4. SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ Zirvesi

18-19-20 Şubat 2021

TÜRKİYE BİLİŞİM DERNEĞİ 1971

SONUÇ RAPORU

DESTEKLEYEN KURULUŞLAR

BİLGİ TEKNOLOJİLERİ VE İLETİŞİM KURUMU

KVKK KİŞİSEL VERİLERİ KORUMA KURUMU

TÜRKİYE CUMHURİYETİ CUMHURBAŞKANLIĞI DİJİTAL DÖNÜŞÜM OFİSİ

www.tbd.org.tr | www.siberguvenlikzirvesi.org.tr

Türkiye Bilişim Derneği Yönetim Kurulu

Rahmi AKTEPE

Genel Başkan

M.Ali YAZICI (2. Başkan)

Atilla AYDIN (Yönetim Kurulu Üyesi)

Levent BERKMAN (Yönetim Kurulu Üyesi)

Nuray BAŞAR (Yönetim Kurulu Üyesi)

Şeyda ERTEKİN (Yönetim Kurulu Üyesi)

Lütfi ÖZBİLEN (Yönetim Kurulu Üyesi)

Ceyda SÜER (Yönetim Kurulu Üyesi)

Prof. Dr. Adem ŞAHİN (Yönetim Kurulu Üyesi)

Ahmet TOSUNOĞLU (Yönetim Kurulu Üyesi)

Fatoş Vural YARMAN (Yönetim Kurulu Üyesi)

Anıl YILMAZ (Yönetim Kurulu Üyesi)

İlyas YILMAZYILDIZ (Yönetim Kurulu Üyesi)

Denetim Kurulu

Hasan Cumhur ERCAN

Vural Rıza İBRİŞİM

Üveyiz Ünal ZAİM

Onur Kurulu

Tayfun ACAR

Sellçuk KAVASOĞLU

İ. İlker TABAK

Prof. Dr. Ali YAZICI

Mehmet YILMAZER

Raporu Hazırlayan: M. Ali YAZICI, TBD 2. Başkanı ve EYK Başkanı

Değerli Siber Güvenlik Ekosistemi Paydaşları,

Çağdaş, refah düzeyi yüksek bir Türkiye özleminin gerçekleşmesi yolunda, Türkiye Bilişim Derneği (TBD) 50 yıldır yılmadan ve büyük bir özveriyle çalışmaktadır. 1994 yılında Kamu Yararına Çalışan Dernek statüsünü kazanan TBD, 12 bini aşkın üyesi, 10 şehrimize yaygınlaşan yapılanması ve 33 üniversitedeki TBD genç örgütlenmesiyle bilişim sektörüne önemli katkılar vermeye devam etmektedir.

TBD olarak ülkemizin tüm kurum ve kuruluşlarını ve toplumun her kesimini ilgilendiren Siber Güvenlik konusunu öncelikli çalışma alanlarımızdan biri olarak görmekteyiz. Ulusal seviyede siber güvenlik kapasitesinin arttırılmasının sürdürülebilir ve güçlü bir siber güvenlik ekosistemi ile mümkün olacağı düşüncesiyle, Bilgi Teknolojileri ve İletişim Kurumu (BTK), Ulaştırma ve Altyapı Bakanlığı ve Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı ile iş birliği içinde, 18-20 Şubat 2021 tarihleri arasında TBD tarafından "Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi"nin dördüncüsü düzenlenmiştir.

Zirvede "İnsan Odaklı Siber Güvenlik Stratejileri", "Yeni Normalde Siber Güvenlik Riskleri", "Yapay Zeka Destekli Siber Dayanıklılık", "Kuantum Sonrası Dijital Güvenlik" ve "Dijital Oyunlar Siber Güvenlikte Bir Açık mıdır?" adında beş (5) oturum kamu, özel sektör ve üniversitelerimizin yöneticileri, öğretim üyeleri, sivil toplum kuruluşlarının temsilcileri, siber güvenlik uzmanları ve öğrencilerin katılımı ile gerçekleştirilmiştir.

Ayrıca, açılış konuşmalarında, siber güvenlik ve bilişim sektörüne yönelik önemli açıklamalar, tespitler ve önerilerde bulunan T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Sayın Dr. Ali Taha KOÇ, T.C. Ulaştırma ve Altyapı Bakan Yardımcısı Sayın Dr. Ömer Fatih SAYAN, BTK Başkanı Sayın Ömer Abdullah KARAGÖZOĞLU ve KVKK Başkanı Sayın Prof. Dr. Faruk BİLİR'e Siber Güvenlik Ekosistemine vermiş oldukları destek için teşekkür ediyoruz.

Bu yolda bizimle beraber mesai harcayan herkese ve sponsorlarımıza teşekkür ediyoruz. Çünkü bilmekteyiz ki "Siber Güvenlik Teknolojileri" alanında milli imkan ve kabiliyetler ile gerçekleştirilen yerli ürün ve/veya hizmet geliştirme faaliyetleri kalkınmamızın ve ülke güvenliğimizin en büyük teminatıdır.

Kamuoyuna saygıyla duyurulur.

Rahmi AKTEPE
Türkiye Bilişim Derneği
Genel Başkanı

Zirvenin Amacı

IV. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'nin amacı; ülkemizde siber güvenlik farkındalığının arttırılmasına, nitelikli insan kaynağı yetiştirilmesi ve sayısının arttırılmasına ve ulusal siber güvenlik stratejilerinin sürdürülebilirliğine ve etkinliğinin arttırılmasına yönelik ortak akıl oluşturulmasına ve milli kabiliyetler ile yerli ve yenilikçi siber güvenlik teknolojilerinin geliştirilmesi ile siber güvenlik ekosisteminin geliştirilmesine katkı sağlanması olarak belirlenmiştir.

Söz konusu amacın gerçekleştirilmesine yönelik olarak konusunda uzman konuşmacıların katıldığı toplam beş (5) oturumda "Siber Güvenlik Ekosisteminin Geliştirilmesi" konusu, insan, süreç ve teknoloji boyutuyla tartışılmış ve ortak akıl oluşturularak ülkemizin karar vericilerine ışık tutulması sağlanmıştır.

Katılımcı Portföyü

Türkiye Bilişim Derneği tarafından Bilgi Teknolojileri ve İletişim Kurumu (BTK), T.C. Ulaştırma ve Altyapı Bakanlığı ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı iş birliği ile düzenlenen IV. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi 18-20 Şubat 2021 tarihleri arasında Bilişim Teknolojileri ve İletişim Kurumu Merkez Binası'nda hibrit konseptiyle gerçekleştirilmiştir. T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Sn. **Dr. Ali Taha KOÇ**, T.C. Ulaştırma ve Altyapı Bakan Yardımcısı **Sn. Dr. Ömer Fatih SAYAN**, BTK Başkanı **Sn. Ömer Abdullah KARAGÖZOĞLU** ve KVKK Başkanı **Sn. Prof. Dr. Faruk BİLİR**, Kamu, Özel Sektör ve Üniversitelerimizin yöneticileri, öğretim üyeleri, Sivil Toplum Örgütlerimizin temsilcileri, Siber Güvenlik Uzmanları ve öğrencilerin katılımı ile gerçekleşen zirvede; alanlarında söz sahibi olan 29 konuşmacı yer almış ve zirveye 1200 kişi çevrimiçi olarak katılım sağlamıştır.

Zirve Açılış Konuşmaları

1. Gün açılış konuşmaları, TBD Genel Başkanı **Sayın Rahmi AKTEPE**, BTK Başkanı **Sayın Ömer Abdullah KARAGÖZOĞLU,** T.C. Ulaştırma ve Altyapı Bakan Yardımcısı **Sayın Dr. Ömer Fatih SAYAN** ve T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı **Sayın Dr. Ali Taha KOÇ** tarafından gerçekleşmiştir. 2. Gün açılış konuşması ise KVKK Başkanı **Sayın Prof. Dr. Faruk BİLİR** tarafından yapılmıştır.

