ULUSAL ELEKTRONİK VE KRİPTOLOJİ

ARAŞTIRMA ENSTİTÜSÜ

BOME 2008 BİLGİ SİSTEMLERİ GÜVENLİĞİ TATBİKATI

TATBİKAT SONUÇ RAPORU

Hazırlayan: 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 düzenlenen BOME 2008 Bilgi Sistem Güvenliği Tatbikatı sonuçlarının paylaşılması amacıyla hazırlanmıştır. Tüm kurum ve kuruluşlar bu dokümandan faydalanabilir.

BİLGİLENDİRME

Bu dokümanın oluşturulmasında emeği geçen TÜBİTAK UEKAE Bilişim Sistemleri Güvenliği personeline ve dokümanı gözden geçirip fikirlerini öne sürerek dokümanın olgunlaşmasına katkıda bulunan Bilge KARABACAK'a, Hayrettin BAHŞİ'ye ve BOME 2008 Tatbikatı'na katılan kurum temsilcilerine teşekkürü borç biliriz.

İÇİNDEKİLER

1. GİRİŞ 5
2. TATBİKAT 6
2.1 Tema 6
2.2 Amacı 7
2.3 Katılımcılar 7
2.4 Senaryolar 8
2.5 Tespitler 11
3. TATBİKAT DEĞERLENDİRMESİ ve ÖNERİLER 13

1. GİRİŞ

Dünyada ve ülkemizde bilgi ve iletişim sistemlerinin kullanımı hızla yaygınlaşmaktadır. Bilgi ve iletişim sistemleri, hayatımızın her alanının önemli bir parçası haline gelmiştir. Gerek kamu kurumları gerekse özel kuruluşlar verdikleri hizmetleri artık bilgi sistemleri üzerinden vermektedir. Bu sayede hem hizmet kalitesinin artırılması hem de iş verimliliğinin yükseltilmesi hedeflenmektedir.

Kurum ve kuruluşların sundukları hizmetlerde bilgi ve iletişim sistemlerini giderek daha fazla kullanmaları ile birlikte, söz konusu bilgi ve iletişim sistemlerinin güvenliğinin sağlanması önem arz eden bir konu haline gelmiştir. Bilgi sistemlerine yönelik olarak gerçekleştirilen saldırılar her geçen gün daha profesyonelce yapılmakta ve saldırganlar koordineli hareket etmektedirler. Saldırılara karşı geliştirilecek olan önleyici ve düzeltici önlemlerin alınabilmesi ve güvenlik problemleri ile ilgili iletişimin sağlanması için tek bir koordinasyon noktasının varlığını gerekli kılmıştır. Bu merkezi iletişim ve koordinasyon noktasının güvenlik bilgileri için güvenilir bir kaynak olması gerekmektedir. 1988'de Internet'in yaklaşık onda birini etkileyen Morris Solucanı'ndan sonra bu merkezlerden ilki olan CERT Coordination Center (Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi) 1988'de ABD'de kurulmuştur.

Bilgisayar olaylarına müdahale ekipleri belirli bir sorumluluk alanı dahilinde faaliyet gösteren, bu sorumluluk alanında olay müdahale hizmeti veya bilgi sistem güvenliği ile ilgili diğer önleyici veya düzeltici hizmetleri veren ekiplerdir. Bilgisayar olaylarına müdahale ekibi koordinasyon merkezleri sorumluluk alanında birden çok kurum /kuruluş olan ve bu kurum/kuruluşlar arasında olay müdahale koordinasyonu yapan merkezlerdir. Bilgisayar olaylarına müdahale ekibi koordinasyon merkezleri, sorumluluk alanındaki kurum ve kuruluşlar arasında bir güven ağı oluşturmayı hedefler ve olay müdahale hizmetini olay müdahale koordinasyonu şeklinde verirler. Olay müdahale koordinasyonu kapsamında, 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.

