# II. SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ ZİRVESİ
# TÜRKİYE BİLİŞİM DERNEĞİ GENEL BAŞKANI
# RAHMİ AKTEPE'NİN AÇILIŞ KONUŞMASI
# 14 ŞUBAT 2019

**Sayın Bakan Yardımcım,**

**Sayın Başkanım**

**Sayın Başkan Yardımcım**

**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. Bilişim teknolojilerinin tüm dünyada üretim şekillerini, yaşam tarzlarını, toplumsal gelişmeleri, ülke ekonomilerini etkileyeceğini öngören kurucularımızı büyük bir saygı ve şükran duygusuyla anıyorum.

Türkiye Bilişim Derneği olarak Dijital Türkiye yol haritasında, ülkemizin dijital olgunluk seviyesinin yükseltilmesine, dijital ekonomisinin büyütülmesine ve toplumun söz konusu dönüşüme uyumlandırılmasına ve hazırlanmasına katkı vermeyi amaçlıyoruz. Çalışmalarımızıda bu yönde gerçekleştiriyoruz.

**Değerli Katılımcılar,**

TBD olarak, sadece eleştiren değil devletin yetişemediği yerlerde insitif alarak karar vericilere iletmek üzere çözüm ve projeler üretebilen bir STK olduğumuzu değerlendiriyoruz.

- Yerli ve Milli Yazılım Raporunun Hazırlanması
- Bilişim Standartlarının oluşturulmasına yönelik olarak imzalanan TBD-TSE İşbirliği Protokolü
- KOSGEB tarafından hazırlanan Dijital Dönüşüm teknolojilerine yönelik KOBİGEL Teşfik Paketine katkı sağlamak

TBD olarak insiyatif alarak geliştirdiğimiz projelere ve çözüm önerilerine örnek olarak sayılabilir. TBD olarak STK'ların sorun çözdükçe güçleneceğine, güçlendikçe de sorunları daha kolay çözebileceğine inanıyoruz.

**Değerli Katılımcılar,**

Son yıllarda devlet destekli siber saldırıların kritik altyapılara yöneldiği bilinmektedir. Diğer taraftan Siber Zorbalığın da özellikle çocukları ve gençleri hedef aldığı görülmektedir.

Diğer taraftan dijital dönüşümü tetikleyen Nesnelerin İnterneti, Bulut Bilişim, Büyük Veri, Kayıt Zinciri ve Yapay Zekâ gibi teknolojilerinin siber güvenliğe yeni bir bakış açısı kazandırdığı açıkça görülmektedir.

Dijital dönüşümle birlikte birbirine bağlantılı ve tamamen dijital teknolojilerle donanmış sistemlerin yaygınlaşması siber güvenliğin önemini arttırmaktadır.

Ayrıca kurumlar arası ve uluslararası işbirliğinin ve bilgi paylaşımının çok önemli olduğunu değerlendiriyoruz. TBD, 19 yıldır Avrupa Profesyonel Bilişim Dernekleri Konseyi CEPIS'e üyedir. 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 AB çalışmalarımızla edinmiş olduğumuz ve edineceğimiz bilgi ve tecrübeleri ülkemizdeki sorunların çözümünde kullannmayı hedefliyoruz.

Siber güvenlikte önemli kurallardan biride, bilişim sistemi içinde yer alan tüm siber güvenlik bileşenlerinin tümleşik olarak çalışabilmesidir. Siber güvenlik bileşenlerinin entegre edildiği bir sistem olan ve milli olarak geliştirilen AHTAPOT ve benzeri yazılımların kullanımının kamu kurumlarında yaygınlaştırılmasının ve sayısının arttırılmasının çok önemli olduğunu değerlendiriyoruz.

Siber güvenlik toplumun tüm katmanlarını ilgilendiren bir konudur. Bütüncül bir yaklaşım gerektirir. Bu amaçlada tüm paydaşların yer aldığı bir ekosistemin oluşturulması ve bu ekosistemin geliştirilmesi ülkemize önemli kazanımlar sağlayacaktır.

TBD olarak ülkemizde gerek kurumsal gerekse bireysel düzeyde siber güvenlik farkındalığının artırılması gerektiğine inanıyoruz. Söz konusu farkındalık sayesinde siber tehditlerle mücadelenin daha etkin ve verimli bir şekilde yürütülmesi sağlanacaktır.

Burada önemli olan diğer husus ise yerli siber güvenlik çözümlerinin hem kamu kurum ve kuruluşlarında hem de özel sektörde yaygın olarak kullanılmasıdır.

**Değerli Paydaşlar,**

Yerli siber güvenlik ürün, sistem, çözüm ve hizmetlerinin milli kabiliyetler ile özgün olarak geliştirilmesi, kritik altyapılarda kullanımının yaygınlaştırılması ulusal seviyede siber güvenlik kapasitesinin geliştirilmesine önemli katkılar sağlayacaktır. En önemlisi de Ulusal Güvenliğimizin bir teminatı olacaktır. Ülkemizin bekası amacıyla TSK ve güvenlik güçlerimiz tarafından gerçekleştirilen operasyonlarda kullanılan savunma sistemlerinin tamamı, bilişim teknolojileri tabanlı ve yazılım kontrollünde çalışan akıllı sistemlerden oluşmaktadır.

Her akılllı sistemde olduğu gibi söz konusu savunma sistemlerinde de siber saldırılar büyük bir risk oluşturmaktadır. Savunma sistemleri başta olmak üzere siber güvenlik teknolojileri alanında yerli ve milli çözümlerin geliştirilmesi ve üretilmesi önemlidir. Ülkemizin bekası ve dışa bağımlılığın asgari seviyeye indirilmesi açısından da yaşamsal öneme sahiptir.

