



Dünyada ve Türkiye'de Siber Güvenlik Tatbikatları

Ünal TATAR
Uzman Araştırmacı

Ankara, Haziran 2011

- Siber Güvenlik Tatbikatları
 - Amaçları
 - Türleri
- Dünyada Siber Güvenlik Tatbikatları
 - Dark Screen
 - CyberStorm
 - APCERT Drill
 - NATO CDX
- Türkiye’de Siber Güvenlik Tatbikatları
 - BOME 2008
 - USGT 2011



Bölüm 1:

Siber Güvenlik Tatbikatları

- Siber güvenlik tatbikatlarının amaçları;
 - bilgi sistemlerini hedef alabilecek saldırılara karşı hazırlıklı olmak,
 - saldırılara karşı kurum içi politikaları ve karar destek mekanizmalarını değerlendirmek,
 - kurumlar arası bilgi paylaşımını, haberleşmeyi ve koordinasyonu test etmek,
 - olası bir saldırıdan sonra geri kurtarma planlarını test etmek ve
 - tehditlere ve açıklıklara karşı farkındalık oluşturmak,
 - Personeli eğitmek olarak sıralanabilir.

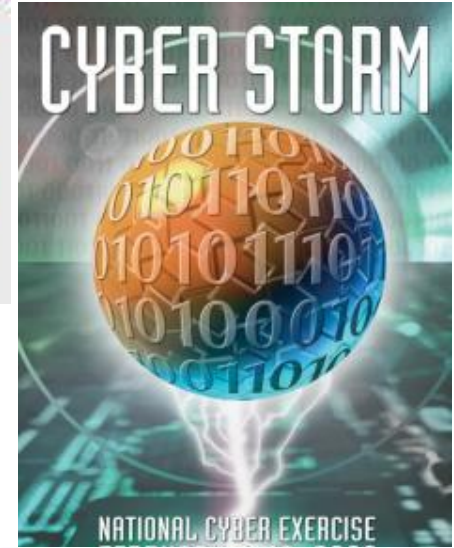
- Alt konu ~ Asıl konu
- Yazı tabanlı ~ Gerçek saldırı
- Merkezi ~ Dağıtık yapı
- Kurum içi ~ Kurumlar arası



Bölüm 2:

Dünyada Siber Güvenlik Tatbikatları

- **Dark Screen**
 - 2002 - 2003
- **Cyber Storm I – II - III**
 - 2006 – 2008 – 2010
- **APCERT Drill 2006-..-2011**
 - Ocak 2010
- **NATO Cyber Defense Exercise**
 - 2008 – 2009 – 2010



- 2002 yılında ABD'nin Texas eyaletinin San Antonio şehrinde gerçekleştirilmiştir.
- Şehirdeki kamu kurumları katılmıştır. Özellikle su, elektrik gibi kritik altyapılarla ilgili kurumların katılması önemlidir.
- Tatbikat üç aşamada gerçekleştirilmiştir.

- Merkezi olarak gerçekleştirilen ilk aşamada, tüm katılımcılar tek bir alanda toplanmışlar ve bir gün boyunca siber güvenlik hakkında bilgi almışlardır.
- İkinci aşamada ise birçok katılımcı kuruluşa sızma testleri gerçekleştirilmiş ve sistemlerdeki açıklıklar raporlanmaya çalışılmıştır.
- Son aşamada ise katılımcıların yaşanan olaya tepki verme yeteneklerini ölçmeyi amaçlamıştır. Bu aşamada, sahip olunan iletişim altyapıları (telefon hatları vb.) zarar gördüğünde kurumlar arası iletişimin nasıl sağlanacağı, kurumlar arası koordinasyonun gerçekleşeceği tespit edilmeye çalışılmıştır.

- Eylül 2010'da gerçekleştirilen CyberStorm III tatbikatında büyük ölçekli ve kritik altyapıları hedef alan siber saldırılar simülasyon ortamında denenmiştir.
- Tatbikata ABD'de bulunan 11 eyalet, 12 ülke (Avustralya, Kanada, Fransa, Almanya, Macaristan, Japonya, İtalya, Hollanda, Yeni Zelanda, İsveç, İsviçre ve İngiltere), 60 özel sektör kuruluşu katılmıştır.
- 3 gün boyunca 1500'ün üzerinde enjeksiyon uygulanmıştır.