CERT Coordination Center'ın kurulmasının ardından diğer ülkelerde de Ulusal BOME Koordinasyon Merkezleri kurulmaya başlamıştır. Bugün birçok ülkede Ulusal BOME Koordinasyon Merkezleri, kendi sınırları içerisinde güvenlik olayları koordinasyonunu sağlamaya çalışmanın yanı sıra birçok güvenlik olayı ülke sınırlarını aştığı için diğer koordinasyon merkezleriyle de iletişim içinde olmaya çalışmaktadır. Günümüzde İnternet ve bilişim sistemleri son derece yaygınlaştığı ve saldırganlar farklı ülkelerden bir araya gelerek son derece organize çalıştıkları için Ulusal BOME Koordinasyon Merkezleri çok daha önemli hale gelmiştir

Ülkemizde ise Ulusal Bilgisayar Olayları Müdahale Ekibi Koordinasyon Merkezi (TR-BOME), Devlet Planlama Teşkilatı'nın 2006-2010 Bilgi Stratejisi Eylem Planı 88. Maddesi gereğince TÜBİTAK UEKAE bünyesinde kurulmuştur. 2009 yılına kadar, Başbakanlık, Adalet Bakanlığı, Sayıştay Başkanlığı, Hazine Müsteşarlığı, Dış Ticaret Müsteşarlığı, Merkez Bankası, Sermaye Piyasası Kurulu, Muhasebat Genel Müdürlüğü ve Tapu Kadastro Genel Müdürlüğü'ne BOME kurma danışmanlığı hizmeti verilmiştir.

TR-BOME, ülkemizin sanal ortamda gerçekleşen saldırılar karşısındaki durumunu tespit etmek amacıyla ilk defa icra edilen bilgi güvenliği tatbikatı olan BOME 2008 Tatbikatı'nı gerçekleştirmiştir.

2. TATBİKAT

Ülkemizdeki ilk Ulusal Bilgi Güvenliği Tatbikatı olan BOME 2008 Tatbikatı, 20-21 Kasım 2008 tarihlerinde icra edilmiştir. BOME 2008 Tatbikatı, mesai saatlerinde (09.00 – 18.00) gerçekleştirilmiştir. Tatbikat dağıtık yapıda gerçekleştirilmiş olup, tatbikat süresince katılımcı kurum temsilcileri kendi kurumlarından çalışmalara katılmıştır.

2.1 Tema

BOME 2008 Tatbikatı'ndaki olay akışı ve senaryolar, hayali bir ülke olan Kamanga'nın devlet başkanı Omyango Osana'nın 20-21 Kasım 2008 tarihlerinde Türkiye'ye resmi ziyarette bulunacağı ve Kamanga'da bulunan muhalif grupların ziyareti protesto etmek için Türkiye'ye sanal ortamda saldırı gerçekleştirebileceği bilgisinden yola çıkılarak hazırlanmıştır.

2.2 Amacı

BOME 2008 Tatbikatı, kurumsal BOME süreçlerinin kontrol edilmesi ve kurumun dış kaynaklı bir olaya maruz kalması durumunda TR-BOME ile işbirliği süreçlerinin kontrol edilmesi maksadıyla yapılmıştır.

a. **Kurumsal BOME Süreçlerinin Kontrol Edilmesi**
   BOME 2008 Tatbikatı ile katılımcı kurumlardaki güvenlik olaylarına müdahale süreçlerinin kontrol edilmesi, bilgisayar güvenlik olaylarına müdahalenin hangi esaslara göre yapıldığının tespit edilmesi ve var olan eksikliklerin ortaya çıkartılması hedeflenmiştir.

b. **TR-BOME ile İşbirliği Süreçlerinin Kontrol Edilmesi**
   Bilgisayar güvenlik olaylarının kaynağı kurum ve kuruluşların, BT üreticilerinin, hizmet sağlayıcıların hatta ülkelerin sınırlarının ötesinde olabilmektedir. Tüm bu gelişmeler bilgisayar güvenlik olayları ile mücadelede kurumlar, BT üreticileri, hizmet sağlayıcıları ve ülkeler arasında koordinasyon sağlanmasını çok önemli bir duruma getirmektedir.

   TR-BOME'nin verdiği hizmetlerden biri de olay koordinasyon hizmetidir. Olay koordinasyon hizmeti, taraflarından en az birinin yurt içinden olması durumunda verilmektedir. TR-BOME, koordinasyon hizmetiyle, birden fazla kurumu ilgilendiren olaylarda kurumlar arası koordinasyonu sağlamayı ve ülke genelinde yaşanan bilgisayar olaylarının büyük resmini görebilmeyi amaçlamaktadır.

   BOME 2008 Tatbikatı'yla kurumların, kurum dışı bir tarafın da içinde bulunduğu bir olayla karşılaşmaları durumunda TR-BOME'yle olan iletişim seviyelerini ölçmek hedeflenmiştir.

