

4. Siber Gvenlik Ekosisteminin Geliřtirilmesi Zirvesi

Trkiye Biliřim Derneęi Genel Bařkanı

Rahmi Aktepe'nin Aılıř Konuřması

18 Őubat 2021

Sayın Bakanım

Sayın BTK Bařkanı,

Deęerli Biliřimciler,

Deęerli Konuklar,

Deęerli Basın Mensupları

Konuřmama bařlamadan nce hepinizi Őahsım, Ynetim Kurulum ve etkinlięe emeęi geen herkes adına selamlıyorum.

Bu yıl Derneęimizin 50. Yılını gururla kutluyoruz. 50 yıldır sren bu kararlı hizmet yolculuęunda TBD, tarafsız ve hibir maddi karřılık beklemeyen her biri deęerli uzmanlardan oluřan yelerinin zveriyle gerekleřtirmiř oldukları uzun soluklu alıřmalarla bu gnlere ulařmıřtır.

Daima takipisi olduęumuz ‘‘Biliřim’le Dnřm’’e katkı verme abalarımız, lkemizin ekonomik kalkınmasında biliřimin bir kaldıra olarak kullanılması; ticari, teknolojik, velhasıl tm retim ve yařam alanlarında kresel rekabetin arttırılması amacıyla yrtmř olduęumuz faaliyetler 50 yıl boyunca her yıl artan bir ivmeyle srmřtr.

Trkiye Biliřim Derneęi olarak:

- lkemizin dijital olgunluk seviyesinin ykseltilmesine,
- Dijital ekonomisinin geliřtirilmesine,
- Toplumun dijital aęa uyumlandırılmasına ve hazırlanmasına,

- Ulusal siber güvenlik kapasitesinin ve yetkinliğinin geliştirilmesine,
- Toplumun tüm katmanlarında siber dayanıklılığın artırılmasına

katkı vermek amacıyla faaliyetlerimizi yürütüyoruz.

Değerli Paydaşlar,

2020 yılında başlayan ve hala yaşamakta olduğumuz Covid-19 pandemisi ile dijital dönüşümün zorunluluk olduğu bir kez daha görülmüş ve digital teknolojilerin kullanımı artmıştır.

Dijital dönüşümlerini gerçekleştirmiş ve siber güvenlik yeteneğine sahip kurum ve kuruluşlar bu süreçte fark yaratarak faaliyetlerine devam etmiştir.

Yeni normalde evden çalışma, uzaktan eğitim ve dijital platformlar aracılığıyla ticaret gibi birçok yeni husus hayatımıza girmiş oldu. Bu süreçte **siber dayanıklılık ve iş sürekliliği** önemli bir kavram olarak karşımıza çıkmıştır.

Dijital becerileri eksik kurum, kuruluş ve bireylerimiz ise siber saldırganların odağı haline gelmiştir.

Covid-19'un başladığı Mart ayından yılsonuna kadar 2020 yılında Siber saldırılar da yaklaşık % 300 artış olduğu bilinmektedir. Söz konusu saldırıların daha çok kimlik avı girişimleri, veri ihlalleri ve rehin alma (fidye) saldırıları üzerinde yoğunlaştığını görüyoruz. Rehin alma saldırılarının yaklaşık 7 kat artmıştır, 2021'de de bu artışın daha da artarak devam edeceği öngörülmektedir. ABD'lerinde 2020'nin ilk çeyreğinde spam e-postalarında 200 kat, kötücül URL sayısında ise % 260 artış olduğu raporlanmıştır. 2019 yılında 119 adet olan koronavirüs temalı alan adının (web sitesi) 2020 yılının 2. çeyreğinde 78.000 adede ulaştığı görülmektedir.

Veri ihlallerinde ele geçirilen dosya sayısının 8 milyarı aştığı görülmektedir. Bir veri ihlalinin tespit edilmesinin ve kontrol altına alınmasının ortalama 280 gün süre aldığı ve küresel ekonomiye maliyetinin yaklaşık 3.9 milyar dolar olduğu düşünülürse siber güvenliğin reaktif olarak değil de proaktif olarak yapılmasının önemi ortaya çıkmaktadır.

