CyberMag, Mayıs 2016

Söyleşi: Ahmet PEKEL, Türkiye Bilişim Derneği Yönetim Kurulu Üyesi

Son dönemdeki siber saldırılardaki artışı nasıl açıklayabiliriz?

Siber saldırı riski bugün her zamankinden daha yüksek.

Bunu daha iyi anlayabilmek için son yıllarda dünyadaki İnternet kullanım oranlarındaki artışa bakmakta fayda var.

Dünya nüfusu, 7,381,337,925 kişi.

İnternet kullanıcı sayısı, 2015 itibariyle 3,270,490,584.

2000 yılında bu sayı 360,985,492 imiş.

2000-2015 yılları arasındaki artış, %806.

Toplam nüfusumuz 79 milyon seviyelerinde.

Türkiye, 46,282,85 İnternet Kullanıcısı ile Avrupa Birliği'nde ilk 5 ülke arasında.

Dünya genelinde ise 16. sıradayız. (kaynak: Internetworldstats)

Ülkemizdeki genç nüfus, teknolojiye kolay uyum (adaptasyon) sağlıyor.

İnternet adı verilen teknolojinin altyapısı bilgisayarlar arasında bilginin çeşitli kurallara (iletişim protokollerine) göre paketler halinde iletilmesine (transfer edilmesine) dayanıyor.

Aslında İnternet, Amerika Birleşik Devletleri'nde, 1960 yılında başlayan ve ARPANET adı verilen araştırmaya dayalı olarak başlatılan bir çalışmanın sonucu.

1990' larda uluslararası düzeyde yaygınlaşması sonucu İnternet, bugün yaşamımızın önemli bir parçası haline geldi.

İnternet kullanım oranları arttıkça ve kullanım alanları genişledikçe siber saldırılarda da belirgin bir artış yaşanıyor.

İnternet kullanım oranlarındaki artışı neye bağlıyorsunuz?

Bu artışı öncelikle bilgi ve iletişim teknolojilerindeki hızlı gelişmelere bağlayabiliriz.

İşlemci hızı her iki yılda bir iki katına çıkıyor. Buna *Moore* yasası deniyor.

Bant genişliği hızla artıyor.

Teknoloji geliştikçe ucuzluyor, ucuzladıkça teknolojiye erişim kolaylaşıyor.

İnternet kullanan araçların satışlarında her yıl artışlar kaydediliyor.

2014'de Dünyada 53.2 milyon *tablet* satılmış. 2015'de bu sayı 57.1 milyon civarında. (kaynak: Worldmeters, Statista)

Diğer taraftan Türkiye'deki hareketli (mobil) telefon abone sayısı, BTK 2015 verilerine göre 73 milyon 235 bin 783 olmuş.

3G abone sayısı 63 milyon 66 bin 580'e ulaşmış.

Taşınabilir (mobil) bilgisayardan ve cepten İnternete erişen abone sayısı bir önceki çeyreğe göre yüzde 6,3 artarak 37 milyon 538 bin 898'e ulaşmış.

2017'de küresel düzeyde İnternete bağlı cihaz sayısının toplam dünya nüfusunun 3 katı olması bekleniyor.

Bu sayıyı akademik, kamusal ve ticari ağlar, kişisel bilgisayarlar, akıllı telefonlar, ev aletleri, kol saatleri, arabalar, elektrik, su ve gaz dağıtım şebekeleri, trafik sinyalizasyon sistemleri oluşturuyor.

Bu durum siber uzayın sürekli genişlediğini ve siber tehditlere maruz kalan cihaz sayısının daha da artacağını gösteriyor.

Küresel olarak İnternette 1 dk' da 1, 572, 877 GB veri transferi gerçekleşiyor. Hareketli aygıtlar üzerinden taşınan verinin (mobil trafiğinin) 2017'de, 2012'deki değerinin 13 katına erişmiş olacağı öngörülüyor.

İnternette 2013 itibarıyla veri büyüklüğünde 4 zettabytes'a ulaşılmış (Kaynak:Intel).

Nesnelerin İnterneti (Internet of Things), gezegenin merkezi sinir sistemini ve kolektif aklını oluşturan birbirine bağlı bilgisayarlar, akıllı telefonlar, giyilebilir teknolojiler, akıllı evler ve şehirlerden oluşan siber uzayın İnternet adres ihtiyacını karşılamak için bugüne kadar kullanmakta olduğumuz İnternet Protokolü IPV4 yetersiz kalmış durumda.

IPV4'de IP adres adeti en fazla 4 milyar olabiliyor.

Buna çözüm için geliştirilen IPV6'da ise adres adeti 340 x trilyon x trilyon x trilyon olacak.

Bu şekilde adres sayısındaki sıkıntı aşılmış olacak ve İnternete bağlanan aygıt (cihaz) sayısı daha da artacak.

İnternet bundan sonra hayatımızı nasıl şekillendirecek?

İnternet bize bankacılık, e-ticaret, e-devlet gibi pek çok işimizde hız, esneklik, zaman ve mekan bağımsız iletişim sağlıyor. İnternet birleştirici bir platform. Bir bilgi paylaşımı ortamı.

İnternetin iletişim gücü işbirliği kültürü yarattı. Açık bilgi ortamı olan Wikipedia bir sosyal üretim ve çevrimiçi dayanışma örneğidir. Bugün Ana Britanica'nın adı bile unutuldu.

İnternet ile birlikte bilimsel gelişme hızı artıyor.

Eğitim, sağlık, teknoloji alanlarında olduğu gibi, bir yerde bir soruna çözüm bulunduğunda pek çok kişinin sorununa çözüm bulunmuş oluyor.

Bugün bilgiye dayalı üretimden, bilgiye dayalı ekonomiden bahsediyoruz. İnternet sayesinde bilgi en değerli emtia haline geldi.

Önümüzdeki dönemlerde herkesin bilgiye dayalı birer tasarımcı ve aynı zamanda birer üretici konumuna geleceği öngörülüyor.

Açık bilgi ortamlarına talep artıyor.

İnsanlar açık bilgi ortamlarına neden bu kadar istekli?

Web yukarıdan aşağıya değil aşağıdan yukarıya bir iletişim yapısı sunuyor. En çekici tarafı bu sanırım. İnternet gönüllülük esasına dayalı üretimleri olanaklı kılan bir teknoloji. Açık kaynak kod (özgür yazılım, Linux) geliştirme topluluklarında, ağ toplumu da diyebiliriz, statü, kişinin yeteneğine, üretilen yazılım kodunun kalitesine, kişinin yaratıcılığına bağlı. Yaratılan ortam bir ölçüde adildir diyebiliriz. Adil sistemler aynı zamanda bir motivasyon aracı. Bu da üretkenliği teşvik ediyor.