Zirvenin açılış konuşmasını Video Konferans platformu aracılığıyla gerçekleştiren T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı **Sayın Dr. Ali Taha KOÇ,** "Dijital dönüşüm, yenilikçi teknolojilerle birlikte sağlıktan eğitime, finanstan endüstriye kadar tüm alanlarda, yolculuğunu sürdürüyor. 1950'li yıllarda Alan Turing'in "Makineler

düşünebilir mi?" sorusuyla 30 tonluk, 167 m2 alanı kaplayan devasa ENIAC ile başlayıp bugün kolumuzdaki akıllı saat boyutuna evrilen baş döndürücü bir teknolojik dönüşümden bahsediyoruz. Bu dönüşüm ile birlikte düşünme, davranma ve iş yapma şekillerimiz de değişiyor. Ekonomide, mesleklerde, sağlıkta, eğitimde, medyada ve sosyal hayatın birçok alanında köklü dönüşümleri hep birlikte yaşıyoruz ve artan bir hızla da yaşamaya devam edeceğiz. Türkiye'nin dijital dönüşümünde en önemli mihenk taşlarından biri şüphesiz e-devlet Kapısıdır. Sayın Cumhurbaşkanımızın Başbakanlığı döneminde, 18 Aralık 2008 tarihinde açılışı yapılan e-Devlet Kapısı bugün 12 yaşını doldurmuştur. 22 kamu hizmetiyle açılan e-Devlet Kapısı, bugün yaklaşık 740 kuruma ait 5 bin 500 ün üzerinde hizmet sunmaktadır. Kullanıcı sayısı 53 milyonu geçmiş durumda olan e-Devlet sistemine 2020'de yıllık giriş sayısı 2,5 milyara yaklaşmıştır. Vatandaşlarımıza sunduğumuz hizmetlerdeki dijital dönüşüm çalışmalarımızın neticesinde bugün ülkemiz uluslararası endekslerde büyük başarılara imza atmaktadır. Ülkemiz 2020 yılı temmuz ayı sonunda yayınlanan Birleşmiş Milletler e-Devlet Gelişmişlik Endeksinde 193 ülke arasında, Çevrim İçi Hizmet Endeksinde 22'nci, e-Katılım Endeksinde ise 23'üncü sıraya yükselmiştir. Benzer şekilde, 23 Eylül tarihinde yayınlanan "AB 2020 Yılı e-Devlet Endeks Çalışmaları"nda ise Kullanıcı Odaklılık başlığında 36 ülke arasından 4'üncü olmuştur. Endeksin genelinde ise 26'ncı sıradan 13'üncü sıraya yükselmiş bulunmaktayız. Amacımız tüm paydaşların destekleriyle, bu tür endekslerde dünya genelinde ilk 10 sıra içerisinde yer almak ve bunu sürdürülebilir kılmaktır." ifadelerini kullanmıştır.

Devletlerin sahip oldukları veri ve bu veriden ürettikleri bilgi nispetinde güce sahip olduklarını belirten **Sayın KOÇ**, "Bu itibarla tüm çabamız, yenilikçi teknolojileri bize özgü değerlerle harmanlayarak, Devletimizin gücüne güç katmaktır. Bu kapsamda, Yerli ve Milli olmanın yanı sıra uluslararası rekabet gücü yüksek ürünlerin geliştirilmesi elzemdir. Gerek pandemi süreci, gerekse ülke olarak karşılaştığımız tek taraflı ve haksız yaptırımlar, milli siber güvenlik teknolojisi geliştirmenin önemini bir kez daha ortaya çıkarmıştır. Siber güvenliği yabancı çözümlerle sağlamaya çalışmanın, sınır güvenliğini yabancı askerlere emanet etmeye eşdeğer olduğu unutulmamalıdır. Yerli ve milli siber güvenlik teknolojilerimizin gelişmesi ve uluslararası pazara ulaşması konusunda tüm paydaşlara önemli görevler düşüyor. Öncelikle kendi dijital altyapılarımızda, bu yerli ve milli çözümlerin tercih edilmesi önem taşımaktadır. Teknolojiyi sadece tüketen değil üreten bir Türkiye olmak için "Milli Teknoloji Hamlesi" vizyonu ile çıktığımız yolda, geliştirilmesini desteklediğimiz yerli ve milli teknolojilerin, başta kamu olacak şekilde tüm sektörlerde yaygınlaştırılmasına yönelik çalışmalarımızı sürdürmekteyiz. Bugün elinde bulundurduğu devasa kullanıcı verisi ile bir tehdit unsuru olan sosyal medya platformlarının arz ettiği tehlikeyi görmezden gelemeyiz. Veri güvenliği bizim için sınırlarımızın güvenliği kadar önemli ve önceliklidir. " şeklinde görüş belirtmiştir.

"Bildiğiniz gibi kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında alması gereken tedbirlerin ana çerçevesi Bilgi ve İletişim Güvenliği Tedbirleri konulu Cumhurbaşkanlığı Genelgesi ile çizildi. Bu genelge doğrultusunda özellikle gizliliği, bütünlüğü bozulduğunda milli güvenliği tehdit edebilecek kritik türdeki verilerin güvenliğinin sağlanmasına yönelik olarak kamu kurumları ve kritik altyapı hizmeti veren işletmelerin uyması gereken tedbirleri detaylı olarak ele aldığımız "Bilgi ve İletişim Güvenliği Rehberi'ni de 27 Temmuz 2020 tarihinde yayımladık. Bu rehber, yasal düzenleme boyutunda ülke çapında bilgi güvenliği seviyesini artırmaya yönelik önemli bir adım olmuştur. Ayrıca, siber güvenlik alanında ihtiyaç duyulan nitelikli işgücü ve istihdamı da olumlu yönde tetikleyecektir. 31 Ocak 2021 tarihi itibarıyla kurum, kuruluş ve kritik altyapı işletmelerince gerçekleştirilmesi planlanan varlık gruplarının belirlenmesi, kritiklik derecelendirme çalışmaları, boşluk analizi ve rehber uyumlaştırma yol haritasının belirlenmesi süreci tamamlanmış, 1'inci seviye tedbirlerin uygulanma aşamasına geçilmiştir. Politika, strateji ve eylem planlarını yakından takip etmekte ve ülke çapında etkin şekilde uygulamasına yönelik çalışmalar da yürütmekteyiz. Bu kapsamda, Ulaştırma ve Altyapı Bakanlığımız ile Dijital Dönüşüm Ofisimiz öncülüğünde yürütülen yeni Ulusal Siber Güvenlik Stratejisi ve Eylem Planı hazırlama çalışmaları tamamlanmıştır. İlgili tüm kurumların katkılarıyla, 8 stratejik amaca yönelik yapılması gereken 40 adet eylem ve 75 adet uygulama adımı belirlenmiştir. 2020-2023 dönemini kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem

planında belirlenen faaliyetlerin hayata geçirilmesi ile uluslararası siber güvenlik endeksindeki seviyemizi yükseltmiş olacağız." olarak görüş bildiren **Sayın KOÇ**, "Dijital Dönüşüm Ofisi olarak tüm bu saydığımız alanlarda politika, koordinasyon ve strateji geliştirmekte ve ülke çapında etkin şekilde uygulamasına yönelik çalışmalar yürütmekteyiz. Bugün, gelişen teknolojilerin ortaya çıkardığı siber güvenlik risklerinin yanında bu teknolojilerin savunma amacıyla kullanılmasının oluşturacağı fırsatların da göz ardı edilmemesi gerektiğini düşünüyoruz. Bunu "Pozitif Siber Güvenlik Yaklaşımı" olarak adlandırıyoruz. Pozitif siber güvenlik yaklaşımı ile bugünden atacağımız adımlar ve alacağımız önlemler, yarının dünyasında teknolojiyi takip eden değil teknolojiye yön veren bir ülke olabilmemiz için oldukça önemlidir." ifadeleri ile konuşmalarını tamamlamıştır.