2.3 Katılımcılar

TÜBİTAK UEKAE bünyesinde faaliyet gösteren TR-BOME koordinatörlüğünde gerçekleştirilen BOME 2008 Tatbikatı'na aşağıda isimleri belirtilmiş olan sekiz kurumun ilgili birimleri katılmıştır.

- Cumhurbaşkanlığı
- Başbakanlık
- Adalet Bakanlığı
- Sayıştay Başkanlığı
- Hazine Müsteşarlığı
- Merkez Bankası
- Sermaye Piyasası Kurulu
- Tapu Kadastro Genel Müdürlüğü

2.4 Senaryolar

BOME 2008 Tatbikatı süresince katılımcı her kuruma dört adet enjeksiyon[1] uygulanmıştır. Enjeksiyonlar içinde,

- Tatbikat merkezi ve katılımcı kurum arasındaki haberleşmede güvenli bir altyapının kullanılmasına,
- Kurum içinde meydana gelen bir olay karşısında izlenen yöntemin tespit edilmesine,
- Kurum dışından kaynaklanan bir olayda TR-BOME ile kurulacak iletişime,
- Kurum dışından yapılan bir saldırının kurum bilgi sistemleri tarafından tespit edilmesine

yönelik dört adet senaryoya yer verilmiştir.

Uygulanan senaryolarda sistemlerin kullanılabilirliğine karşı herhangi bir zarar verilmemesi prensibiyle hareket edilmiştir. Tatbikatta yapılan üç enjeksiyonda kurum sistemlerine bir temasta bulunulmamıştır. Bir enjeksiyonda ise kurum bilgi sistemlerine temasta bulunulmuştur. BOME 2008 Tatbikatı süresince katılımcı kurumlarda tatbikat sebebiyle bir hizmet kesintisi yaşanmamıştır.

Senaryo 1: Güvenli haberleşme senaryosu

Olay müdahale esnasında paylaşılacak bilgiler kritik içeriğe sahip olabilmektedir. Mesajlaşmalarda saldırıya uğrayan bilgisayarların isimleri ve IP adresleri, sistemde bulunan bir açıklık ile ilgili bilgiler bulunabilmektedir. Bu bilgiler İnternet üzerinde açık olarak iletilirse üçüncü kişiler tarafından okunabilir, değiştirilebilir. Bu bilgilerin bir saldırganın eline geçmesi durumunda sistem ciddi tehditlere maruz kalabilmektedir. Kritik öneme sahip bilgilerin üçüncü kişilerin eline geçmemesi için haberleşmenin gizlilik ve bütünlüğünü sağlayacak kriptografik sistemler kullanılmalıdır.

[1] Enjeksiyon, tatbikat esnasında uygulanacak olan senaryonun olay haline getirilip senaryonun uygulanacağı katılımcıya gönderildiği mesajdır.

BOME kurulum danışmanlığı çalışmalarında güvenli haberleşmeyi sağlamak için açık anahtar şifrelemesi yapabilen, açık kaynak kodlu, ücretsiz GPG yazılımı kullanılmıştır. Tatbikat öncesinde de katılımcı kurumlar ve TR-BOME kendilerine ait açık anahtar bilgilerini güncellemişlerdir. Tatbikat süresince tüm yazışmaların bu sistem kullanılarak şifreli ve imzalı olarak yapılması hedeflenmiştir.

Senaryo 2: Kurum içi süreç senaryosu

Kurum içerisinde meydana gelen bir bilgisayar güvenlik olayı sadece bilgi işlem birimini veya varsa bilgi işlem biriminin içerisindeki güvenlik birimini ilgilendirmeyebilir. Bu durumda kurum içi birimlerin koordinasyon içerisinde çalışması, olay müdahalede kendilerine düşen görevi bilmesi ve yerine getirmesi etkin müdahale için gereklidir. Örneğin, saldırının veritabanı sistemlerini hedef alması durumunda sadece güvenlikten sorumlu bilgi işlem personelinin müdahalesi yeterli olmayabilir. Basına yansımış olan bir olayda basın ve halkla ilişkiler biriminin bir duyuru yapması gerekebilir. Adli boyutu olan bir olayda kurumun hukuk müşavirliği biriminin bu konuda çalışma yapması gerekebilmektedir.

Bu senaryoyla hem kurumun bir olay karşısındaki tepki mekanizması hem de kurum içinde farklı birimler arası koordinasyon yeteneği ölçülmeye çalışılmıştır.