21. YY'da başarıyı ağırlıklı olarak topluluk odaklı gelişmeyi benimseyenlerin yakalayabileceği öngörülüyor.

Kendi topluluklarını kendiliğinden oluşturan ürünler görmeye başladık. Bu topluluklar İnternet ortamında, ürünlerle ilgili geliştirme önerilerinde bulunuyorlar ve bir üründe yetersiz gördükleri

konuları, çözüm yöntemlerini önererek paylaşıyorlar, kullandıkları ürünlerin gelişmesine katkıda bulunuyorlar. Bu şekilde, ürün geliştirme toplulukları oluşuyor. Topluluklarını oluşturmuş olan ürünlerin daha hızlı tanındığını ve kullanıldığını gözlemliyoruz.

Firefox, Android bu şekilde geliştirilmiş ürünlere örnek verilebilir.

İleride belki açık donanımlardan da söz ediyor olabiliriz. Ev tasarımları, ev üretimleri gibi. Bu da üç boyutlu yazıcıların kullanımının yaygınlaşmasıyla ivme kazanabilir.

Bu şekildeki bir üretim biçimine, çocukların da katılabileceği öngörülüyor.

Çocuklar denilince oyun akla geliyor. Bilişim sayesinde öğretim de oyunsallaşıyor ve hatta kişiselleşiyor. Oyuna dayalı öğrenim şekli ileride daha çok benimsenecek, yaygınlaşacak. Bu gibi sistemlerle yaparak öğrenen, katılımcı, merak eden, belli hedefler için yarışan, üreten çocuklar çoğalacak.

Herkes için tek tip öğretimden kişiselleştirilmiş öğretime geçilmesi söz konusu olabilecek.

Geliştirilecek ürünler küresel pazara İnternet sayesinde daha kolay sunulabilecek (arz edilebilecek).

Uzmanlar üretim şekillerine göre sanayi devrimini dört bölümde ele alıyorlar.

Birinci dönem, üretimin su ve buhar gücüne dayalı olduğu dönem.

İkinci dönem üretimin elektrik enerjisine bağlı olduğu dönem.

Üçüncü dönem, üretimin elektronik cihazlara, bilişime bağlı olduğu dönem.

Şu an yaşanan ve dördüncü dönem ise Sanayi 4.0 olarak anılıyor. Akıllı cihazlarla üretim dönemi.

Sanayi 4.0, İnternet teknolojisini kullanan, birbirine bağlı cihazlarla gerçekleştirilen üretim biçimi.

Diğer taraftan, küresel ekonomide teknolojik bir ürünün nerede üretildiğinden çok nerede tasarlandığı ve geliştirildiği önemli.

Örneğin, ABD iphone'u %100 üretemiyor. Bununla birlikte satıştan elde edilen gelirin büyük kısmı cihazın üretildiği yer olan Çin'de değil Amerika'da kalıyor.

Ürün geliştirmenin ileride ucuz iş gücü maliyetine değil en iyi yenileşim (inovasyon) modeline bağlı olacağı öngörülüyor.

Önümüzdeki dönemlerde bilişim teknolojileri en iyi yenileşim modeline bağlı ekonomi yaratan bir sektör olarak daha da önem kazanacak.

İnternet yoluyla işlenen suçlarda artış var. Bunu nasıl açıklayabiliriz?

Ne yazık ki, İnternet teknolojilerinin kötüye kullanıldığı alanlar da var.

Dolandırıcılık, çocuk istismarı, kumar gibi pek çok geleneksel suçta İnternet bir araç olarak kullanılıyor.

Bu yönüyle İnternet yönetilmesi zor bir ortam.

Geçen süreç içinde siber suçlar da profesyonelleşti.

Geleneksel suçlar ve siber suçlar büyük oranda hizalandı.

Siber suçlar aynı zamanda küresel ekonomiyi de etkilemeye başladı.

22 Ocak 2016'da Dünya Ekonomik Forum'unda (World Economic Forum) siber suçlarla mücadele konusunda ortak görüş açıklandı.

Kamu ve özel sektör işbirliğinin altı çizildi.

Olası siber ataklar öncesinde, gerçekleşen olaylar sırasında veya saldırılar sonrasında ülkeler arasında gereksinim duyulan bilgi paylaşımının ve işbirliğinin önemi vurgulandı.

2014'de Türkiye'de alışveriş yoğunluklu olmak üzere e-ticaret kanalıyla harcanan tutar 18.9 milyar TL olmuş. 2013'den 2014'e artış, %35.

G20 ülkelerinin İnternet ekonomisinin 2016 yılında 4.2 trilyon ABD Doları seviyesinde olacağı tahmin ediliyor. (UDHB, 2015)

Sayısal ekonomi her geçen gün büyürken, siber suçların dünya ekonomisine yıllık maliyetinin 445 milyar ABD Dolar seviyelerinde olduğu değerlendiriliyor. (Intel Security, 2014)

Geçtiğimiz günlerde bir Türk siber korsan (Hacker) çevrimiçi bankacılık dolandırıcılığı suçundan 334 yıl hüküm giydi. 2013 yılında 11 arkadaşı ile pek çok bankanın internet bankacılık sistemlerini kopyalayarak müşterileri dolandırmış ve kredi kartı bilgilerini ele geçirmişti.

Suç şebekeleri ve terör örgütleri İnternet'i kendi amaçları doğrultusunda kullanabiliyor.

Diğer taraftan ülkeler siber savaşlar için siber ordular kuruyor.

Siber savaşları, bir ülkenin örneğin anlaşmazlık yaşadığı diğer bir ülkenin bilgisayar sistemlerine zarar vermek amacıyla yaptığı saldırılar olarak tanımlayabiliriz.

Siber savaş gerekçeleri, politik anlaşmazlıklar, siyasi bunalımlar, ekonomik yarış gibi öğelere bağlı olabiliyor.

Siber savaşlara karşı siber güvenliğin sağlanabilmesi için vatandaştan kurumlara kadar hepimizin sorumlulukları var.

2016 yılında Dünya Ekonomik Forumu, siber saldırıları 140 ekonomide, iş dünyasındaki en büyük tehlikelerden biri ilan etti.

Siber saldırı yöntemleri nelerdir?

- Zararlı yazılımlar,
- Hizmet dışı bırakma, (DDOS saldırıları şu anda en etkili teknolojik silahlardan biri),
- Siber casusluk,
- Sosyal mühendislik,
- Oltalama (Phishing),

- APT (Gelişmiş Kalıcı Tehditler),
- Mobil ve sosyal medya aracılığıyla yapılan saldırılar,
- Güvenlik zafiyetleri kullanılarak yapılan saldırılar

siber saldırılara örnek olarak verilebilir.

Siber saldırılarda kullanılan araçlar bakımından %25'le zararlı yazılımlar ilk sırada.

%23'le DDOS atakları ikinci sırada yer alıyor.

DDOS ataklarını %12 ile web tabanlı ataklar, %11'le oltalama saldırıları izlemekte. (Kaynak HP)

Bir siber savaşta neler tehdit altında?