Zirvenin açılış konuşmasını yapan T.C. Ulaştırma ve Altyapı Bakan Yardımcısı **Sayın Dr. Ömer Fatih SAYAN** "İnternet, kuruluşundan bu yana bir bilgi alışverişi platformundan evrim geçirerek modern işin, kritik hizmetlerin ve altyapının, sosyal ağların ve bir bütün olarak küresel ekonominin bel kemiği haline gelmiştir. ITU'nun resmi istatistiklerine göre dünya nüfusunun yarısından fazlası, 15-24 yaş arası nüfusun ise neredeyse yüzde 70'i internet kullanıyor. İnternet kullanıcıları arasına ise her gün 1 milyon yeni insan dâhil oluyor. İçinde bulunduğumuz Covid-19 salgınının da dijital dönüşümü önemli ölçüde hızlandırdığını görüyoruz. Bilişim ve iletişim teknolojileri, yaşadığımız COVID-19 krizi sırasında ekonomimizi ve toplumsal hayatımızı işler durumda tutmak için hiç bu kadar hayati olmamıştı. Küresel salgının toplumu normalinden daha fazla internet kullanımına teşvik etmesiyle beraber, geride bıraktığımız 2020 yılının son çeyreğinde toplam mobil internet kullanım miktarı 1,9 milyon Terabayt seviyelerine yükselirken, aylık veri kullanımında sabit genişbant abonelerinde 178 Gigabayt, mobil genişbant abonelerinde 9,9 Gigabayt seviyelerine ulaşmış durumdadır. Küresel uluslararası bantgenişliği kullanımı ise 2015 yılında 154 Terabit/sn iken 2020 yılında 718

Terabit/sn'ye ulaşmıştır" bilgisini paylaşmıştır. 2020 yılının siber kapasite açısından önemli olduğunu dile getiren **SAYAN**, "Geçtiğimiz 10 yılda tüm dünyada hükümetleri, şirketleri ve bireyleri hedef alan fidye yazılımı saldırıları, Covid-19 döneminde hastaneleri de hedef alarak artmaya devam etti. Covid-19 gölgesinde geçen 2020 yılında, dünya ekonomisinde hemen her sektörde daralma yaşanırken, siber güvenlik harcamalarının artarak devam etmesi, siber güvenlik faaliyetlerinin önemini bir kez daha gözler önüne seriyor. 2020 yılında dünya genelinde siber güvenlik harcama tutarı bir önceki yıla göre %2,4 oranında artarak 124 milyar Amerikan Dolarına ulaştığı görülüyor. 2022 yılında ise siber güvenlik yatırım harcamalarının 134 milyar Amerikan Dolarına çıkması öngörülüyor. Söz konusu harcamaların %50'ye yakını güvenlik hizmetleri olarak adlandırılan insan kaynağına, uzmanlığa ve bilgi paylaşımına ilişkin harcamalardan oluşuyor. Siber güvenlik alanında yetişmiş insan kaynağına sahip olma veya bu kaynağa erişebilme ülkeler için zenginlik meselesi. Biz de Bakanlık ve BTK olarak siber alanda yetkinliğimizi artırmak amacıyla düzenlediğimiz Siber Yıldız yarışmaları, siber talimhanelerimiz ve BTK Akademi eğitim faaliyetlerimiz ile bu alanda gücümüze güç katıyoruz" şeklinde konuşmalarına devam etmiştir.

Yapay zekâ konusuna da değinen **SAYAN**, "Yakın gelecekte yapay zekânın 2030 yılına kadar küresel büyümenin %14'ünü tek başına sağlayacağı öngörülüyor. Yapay zekâ da hem en etkili bir buluş hem de en büyük varoluşsal tehdit olarak adlandırılıyor. Sahte haberler ve derin sahtekarlık (deep fake) adı verilen manipülasyonlar gibi bazı riskler iyi bilinmekle birlikte, günümüzde şirketleri dolandırmak için tasarlanan yeni nesil oltalama saldırılarında yapay zeka tabanlı görüntü, ses, video formatlarının ve araçlarının kullanıldığı da görülebiliyor. İşin savunma tarafına bakıldığında ise veri analizleriyle beslenen yapay güvenlik sinir ağlarının kimlik avı saldırılarını önlemek için etkin bir şekilde kullanılabildiğini görüyoruz" ifadelerini kullanmıştır.

Gerek ulusal gerekse uluslararası düzeyde, siber güvenliği politika veya güç savaşı malzemesi yapmanın ilgili tarafların değil siber saldırganların hayatını kolaylaştırdığını vurgulayan **Sayın SAYAN**, bu anlamda yapılan siber tatbikatların önemli olduğuna değindi. **SAYAN**, "Dijital varlıklara olan güven ve bağımlılık, toplumlarımızı daha açık ve yenilikçi hale getirirken, madalyonun diğer tarafı ise siber risklere karşı artan bir savunmasızlıktır. Bu nedenle yeni teknolojileri ve fırsatları en güvenli biçimde vatandaşlarımızın istifadesine sunmak için güç birliğinde hepimizin üzerine düşeni yapacağına inancım tam. Bu amaca hizmet için bir araya geldiğimiz Zirvenin de güzel sonuçlara vesile olmasını temenni ediyorum." sözleriyle konuşmasını sonlandırmıştır.

Zirve'ye ev sahipliği yapan BTK Başkanı **Sayın Ömer Abdullah KARAGÖZOĞLU** ise "COVID-19'un siber suç üzerindeki etkisine ilişkin bir INTERPOL değerlendirmesine göre, bireylerden ve küçük işletmelerden büyük şirketlere, hükümetlere ve kritik altyapıya önemli bir hedef kayması olduğu görülüyor. Evden çalışan personeli desteklemek için uzak sistemler ve ağlar kullanan kuruluşlar ve işletmelere yapılan siber saldırılarda suçlular; veri çalmak, kar elde etmek ve kesintiye neden olmak için artan güvenlik açıklarından yararlanıyor. 2020 yılı dört aylık bir dönemde yaklaşık 907.000 spam ileti, kötü amaçlı yazılımla ilgili 737 olay ve 48.000 kötü amaçlı URL'nin tümü COVID-19 ile ilgili INTERPOL'ün özel sektör ortakları tarafından tespit edildi. Aynı değerlendirmede pandemi konulu yapılan siber saldırıların %59'unun oltalama ve kimlik avı, %36'sının kötü amaçlı yazılımlar (fidye yazılımı, DDOS vb.), %22'sinin sahte alan adları, %14'ünün ise yanıltıcı bilgi şeklinde gerçekleştirildiği belirtiliyor." bilgisini paylaşmıştır.

Bilişim ve iletişim destekli altyapının ve internet uygulamalarının yaygınlaşmasıyla birlikte ortaya çıkan güvenlik risklerinin çalışmaları hızlandırma noktasında büyük katkısı olduğunu belirten **Sayın KARAGÖZOĞLU**, "Yapılan araştırmalara göre siber saldırıların 2021 yılında yıllık 6 trilyon Amerikan Doları tutarında zarara sebep olacağı hesaplanırken, bu zararın 2025 yılında 10 trilyon Amerikan Dolarını aşması bekleniyor. Siber suçların yarattığı zarar bu kadar büyükken, örneğin Amerika'da siber suçluların yakalanma ve tespit edilme oranının onbinde 5 olduğu tahmin ediliyor. Diğer ülkelerde de durum çok farklı değildir. Yapılan siber saldırıların %86'sının amacının finansal fayda sağlamak amaçlı olduğu hesaplanırken, siber saldırıların %30'unun iç aktörlerden geldiği değerlendiriliyor." şeklinde konuşmalarına devam etmiştir.