Dolayısıyla bu konuya devlet olarak sektör olarak STK'lar olarak odaklanmalıyız. Siber güvenlik alanında iyi bir kullanıcı konumundan bir an önce teknoloji üretir ve teknolojiye yön verir bir konuma geçmeliyiz.

TBD olarak bu amaçlara ulaşabilmek için Siber Güvenlik Ekosisteminin güçlendirilmesi gerektiğini değerlendiriyoruz. Ayrıca, "**Siber Güvenlik Ekosistemi**" nin geliştirilmesi ve güçlendirilebilmesine yönelik yasal çerçevenin bir an önce oluşturulması ve yasal düzenlemelerin yapılması gerektiğine inanıyoruz. Sürdürülebilir siber güvenlik ekosisteminin geliştirilmesi, ulusal seviyede siber güvenlik kapasitesinin arttırılmasına ve toplumun tüm katmanlarında farkındalık yaratılmasına olanak sağlayacaktır.

**Değerli Katılımcılar,**

TBD olarak "Siber Güvenlik Ekosistemi" nin geliştirilebilmesi amacıyla öncelikle Cumhurbaşkanlığı sistemine uygun olarak "**Ekosistemin Yeniden Yapılandırılması**" gerektiğini değerlendiriyoruz. Söz konusu ekosistem içerisinde tüm paydaşlar aktif olarak yer almalıdır. Karar verici Ofis ve Kurullar, tedarikçiler, teknoloji, ürün ve hizmet geliştiriciler, standardizasyon ve sertifikasyon kuruluşları, akreditasyon ve eğitim kurumları, üniversiteler ve STK'lar. Söz konusu paydaşların rolleri açıkça tanımlanmalı ve yasal çerçeve oluşturulmalıdır.

İkinci olarak ise "**Siber Güvenlik Strateji ve Eylem Planlarının**" hazırlanmasında "Sivil İnsiyatifler" oluşturulması önemli kazanımlar sağlayacaktır. Kamu, özel sektör, STK ve üniversitelerden uzman kişilerin görevlendirileceği teknik çalışma grupları ile izleme komitelerinin oluşturulmasına acil ihtiyaç olduğunu değerlendiriyoruz.

Üçüncü olarak ise "**Nitelikli İnsan Kaynağının Yetiştirilmesi"** için bir program oluşturulmalıdır. Yenilikçi ve özgün teknolojilerin geliştirilmesine yönelik kamusal ve Sektörel SOME'ler başta olmak üzere bilişim ve siber güvenlik sektörleri tarafından ihtiyaç duyulan "**Nitelikli İnsan Kaynağının"** yetiştirilmesi ve sayısının arttırılması amacıyla ulusal bir programın acilen oluşturulması gerektiğini değerlendiriyoruz.

**Değerli Katılımcılar,**

Dördüncü olarak ise **"Yerli Sektörün Güçlendirilmesi"** ne ve markalaşmaya önem verilmesi gerektiğine inanıyoruz. Siber güvenlik ürün, sistem, çözüm ve hizmetlerinin milli kabiliyetler ile özgün olarak geliştirilmesi, kritik altyapılarda

kullanımının yaygınlaştırılması ulusal seviyede siber güvenlik kapasitesinin geliştirilmesine önemli katkılar sağlayacaktır.

Siber Güvenlik alanında milli kabiliyetler ile hangi teknolojilerin geliştirilmesine ihtiyaç olduğu ve ihtiyaçların önceliklendirildiği "**Ulusal Siber Güvenlik Teknoloji Yol Harita**" sının oluşturulması ve sektör ile paylaşılması kaynak israfının engellenmesine, hem sektörün hemde ulusal seviyede siber güvenliğin sürdürülebilirliğine önemli kazanımlar sağlayacaktır.

Diğer taraftan sırasıyla; **"Standartlara Uyum ve Ürün Serifikasyonu"**nun çok önemli olduğunu değerlendiriyoruz. Siber güvenlikte en önemli konu hiç şüphesiz standartlara uyumdur. Siber güvenlik ürün, sistem ve hizmetlerine yönelik asgari güvenlik isterleri tanımlanmalı, standartlar oluşturulmalı ve ürün sertifkasyon süreçleri belirlenmelidir.

Ayrıca, Kamu kurumları ile kritik altyapıların siber saldırılara karşı dirençlerinin arttırılması, siber saldırı sonrasında ise sistemlerin en kısa sürede hizmete alınabilmesi amacıyla "Sektör Odaklı ve Katılımı Zorunlu Siber Güvenlik Tatbikatları" düzenli olarak yapılmalıdır.

**Değerli Paydaşlar,**

II. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi kapsamında;

- Mobil Ağlarda Siber Güvenlik
- Dijital Dönüşümde Siber Güvenlik: Yapay Zeka ve Kayıt Zinciri
- Savunma, Havacılık ve Uzay Teknolojilerinde Siber Güvenlik
- Siber Güvenlik Hukuku ve Adli Bilişim

olmak üzere 4 oturum gerçekleştirilecektir. Değerli katımlarınızla oluşturulacak Zirveye ait "Sonuç Bildirgesi" her zaman olduğu gibi karar verici noktalara ulaştırılacaktır.

**Değerli Katılımcılar,**

Sözlerimi daha fazla uzatmak ve sizleri de sıkmak istemiyorum. Başarılı bir zirve olmasını temenni ediyor ve hepinize saygılarımı sunuyorum.