Bir siber savaşta öncelikle,

- Savunma sistemleri,
- Telekomünikasyon sistemleri,
- Su ve enerji dağıtım şebekeleri,
- Ulaşım sistemleri,
- Finansal altyapılar,
- Sağlık sistemleri,
- Kamu kurumları,
- ve vatandaş

tehdit altında.

Son dönem itibarıyla en çok bilgi teknolojileri ve bulut servislerine yönelik olarak DDOS saldırıları yapılmış (%33).

Finansal altyapılara yönelik olarak yapılan saldırılar %22'lik bir oranla ikinci sırada.

Bunu %20'lik bir oranla web içerik sitelerine yapılan saldırılar takip etmekte.

Telekom sektörüne yönelik saldırılar %11'lik, kamu sektörüne yapılan saldırılar %9'luk ve imalat sektörüne yönelik saldırılar %5'lik paya sahip. (Kaynak: Verisign)

DDOS saldırılarının kurum ve kuruluşlara verdiği zararlardan bahsedebilir misiniz?

DDOS saldırıları nedeniyle işletmeler ticaret yapma imkanlarını yitirebiliyor, itibar kaybına uğrayabiliyor, güvenilirliliklerini kaybedebiliyor, iş olanaklarını kaçırabiliyor, önemli bilgilerine ihtiyaç duydukları anda ulaşamayabiliyorlar.

Saldırılar işletmelerin bilişim altyapı maliyetlerini artırıyor, bilgi güvenliği uzmanlarına, risk yönetimi danışmanlarına, hukukçulara, bağımsız denetçilere, hatta imaj danışmanlarına daha fazla ihtiyaç duyuluyor. Her bir saldırının büyük ölçekli kurumlara olan maliyetinin maddi anlamda 444,000 ABD Dolar seviyelerine kadar çıktığı tahmin ediliyor (Kaynak: Karspersky).

Diğer taraftan DDOS için kullanılan araçlar İnternette kolaylıkla bulunabiliyor ve bir saldırı başlatmak için yeterli olabiliyor.

DDOS saldırılarını;

- Bant genişliğini doldurma amaçlı hacimsel (volumetric) ataklar,
- Web sunucularını çalışamaz hale getirmek için uygulama düzeyindeki ataklar (Layer 7),
- Kurum bilgisayarlarını gelen isteklere karşı cevap veremez duruma getiren ataklar (İnternet Protokol Atakları)

olarak sınıflandırabiliriz.

Bu saldırılar başlatılması kolay ve ucuz, savunması zor ve pahalı saldırılar.

DDOS aslında TCK 244'e göre bir suç olarak da tanımlanmış durumda. Bilişim sistemini engelleme, bozma, verileri yok etme veya değiştirme, kanunlarımıza göre suç.

DDOS yöntemi hedef sistemin (sunucu, iletişim ağı) kaynaklarını ya da bant genişliğini sahte trafikle doldurmak için kullanılıyor.

Birden fazla kaynaktan atak yapılması DDOS'un engellenmesini zorlaştırıyor. DDOS yapacak yazılım parçacığının bir bilgisayarda kurulu olması kişinin rızasına bağlı olabileceği gibi (hacktivist - siber eylemci gruplar organize olarak kullanabiliyorlar) kişinin isteği dışında dışarıdan bilgisayarına yüklenmiş olması da olası (köle bilgisayar).

DDOS saldırılarına karşı ne gibi tedbirler alınabilir?

Öncelikle iletişim ağı seviyesinde mevcut durum analizi, devamında düzenli testler yapılmalı.

- Atak öncesinde iletişim politikaları belirlenmiş olmalı.
- İnternet yoluyla gelen trafiğin zararlı trafikten arındırılması, sadece temiz trafiğin kurum sistemlerine yönlendirilmesi yoluna gidilmeli.
- İçerik çoklu sunuculara dağıtılabilir.
- Şüpheli adresler için IP adres ayrıştırma, adres engelleme (bloklama) yapılmalı.
- Web sitesi sadeleştirilmeli. Büyük hacimli veriler bant genişliğinde sorun yaratabilir.
- Uygulamalara yönelik saldırılar için saldırı zamanında bazı uygulama işlevlerinin kapatılması düşünülebilir.
- Atak sonrası zarar ve kayıplar değerlendirilmeli, iyileştirmeler yapılmalı, gereken önlemler alınmalı.

Saldırı hacmi 2013 yılında 140 Gbps iken son dönemde saldırı hacminin 500 Gbps'a kadar çıktığına dair raporlar var (ARBOR Networks).

Burada;

- Tepki verme yeteneği ve hızı önemli,
- Paydaşlar arasında hızlı bilgi akışının sağlanması önemli,
- Yetkin bilgi güvenliği uzmanlığı gerekli,

- Sistemlerin üretmiş olduğu uyarı mesajlarının takibi, bunların birbiriyle ilişkilendirilmesi, sorunların erken farkına varabilmek için önemli (SIEM: Security Information and Event Management),
- Web hizmetlerinde sadece kritik servislere izin verilmeli, kullanılmayan servisler kapatılmalı,
- Kurumun İnternete açık ağında güncel teknolojiye sahip güvenlik cihazları konumlandırılmalı (FW, WAF, IPS cihazları gibi),
- İnternet hat kapasitesi verilen web hizmetlerini karşılayacak genişlikte olmalı,
- ISS'den DDOS korunma hizmeti alınmalı,
- ISS'in de yedeklenmesi değerlendirilmeli,
- ISS'in DDOS'dan korunma yöntemleri de önemli.

Aralık 2015'de ülkemize yönelik gerçekleştirilen siber saldırılar nasıl gerçekleşti? Bundan sonrası için neler yapılmalı?

14 ve 24 Aralık 2015 tarihlerinde ülkemize yönelik olarak gerçekleştirilen siber saldırıların arka planını daha iyi anlayabilmek için öncelikle belli tarihlerde yaşanmış olan olayları tekrar hatırlamakta fayda var.

Bilindiği üzere, 13 Kasım 2015 tarihinde Paris'de gerçekleştirilen ve IŞİD tarafından üstlenilen bir seri terör eylemi sonrasında Anonymous adıyla bilinen siber eylemci bir grup (haktivist: politik bilgisayar eylemcisi, siber muhalif) Türkiye'nin IŞİD'e destek verdiği iddiasıyla ülkemizde önemli altyapılara yönelik olarak siber saldırılar düzenleyeceğini ilan etti.

24 Kasım 2015 tarihinde Türkiye Suriye sınırı üzerinde uçan SU-24 tipi Rus savaş uçağı Türkiye sınırlarını ihlal ettiği için düşürüldü. Yaşanan olay Rusya ve Türkiye arasında siyasi gerginliğe neden oldu.

14 Aralık 2015 tarihinde tüm Türkiye'yi etkileyen ve ülkemizde alan adı kayıtlarının yapıldığı Nic.TR'yi hedef alan saldırılar yapıldı.

18 Aralık 2015 tarihinde Anonymous yayımladığı bir video kaydıyla saldırıları üstlendi ve bu saldırıların devam edeceğini duyurdu.