USOM'un çalışmalarının pandemi sürecinde daha da arttığına vurgu yapan **Sayın KARAGÖZOĞLU**, "Bakanlığımızın desteği ile BTK olarak salgının başlangıcında paydaşlarımızla birlikte önleyici tedbirler aldık. "Uzaktan Erişim Servislerine Yönelik Önlemler" dokümanı, oltalama saldırıları ile bu kapsamdaki sahte uygulamalara yönelik

alınacak tedbirlere ilişkin doküman ve video konferans ve toplantı yazılımlarının kullanımında siber güvenlik açısından dikkat edilmesi gereken hususları içeren tavsiye dokümanı hazırlayarak yayımladık. Bu süreçte siber saldırı ve tehditlerle ilgili kaydettiğimiz bazı rakamları sizlerle paylaşmak istiyorum. Pandemi sürecinde yerli ve milli uygulamalarımızla; yapay zeka teknolojileri kullanılarak 211 adet sahte konferans uygulaması ve uzaktan yönetim servislerinde 19.350 adet zafiyet tespit edilmiştir. COVID-19 ile alakalı 42 adet zararlı yazılım incelemesi ve 569 adet zararlı yazılım bilgisi SOME'lerle paylaşılmıştır. COVID-19 ile alakalı 987 adet zararlı dropper ve komuta kontrol merkezi engellenmiştir. Tüm bu çalışmalar USOM bünyesinde yetkin uzmanlarımızın yoğun gayretleri ve donanımları ile mümkün oluyor" ifadelerinde bulunmuştur.

Ülkemizde siber güvenlik alanında uzman ihtiyacının karşılanması amacıyla, 24 saat boyunca süren "SİBER YILDIZ" bayrağı yakala (capture the flag)" yarışmalarını düzenli olarak organize ettiklerini, söz konusu yarışmalara yoğun katılım olduğunu, yarışmalar sonucunda başarılı olan siber güvenlik uzmanlarına ise BTK/USOM'da istihdam olanağı yarattıklarını belirten **Sayın KARAGÖZOĞLU**, siber güvenliğin de milli güvenlik kadar önemli olduğu vurgusuyla konuşmasını tamamlamıştır.

Zirvenin 2. Günü açılışında konuşan KVKK Başkanı **Sayın Prof. Dr. Faruk BİLİR** ise "İnsan hakları düşüncesinin merkezinde, insanın sadece insan olmasından ötürü değerli olduğu ve insan onurunun korunması fikri yer almaktadır. Kişisel verilerin korunması temel bir insan hakkıdır. Temelinde insan onurunun korunması vardır. Kişisel verilerin korunmasını isteme hakkı, ülkemizde Anayasal güvence altındadır. Bu bağlamda 2010 Anayasa değişikliği, ülkemizde kişisel verilerin korunması bakımından dönüm noktası olmuştur. Elbette bu değişikliğin öncesinde de ülkemizde kişisel veriler çeşitli mevzuatlar kapsamında koruma altındaydı. Fakat Anayasa değişikliği, kişisel verilerin korunması noktasında bireylere; bilgilendirilme, kişisel verilere erişim ve silme gibi doğrudan ve dolaylı olarak birtakım haklar getirmiştir. Yine Anayasa değişikliği ile eklenen ilgili hüküm gereği, kişisel veri işlemede uyulacak usul ve esasların Kanunla düzenleneceği öngörülmüştür. Bu açıdan bizzat kişisel verilerin korunması alanına özgü bir düzenlemenin önü açılarak ülkemizde kişisel verilerin korunmasının temeli atılmıştır. Bunun bir sonucu olarak Kişisel Verilerin Korunması Kanunu 7 Nisan 2016 tarihinde yürürlüğe girmiştir. Dijital ayak izlerimizin geleceğimizi şekillendirebildiği bir dünyada, kişisel verilerin korunmasını ''dijital çağda insan kalabilme'' idealine hizmet eden önemli araçlardan biri olarak görüyorum. Bu çerçevede bizler, teknolojinin iyi ve güzel amaçlarla kullanılması, insan odaklı bir anlayışla kullanılması gerektiğine inanan insanlar olarak; dijital faşizmin, dijital sömürünün karşısında olmalıyız. Dijital tekelleşmenin kişisel veri

güvenliği üzerinde meydana getirdiği risk ve tehditlere karşı veri mahremiyetini savunmalıyız diye düşünüyorum." şeklinde görüşlerini belirtmiştir.

Sayın BİLİR, sözlerine şöyle devam etmiştir: "İçinde bulunduğumuz çağda hem gerçek hem de siber ortamlarda kişisel verilerin korunmasını temin edebilmek için Kişisel Verilerin Korunması Kanununa uyum göstermek gerekmektedir. Kanun, kişisel veri işlemeyi yasaklamamakta, hukuka uygun veri işlemeyi öngörmektedir. Kanunun getirdiği denetim mekanizmaları, bireylere verileri üzerinde kontrol ve söz sahibi olma ve kişisel verilerinin akıbetini belirleme hakkını getirmiştir. Ülkemizde doğrudan kişisel verilerin korunmasına yönelik olarak ilk ve temel düzenleme olarak kabul edilen 6698 sayılı Kanun, 95/46 sayılı AB Veri Koruma Direktif'i mehaz alınarak hazırlanmıştır. Bundan dolayı amaç, kapsam ve diğer hükümleriyle birlikte değerlendirildiğinde 95/46 sayılı Direktif ile büyük ölçüde uyumluluk arz etmektedir. Bununla birlikte bizim Kanunumuzdan 2 yıl sonra yürürlüğe giren Avrupa Birliği Genel Veri Koruma Tüzüğü (GDPR), Avrupa ülkeleri arasında bu alandaki çok başlılığı ve uygulama farklılığını gidermeyi amaçlamış, bireylere üst düzey bir koruma getirmiştir. Kurumumuz, hem KVKK-GDPR uyumu hem de 108 sayılı Sözleşme'nin modernizasyonu gibi konularda çalışmalarına aralıksız devam etmektedir."

Konuşmasında, veri güvenliğini temin etmenin hukuka uygun veri işlemenin adımlarından biri olduğunu kaydeden **Sayın BİLİR**, "Veri sorumlusu; kişisel verilerin hukuka aykırı olarak işlenmesini, erişilmesini önlemek ve kişisel verilerin muhafazasını sağlamak amacıyla gerekli olan her türlü teknik ve idari tedbirleri almak durumundadır. Bu ifadeden yola çıkarak, teknik ve idari tedbirlerin alınması da esasında hukuka uygun veri işlemenin bir parçasıdır diyebiliriz. Güvenliği sağlamanın bir diğer ayağı da veri ihlal bildirimidir. Veri ihlali gerçekleşmesi halinde Kurula ve ilgili kişilere bildirimde bulunmak, veri güvenliğine ilişkin yükümlülükler arasındadır. Dolayısıyla işlenen kişisel verilerin kanuni olmayan yollarla