- Asya Pasifik Bilgisayar Olayları Müdahale Ekibi (APCERT) tarafından organize edilen APCERT DRILL'in yedincisi 2011 yılında düzenlenmiştir.
- Tatbikatta 14 ülkeden 16 katılımcı yer almıştır ve tatbikat bir gün sürmüştür.
- Katılımcı ülkeler, Avustralya, Brunei, Çin, Tayvan, Hong Kong, Hindistan, Endonezya, Japonya, Kore, Malezya, Singapur, Sri Lanka, Tayland ve Vietnam'dır.
- Yapılan tatbikatın teması finans sektörüne yönelik saldırılar olarak belirlenmiştir.
- Tatbikat esnasında hem ülkelerin yaşanan olaylara tepki vermesi hem de kendi aralarında koordine olmaları sağlanmaya çalışılmıştır.

- “NATO Cyber Defence Exercise”, ilki 2008 yılında gerçekleştirilen, siber savunma amaç ve kapasitelerini hedef alan NATO tatbikatıdır.
- Tatbikatın amaçları:
 - Stratejik karar verme süreçlerini,
 - NATO ve ulusal siber savunma sorumluluklarını,
 - NATO ve üyesi ülkeler arasındaki siber savunmaya katılım yeteneklerinitespit etmek olarak belirtilmiştir.
- Tatbikat, Brüksel ve Mons'taki NATO NCIRC merkezlerinde ve katılımcı ülkelerin BOME merkezlerinde gerçekleştirilmiştir.

- Katılımcı NATO üyeleri: Fransa, Almanya, Yunanistan, İtalya, Litvanya, Norveç, İspanya, Türkiye, ABD'dir.
- Gözlemci NATO üyeleri ise Bulgaristan, Hırvatistan, Çek Cumhuriyeti, Danimarka, Estonya, Letonya, Hollanda, Polonya, Romanya, Slovakya, Slovenya ve İngiltere'dir.
- 2010 yılında düzenlenen tatbikatta ülkemizi Genelkurmay Başkanlığı ve TÜBİTAK UEKAE temsil etmiştir. 2011 yılında düzenlenecek olan tatbikatta ise ülkemizi Genelkurmay Başkanlığı ve TÜBİTAK UEKAE temsil edecektir.



Bölüm 3:

Türkiye'de Siber Güvenlik Tatbikatları

- Hedefler
 - Kurumsal BOME süreçlerinin kontrol edilmesi
 - TR-BOME işbirliği süreçlerinin kontrol edilmesi
 - Olay Müdahale sürecindeki eksikliklerin ortaya çıkartılması



- Cumhurbaşkanlığı



- Başbakanlık



- Adalet Bakanlığı



- Hazine Müsteşarlığı



- Sayıştay Başkanlığı



- Merkez Bankası



- Sermaye Piyasası Kurulu



- Tapu Kadastro Genel Müdürlüğü

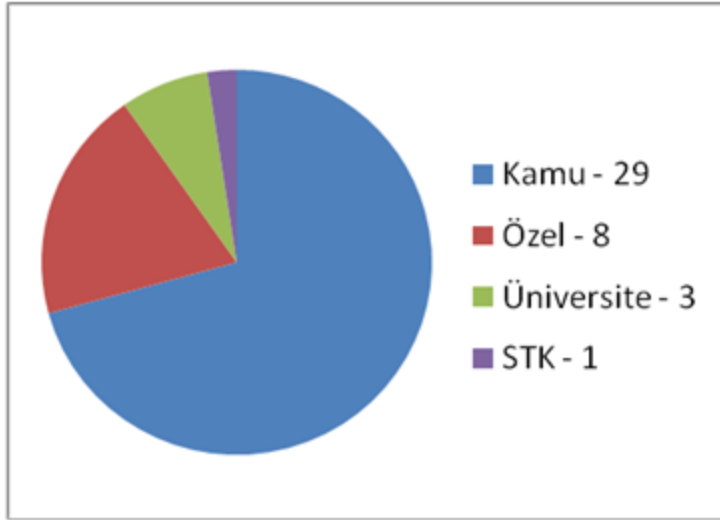
- Alt konu ~ **Asıl konu**
- **Yazı tabanlı** ~ **Gerçek saldırı**
- Merkezi ~ **Dağıtık yapı**
- Kurum içi ~ **Kurumlar arası**