24 Aralık 2015 tarihinde ülkemizdeki büyük bankaları hedef alan siber saldırılar yapıldı, bu saldırılar bankacılık işlemlerinde gecikmelere yol açtı.

NIC.TR'yi ve bankaları hedef alan saldırıların organize ve hedefli DDOS (Distributed Denial of Service: Dağıtık Hizmet Durdurma) saldırıları olmaları ile kısa bir süre öncesinde yaşanan siyasi gerginlik nedeniyle bu saldırıların arkasında Rusya'nın da olduğu yönünde değerlendirmeler yapıldı.

DDOS saldırıları birden fazla noktadan aynı anda tek yöne başlatılabildiği için saldırının gerçek çıkış noktasını tespit etme konusunda açık bir bilgi elde edinilemedi. Böyle bir saldırıda Türkiye içinde daha önce ele geçirilmiş köle bilgisayarların da kullanılmış olması ihtimal dahilinde. Saldırıların yoğunlaştığı sıralarda Türkiye yurtdışı İnternet trafiğini keserek saldırının etkisini azaltmaya çalıştı.

Önceki saldırılara göre bu saldırıların belirli hedefleri gözetmesi ve organize yapısı dikkat çekti. Bu durum Rusya'nın Estonya, Gürcistan ve Ukrayna ile yaşadığı siyasi krizlerde de gözlemlenmişti.

Sonuçta saldırıları üstlenmiş olan Anonymous küresel bir grup olma özelliği taşımakta. Uçak krizinden sonra Anonymous'un eylemlerine Rus desteğinin de eklenmiş olması beklenebilecek bir durumdur.

Son yaşananlardan çıkarılacak en önemli ders öncelikle yetkili makamların bu ve benzeri olaylarda gecikmeksizin doğru bilgiyi kamuoyu ile paylaşmalarının en doğru yaklaşım olduğu gerçeğidir. Bilgilendirmenin zamanında ve doğru bir şekilde yapılması, ülkemize fayda getirmeyecek gereksiz tartışmaların önüne geçecektir.

Bilindiği üzere, siber saldırılara hedef olan ".tr" uzantılı alan adı sunucularının yönetimi 1991 yılından bu yana Orta Doğu Teknik Üniversitesi (ODTÜ) tarafından yapılmaktadır. Türkiye ilk kez bu tarihte İnternet'e bağlanmış ve ".tr" alan adı dağıtımı başlamıştır.

Nic.TR, ODTÜ küresel alan adı yönetiminden sorumlu İnternet Tahsisli Sayılar ve İsimler Kurumu (ICANN : The Internet Corporation for Assigned Names and Numbers)'nun bir üyesidir. ICANN kar amacı gütmeyen, üyelerinin uymaları gereken kural ve politikaların belirlendiği uluslararası bir kuruluştur.

Nic.TR, ODTÜ bugüne kadar tahsis ve yürütme sorumluluğu kapsamında çalışmalarını yürütmüştür. İnternet Kurulu 2000 yılında konuyla ilgili politika ve kural belirlemek amacıyla sektör temsilcilerinden oluşan DNS Çalışma Grubunu kurmuştur.

Daha sonra, 5 Kasım 2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu ile "İnternet alan adlarının tahsisini yapacak kurum veya kuruluşun tespiti ile alan adı yönetimine ilişkin usul ve esaslar Bakanlık tarafından belirlenir" hükmü uyarınca Bilgi Teknolojileri ve İletişim Kurumu (BTK) görevlendirilmek suretiyle 7 Kasım 2010 tarihinde 27752 sayılı Alan Adları Yönetmeliği Resmi Gazete'de yayımlanmıştır.

Yönetmelikte BTK'ya verilen görevler arasında "TRABİS (.tr ağ bilgi sistemi)'i kurmak ve işletmek veya belirlediği usul ve esaslar çerçevesinde TRABİS'in üçüncü bir tarafça kurulması ve işletilmesini sağlamak" hükmü de yer almıştır.

Alan adları sunucularının yönetiminin BTK'ya devredilmesi konusu halihazırda Nic.TR, ODTÜ ile davalık durumdadır.

Bu kapsamda, "tahsis ve yürütme" ile "konuyla ilgili politika belirleme ve denetleme" yetkisinin aynı organ üzerinde toplanmaması en uygun yaklaşım olacaktır.

Bilindiği gibi, DNS Yükseltme Saldırısı (DNS Amplification Attack) olarak gerçekleşen son saldırılarda ODTÜ'nün, yönetimindeki alan adı sunucularını BTK'ya devretmediği için İnternet erişiminde uzun süreli aksaklık yaşandığı iddia edilmişti. Siber saldırı sırasında 6 adet olan bu sunuculardan ikisinin ODTÜ'de, geri kalanların ise RIPE (Bulunduğumuz bölge için IP adres tahsisi ve alan adları yönetimi yapan kuruluş), ULAKBİM (Tübitak Ulusal Akademik Ağ ve Bilgi Merkezi), Vodafone A.Ş ve 3C1B Telekom'da konumlandırılmış olduğu, yurt dışında (RIPE) konumlanmış olan sunucunun da bu saldırılardan olumsuz etkilendiği yapılan resmi açıklamalar sonrasında anlaşılmıştır.

Ayrıca, 40 Gbps düzeylerine ulaşan saldırılar nedeniyle ULAKNET (Ulusal Akademik Ağ ve Bilgi Merkezi) erişiminde problemler yaşanmıştır.

Saldırı esnasında, saldırıların etkisini azaltmak amacıyla saldırıyı İnternet Servis Sağlayıcı (İSS) düzeyinde engelleme, telekom operatörleri seviyesinde yurtdışından yurtiçine gelen İnternet trafiğini

engelleme, DNS alan adı sunucu sayısını artırma, farklı yerleşkelerde konumlandırma da dahil bir dizi önlem alınmıştır.

Telekom operatörlerinde 200 Gbps seviyelerinin üzerine çıkan bir trafiğin gözlemlendiği saldırılarla ilgili olarak Nic.TR, ODTÜ tarafından 21 Aralık 2015 tarihinde yapılan basın duyurusunda saldırı sonrasında üçü yurtdışında olmak üzere toplam 11 adet alan adı yönetim sunucusunun farklı yerleşkelerde konumlandırılmış olduğu ifade edilmiştir.

DNS alan adı yönetim sunucularına yönelik ataklara karşı alınan önlemler sonrasında, 24 Aralık 2015 tarihinde, saldırılar bu kez Türkiye'deki büyük bankalara yöneltilmiştir. Bu saldırılar bankacılık işlemlerinde gecikmelere sebep olmuş, çevrim içi işlemler zamanında yapılamamış, POS cihazlarının çalışmadığı gözlemlenmiştir. Bu süreç içinde DDOS saldırılarının, doğası gereği tamamen önlenmesi mümkün olmasa da etkisini azaltmak amacıyla İSS düzeyinde alınan önlemler işletilmiştir. İSS düzeyinde alınan önlemlerin etkinliği ise nihayetinde İSS'in sahip olduğu altyapı, kapasitesi, kullanılan teknolojinin güncelliği ve hizmet verilen kuruluşların, İSS'in teknolojik altyapısındaki konumlandırılma biçimiyle ve elbette bu hizmeti alan kuruluşlardaki bilişim altyapılarının yeterliliği ile doğru orantılıdır.