başkaları tarafından elde edilmesi halinde, veri sorumlusu bu durumu en kısa sürede ilgilisine ve Kurula bildirmelidir. Kurula ve ilgili kişilere bildirim yapılmasındaki amaç; ihlal nedeniyle ortaya çıkan veya çıkması muhtemel olan olumsuz sonuçların ivedilikle önüne geçilmesi veya bu olumsuz sonuçların etkilerinin minimum seviyeye indirilmesidir. Veri sorumluları bu tür durumlara hazırlıklı olmak amacıyla bir ''veri müdahale planı'' hazırlamalıdır. Veri müdahale planı, siber saldırıların siber felaketlere dönüşmesini önleyici nitelikte bir tedbirdir. Bu sebeple veri müdahale planı belli aralıklara gözden geçirilmeli, gelişmeler ve yenilikler doğrultusunda güncellenmelidir. Tabii meydana gelen her veri ihlali, veri sorumlusu tarafından gerekli tedbirlerin alınmadığı anlamına gelmez. Teknolojinin gelişmesiyle doğru orantılı olarak siber saldırılar da gün geçtikçe nitelikli hale gelmekte ve karmaşık bir yapıya bürünmektedir. Bundan dolayı her ihlal bildirimi kendi özel şartları içerisinde incelenmektedir. Gerekli bütün önlemlerin alınmasına rağmen yine de bir veri ihlali ile karşılaşılmış ise; veri sorumlusu proaktif bir yaklaşım sergilemiş mi, Kurum tarafından yayınlanan Kişisel Veri Güvenliği Rehberi'nde belirlenen tedbirleri uygulamış mı, özel nitelikli kişisel veri işlemiş ise bunlar için gerekli olan ek tedbirleri uygulamış mı, kişisel verilerin gizliliği ve bütünlüğü için yeterli aksiyonları almış mı, elbette bunlar göz önünde bulundurulmaktadır. Örneğin geçtiğimiz günlerde Kurulun yayımladığı bir Karar Özetinde; meydana gelen ihlalin veri sorumlusunun tedbir eksikliğinden kaynaklanmadığı ve gerekli teknik ve idari tedbirlerin alındığı belirtilmiş, söz konusu veri ihlal bildirimi ile ilgili olarak Kanun kapsamında yapılacak bir işlem bulunmadığına karar verildiği ifade edilmiştir. Veri sorumlusu gerçekleşen ihlalin öncesinde ve sonrasında gerekli olan yükümlülükleri yerine getirmişse, burada idari yaptırım uygulanmayabilir. Buna rağmen bir yaptırım uygulansaydı, o zaman teknik ve idari tedbirleri almanın ve diğer yükümlülükleri yerine getirmenin bir anlamı kalmazdı." ifadelerinde bulunmuştur.

Kişisel verileri aktarmanın da bir veri işleme faaliyeti olduğunu hatırlatan **Sayın BİLİR**, Kişisel Verileri Koruma Kurulunun yurt dışına kişisel veri aktarımı ile ilgili bugüne kadar yaptığı çalışmaları özetleyerek, Kurulun geçtiğimiz günlerde ilk defa bir taahhütnameyi onayladığını, gerekli şartlar yerine getirildiği takdirde taahhütnamelerin onaylanabileceğini dile getirmiştir. Bununla birlikte güvenli ülke ilanı veya taahhütnamelere onay vermenin, Kurulun görev alanı içerisinde olduğunu belirten **Sayın BİLİR**, bu konuda Kanunda belirli kriterler sayıldığını ve Kurulun karar verirken Kanunda düzenlenen hükümlere uygun şekilde hareket etmek durumunda olduğunu vurgulamıştır. **Sayın BİLİR**, Kanunun veriden değer üretebilen teknolojilerden faydalanılmasını engellemediğini, Kurulun Türkiye'de yerleşik firmaların yurt dışında rekabet gücünün artmasından yana olduğuna vurgu yapmıştır. **Sayın BİLİR,** "Mahremiyet, kişinin özgürlüğünün bir parçasıdır. Algoritmalar, kişiye geleceğini belirlemede yardımcı olabilir.

Ancak kişinin geleceği üzerinde asıl söz sahibi algoritmalar değil, kişinin kendisi olmalıdır. Dijital çağda öncelik, güvenliktir. Güvenliğin anahtarı ise farkındalıktır." şeklinde konuşmasını tamamlamıştır.

TBD Genel Başkanı **Sayın Rahmi AKTEPE** "Bu yıl Derneğimizin 50. Yılını gururla kutlayacağız. 50 yıldır süren bu kararlı hizmet yolculuğunda TBD, tarafsız ve hiçbir maddi karşılık beklemeyen her biri değerli uzmanlardan oluşan üyelerinin özveriyle gerçekleştirmiş oldukları uzun soluklu çalışmalarla bu günlere ulaşmıştır. Daima takipçisi olduğumuz "Bilişim'le Dönüşüm"e katkı verme çabalarımız, ülkemizin ekonomik kalkınmasında bilişimin bir kaldıraç olarak kullanılması; ticari, teknolojik, velhasıl tüm üretim ve yaşam alanlarında küresel rekabetin arttırılması amacıyla yürütmüş olduğumuz faaliyetler 50 yıl boyunca her yıl artan bir ivmeyle sürmüştür." ifadeleri ile konuşmasına başlamıştır. **Sayın AKTEPE**, "2020 yılında yaşamış olduğumuz ve halen de yaşamakta olduğumuz Covid-19 pandemisi ile dijital dönüşüm bir zaruret haline gelmiş ve dijital 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 yıl sonuna kadar 2020 yılında Siber saldırlar da yaklaşık % 300 artış olduğu bilinmektedir. Söz konusu saldırıların daha çok kimlik avı girişimleri, veri ihlalleri ve rehin alma (fidye) saldırıları üzerinde yoğunlaştığını gördük. Rehin alma saldırılarının yaklaşık 7 kat arttığı ve 2021'de de bu artışın daha da artarak devam edeceği öngörülmektedir. ABD'de 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 ne kadar önemli olduğu ortaya çıkmaktadır." ifadelerini kullanmıştır.

"Siber Güvenlik artık ulusal güvenliğin en önemli bileşeni haline gelmiştir. Klasik savaşlar şekil değiştirmiş önce siber savaşlara daha sonra ise hibrit savaşlara 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 önemli olduğunu değerlendiriyoruz" şeklinde görüşlerini belirten **Sayın AKTEPE**, uluslararası iş birliğinin ve bilgi paylaşımının siber güvenlik ekosisteminin gelişimine önemli katkılar sağladığını, TBD olarak Avrupa Profesyonel Bilişim Dernekleri Konseyi CEPIS'in 20 yıldır üyesi olduklarını, CEPIS'in dijital dönüşüm ile ilgili beş (5) çalışma grubunda aktif olarak görev yaptıklarını, bunlardan birinin de "Siber Güvenlik ve Yasal Mevzuat" çalışma grubu olduğunu, söz konusu çalışmalarla AB konseyi nezdinde yürütülen siber güvenlik ile ilgili konuları yakından takip ettiklerini, edinmekte oldukları söz konusu uluslararası bilgi ve tecrübeleri ülkemizdeki sorunların çözümünde kullanmayı hedeflediklerini, Ülkemizde sürdürülebilir ve güçlü bir siber güvenlik ekosisteminin oluşumuna katkı sağlamak amacıyla devletin ilgili kurumlarıyla yakın iş birliği içerisinde olduklarını, farkındalık yaratmak amacıyla tüm etkinliklerde siber güvenlik konusunu teknoloji, süreç ve insan boyutuyla işlemekte olduklarını, 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 bulmadıklarını, Ülkemizde bu konuda gerekli yasal düzenlemelerin ilgili kurumlarca acilen yapılması gerektiğini, Cumhurbaşkanı tarafından açıklanan Milli Uzay Programını, 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 önemsediklerini, 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 belirterek konuşmalarını sonlandırmıştır.

Zirve Oturumları

Zirvede "İnsan Odaklı Siber Güvenlik Stratejileri", "Yeni Normalde Siber Güvenlik Riskleri", "Yapay Zeka Destekli Siber Dayanıklılık", "Kuantum Sonrası Dijital Güvenlik" ve "Sosyal Medya ve Dijital Oyunlar Siber Güvenlikte Bir Açık mıdır?" adında beş (5) oturum gerçekleştirilmiştir.

