TÜRKİYE BİLİŞİM DERNEĞİ

Ceyhun Atuf Kansu Cd.
1246 Sk. No: 4 / 17
06520 Balgat
Çankaya – Ankara
TÜRKİYE

T +90 312 473 8215
F +90 312 473 8216
E tbd@tbd.org.tr
W www.tbd.org.tr

3. SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ ZİRVESİ
TÜRKİYE BİLİŞİM DERNEĞİ GENEL BAŞKANI
RAHMİ AKTEPE'NİN AÇILIŞ KONUŞMASI
20 ŞUBAT 2020

Sayın Bakan Yardımcım,

Sayın KVKK Başkanım,

Sayın BTK Başkanım,

Değerli Bilişimciler,

Değerli Konuklar,

Değerli Basın Mensupları

Konuşmama başlamadan önce hepinizi Şahsım, Yönetim Kurulum ve etkinliğe emeği geçen herkes adına selamlıyorum.

50 yıla yakın bir süre önce Türkiye Bilişim Derneği yarınları düşünen bir öncü sivil toplum inisiyatifi olarak yola çıkmıştır.
O tarihlerde bilişim teknolojilerini sosyal refahın arttırılması ve sayısal uçurumun kapatılmasında bir araç olarak kullanmayı öngören
Türkiye Bilişim Derneği; günümüzde:

- **Ülkemizin dijital olgunluk seviyesinin yükseltilmesine,**
- **Dijital ekonomisinin geliştirilmesine,**
- **Toplumun dijital çağa uyumlandırılmasına ve hazırlanmasına,**
- **Ulusal siber güvenlik kapasitesinin ve yetkinliğinin geliştirilmesine,**
  ve toplumun tüm katmanlarında siber dirençliliğin artırılmasına katkı vermeyi amaçlıyor.

Her teknolojik ve bilimsel gelişimin insanlığa getirdiği olumlu etkisinin yanı sıra olumsuz etkilerinin olabildiği ve kötücül amaçlar için de kullanılabildiği malumdur.

21. yüzyılın koşullarından bir değerlendirme yaptığımızda; bu günkü kadar belirsiz, gerçekleştirilmesi bir o kadar kolay, elle tutulamayan ancak yıkıcı sonuçları gözle görülebilen ve hissedilebilen başka bir tehlike var olmamıştır.

“Siber Tehdit ” olarak tanımlanan bu tehlike, bireyden sektöre, sektörden devlete, yani toplumun tüm katmanlarında maddi veya manevi çok büyük zararlar oluşturabilecek bir etkiye sahiptir.

Şöyle bir karşılaştırma yapalım:
II. Dünya Savaşı yıllarında bir füzenin fırlatılması için 20 dakika gibi bir süre gerekirken ve sadece lokal etki yaratırken, günümüzde siber saldırılar ışık hızında gerçekleşebilmekte ve küresel etki yaratmaktadır.

Devletler tarafından da bir savaş aracı olarak kullanılmakta olan siber saldırıların, dünya genelinde her yıl katlanarak arttığı bilinmektedir.

Bu tehditler ile mücadeleye bağlı olarak dünya genelinde;
Yeni teknolojiler,
Standartlar,
Yeni mesleki kriterler,
Tedarik zincirleri,
Uluslararası iş birlikleri ve
Özgün diplomasilerden oluşan bir küresel “Siber Güvenlik Ekosistemi” oluşmuş durumdadır.

Dijital çağda güç dengelerini ölçmek de, **yeni küresel düzende** hayatta kalmayı sağlayacak başarılı stratejileri belirlemek de artık kolay değil.

Devlet dışı oluşumlar asimetrik olarak büyük tehditler oluşturabilmekte ve bu tehditler devletler tarafından da kullanılabilmektedir.

Siber güvenlik, çevre ve salgın hastalıklar ile birlikte 21. yüzyılın en büyük riskleri arasında yer almaktadır.