Son dönemde yaşanan siber saldırılar ülke genelinde konuyla ilgili alınmış ve alınabilecek önlemleri bir kez daha gündeme getirmiştir.

Söz konusu önlemleri stratejik ve taktik önlemler olarak iki başlıkta ele alabiliriz.

Bilindiği gibi Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanan kararı gereğince Siber Güvenlik Kurulu oluşturulmuştur.

Siber Güvenlik Kurulu ilk toplantısını 21/12/2012 tarihinde yapmış, "Siber Güvenlik Kurulunun Görevleri, Çalışma Usul ve Esasları Yönergesi" ve "Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı" kabul edilmiştir.

Siber Güvenlik Kurulu ikinci toplantısını 20/06/2013 tarihinde yapmış, bu toplantıda Ulusal Siber Olaylara Müdahale Merkezi'nin (USOM) kurulduğu ve 15 Mayıs 2013 tarihi itibarıyla USOM'un faaliyet göstermeye başladığı bildirilmiştir.

Siber Güvenlik Kurulu üçüncü toplantısını 19/12/2013 tarihinde yapmıştır.

Kurul 10/02/2016 tarihinde dördüncü toplantısını yapmıştır.

2013-2014 yıllarını kapsayacak şekilde 20 Haziran 2013 tarihinde Bakanlar Kurulu Kararı ile yayımlanan ilk Ulusal Siber Güvenlik Strateji belgesinde yer alan hedeflerle ilgili olarak geçen süreçte UDHB koordinasyonunda bir dizi toplantılarla gelinen aşamalar ele alınmış, yapılan değerlendirmeler sonrasında Haziran 2015'de, 2015-2017 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ilgili paydaşların görüşleri de alınarak hazır hale getirilmiştir. 21 Mart 2016 tarihinde onaylı 2016-2019 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı'nın duyurusu yapılmıştır.

Stratejik önlemler başlığı altında ele alınabilecek yukarıdaki mevzuat ve düzenlemeler kapsamında hedeflenen eylemlerin takibi büyük önem arz etmektedir. Yukarıdaki bilgilerden anlaşılacağı üzere, siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik kararları almak Siber Güvenlik Kurulu'nun görevleri arasındadır.

Gelinen aşama itibariyle Siber Güvenlik Kurulu'nun çalışmalarına işlerlik ve etkinlik kazandırılmalıdır.

Diğer taraftan, 2015-2018 Bilgi Toplumu Stratejisi ve Eylem Planının sekiz ana ekseninden birisi "Bilgi Güvenliği ve Kullanıcı Güveni"dir. Bu eksen dahilinde hedeflenen,

- Ulusal Bilgi Güvenliği Kanununun Çıkarılması,
- Kişisel Verilerin Korunması Mevzuatının Çıkarılması,
- Siber Suçla Mücadele Stratejisi ve Eylem Planının Oluşturulması,
- Güvenli İnternet Kullanımında Farkındalığın Artırılması,
- Bilişim Suçları İhtisas Mahkemelerinin Kurulması

yönündeki çalışmalarla Ulusal Siber Güvenlik Stratejisi ve Eylem Planında hedeflenen çalışmaların uyumlulaştırılması gerekmektedir.

İlaveten, siber güvenliğe ilişkin olarak yapılacak çalışmaların uluslararası bilgi alışverişini ve işbirliğini gerektirmesi sebebiyle Ülkemizin uluslararası sözleşmeler çerçevesinde uyum çalışmalarını yapmış, ilgili mevzuatlarını tamamlamış olması önemlidir.

Bunlardan ilki Avrupa Siber Suçlar Sözleşmesidir. İlgili Sözleşme Türkiye tarafından 10 Kasım 2010 tarihinde imzalanmış, Sözleşmenin yasalaşması için Sanal Ortamda İşlenen Suçlar Sözleşmesinin Onaylanmasının Uygun Bulunduğuna Dair Kanun Tasarısı ve Dışişleri Komisyonu Raporu 3 Eylül 2012'de TBMM Başkanlığına gönderilmiş ancak henüz yasalaşmamıştır.

Türkiye'nin uluslararası sözleşmeler çerçevesinde uyum çalışmalarını tamamlaması gereken bir diğer konu kişisel verilerin korunmasına ilişkindir. Bakanlar Kurulu'nun imzaladığı tasarı 24 Mart 2016'da TBMM'nde yasalaşmıştır.

Ulusal Siber Güvenlik Stratejisi kapsamında bilgi güvenliği konusunda uzman yetiştirilmesi konusuyla bağlantılı olarak ise bu konuda çalışacak personelin yetiştirilmesi için YÖK tarafından Üniversitelerin Bilgisayar Mühendisliği müfredatlarına bilgi güvenliği yönetimi, güvenli yazılım geliştirme ve adli bilişime ilişkin eğitimlerinin konulması, bunun master ve doktora programlarıyla desteklenmesi önemlidir.

Ülkemizde bilgi güvenliği farkındalığını vatandaş düzeyinden başlatma zorunluluğu bulunmaktadır. Bunun için vatandaşa yönelik bilgi güvenliği eğitim ve farkındalık programların işler hale getirilmesi gerekmektedir.

Bundan sonra tekrarlanması muhtemel bu tip saldırılar için taktik boyutta alınabilecek önlemleri şu şekilde özetleyebiliriz:

Kritik kurum ve kuruluşlar bilişim altyapılarında ağ güvenlik cihazları konumlandırmalı, şüpheli ağ paketlerini engellemeli, gereksiz İnternet hizmetlerini kapatmalı, yaptıracakları DDOS testleri ile hizmet aldıkları İSS'lerin yetkinliklerinden, güvenlik aygıtlarının kapasitelerinin muhtemel bir DDOS saldırısının etkisini azaltmak için uygun seviyelerde olduğundan emin olmalıdırlar.

Dünya genelinde gerçekleşen saldırılarda saldırı hacminin en son olarak 300 Gbps'lardan Ocak 2016 itibariyle 500 Gbps sınırlarına ulaştığı ölçümlenmiştir. Birinci öncelikli konu İSS'lerin yapay olarak oluşturulabilmekte olan bu yoğunluktaki trafiği karşılayabilecek altyapı yatırımlarını yapmalarıdır. Diğer taraftan bu hacimdeki bir saldırıyı karşılayabilmek için son dönemde dünyada trafiği üzerine alabilen bulutta verilen hizmetler de kullanılmaya başlanmıştır. Bu hizmetler dünyada farklı yerleşkelerde yer alan veri merkezleri üzerinden verilmektedir.