Oturum-1: İnsan Odaklı Siber Güvenlik Stratejileri

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı Sayın Yavuz Emir BEYRİBEY'in moderatörlüğünü yaptığı "İnsan Odaklı Siber Güvenlik Stratejileri" Oturumunda; AKGÜN Yönetim Kurulu Başkan Vekili Sayın Ahmet Hamdi ATALAY, Mitsubishi Electric Fabrika Otomasyon Sistemleri Ürün Yönetimi ve Pazarlama Birim Müdürü Sayın C. Tolga BİZEL, Fortinet Sistem Mühendisleri Müdürü Sayın İlker İMAMOĞLU, T.C. UAB HGM Siber Güvenlik Daire Başkanı Sayın Özgür ÖZTÜRK ve ULAK Haberleşme A.Ş. Genel Müdür Yardımcısı Sayın Aziz SEVER konuşmacı olarak yer almıştır.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkan Yardımcısı **Sayın Yavuz Emir BEYRİBEY** panel açılış konuşmasında dijitalleşmenin teknoloji ile birlikte, insanların düşünme, davranma ve iş yapma şekillerinin dönüşmesi ile kendini gösterdiği bir döneme tanıklık ettiğimizi ve siber güvenlik konusunun da "dijital dönüşüm"ün ana esasları arasında yerini aldığını ifade etmiştir.

İnsan odaklı siber güvenlik stratejilerinin temelinde siber saldırılara karşı toplumsal bağışıklığın kazandırılmasının yer aldığı ve bunun yolunun da siber güvenlik okur yazarlığının artırılması ve kurumsal siber dayanıklılığın bel kemiği noktasındaki personellerin yetkinliklerinin artırılmasından geçtiği belirtilen **Sayın BEYRİBEY**, 2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem planında ortaya konan hedeflere ancak ulusal kapasitenin gelişmesi ile ulaşılabileceğini, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından yayınlanan Bilgi ve İletişim Güvenliği Rehberi'nde siber güvenlik kurumsal farkındalık ve yetkinliğinin artırılmasına katkı sağlayacak birçok tedbire yer verildiğini ifade etmiştir.

Sayın Yavuz Emir Beyribey "Siber tehditlerle mücadelede gereken ciddi savunma ve karşı tedbir geliştirme yeteneğinin geliştirilmesinde kurumlar arası iş birliğini de dikkate alan bütüncül ve çevik bir siber güvenlik yaklaşımının benimsenmesi büyük önem arz etmektedir. Dijital Dönüşüm Ofisi olarak "Dijital Türkiye" sloganıyla çıktığımız bu yolda; kamu, özel sektör, üniversite ve sivil toplum kuruluşları işbirliğiyle ülkemizin dijital dönüşümünü gerçekleştirmeyi hedefliyoruz." ifadelerini kullanmıştır. Ayrıca, ulusal siber

güvenliğin ve dijital dönüşümün sağlanmasında ortak iş birliği, bütüncül ve çevik bir yaklaşımın benimsenmesinin önemine vurgu yapmıştır.

AKGÜN Yönetim Kurulu Başkan Vekili **Sayın Ahmet Hamdi ATALAY**, "Farklı tanımları yapılabilmekle birlikte Bilgi Güvenliği Derneğince yapılan ve genel kabul görmüş tanımıyle Siber Güvenlik; veri bütünlüğünün korunması, mahremiyetin ve gizliliğin korunması, yetkisiz erişimin engellenmesi, bilgiye erişimin, erişim hız ve kalitesinin korunması, Bilişim sistemlerinde iş sürekliliği ve performansının devamlılığının sağlanmasıdır. Siber Güvenliğin sağlanmasında üç ana unsur, Teknoloji, Süreçler ve İnsan dır. Bu zincirin en zayıf halkası ise "İnsan" faktörüdür. Dolayısıyle belirlenecek stratejiler ve yapılacak tüm planlamalarda bu faktör göz önünde bulundurulmalıdır. İnsan faktörüne odaklanarak iş ve işlemler gerçekleştirilmeli; insan faktörünü güçlendirecek aksiyonlar önceliklendirilmelidir. Siber Güvenlikte insan faktörünün zayıflığının risklerini azaltmak için önerilen çözüm Siber Hijyen'dir. Siber Hijyen, güvenliği sağlamak üzere alınması gereken tedbirlerin ve yapılması gereken şeylerin alışkanlık haline getirilmesi ve günlük hayatın parçası haline getirilmesidir. " ifadelerinde bulunmuştur.

T.C. UAB HGM Siber Güvenlik Daire Başkanı **Sayın Özgür ÖZTÜRK** , "Planlı, etkin, ilkeli ve hedefli stratejiler fark yaratır. Güçlü bir siber güvenlik, güçlü stratejilerle mümkündür. Ülkemizde siber güvenlik alanında stratejik yaklaşımın geliştirilmesi, 2012 yılından itibaren ivme kazanmıştır. Çalışmalar kapsamında, Bakanlığımız koordinasyonunda ulusal siber güvenlik organizasyonu oluşturulmuş, 2013-2014 ve 2016-2019 dönemlerini

kapsayan Ulusal Siber Güvenlik Stratejisi ve Eylem Planları yayımlanmış ve eylem planlarına ilişkin çalışmalar tamamlanmıştır. “ ifadelerini kullanmıştır.

Sayın ÖZTÜRK, “İlgili kurum ve kuruluşların katkılarıyla Bakanlığımızca gerçekleştirilen çalışmalar neticesinde; Ülke ekonomisinin geliştirilmesini, toplumsal yaşamın korunmasını ve milli güvenliğin sağlanmasını desteklemek için; ülkemizde güvenli biçimde işleyen bir siber ortama sahip olmak ve siber güvenlikte uluslararası alanda marka haline gelmek vizyonuyla "2020-2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı" hazırlanmıştır. 29.12.2020 tarihli ve 31349 sayılı Resmi Gazete'de yayımlanan 2020/15 sayılı Cumhurbaşkanlığı Genelgesi ile onaylanan strateji ve eylem planı, 8 stratejik amaç kapsamında 40 eylem maddesi ve 75 uygulama adımı içermektedir. İnsan odaklı bir bakışla, ilkeler ve hedefler çerçevesinde inşa edilen eylem planı içerisinde özellikle, farkındalık ve insan kaynağının artırılarak ulusal kapasitemizin geliştirilmesi ön plana çıkan hususlardan biridir ve “Ulusal Kapasitenin Geliştirilmesi” stratejik amacıyla ele alınmıştır.” şeklinde konuşmasına devam etmiştir.

Sayın ÖZTÜRK, “Önümüzdeki dönemde yapılacak çalışmalarla olay müdahale kabiliyeti ve USOM-SOME koordinasyonu daha da geliştirilerek mevcut insan kaynağımızdan en üst seviyede faydalanılacak, yetkinliği artırılacaktır. Özellikle SOME’lerin olgunluk seviyelerinin ölçülmesi sağlanarak gelişim alanları belirlenecek ve buralarda görevli uzmanların gelişimini, yetkinliğini artıracak eğitim faaliyetleri ve diğer tamamlayıcı çalışmalar yürütülecektir. Diğer yandan ülkemizin bu alandaki ihtiyaç duyduğu ilave insan kaynağının sektörümüze kazandırılması için lise ve üniversitelerde farklı kademelerdeki eğitim programlarının sayıları ve kapasitelerinin artırılması

sağlanacaktır. Ayrıca kamu ve özel sektör çalışanlarının yanı sıra aileler, gençler, çocuklar, yaşlılar, engelliler gibi toplumun farklı kesimlerinde siber güvenliğe ilişkin bilgi ve bilinç seviyesinin artırılması, önümüzdeki süreçte gerçekleştirilecek faaliyetler arasında yer almaktadır." vurgusu yaparak konuşmasını tamamlamıştır.