Dijital dönüşümü oluşturan; Nesnelerin İnterneti, Bulut Bilişim, Büyük Veri, Kayıt Zinciri ve Yapay Zekâ gibi teknolojilerin siber güvenliğe hem savunma hem de saldırı perspektifinde katkıda bulunduğu ve yeni bir bakış açısı kazandırdığı muhakkak.

Değerli konuklar,

Dijital dönüşümle birlikte birbirine bağlantılı ve tamamen dijital teknolojilerle donanmış sistemlerin yaygınlaşması ve **nesnelerin interneti olarak adlandırılan internete bağlı sensör sayısının 200 milyarı aşması siber güvenliğin önemini de aynı oranda arttırmaktadır.**

Türkiye, dünyada en fazla siber saldırıya uğrayan ilk 5 ülke arasında yer alıyor. ABD, Rusya, Çin ve Hindistan'ın ardından Türkiye geliyor.
Siber saldırıların ülkemizde raporlanan sayılarına bakacak olursak, hızla artan bir grafik görüyoruz.

Ulusal Siber Olaylara Müdahele Merkezi (USOM) tarafından;

2016'da 8 bin 625,
2017'de 99 bin 600
2018 de 72 bin 975 ve,
2019 da ise 136 bin 411
siber saldırının raporlandığı bildirdi.

2019 özellikle kurumsal ve kişisel verilere yönelik tehditlerin büyük oranda arttığı ve siber saldırganların yapay zekâyı daha yoğun olarak kullandıkları bir yıl oldu.

Bu yıl ise siber saldırıların daha da karmaşıklaşacağı ve gelişen teknolojilerle birlikte yeni saldırı yöntemlerinin ortaya çıkacağı öngörülüyor.

TBD olarak ülkemizin tüm kurum ve kuruluşlarını ve toplumun her kesimini yakından ilgilendiren “Siber Güvenlik” konusunu uzun yıllardan bu yana öncelikli çalışma alanlarımızdan biri olarak görüyoruz.

“Siber Güvenlik” ve “Yapay Zekâ” başta olmak üzere dijital dönüşüm teknolojileri konularında icra kurulumuz altında faaliyet gösteren odak eksen gruplarımız özenle çalışmaktadır.

Ayrıca Siber Güvenlik alanında farkındalık eğitimleri de verilmektedir.

Diğer yandan, uluslararası işbirliğinin ve bilgi paylaşımının siber güvenlik ekosisteminin geliştirilmesi amacıyla çok önemli olduğunu değerlendiriyoruz.

TBD, 20 yıldır Avrupa Profesyonel Bilişim Dernekleri Konseyi olan CEPIS’in üyesidir.

CEPIS’in dijital dönüşüm ile ilgili 5 çalışma grubunda aktif olarak görev yapıyoruz. Bunlardan biri de “Siber Güvenlik ve Yasal Mevzuat” çalışma grubudur.

Söz konusu çalışmalarımızla edinmekte olduğumuz uluslararası bilgi ve tecrübeleri ülkemizdeki sorunların çözümünde kullanmayı hedefliyoruz.

Ülkemizde sürdürülebilir ve güçlü bir siber güvenlik ekosisteminin oluşturulabilmesi için devletimizin ilgili kurumlarıyla işbirliği içerisindeyiz.

Ayrıca, siber güvenlik konusunda farkındalık yaratmak amacıyla etkinliklerimizde konu teknoloji, süreç ve insan boyutuyla işlenmektedir.

Değerli Katılımcılar,

Siber Güvenlik konusunda ele alınması gereken birkaç katman bulunmaktadır;

Devlet destekli saldırıların özellikle siber casusluk ve siber sabotajlara yönelmekte olduğunu biliyoruz.

Dolayısıyla; başta telekom altyapısı olmak üzere kritik altyapıların ve kamu kurumlarının siber tehditlerin odağında bulunması riskine karşı yapılacaklar önemli.