DDOS saldırıların kritik kurumlara ulaşmadan İSS'ler tarafından karşılanması ve etkisinin azaltılması doğru ve önemli bir başlangıçtır. Bu nedenle İSS'lerin bant genişliği bazında güçlendirilmesi yanında

İSS'ler düzeyinde konumlandırılan DDOS saldırı önleme cihazlarının kapasiteleri ve yetenekleri son saldırıların boyutları ve çeşitliliği de dikkate alınarak İSS'lerce yeniden değerlendirilmelidir.

DDOS hizmeti alan kurumların İSS'lerdeki DDOS saldırı önleme cihazlarındaki dağılımları gerekmesi durumunda yeniden düzenlenmelidir.

Kritik kurumlar, birden fazla İSS'den İnternet hizmeti alınmasını, İnternet hat kapasitelerini muhtemel bir DDOS saldırısının etkisinin azaltılması amacıyla uygun seviyelere çıkarma konusunu değerlendirmelidirler.

Ülke genelini etkileyen bu tür siber saldırılarda Ulusal Siber Olaylara Müdahale Merkezi (USOM) ile kurumlardaki Siber Olaylara Müdahale Ekipleri (SOME) arasında daha etkin eşgüdüm sağlanmalıdır.

Geçtiğimiz yıl yaşanan elektrik kesintisi bir siber saldırının sonucu muydu?

31 Mart 2015'de saat 10:36'da bütünleşik elektrik dağıtım sisteminde büyük bir yük değişikliği oldu ve büyük illerimizde elektrik kesintileri meydana geldi.

İlk uyarılar 30 Mart 2015'de İzmir'deki iki santralin devre dışı kalmasıyla gelmeye başlandı.

Petkim olağandışılığı görüp sistemlerini devre dışı bıraktı.

31'inde yaşanan daha büyük yük değişikliği sonrasında Petkim üretimi durdurdu.

Yetkili makamlarca kesintinin bir iletim hattındaki arızadan kaynaklandığı, doğudan batıya gelen yükte artış olduğu, 5 iletim hattının devre dışı kaldığı, doğu ile batının arasındaki bağlantının koptuğu açıklandı.

Sorunun siber saldırı olup olmadığı yönünde kesin bir bulgu yok.

Ancak yük dengesindeki değişimlerin etkilerinin sorun öncesinde iyi çözümlenmiş olması, önlem alınması önemli.

Yaşanan sorunun iletim hatlarındaki arızaların yönetilmesiyle ilgili bir sorun olma olasılığı yüksek.

Bir iletim hattı arızalandığında ya da bakıma alındığında yerine yedeği devreye alınabilmeli.

O tarihte bu süreçlerin yönetiminde aksaklıklar yaşanmış olmalı.

Bir siber saldırı halinde meydana gelecek yük değişikliğinin benzer bir etki yaratabileceğini söyleyebiliriz.

Dünyada benzer elektrik kesintilerine örnek olarak ABD'de 2003'de yaşanan 36 saatlik elektrik kesintisini verebiliriz.

Yüksek ve düşük yük dengesi bütünleşik çalışan bir elektrik dağıtım sistemi için önemli, iyi takip edilmeli.

Bu tip arızalara karşı hazırlık yeteneklerimizi yükseltmemiz gerekiyor.

Siber güvenlikte teknik tedbirleri destekleyecek diğer etkenler nelerdir?

Pek çok etken var. Şöyle özetleyebiliriz:

- Bütçe: Siber ataklar gerçekleştirilmesi kolay ve ucuz, savunması zor ve pahalıdır. Siber güvenliğe yeterli bütçe ayrılabilmelidir.
- Eğitim: İlk ve orta öğretimden başlayarak anne ve babaları da kapsayacak şekilde İnternet ve sosyal medya kullanımında dikkat edilecek hususlarda farkındalık oluşturulmalıdır.

- Danışmanlık: Mevcut durumu görebilmek ve nereden başlamak gerektiği sorusuna cevap verebilmek için değerlendirilebilir.
- Risk Yönetimi: Risk azaltma, ortadan kaldırma, riski aktarma (transfer etme) konuları değerlendirilmelidir.
- Sigortalama: Siber güvenlik risklerinin aktarılması (transfer edilmesi) için değerlendirilebilir.
- Mevzuat: Kurallara, yaptırımlara (müeyyidelere), uluslararası benimsenmiş kurallara (normlara) uyum gözetilmelidir.
- Kurumlararası işbirliği: Sorunların hızlı çözümü için bilgi paylaşımı ve işbirliği yapılmalıdır.
- Uluslararası işbirliği: İnternet ortamında sınırların olmadığı dikkate alındığında yukarıda ifade edilen işbirliği ülkeler açısından da geçerlidir.
- Kritik altyapılar: Ülke düzeyinde kritik altyapı bileşenleri açısından risk önceliklendirme yapılmalı, koruma önlemleri alınmalı ve düzenli sınama çalışması yapılmalıdır.
- Strateji ve politikalar: Taktik önlemlerin stratejik hedefler konulmadan başarıya ulaşması zordur. Alınacak tedbirler strateji ve politikalarla desteklenmelidir.

Siber güvenlikle ilgili strateji ve politikalar nasıl oluşturulmalı? Türkiye'de siber güvenlikten kim sorumlu? Bugüne kadar bu konuda neler yapıldı?

Bakanlar Kurulunca alınan 11/6/2012 tarihli ve 2012/3842 sayılı Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin 20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanan kararı gereğince, ülkemizde Siber Güvenlik Kurulu oluşturulmuş, Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na siber güvenlik alanında görev ve yetkiler verilmiş, siber güvenlik ile ilgili çalışma grupları ve geçici kurulların oluşturulabileceği hususları karara bağlanmıştır.

20/10/2012 tarihli ve 28447 sayılı Resmi Gazetede yayımlanan kararın içeriği, 06/02/2014 tarihinde yayımlanan 6518 saylı kanun ile 5/11/2008 tarihli ve 5809 sayılı Elektronik Haberleşme Kanunu'na ilave edilen Ek Madde 1 ile yeniden düzenlenmiştir.

İlgili maddede, "Siber güvenlikle ilgili olarak kamu kurum ve kuruluşları ile gerçek ve tüzel kişiler tarafından alınacak önlemleri belirlemek, hazırlanan plan, program, rapor, usul, esas ve standartları onaylamak ve bunların uygulanmasını ve koordinasyonunu sağlamak amacıyla; Bakanın başkanlığında Siber Güvenlik Kurulu kurulmuştur. Siber Güvenlik Kurulunda yer alacak bakanlık ve kamu kurum ve kuruluşları ile üyelerinin temsil düzeyi Bakanlar Kurulu tarafından belirlenir" denilmektedir.