Ulak Haberleşme A.Ş. Teknoloji Geliştirme Genel Müdür Yardımcısı **Sayın Aziz SEVER**, "İletişim teknolojilerinin gelişimi, bu teknolojilerin her geçen gün daha çok insan için ulaşılabilir hale gelmesi beraberinde pek çok alanda dijitalleşmenin hayatımıza girmesini sağladı. İletişim altyapılarının sağladığı imkan sayesinde eğitimden sağlığa, kamu hizmetlerinden elektronik ticarete pek çok alanda alışkanlıklardaki değişimi çok kısa zamanda yaşadık. Dijitalleşmenin bu denli hızlı biçimde hayatımıza girmesi beraberinde birtakım riskleri de getirdi. Bunların başında da Siber Güvenlik gelmekte. Kullanıcıların servislere kesintisiz ve hızlı erişimini sağlarken aynı zamanda verilerin güvenliğini sağlamak kritik öneme sahip. Hem kullanıcı bilgilerinin hem de erişilen servislerin güvenliği bütüncül şekilde ele alınması gereken başlıklar. Kişisel verilerin mahremiyetinin korunması kişilere karşı bir yükümlülük olmasının yanında Milli güvenlik için risk oluşturabilecek kritik verilerin ve servislerin güvenliğinin sağlanması bir ülke için hayati öneme sahip. Bu sebeple iletişim altyapılarının ve siber güvenlik çözümlerinin yerli ve milli olması ülkeler için bir zorunluluk haline gelmiştir. " şeklinde görüşlerini belirtmiştir.

Sayın SEVER, "ULAK Haberleşme uçtan uca yerli ve milli iletişim altyapıları sloganı ile çıktığı yolda, geliştirdiği çözümlerin güçlü milli siber güvenlik altyapısının bir parçası olması için yoğun şekilde çalışmaktadır. Uçtan uca iletişim altyapısını oluşturan Erişim Şebekesi (Baz İstasyonu), Taşıyıcı Şebeke (SDN/NFV Maya çözümleri) ve Çekirdek Şebeke (Çınar 5G Çekirdek Şebeke) çözümlerinde artırılmış siber güvenlik yeteneklerini ürünlerin ayrılmaz bir parçası olarak değerlendirmektedir. Aynı zamanda MAYA SD-WAN çözümü ofisler arası ve bulut tabanlı servislere güvenli erişimi de garanti altına almaktadır. ULAK Haberleşme' nin diğer bir çözümü de Yazılım Tanımlı Veri Merkezi Çözümü MAYA SD-DC. Kurumların artan servis taleplerini karşılayabilmeleri için gerekli Veri Merkezi altyapılarını oluşturmalarına, kendilerine özel bulut mimarilerini kurgulamalarına olanak tanıyan Yazılım Tanımlı Ağ (SDN) tabanlı bir çözümdür. Bu çözümler yaklaşık iki seneden beri ülkemizdeki kurumlarımızın altyapılarında kullanılıyor. Bu çözümlerin daha fazla yaygınlaşması ve kullanılması en büyük temennimizdir." ifadelerinde bulunmuştur.

Mitsubishi Electric Fabrika Otomasyon Sistemleri Ürün Yönetimi ve Pazarlama Birim Müdürü **Sayın C. Tolga BİZEL**, "Mitsubishi Electric olarak sisteme faydalı olmayan yazılımların ve virüslerin fabrika otomasyon sistemlerine erişmesine engel olmak ve

önlemek için çalışıyoruz. Mitsubishi Electric, yeni siber saldırı tespit teknolojisi geliştirdi. Her yıl 300 milyon yeni virüs ortaya çıkıyor, bu nedenle tek tek virüsü tanımlamaya çalışan mevcut siber saldırı tespit teknolojisi şu anda çalışmıyor. Bilgisayar korsanları siber saldırılar için çok sayıda virüs kullansa da, ağ iletişim günlükleri aracılığıyla izlenen bilgisayar korsanlarının etkinliklerinin sayısı 50 civarında bulundu. Mitsubishi Electric'in patentli teknolojisi, bilgisayar korsanlarının faaliyetlerini belirleyebilir. Gelişmiş siber saldırılar için iyi bir çözümdür. Bir siber saldırı sırasında virüs, hedeflenen bir bilgisayara bulaşmak, saldırgandan komutlar almak, virüs bulaşmış bilgisayarı araştırmak ve ardından yasa dışı olarak faaliyetlerini daha da genişletmek için erişim haklarını elde etmek gibi çeşitli adımlar atmalıdır. Bu adımların her biri ayrıca bir dizi ilişkili davranış modeline sahiptir. Örneğin, virüs bulaşmış bir bilgisayarı araştırırken, saldırgan belgeleri arayarak, iletişim yollarını bularak ve güvenlik önlemlerinin yapılandırmasını kontrol ederek hangi bilgilerin nasıl elde edilmesi gerektiğini belirler. Mitsubishi Electric, yaklaşık 50 davranış modeli belirledi ve her biri için sistemin şüpheli etkinlikleri izlemesine ve bilgi sızıntısını önlemek için bir virüsü doğru bir şekilde tespit etmesine olanak tanıyan özel günlük analizi kuralları tanımladı. Her yıl yeni virüslerin sayısı astronomik olarak artarken, her yıl bir düzine ortak davranış modelinin gelişmesi bekleniyor. Bu modeller, tespit sistemine hızlı bir şekilde eklenebilir ve bu kalıptan yararlanma arayışında olabilecek tüm yeni virüsleri durdurabilir." ifadelerinde bulunmuştur.

Fortinet Sistem Mühendisleri Müdürü **Sayın İlker İMAMOĞLU**, "Oltalama saldırıları kamuda en çok karşılaşılan saldırı yöntemi. Son kullanıcılar için de oldukça tehlikeli bir saldırı. İnsan faktörü güvenlikte çok önemli noktalardan bir tanesi. Dünyadaki istatistiklere göre hala aldığımız e-postaların %50' si Spam. Bu spamların içerisinde de %90 oranında oltalama saldırıları oluyor. Kullanıcıların spam e-postalar içindeki oltalama saldırılarına tıklama oranları oldukça yüksek. İnsan faktörü çok önemli ve etkileri de çok geniş. Birkaç farklı noktada etkisi var. Birincisi parasal anlamda etki. İkincisi bizim için önemli olan bilginin kaybolması etkisi bir de insan hayatına değebilecek etkileri var. Mesela dünyada pandemi ile birlikte oltalama saldırılarının oranı artmaya başladı. Yaklaşık 4 milyar $' lık parasal karşılığı olan bir veri kaybından bahsediyoruz. Panelin de önemli noktalarından bir tanesi etkisel olarak da özellikle teknolojinin önemli bir unsuru enerji gerekliliği ve üretim. Oltalama saldırıları üretimi durdurabilecek ve/veya enerjiyi minimize edebilecek nitelikte olabiliyor. Dünyada da bu durumun örnekleri var; oltalama olarak gönderilen bir e-posta ile ülkelerin elektrikleri dahi kesilebiliyor; örneğin Ukrayna. Dolayısıyla aslında bu saldırılarda bizim gördüğümüz buz dağının görünen kısmı diyebiliriz. Burada atıfta bulunduğumuz önemli noktalardan bir tanesi kişinin eğitimli olması. Teknolojik olarak ne kadar yatırım yaparsanız yapın %100 güvenlik sağlanamayacağından yola çıkarsak kültürel olarak da siber güvenlik anlamında belli bir

bilince ulaşmamız gerekiyor. Fortinet olarak biz pandeminin başından beri hem giriş seviyesinde hem de ileri seviyelerde birtakım teknoloji eğitimlerini ücretsiz hale getirdik. Dünya üzerinde yaklaşık 1 milyon' a yakın kişiyi bu konuda sertifikalandırdık. Dünya ekonomik forumunda siber güvenlik eğitim hub' ının önemli destekçilerinden biriyiz. Güvenliğin diğer bir ayağı ise teknolojik kısmı. Fortinet siber güvenlikle ilgili teknolojik kısımda; mesela günlük 100 milyardan fazla veriyi inceliyor. Bu anlamda baktığınız zaman devasa boyuttaki büyük veriyi inceleyerek elde ettiği sonuçlarla, yapay zeka ve makine öğrenimi teknolojilerini de kullanarak kurumların ve müşterilerin saldırı öncesinde önlem almalarını sağlamaya çalışıyor. Dolayısıyla eğitim ve teknolojik kısımlar bizim Fortinet olarak sağladığımız hizmetler. Bir yandan da teknoloji ayağında şunu da eklemek lazım; biz ne kadar eğitimli olursak olalım hala insan faktörü ve bilinç seviyesi belli bir seviyenin üstüne geçemeyeceği düşüncesinden yola çıkarak teknolojiyi bu bağlamda da evriltmeye çalışıyoruz. Bu noktada Fortinet özellikle e-posta sistemlerini korurken aynı zamanda izolasyon dediğimiz birtakım teknolojilerle beraber kullanıcı o linke tıklasa bile olası riskin karantina alanında kalmasını sağlayacak bazı uygulamaları da kurumların kullanımına sunuyor." ifadelerine yer vermiştir.