Senaryo 3: İş birliği senaryosu

Günümüzde bilgisayar güvenlik olaylarının büyük kısmı birden fazla kişi/kurum arasında gerçekleşmektedir. Gerek taraflar arasında koordinasyonun sağlanması gerekse ülke çapındaki tehditleri, güvenlik olaylarını ve bunlardaki gelişmeleri içeren genel görünümün bir merkezde gözlemlenip bilgi havuzu oluşturulabilmesi için bir koordinasyon merkezine ihtiyaç duyulmaktadır. Bu merkez ile kurumlar/kişiler arasındaki iletişimin güçlü olması koordinasyonu daha etkili hale getirecektir. Ülkemizde bu koordinasyon faaliyetini yürütmeyi amaçlayan TR-BOME ve tatbikata katılan kurumlar arasındaki işbirliğini değerlendirmek ve bu süreçteki eksiklikleri tespit etmek amacıyla kurumlara dışı kaynaklı saldırıları içeren enjeksiyon uygulanmıştır.

Senaryo 4: Dışarıdan yapılan saldırılar

Bilgisayar güvenliğinde kullanılan yazılım ve donanımların temel özelliklerinden biri tak/çalıştır cihazlar olmamalarıdır. Bu cihazlar sistem gereksinimlerine göre yapılandırılmalı ve kayıtları düzenli olarak incelenmelidir. Katılımcı kurumlarla BOME 2008 tatbikatı öncesinde yapılan toplantılarda, kurumların saldırı tespit konusundaki yetenekleri tespit edilmiş olup dördüncü senaryo bu bilgi ışığında geliştirilmiştir.

Bu senaryo kapsamında kurum dışından belli zaman aralıklarında kurum bilgi sistemlerine yönelik olarak, sistemlere zarar vermeyecek ama kayıt oluşturacak olan saldırılar yapılmış ve katılımcı kurumların ellerindeki imkânlarla bu saldırıları tespit etmesi beklenmiştir. Bu kapsamda port taraması, javascript enjeksiyonu, sql enjeksiyonu, uzaktan dosya çalıştırma ve php kod enjeksiyonu saldırıları gerçekleştirilmiştir.

2.4.1 Örnek Senaryo

Tatbikat esnasında uygulanan kurum içi süreç ve iş birliği senaryolarına ait enjeksiyon aşağıda verilmiştir.

SPAM E-Posta:

Tatbikata katılan kurumda meydana gelen olaylar:

1. İNTERNET ÜZERİNDEN KURUMUNUZ ADINA GÖNDERİLMİŞ E-POSTALAR BAZI İNTERNET KULANICILARI TARAFINDAN GÖZLEMLENMEYE BAŞLAMIŞTIR VE BU KONUDA KURUMUNUZA BİLDİRİMDE BULUNULMUŞTUR.
2. KURUMUNUZDAN GÖNDERİLMİŞ OLARAK GÖRÜNEN E-POSTALARDA, KULLANICILARIN WEB SAYFANIZDAN İNDİRECEKLERİ YAZILIMLA SİSTEMİNİZDEN FAYDALANABİLECEKLERİ BELİRTİLMİŞTİR.
3. SAHTE E-POSTADAKİ BAĞLANTI İLE ULAŞILAN WEB SAYFASI KURUMUNUZUN SAYFASININ KOPYALANMIŞ HALİDİR.
4. SAYFA ÜZERİNDEN İNDİRİLMESİ İSTENEN YAZILIM ZARARLI KOD İÇERMEKTEDİR VE KULLANICILARIN KİŞİSEL BİLGİLERİNİ ÇALMAYI AMAÇLAMAKTADIR.
5. SAHTE SAYFA KAMANGA ÜLKESİNDEN YAYIN YAPMAKTADIR.

Katılımcı kurumların bu senaryoya karşı bünyelerinde bulunan ilgili birimlerle koordineli olarak tepki üretmesi ve bunun uluslararası bir olay olmasından dolayı TR-BOME ile iletişime geçmeleri beklenmiştir.

2.5 Tespitler

BOME 2008 Tatbikatı sonucunda elde edilen tespitler aşağıda açıklanmıştır.