Kurulun görevleri aşağıdaki şekilde belirlenmiştir:

- Siber güvenlik ile ilgili politika, strateji ve eylem planlarını onaylamak ve ülke çapında etkin şekilde uygulanmasına yönelik gerekli kararları almak,
- Kritik altyapıların belirlenmesine ilişkin teklifleri karara bağlamak,
- Siber güvenlikle ilgili hükümlerin tamamından veya bir kısmından istisna tutulacak kurum ve kuruluşları belirlemek,
- Kanunlarla verilen diğer görevleri yapmak.

Siber Güvenlik Kurulu Ulaştırma, Denizcilik ve Haberleşme Bakanı'nın başkanlığında,

- Dışişleri Bakanlığı Müsteşarı,
- İçişleri Bakanlığı Müsteşarı,
- Milli Savunma Bakanlığı Müsteşarı,
- Ulaştırma, Denizcilik ve Haberleşme Bakanlığı Müsteşarı,
- Kamu Düzeni ve Güvenliği Müsteşarı,
- Milli İstihbarat Teşkilatı Müsteşarı,
- Genelkurmay Başkanlığı Muhabere Elektronik ve Bilgi Sistemleri Başkanı,
- Bilgi Teknolojileri ve İletişim Kurumu Başkanı,
- Türkiye Bilimsel ve Teknolojik Araştırma Kurumu Başkanı,
- Mali Suçları Araştırma Kurulu Başkanı,
- Telekomünikasyon İletişim Başkanı

ile Ulaştırma, Denizcilik ve Haberleşme Bakanınca belirlenecek bakanlık ve kamu kurumlarının üst düzey yöneticilerinden oluşmuştur.

Ülkemizde siber güvenliğe ilişkin yapılan bu çalışmaların öncesine bakacak olursak, 2006 yılında Bilgi Toplumu Stratejisi ve Eylem Planı'nın 88 nolu eylemi TR-BOME (Türkiye Bilgisayar Olaylarına Müdahale Ekibi)'nin kurulması olarak belirlendi. TR-BOME 2008 yılında kuruldu.

İlk siber güvenlik tatbikatı 2008 yılında 8 kurumla birlikte yapıldı, Tübitak-Bilgem bu tatbikatın koordinasyonunu sağladı.

Siber Tehditlerin 2010 Ekim'inde Milli Güvenlik Kurulu Siyaset Belgesine girdiği basına yansıdı.

25-28 Ocak 2011 tarihlerinde 1. Ulusal Siber Güvenlik Tatbikatı Tübitak-Bilgem ve BTK koordinasyonunda yapıldı. Tatbikata 44 kurum katıldı.

10-11 Ocak 2013 tarihlerinde BTK koordinasyonunda 2. Ulusal Siber Güvenlik Tatbikatı yapıldı.

Uluslararası Telekomünikasyon Birliği (ITU), Bilgi Teknolojileri ve İletişim Kurumu (BTK) ile ITU-IMPACT işbirliğiyle düzenlenen "Uluslararası Siber Kalkan Tatbikatı 2014", 15-16 Mayıs 2014 tarihlerinde 20 ülkenin katılımıyla İstanbul'da gerçekleştirildi.

Siber saldırıların mağduru ya da bu saldırılara istemeden alet olmamak için vatandaşlarımızın alabileceği önlemler nelerdir?

Siber güvenlik, toplumun tüm kesimlerini ilgilendiriyor. Bugün akıllı telefon kullanan herkes siber tehditlerin birer muhatabı durumunda.

Vatandaşlarımız şunlara dikkat etmeli;

- Lisanslı yazılımlar kullanılmalıdır.
- Kişisel güvenlik paketi kullanılmalıdır.
- Yazılım güncellemeleri düzenli olarak yapılmalıdır.
- Sorun tespit ve güvenlik çözümlemeleri için bilgisayarlarda sistem ve güvenlik kayıtlarının alındığından emin olmalıyız.
- Bilgisayarlarda ilk kuruluşla birlikte gelen yetkili kullanıcı isimleri değiştirilmelidir (administrator, admin gibi).
- İyi bir parola seçilmelidir. Kolay hatırlanabilecek zor tahmin edilebilecek bir parola kullanılmalıdır (en çok kullanılan ve kolay tahmin edilenler: 123456, password, qwerty v.b.).
- Tüm hesaplara aynı parolanın verilmesi alışkanlığından vazgeçilmelidir (kurumsal hesaplar, sosyal medya hesapları, banka hesapları, kişisel üyelikler, e-ticaret siteleri için farklı parolalar tanımlanmalıdır).
- Parolalar kimseyle paylaşılmamalıdır.
- Açılan oturumlarda "beni hatırla" seçeneği kullanılmamalıdır.
- Belli aralıklarla parolalar değiştirilmelidir.
- Kullanılmayan hesaplar kapatılmalıdır.
- Fidye saldırılarına bir önlem olarak, önemli görülen dosyalar (kaybından zarar göreceğimizi düşündüğümüz) düzenli olarak yedeklenmelidir.
- Kurumsal bilgisayarlarda Yerel Yönetici (Local Administrator) yetkileri ile çalışılmamalıdır.
- Kullanmadığımız zamanlarda cihazlarımızın ekranları kilitli tutulmalıdır.
- E-posta, SMS, Twitter, Facebook mesajı ile aldığımız iletilerin kaynağının güvenilir olduğundan emin olunmalıdır.
- Telefonla arayan, kendilerini banka görevlisi veya teknik destek elemanı olarak tanıtan, "kazandınız, hediyenizi alabilmek için şu hesaba para yatırın" diyen veya banka parolalarınızı isteyen kişilere inanılmamalıdır. Öncelikle gerçek kişiler olup olmadığı konusunda kesin bilgi edinilmelidir. Bu anlamda sosyal mühendislik saldırılarına karşı farkındalık artırılmalıdır.
- Dizüstü bilgisayar, tablet, harici bellek ve akıllı telefonların fiziksel güvenliği konusunda gereken önem gösterilmeli, bu aygıtlarda unutulma veya çalınma risklerine karşı disk şifreleme yapılmalı, cihaz açılışları güçlü parola ve biyometrik araçlarla yapılmalıdır.
- Virüs ya da zararlı yazılım riski nedeniyle CD'ler, USB bağlantılı cihazlar paylaşılmamalıdır.
- İleti ile gelen bağlantılara tıklanmamalı, adres kısmı kopyalanarak tarayıcıya yazılmalı, güvenli bir bağlantı olup olmadığı (*SSL-Secure Sockets Layer* Sertifikası) kontrol edilmeli, erişilen sayfalarda kişisel bilgilerin istenmesi durumunda giriş yapılmamalı, iletişim yönteminin çevrimiçi alışveriş sitelerinde *https*, dosya indirirken *secure ftp* olmasına dikkat edilmelidir.
- Tarayıcı ayarları yardımıyla zararlı bileşenlere önlem olarak otomatik açılan pencereler engellenmelidir.
- Halka açık yerlerde kablosuz bağlantı ile ücretsiz İnternet kullanımında dikkatli olunmalıdır. Bu tip bağlantıların pek çoğu güvenlik risklerine açıktır.
- Evimizde kullandığımız kablosuz bağlantı aygıtları şifreli iletişim yapacak şekilde ayarlanmalı, parolaları güçlendirilmeli ve belli aralıklarla değiştirilmeli, aygıt adres bilgileri dış dünyadan gizlenmelidir.
- Kurumsal bilgisayarlar kişisel amaçlı kullanılmamalıdır.
- Kurumsal e-posta adresleri çevrimiçi alışveriş sitelerinde ya da özel amaçlı iletişim gruplarında paylaşılmamalıdır.
- Kullanılan sosyal medya hesaplarında iki aşamalı doğrulama yöntemi tercih edilmelidir.