- TÜBİTAK BİLGEM ve BTK koordinasyonunda 39 kurum/kuruluşun katılımıyla 25-28 Ocak 2011 tarihlerinde gerçekleştirilmiştir.
- Alt konu ~ **Asıl konu**
- **Yazı tabanlı** ~ **Gerçek saldırı**
- **Merkezi** ~ **Dağıtık yapı**
- Kurum içi ~ **Kurumlar arası**

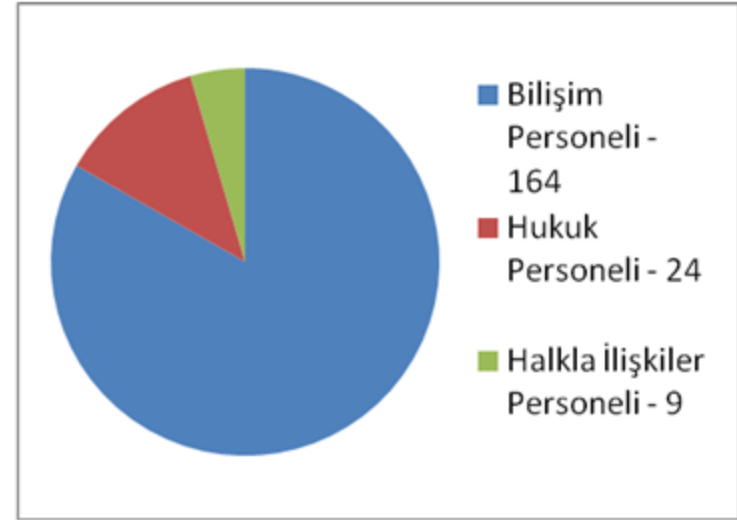


- USGT 2011 ile,
- Gün geçtikçe daha somut bir tehlike haline gelen siber tehditlere karşı hazırlıklı olunması,
- kurumların bilgi sistemi güvenliği olaylarına müdahale ve kurumlar arası koordinasyon yeteneklerinin tespit edilmesi,
- kurumlar arası iletişimin arttırılması,
- bilgi ve tecrübe paylaşımının ve
- ulusal siber güvenlik bilincinin arttırılması amaçlanmıştır.

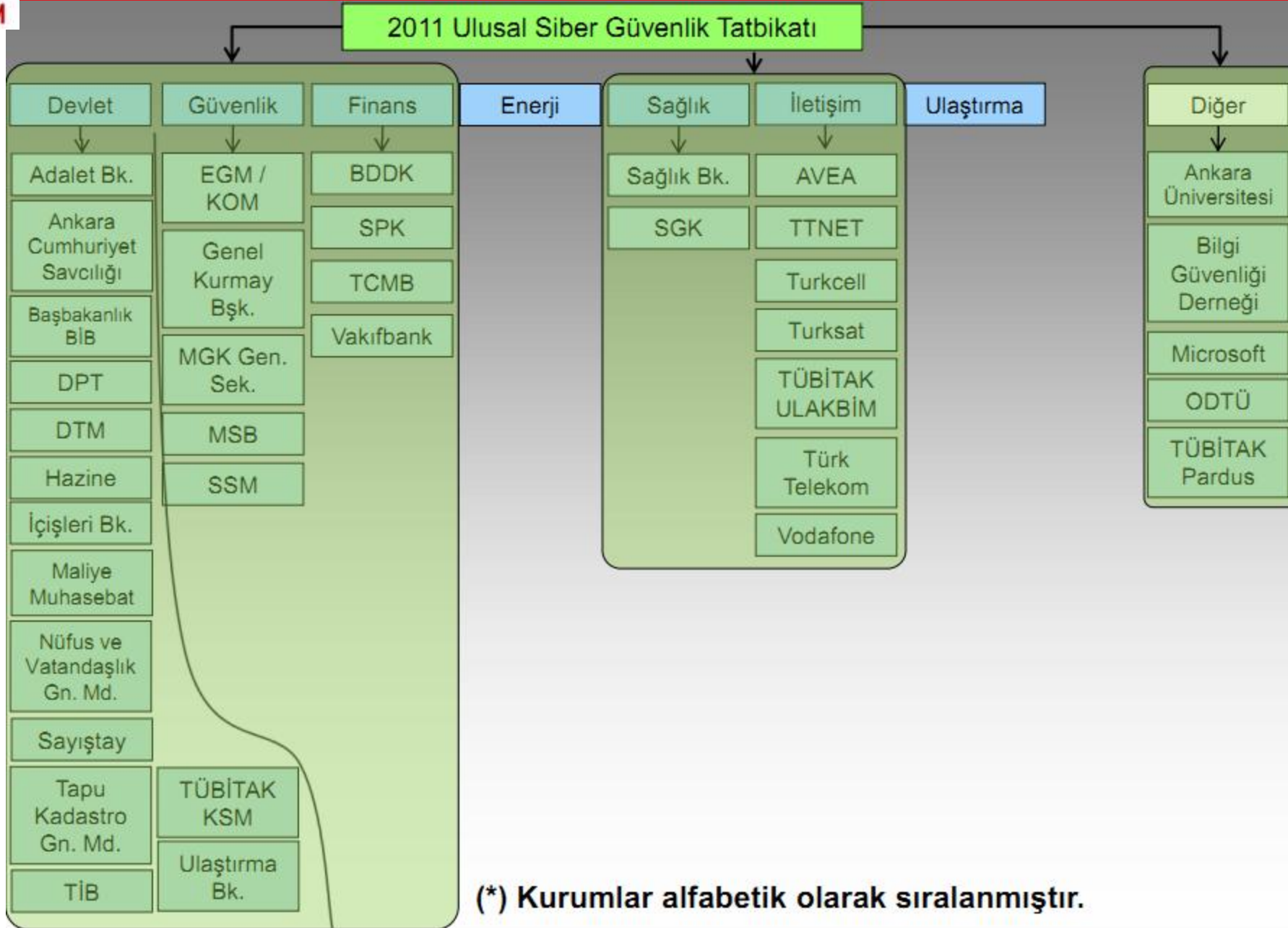
- TÜBİTAK BİLGEM ve BTK düzenleyici kurumlar olmak üzere 39 kurum ve kuruluşun katılımıyla gerçekleştirildi.