Veri temelli bir ekonomiden bahsettiğimiz günümüzde veri, çağımızın petrolü olarak da öngörülmektedir. Ancak, veriyi işlemeden yani bilgiye dönüştürmeden ve bilgi paylaşımı yapmadan ekonomik bir değer yaratmak olası değildir.

Bu bağlamda veri güvenliği ve kişisel verilerin korunması ekseninde siber güvenliğin ön plana çıktığını görmekteyiz. Küreselleşme ile veri güvenliği arasında oluşan ikilemin ise getiri-götürü analizi yapılarak risk tabanlı yaklaşımlarla giderilmesinin önemli olduğunu değerlendiriyoruz.

Diğer taraftan, hem yapay zekâ, bulut bilişim, nesnelere interneti başta olmak üzere dijital teknolojilerdeki gelişmeler, hem de uzaktan çalışmanın getirdiği yeni riskler siber saldırıların gelişmesine ve saldırı yüzeyinin artmasına neden olmuştur. Yapay zekâ, makine öğrenmesi ve derin öğrenme gibi dijital teknolojiler siber saldırı araçlarında ve siber savunma araçlarında etkin olarak kullanılmaktadır.

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

Değerli Paydaşlar,

Ülkemizde kritik altyapılarda kullanılan siber güvenlik ürünlerinin % 90'dan fazlası yurtdışı kaynaklıdır. Bir önceki yıl 5 Milyar dolara yaklaşan ileri teknoloji

İhracatımızda ise siber güvenlik ürünlerinin payı sadece binde 9 olup, büyüklüğü 45 Milyon dolardır.

Siber Güvenlik artık ulusal güvenliğin en önemli bileşeni haline gelmiştir. Savaşlar şekil değiştirmiş önce siber savaflara daha sonra ise hibrit savaflara evrilmiştir. Bu kapsamda Siber Güvenlik teknolojilerinde dışa bağımlılığın azaltılması ve teknolojik egemenliğin arttırılmasının çok önemli olduğunu değerlendiriyoruz.

Siber güvenlik teknolojilerinin yani ürün, sistem, çözüm ve hizmetlerinin yerli ve 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.

Bu kapsamda ihtiyaç duyulan teşvik ve destek mekanizmalarının oluşturulması ve nitelikli insan kaynağının yetiştirilmesinin çok önemlidir.

Uluslararası Telekomünikasyon Birliđi Global Siber Güvenlik Endeksi'nin 2019 yılında yayımlanan raporuna göre ülkemiz bir önceki yıla göre, 23 sıra birden yükselerek, Dünyada 20'da sırada, Avrupa'da ise 11'inci sırada yer almıştır.

Önümüzdeki yıllarda, yerli ve milli kabiliyetler ile geliştirilen siber güvenlik teknolojilerinin yaygınlaşması sonucu söz konusu sıralamada ülkemizin daha iyi konuma geleceğini öngörmekteyiz.

Sayın Bakanım,

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. Derneğimizin bu alandaki ilk çalışma grubu olan Bilgi Güvenliği Çalışma Grubu 1990 yılında göreve başlamıştır.

“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 TBD akademi bünyesinde farkındalık eğitimleri de verilmektedir. Bu etkinlik kapsamında da;

- Siber Güvenilir Kullanıcı
- Bilgi Güvenliği Yönetim Sistemi (27001) Bilgi Güvenliği Farkındalığı
- Bulut Bilişim ve Güvenliği
- İşletim Sistemi Güvenliği
- Kişisel Verileri Koruma (KVKK ve GDPR)

olmak üzere 5 adet siber güvenlik eğitimi uzman eğitmenler tarafından verilecektir.

Diğer yandan, uluslararası işbirliğinin ve bilgi paylaşımının siber güvenlik ekosisteminin gelişimine önemli katkılar sağladığını 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 AB konseyi nezdinde yürütülen siber güvenlik ile ilgili konuları yakından takip etmekteyiz. Edinmekte olduğumuz söz konusu

uluslararası bilgi ve tecrübeleri ülkemizdeki sorunların çözümünde kullanmayı hedefliyoruz.

Ülkemizde sürdürülebilir ve güçlü bir siber güvenlik ekosisteminin oluşumuna katkı sağlamak amacıyla devletimizin ilgili kurumlarıyla yakın işbirliği içerisindeyiz.