- Sosyal medya hesaplarından paylaşılan bilgiler, resimler ve videolar, dolandırıcılar ve suç örgütleri için çok şey ifade ediyor olabilir, dikkatli olunmalıdır. Paylaşılan bilgiler minimize edilmelidir.
- Sosyal medya kimlik bilgilerinde gizlilik ayarları (herkese açık, sadece arkadaşlara açık gibi) kontrol edilmeli, dikkatli tanımlanmalıdır.
- Akıllı telefonlarımızın konum servisleri sürekli açık tutulmamalıdır.
- Akıllı telefon uygulamalarının kişisel bilgilerimize erişme isteğine karşı dikkatli olunmalı, güvenilirliğinden emin olunmayan uygulamaların kuruluşu yapılmamalıdır.
- Akıllı telefonlar elden çıkarılırken, ilk satın alındıktan sonra yüklenen her şey silinmeli, telefon fabrika ayarlarına döndürülmelidir.
- Alınması gereken yukarıdaki temel önlemler konusunda anne ve babalar tarafından çocuklar bilgilendirilmeli, İnternette dolaştıkları web siteleri, parola kullanımı, sosyal medya arkadaşlıkları ve paylaştıkları bilgiler konusunda dikkatli olmalarını sağlamak üzere küçük yaşlardan itibaren siber güvenlik bilinci ve farkındalığı oluşturulmalıdır.

Son olarak siber güvenlikle ilgili olarak Türkiye Bilişim Derneği'nin çalışmaları hakkında bilgi verebilir misiniz?

TBD, bilişim teknik bilimini ulusal kalkınma aracı olarak öngörüp 1971 yılında bilişimin ülkemizde gelişmesine katkıda bulunmak üzere kurulan, toplumun her katmanından üyesiyle bilişim kültürünü yaymaya çalışan, bilişim kesiminin sorunlarına çözüm arayan, özlük haklarına sahip çıkan bir sivil toplum öncü hareketidir. TBD, 12000'e yaklaşan üye sayısı, 7 şubesi, 12 il temsilciliği, 33 üniversitede TBD Genç yapılanması ile çalışmalarını sürdüren kamu yararına bir dernektir.

TBD anılan hedeflere ulaşılması için her yıl çeşitli etkinlikler düzenlemektedir.

Bunlardan ilki **Bilgi İşlem Merkezi Yöneticileri Semineri (BİMY)**'dir. **Bugüne kadar 22 kez gerçekleştirilmiştir.** TBD'nin her yıl düzenlediği geleneksel etkinliklerinden biri olan BİMY Semineri kamu ve özel kesimde çalışan üst ve orta düzey yöneticilerin mesleki gelişimi ve dayanışmalarını artırmayı amaçlamaktadır.

TBD'nin yıl içinde yapmış olduğu ikinci büyük etkinlik **TBD Kamu Bilişim Merkezleri Yöneticileri Birliği (TBD Kamu-BİB) Kamu Bilişim Platformu'**dur. **Bugüne kadar 17 kez gerçekleştirilmiştir.** TBD Kamu-BİB TBD'nin bir çalışma grubudur. 1995 yılında bilişim politikalarının oluşmasına ve toplumun e-dönüşüm'üne katkı sağlamak amacıyla kurulmuştur. Temel amacı çözüm üretmek ve yol göstermek suretiyle Kamunun bilişim alanındaki etkinliğinin ve farkındalığının artırılmasıdır. Gönüllü uzman ordusuyla, dönemsel olarak belirlenen konularda raporlar hazırlamakta, kamuoyu ile paylaşmaktadır. TBD Kamu-BİB bir kamu bilişim markası olmuştur.

Türkiye Bilişim Derneği' nin 1976 yılından bu yana geleneksel olarak her yıl düzenlediği ve Bilişim Sektörünün en büyük buluşması niteliğinde olan üçüncü etkinliği ise **Ulusal Bilişim Kurultayı**'dır. Bu güne kadar 32 kez gerçekleştirilmiştir. Ülkemizin bilişim kesiminin en büyük buluşması niteliğinde olan bu etkinlikte bilişim alanına ilişkin sorunlar, ülkemizin bilişim vizyonu, gelecek beklentileri ve hedefler en üst düzeyde ele alınmaktadır.

Türkiye Bilişim Derneği yukarıda açıklanan üç büyük etkinlik dışında yıl içinde bilgi alışverişini ve işbirliğini artırmak amacıyla şubeleri aracılığıyla bu yıl 10.su **gerçekleştirilecek olan İstanbul Bilişim Kongresi** ile **4. sü gerçekleştirilecek olan İzmir Uluslararası Bilişim Hukuku Kurultayı** gibi etkinlikler

düzenlemekte, **Sayısal Gündem 2020** gibi çalışma gruplarıyla **Dijital Türkiye** çalışmalarına katkı sunmaktadır. Derneğimiz aynı zamanda 33 Avrupa ülkesinin üyesi olduğu **Avrupa Profesyonel Bilişim Dernekleri Konseyi**'nin (CEPİS: Council of European Professional Informatics Societies) bir üyesidir.

TBD, ülkelerin 21. Yüzyıldaki yerini belirleyecek en önemli etkenlerden birinin bilişim olduğuna, ulusal kalkınmada bilişimin kaldıraç gücünü kullanarak büyüyen, üretken bir ülke olmanın bilişim stratejilerini doğru bir şekilde ortaya koymaktan ve uygulamaktan geçtiğine inanmaktadır.

Bu hedefler doğrultusunda kamu yararına çalışan bir sivil toplum kuruluşu olarak TBD, ilgili paydaşları bir araya getirdiği etkinliklerde siber güvenlik konusunu gündeme taşımakta, bu konuda eğitim programları düzenlemekte, ulusal siber güvenlik strateji ve politikalarının oluşturulması amacıyla yapılan çalışmalara katılım sağlamakta, ülke düzeyinde konuyla ilgili farkındalığın ve bilinç düzeyinin yükseltilmesi amacıyla gönüllülük temelinde pek çok farklı alandan uzman üyesiyle siber güvenlik konusunda yapılan çalışmalara katkı sağlamaktadır.

http://www.cybermagonline.com/, Mayıs 2016