulu			
Sosyal Güvenlik Kurumu			
Tapu ve Kadastro Genel Müdürlüğü			
TÜBİTAK BİLGEM KSM			
TÜBİTAK BİLGEM Pardus			
TÜBİTAK BİLGEM UEKAE			
TÜBİTAK ULAKBİM			
Ulaştırma Bakanlığı			

EK 2: USGT 2011'DEN FOTOĞRAFLAR


ULUSAL
U S


U S G T
2011
Prof.Dr.
Mehmet AYDIN


DEVLET PLANLAMA
TEŞKİLATI


ULUSAL SİBER GÜVENLİK TATBİKATI
USGT
2011
ANKARA ÜNİVERSİTESİ


ANKARA CUMHURİYET
BAŞSAVCILIĞI


ATAVİZYON

BTK
BİLGİ TEKNOLOJİLERİ
VE İLETİŞİM KURUMU

TÜBİTAK