Tespit 1: Haberleşme bilgilerinin güncelliği kriz anında hızlı tepkinin verilmesine olanak sağlar

BOME 2008 Tatbikatı esnasındaki tüm haberleşmenin imzalı ve şifreli olarak e-posta ile yapılması gerekmektedir. Bu hizmetler açık kaynak kodlu, ücretsiz bir yazılım olan ve açık anahtar şifrelemesi yapabilen GPG yazılımıyla sağlanmıştır. Tatbikat esnasında aşağıdaki aksaklıklar yaşanmıştır:

- Katılımcı kurumlardan bir kısmı imzalı-şifreli e-posta gönderememiştir, imzalı ve şifreli gönderilen e-postaları açamamıştır,
- Katılımcı kurumların bir kısmına ait e-posta sistemi şifreli ve imzalı dosyayı tanımadığı için engellemiştir.

Bu tür aksaklıkların tekrar yaşanmaması için kurumlar olay müdahale kapsamındaki haberleşmelerinde kullandıkları GPG yazılımı üzerindeki pratiklerini artırmalıdır. Ayrıca, haberleşmede kullanılan e-posta adresleri, bu adreslere ait açık anahtar bilgisi yılda en az bir kez olmak üzere güncellenmelidir.

Tespit 2: Güvenlik kayıtlarını tutan sistemlerin kullanılabilirliği olay müdahalenin etkin ve hızlı yapılmasını sağlar

BOME 2008 Tatbikatı'nda katılımcı kurumların yapılan saldırıları tespit etmede kullandıkları sistemlerin işlevselliğini test etmek amacıyla belirli IP adreslerinden port taraması gibi sisteme zarar vermeyecek ama kayıt oluşturacak saldırılarda bulunulmuştur. Bu saldırıların katılımcı kurumlar tarafından tespit edilmesi beklenmiştir. Bazı kurumların, saldırıların sistemler tarafından kayıt altına alınmasına rağmen raporlama ara yüzlerinden bu kayıtlara ilişkin rapor üretemedikleri gözlemlenmiştir. İlgili sistemde kayıtların sadece bir gün süreyle saklanmasının bu probleme sebep olduğu yapılan incelemede tespit edilmiştir.

Bu tür problemlerin tekrarını önlemek için;

- Güvenlik kayıtlarını tutan sistemlerin kayıtları eksiksiz tutması,

- Sistem üzerinde kayıt bilgisinin canlı olarak tutulması ve yedeklendikten sonra da saklanması için gerekli süreler, kullanılabilirlik göz önünde bulundurularak, kurum politikası içerisinde belirlenmelidir,
- Sistem yöneticileri tarafından belirli periyotlarla kayıt dosyalarının incelenmesi gerektiği tespit edilmiştir.

Tespit 3: Kurum dışıyla bağlantılı olaylarda TR-BOME ile iletişim olay müdahalenin önemli bir adımıdır

TR-BOME bilgisayarlar olayları için bir koordinasyon merkezi olarak hizmet vermektedir. TR-BOME'nin bu hizmeti etkin bir şekilde verebilmesi için irtibatta olduğu kurumlar ile kurulacak iletişim ve bilgi paylaşımı hayati öneme sahiptir. Bu kurum ve kuruluşlarla yapılacak olan bilgi paylaşımları hem bilgisayar güvenlik olayıyla karşı karşıya olan kurumun olaya daha etkin müdahalesini hem de ülke çapındaki olayların büyük resminin bir merkezde görülmesiyle diğer kurumların da önceden bilgilendirilmesini, muhtemel zararların önlenmesini ya da en aza indirilmesini mümkün kılmaktadır. Özellikle yurt dışı kaynaklı olaylarda TR-BOME daha hızlı çözüme ulaşmayı sağlayabilmektedir.

BOME 2008 tatbikatı süresince bazı katılımcı kurumların dış saldırganların oluşturdukları tehditler ve saldırılar karşısında verdikleri tepkilerde TR-BOME ile iletişime geçmedikleri tespit edilmiştir. Daha etkin olay müdahale için kurumların yaşadıkları güvenlik olayları hakkında TR-BOME'yi bilgilendirmeleri ve bu olayların kurum dışı saldırganlar tarafından gerçekleştirilmesi durumunda TR-BOME'nin olay müdahale koordinasyon desteği verebilmesi için de TR-BOME'ye ihbarda bulunmaları gerekmektedir.