Dijital dönüşümde Nesnelerin Interneti, Büyük Veri, Yapay Zekâ ve Blok Zincir gibi teknolojilerdeki hızlı gelişmeler siber güvenliğin kapsamını ve önemini değiştirmeye başladı.

Yani bir nevi zehir-panzehir savaşı içerisinde olmamız söz konusu.

Dijital dönüşüm sürecinde, geleneksel idari yapılar şekil değiştirmekte **ve mevcut hukuk kuralları bu yeni etkileşime ayak uydurmakta zorlanmaktadır.**

Ayrıca veri güvenliği artık devletler tarafında uluslararası stratejik bir konu olarak ön plana çıkmaktadır.

Bu nedenlerle de, akıllı, etkin ve sürdürülebilir siber güvenlik altyapılarının kurulması, entegrasyonu ve otomatik olarak işletilebilmesi hayati önem kazanmıştır.

Araştırma şirketi Gartner'ın verilerine göre 2018 yılında yaklaşık 114 milyar dolar olan siber güvenlik pazarı 2019 yılında 125 milyar dolara ulaşmıştır. 2023 yılında ise bu rakamın 240 milyar doların üzerine çıkması beklenmektedir.

Bu pazarda lider konumda yer alabilmek ve mevcut pazar paylarımızın arttırılması ancak güçlü bir ekosisteme sahip olmamız ile gerçekleştirilebilir.

Değerli Katılımcılar,

Bu alanda "Standartlara Uyum" ve "Ürün Sertifikasyonu" nun çok önemli olduğunu değerlendiriyoruz.
Siber güvenlikte en önemli konu hiç şüphesiz standartlara uyumdur.
Ürün, sistem ve hizmetlere yönelik asgari güvenlik kriterlerinin tanımlanması ve ilgili standartların oluşturulması konularında Türk Standartları Enstitüsü ile birlikte çalışıyoruz.

Konuya bir de yaşanan riskler ve zararlar cephesinden bakarsak;
Genel anlamda, internete bağlanan her yeni cihaz ya da alınan her yeni parola, potansiyel saldırı alanlarının sayısını artırmaktadır.

Uçak, otomobil veya bir tıbbi cihazların korunması bazen sözkonusu ekipmanların değerini aşan yüksek maliyetler gerektirebilmektedir.

Ayrıca son birkaç yıldır yaygınlaşan ve 2019 yılında da kurumları zorlayan fidye yazılım tehdidinin 2020 yılında da etkisini sürdüreceği öngörülüyor.
Dünyada, haftada ortalama yüz binin üzerinde siber saldırı gerçekleşmektedir.
Saldırıların sayısı kadar gerçekleştirdikleri hasarın da parasal boyutları ürkütücü boyutlara ulaşmıştır.

Yıllık 400 milyar dolar kayıptan bahsediliyor. 2021'de ise bu rakamın birkaç trilyon doları bulabileceği ön görülüyor…

Türkiye'deki kritik altyapılarda kullanılan siber güvenlik ürünlerinin %90 dan fazlasının yurtdışı kaynaklı olduğu bilinmektedir.

Siber Güvenlik ekosisteminin geliştirilebilmesi ve ancak özgün olarak geliştirilen milli ve yerli ürün sayılarının arttırılması ile sağlanabilir.
Tabii, bu ürünlerin yaygın etkisinin yükseltilmesi kaydıyla.

Bu yönde hareket etmek, ulusal güvenliğimizi farklı küresel oyunculara emanet etmekten çok daha güvenli olacak ve önemli kazanımlar sağlayacaktır.

Değerli Katılımcılar,

2019 yılında, yüksek teknoloji ihracatımızın 5 Milyar Dolara yaklaşmış olduğu, imalat sanayii ürünleri ihracatındaki payın ise yüzde 4 civarında olduğu bilinmektedir. Siber güvenlik kümesinin tüm bu toplamlar içindeki yeri ise sadece 45 Milyon Dolardır. Yani toplam ihracatın ancak %0.9 u kadardır.
Yüksek teknolojili ürünlerin, imalat sanayii ürünleri ithalatı içindeki payı **ise yüzde 15** civarında gerçekleşmiştir.