Ayrıca, farkındalık yaratmak amacıyla tüm etkinliklerimizde siber güvenlik konusu teknoloji, süreç ve insan boyutuyla işlenmektedir.

Sayın Bakanım,

Bir diğer önemli konu ise anlık ileti ve sosyal medya uygulamalarında yaşanan ciddi siber güvenlik açıklarıdır. WhatsApp'ın Kullanım Koşulları ve Gizlilik politikasında 4 Ocak 2021 tarihinde yaptığı değişiklik ile topladığı kişisel verileri Facebook ve/veya diğer üçüncü taraflar ile hedefli reklamcılık amacıyla paylaşacağını duyurmuş ve kullanıma devam için zorunlu olarak açık rıza talebinde bulunmuştur.

Diğer taraftan 2016 ABD Başkanlık seçimlerinde ortaya çıkan " Cambridge Analytica" skandalı, 2020 ABD seçimlerinde Trump'ın Tweet'lerinin mahkeme kararı olmaksızın engellenmesi reklam amacından uzak dijital ekonomi savaşlarının bir parçası olarak görülebilir. TBD olarak mahkeme kararı olmaksızın sosyal medya kanallarının kapatılmasını ve/veya anlık ileti programları ile sosyal medya kanalları tarafından toplanan kişisel verilerin kullanıcılardan özgürce açık rıza alınmaksızın üçüncü taraflara paylaşılmasını etik bulmuyoruz. Bu konuda gerekli yasal düzenlemelerin ilgili kurumlarca acilen yapılması gerekmektedir.

Türkiye Uzay Ajansı tarafından açıklanan Milli Uzay Programını, bazı maddeleri bütçe ve zamanlama açısından çok gerçekçi olmasa da, hem ülkemizin savunması hem de teknolojik olarak kritik öneme sahip ve diğer sektörlerin gelişimine itici güç olan uzay teknolojileri alanında dışa bağımlılığın azaltılması ve nitelikli insan kaynağının yetiştirilmesi anlamında çok önemsiyoruz. Yapay zeka, derin öğrenme, otonom araçlar, nesnelerin interneti, eklemeli imalat ve siber güvenlik başta olmak üzere dijital teknolojilerin yoğun olarak kullanıldığı uzay teknolojilerindeki kazanımlarımızın, bilişim ve siber güvenlik ekosisteminin sürdürülebilirliğine önemli katkılar sağlayacağını değerlendiriyoruz.

Değerli Konuklar,

Ülkemizin siber Uzayda;

- Uluslararası normlar ve standartlar konusunda lider konuma gelmesine,
- Siber dayanıklılığın arttırılmasına,
- Teknolojik egemenliğin sağlanmasına,
- Yerli ve Milli Teknolojilerin geliştirmesine,
- Nitelikli insan kaynağının yetiştirilmesine,
- Hukukun üstünlüğüne, çevrimiçi insan haklarının ve temel özgürlüklerin korunmasına yönelik uluslararası paydaşlarla işbirliğinin güçlendirmesine

olanak sağlayan, insan **odaklı Siber Güvenlik Stratejilerinin** Avrupa Birliğinde 'de olduğu gibi Ülkemizde de oluşturulması, ekosistemin gelişimine önemli katkılar sağlayacaktır.

Ayrıca, yine Avrupa Birliği'nde olduğu gibi, **Siber Güvenlik Yasasının** ülkemizde çıkartılmasının, **Siber Güvenlik Sertifikasyon Programı, Siber Güvenlik Bilgi**

Paylaşım Platformu ve Yapay Zekâ destekli Siber Güvenlik Kalkanı oluşturulmasının ülkemizin siber dayanıklılığının arttırılmasına önemli kazanımlar sağlayacaktır.

Değerli Paydaşlar,

Uzun süredir ortak çalışmalarımızla önemli yol kat ettiğimiz değerli Ulaştırma ve Altyapı Bakan Yardımcımıza ve BTK Başkanımıza gönülden şükranlarımızı sunmak isterim.

Sözlerime burada son verirken 4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesine katılımınız ve katkılarınızdan dolayı hepinize çok teşekkür ediyor, başarılı bir zirve olmasını temenni ediyor ve saygılar sunuyorum.