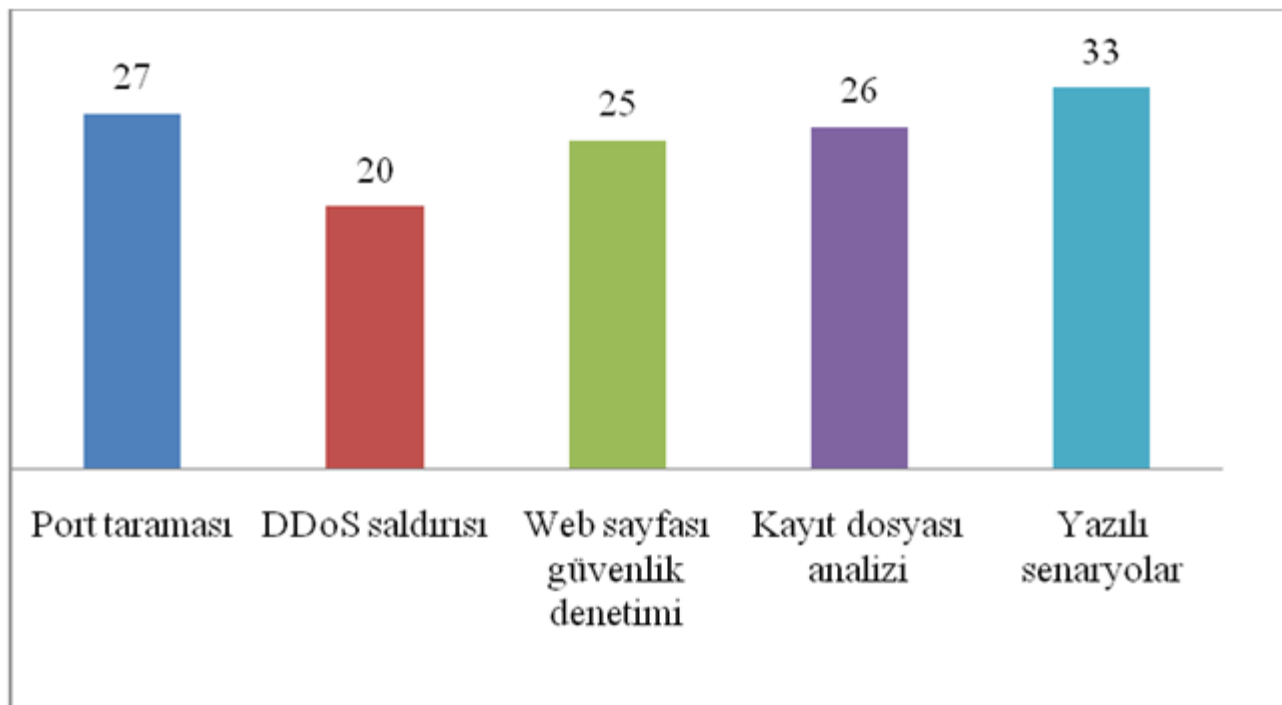
Sektör Bazında Katılımcı Kurum ve Kuruluşların Profili



Kurum Temsilcilerinin Uzmanlık Bazında Profili



- Tatbikatta yazılı enjeksiyonlar tüm kurumlara uygulandı.
- Gerçek saldırılar gönüllülük esasına göre uygulandı.