Orta teknoloji ürünleri ithalat ve ihracatımız ise daha dengeli hemen hemen aynı miktarda ithalat ve ihracat olduğu görülüyor.

Oysa, 4. Sanayii Devrimi kapsamında kendimizi küresel olarak konumlandırırken gücümüzü orta teknolojiden daha yukarı noktalara ulaştırmak için acele etmeliyiz.

Dijital dünyadaki tehditler, anlık önlemler gerektirmektedir.

Bu anlamda Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Sektörel Güvenlik Operasyon Merkezleri'nin ulusal seviyede büyük veriyi kullanabilmesi, buradan elde edilecek bilgileri uluslararası ağlardan gelen bildirimlerle eşleyebilmesi beklenmektedir.

Siber güvenlik alanında yetişmiş insan gücünün yetersiz olması da siber saldırıların oluşumunda ve başarısında önemli bir rol oynamaktadır.

Türkiye'de 20 bin, dünyada ise 3 milyona yakın siber güvenlik uzmanına ihtiyaç olduğu bilinmektedir.

Yetişmiş insan gücüne,
Kullanıcı farkındalığına,
Yerli üretim yeteneğine ve
SOME'lerde ihtiyaç duyulan yetkinlik ve becerilere
Uzun süreli ve özverili çalışmalar ile yıllar içinde ulaşılabilmektedir.

Bu amaçla nitelikli insan kaynağının yetiştirilmesine ve becerilerinin arttırılmasına yönelik programların planlanması ve uygulamaya alınması önem arz etmektedir.

Sayın Cumhurbaşkanımızın geçenlerde bu konuda yaptıkları konuşmayı dinlerken görüş ve düşüncelerimizin kendileriyle aynı paralelde olduğunu görerek bir kez daha kendi bakış açımızı da bir nevi doğrulamış olduğumuzu mutlulukla gördük.

Bundan ötürü umutlarımız hakkında daha somut bir gelecek görebiliyoruz.

Değerli katılımcılar,

Son söz olarak,
Büyük çaba içinde olduğunu gördüğümüz karar vericiler ile devlet organlarını ve kamu kurumlarımızı ortak akıl oluşturmaya davet etmek isterim.

Söz konusu ortak aklın oluşturulmasında elbette özel sektör, üniversiteler ve STK'lar da etkin olarak yer almalıdır.

Biz, TBD olarak 700 kişilik uzman gönüllümüz ve 13.000 i aşkın üyemizle her zaman her düzeyde katkı vermeye hazırız.

Değerli Paydaşlar,

3. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi kapsamında;

- **Kamuda Siber Güvenlik Stratejileri**
- **Dijital Dönüşümde Siber Güvenlik: Yapay Zeka ve Kayıt Zinciri**
- **Küreselleşmede Veri Güvenliği**

olmak üzere 3 oturum gerçekleştirilecektir.

Ayrıca sosyal sorumluluk projesi kapsamında 14-16 yaş grubundaki 150 öğrenciye

- **Geleceği Şekillendiren Yapay Zekâ ve Siber Zorbalık Korunma Eğitimleri**

verilecektir.

Değerli katımlarınızla oluşturulacak Zirveye ait "Sonuç Bildirgesi" her zaman olduğu gibi karar verici noktalara ulaştırılacaktır.

Bu arada uzun süredir ortak çalışmalarımızla önemli yol kat ettiğimiz değerli BTK Başkanımız, KVKK Başkanımız ve Ulaştırma ve Altyapı Bakan Yardımcımıza da gönülden şükranlarımızı sunmak isterim.

Başarılı bir zirve olmasını temenni ediyor ve katılımınız için hepinize çok teşekkür ediyor, saygılar sunuyorum.