Tespit 4: Kurum içi olay müdahalenin belirli politika ve prosedürlere göre yapılması devamlılığı ve izlenebilirliği sağlar

BOME 2008 Tatbikatı'nda, katılımcı kurumların tatbikat merkezine gönderdikleri olay tepki mesajlarında yaptıkları çalışmaların yazılı olarak belirlenmiş ve onaylanmış bir sürece göre yapılmadığı tespit edilmiştir. Olay müdahale kapsamındaki aktivitelerin onaylanmış yazılı bir sürece göre yapılması hem yapılan çalışmaların verimini ölçebilmeyi hem de bu çalışmaların kişilere bağlı olmadan kurumsal olarak yürütülebilmesini sağlamaktadır.

Kurumların olay müdahale esaslarını belirleyecekleri yazılı dokümanların üretilmesi ve bunların kurum içi ilgili makamlar tarafından onaylanması sağlanmalıdır.

Tespit 5: Olay anında kurum içi koordinasyonun sağlanabilmesi için kurum içi birimler arası iletişim geliştirilmelidir

BOME 2008 Tatbikatı'nın amaçlarından biri de kurumsal BOME süreçlerinin kontrol edilmesidir. Bu kapsamda uygulanan senaryolar ile katılımcı kurumun içinde bulunan Basın ve Halkla İlişkiler, Hukuk İşleri Birimi gibi birimlerle ortak çalışmalar yapmalarını sağlamak hedeflenmiştir.

Tatbikat sonrası yapılan toplantılarda, katılımcı kurumlar tarafından, kurum içi birimlerle koordinasyon sıkıntısı çekildiği, bilgi güvenliği olaylarına müdahalenin sadece bilgi işlem biriminin görevi olduğu gibi bir yanlış algılamanın olduğu belirtilmiştir.

Bu problemlerin çözümü için kurum içerisinde üst yönetim tarafından olay müdahale konusundaki roller ve sorumluluklar netleştirilmeli, birimler arası koordinasyonun ve iletişimin artırılmasına önem verilmelidir. Ayrıca olay müdahale konusunda kurum içi birimlere eğitim verilmeli, bilinçlendirilmeleri sağlanmalıdır.

3. TATBİKAT DEĞERLENDİRMESİ VE ÖNERİLER

BOME 2008 Tatbikatı değerlendirme toplantısında katılımcı kurumlar tatbikatın hedeflerine ulaştığını belirtmiştir. BOME 2008 tatbikatı, gerek kurum içi gerek kurum dışı olay müdahale süreçlerindeki eksikliklerin ortaya çıkartılması açısından çok faydalı bulunmuştur.

Yapılan değerlendirme toplantısında aşağıdaki tavsiye kararları alınmıştır:

- Bundan sonra yapılacak olan tatbikatın kurumların yıl içi çalışma planları da göz önünde bulundurulduğunda, 2010 yılının 2. çeyreğinde yapılması katılım ve kurum içi koordinasyon açısından daha uygun olacaktır.
- BOME 2008 Tatbikatı dağıtık yapıda icra edilmiş bir tatbikattır. Tatbikat süresince her kurum temsilcisi kendi kurumunda bulunmuş, tepki mesajlarını oluşturup e-posta ile göndermiştir. Yapılması planlanan sonraki tatbikatın merkezi ve dağıtık olarak iki aşamadan oluşması faydalı olacaktır. Yapılacak olan tatbikatın belli bir kısmının tek merkezde gerçekleştirilmesi, tüm kurum temsilcilerinin etkileşimde bulunabileceği bir ortamda yapılması, kalan kısmının ise BOME 2008 Tatbikatı'daki gibi dağıtık yapıda, tüm kurum temsilcilerinin kendi kurum binalarında bulunarak kurum içi birimlerle etkileşimle gerçekleştirilmesi yapılan çalışmanın verimini artıracaktır.
- 2010 yılında yapılması planlanan tatbikatta, katılımcı sayısı artırılmalıdır. Özel sektörde faaliyet gösteren anti virüs üreticisi, İnternet hizmet sağlayıcı,

yer sağlayıcı firmaların da tatbikata dahil edilmesi, koordinasyon yeteneğinin daha etkin test edilmesine olanak sağlayacaktır. Ayrıca, bu tatbikata kamu kurumlarında da çalışma alanları gözetilerek daha geniş katılım sağlanmalıdır

- Tatbikat öncesi yapılan hazırlık toplantılarına katılımcı kurumların sadece bilgi işlem biriminde çalışan personelin katılması kurum içi koordinasyonunun sağlanması noktasında eksiklik meydana getirdiğinden, yapılması planlanan tatbikat öncesi hazırlık ve planlama toplantılarına katılımcı kurumların ilgili tüm birimlerinden personel katılması sağlanmalıdır.