Gerçek Saldırı ve Yazılı Senaryoların Uygulandığı Kurum Sayısı

Yazılı Enjeksiyon Konuları

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 spam mesajlar 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 “spam” mesajlar 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

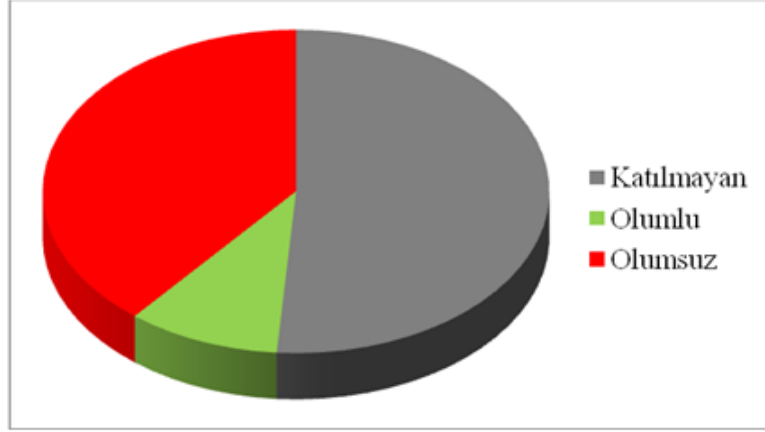
Kurumun Web Sayfasının İçeriğinin Yetkisiz Kişilerce Değiştirilmesi

ENJEKSİYON İÇERİĞİ

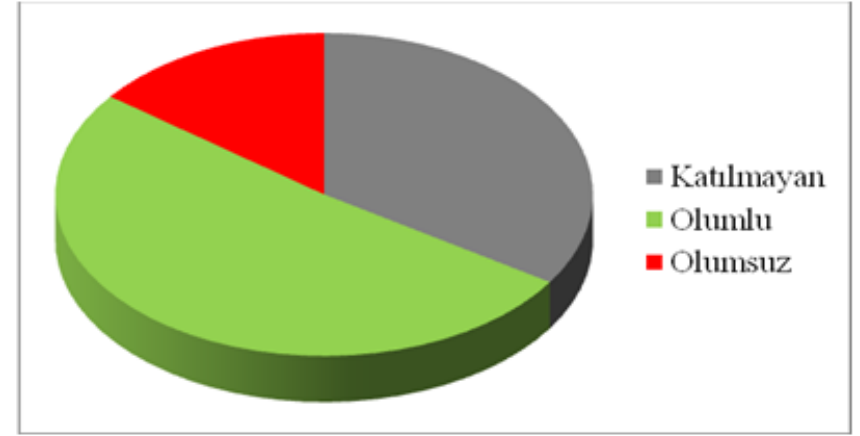
1. Kurumunuzun resmi web sayfasının içeriği yetkisiz kişilerce gerçekleştirilen saldırı sonrasında değiştirilmiştir.
2. Giriş sayfanıza saldırgan tarafından eklenen yazıda kurum çalışanlarınıza ve kurumunuzdan hizmet alan vatandaşlara ait bilgilerin ele geçirildiği ve yakında bu bilgilerin İnternet üzerinden yayımlanacağı görülmektedir.
3. 25 Ocak 2011 tarihinde saat 13.35'te bilgi işlem biriminizi arayan kurum içi bir kullanıcıyı sayesinde durumdan haberdar olunmuştur.
4. Kurumunuzun uğradığı saldırıyla ilgili ulusal basın yayın organlarında 25 Ocak 2011 tarihinde saat 15.23'te haberler çıkmaya başlamıştır.

TEPKİ MESAJINDA AŞAĞIDAKİ SORULARIN CEVAPLARI BULUNMALIDIR.

1. Bilgi işlem birimine kurum içi kullanıcı tarafından ihbar geldikten sonra olay nasıl doğrulanmıştır?
2. Sayfanın ele geçirildiği belirlendikten sonra yapılan teknik faaliyetler nelerdir?
 - a . Sistemin ne zaman ele geçirildiği nasıl tespit edilmiştir?
 - b. Sistemin nasıl ele geçirildiği tespit edilmeye çalışılmış mıdır? Neler yapılmıştır?
 - c. Veri sızması olup olmadığı nasıl tespit edilmiştir?
3. Sayfanın tekrar uygun içerikle erişilebilir olması nasıl, ne kadar sürede sağlanmıştır?
4. Diğer sistemlerin zarar görmesi nasıl önlenmiştir?
5. İlgili olayda **hukuki** olarak bir çalışma yapılmış mıdır?
 - a. Suç duyurusu ve ekleri hazırlanmalıdır.
6. **Basında çıkan haberler**den kurumun etkilenmemesi için ne yapılmıştır?

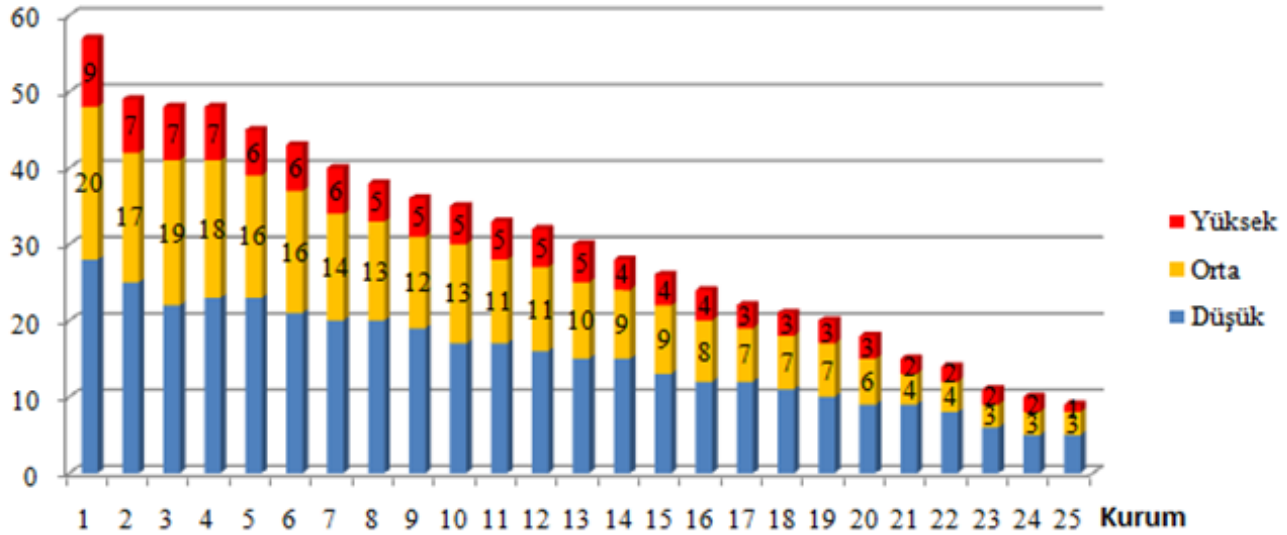


Dağıtık Servis Dışı Bırakma Saldırısının Sonuçları



Port Tarama Saldırısının Sonuçları

Açıklık Sayısı



Kurumlarda Tespit Edilen Web Açıklıklarının Sayıları

- Siber güvenlik konusunda durum tespiti, olası saldırılara karşı hazırlıklı olmak, iletişim kanallarını kontrol etmek ve farkındalık oluşturmak gibi amaçlarla düzenlenen siber güvenlik tatbikatlarına verilen önem artmaktadır.
- Gerek kurum içi gerekse kurumlar arası koordinasyon ve olay müdahale yeteneğine katkı sağlayacak olan siber güvenlik tatbikatlarının ülkemizde de 2008 ve 2011 yıllarında yapılmıştır.
- Siber güvenlik tatbikatlarının hem ulusal çapta devam etmesi hem de kurumsal ve sektörel çapta tatbikatların düzenlenmeye başlanmasının ülkemize fayda sağlayacağı değerlendirilmektedir.



TÜBİTAK-BİLGEM-UEKAE Bilişim Sistemleri Güvenliği Bölümü

tatar@uekae.tubitak.gov.tr

0 312 427 73 66

www.uekae.tubitak.gov.tr

www.bilgiguvenligi.gov.tr