Oturum-2: Yeni Normalde Siber Güvenlik Riskleri

Hacı Bayram Veli Üniversitesi Öğretim Üyesi Sayın Prof. Dr. Türksel Kaya BENSGHİR'in moderatörlüğünü yaptığı "Yeni Normalde Siber Güvenlik Riskleri" Oturumunda; Bilge SGT Genel Müdürü Sayın Burak ÇİFTER, Boğazici Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi Yöneticisi Sayın Doç. Dr. Bilgin METİN, EY Türkiye Şirket Ortağı ve Siber Güvenlik Hizmetleri Lideri Sayın Ümit Yalçın ŞEN, T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Birim Müdürü Sayın Salih TALAY, Türk Telekom Siber Güvenlik & Şebeke Güvenliği Grup Müdürü Sayın Selahattin Ahmet TOK ve TURKCELL Siber Savunma Müdürü Sayın Cihan YÜCEER konuşmacı olarak yer almıştır.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Siber Güvenlik Birim Müdürü **Sayın Salih TALAY**, "Yeni Normalde Siber Güvenlik Riskleri" konu başlıklı oturumda ulusal siber dayanıklılığı sağlamaya yönelik olarak 27 Temmuz 2020 tarihinde yayımlanan Bilgi ve İletişim Güvenliği Genelgesi ve genelge kapsamında verilen görev uyarınca T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi tarafından hazırlanan ve alanında ülkemize özgün ilk referans doküman olma özelliği taşıyan Bilgi ve İletişim Güvenliği Rehberi'nin önemine vurgu yapmıştır.

Sayın TALAY, Özellikle pandemi ile birlikte ivmelenen dijital dönüşümün yaygınlaştırdığı uzaktan çalışma sürecinin güvenliği konusunun, Bilgi ve İletişim Güvenliği Rehberi'nin 3. Bölümü olan "Varlık Gruplarına Yönelik Güvenlik Tedbirleri" içerisinde özel bir başlık

altında ele alındığını belirtmiş, Rehber kapsamında kurumların uygulaması gereken ilk tedbir maddesinin "Uzaktan Çalışma Politikasının Hazırlanması ve Uygulanması" hususunu içerdiğinin altını çizmiştir.

Oturumda, yeni normalde karşımıza çıkan siber güvenlik risklerine karşı alınması gereken tedbirlerin ve bu alanda toplumda siber güvenlik kültürünün yaygınlaştırılması konusundaki ihtiyacın, yerli ve milli siber güvenlik ekosistemi yetkinlikleri ile karşılanabileceğine vurgu yapan **Sayın TALAY**, bu kapsamda güçlü bir siber güvenlik ekosistemine sahip olmanın, hem salgın sonrası oluşan küresel ekonomik daralmadan çıkış, hem de haksız biçimde ülke olarak karşı karşıya kaldığımız uluslararası yaptırımlara karşı en büyük gücümüz olacağını belirtmiştir.

TURKCELL Siber Savunma Müdürü **Sayın Cihan YÜCEER**, "Dijital dönüşüm pandeminin etkisiyle son sürat hayatımızı değiştirmeye devam ediyor, tabii bu kültürel yaklaşım değişimlerinin sancılarını da kurumlar ve bireyler olarak yaşamaktayız. Her iş alanında inovatif bakış açısıyla fikirler ortaya koymak ve bunları aksiyona dönüştürüp ürün ya da hizmet olarak ete kemiğe büründürmek gerekmektedir. Burada bu inovatif işleri hayata alırken, kötü niyetli siber saldırganların da ekmeğine yağ sürülen kritik noktalar da artmaktadır. Saldırı yüzeyi gün geçtikçe artmakta ve bunları kontrol noktaları koyup takip edebilmek biz siber güvenlik ailesini oldukça zorlama devam etmektedir. Geliştirme ve operasyon süreçlerinin çok hızlı hale geldiği bu günlerde, araya güvenlik yaklaşımını koymak iş birimlerini tedirgin edebiliyor. Çevik mimariye geçiş, sprintlerde güvenlik

bakış açısının yer almasını sağlarken iş birimlerinin önünde bir engel gibi olmadan, onların bir parçası gibi hareket edecek süreç tasarımlarına ihtiyaç bulunmaktadır. Burada güvenlik bakış açılarının self servis şeklinde iş birimleri tarafından kullanılabileceği daha fazla otomasyon süreçlerini devreye alarak , servislerin geliştirilmesindeki hızı minimum etkileyerek siber güvenlik dayanıklılığını arttırabileceğimizi düşünmekteyim. Biraz daha net anlaşılması açısından örneklemem gerekirse; Zafiyet yönetimi ve yama yönetimi süreçlerini self servis ve otomasyona yönelik süreçlere dahil etmek, her agile ekibin kendi kendine bu süreci yönetmesini sağlayabilmek gerekir. Yine Agile iş yönetimdeki Jira akışlarında kaynak kod analizi süreçlerini otomatize ederek sürece align edebilmek siber güvenlik dayanıklılığını arttıracaktır." ifadelerinde bulunmuştur.

Sayın YÜCEER, "İşlerin akışlarını hızlandırabilmek için yine makine öğrenmesi yeteneklerini siber güvenlik süreçlerimize dahil etmemiz sağlıklı olacaktır. Zafiyetlerdeki false positiveleri ayıklama noktasında, kaynak kod analizindeki false positivelerin ayıklanmasında makine öğrenmesi tekniklerini kullanmak ciddi katma değer sağlayacaktır. Kurumların kendi ana işleriyle ilgilenmesi ve siber güvenlik süreçlerini outsource etmesi de kaçınılmaz bir nokta haline gelmiştir. Bu noktada yönetilebilir güvenlik servisleri hizmetlerimiz ile kurumlarımızın ana işlerine odaklanmalarını ve siber güvenlik dayanıklılıklarını arttırabileceğimizi düşünmekteyiz. 7x24 SOC izleme süreçleri, yönetilebilir SOAR hizmeti, vaka müdahale ve dijital forensic hizmetleri, yerli milli tehdit

istihbarat servislerimizin kullanılması kurumlarımıza ciddi katma değer sunmaktadır. Bildiğiniz üzere Siber Güvenlik Operasyon Merkezimiz ile kamu ve özel şirketlere hizmetler sunmaktayız. Birçok kurumumuzun uzaktan siber güvenlik operasyonlarını yönetmekteyiz. Covid19 süreciyle birlikte şirketlerin yönetilebilir güvenlik hizmetlerine ağırlık verecekleri bir dönemdeyiz. Bu noktada kurumlarımızın bu süreci en az hasar ile atlatılabilmesi için yardımcı olmaya hazırız. Pandemi sürecinde phishing saldırıları oldukça artmış durumdadır. Bu kapsamda da geliştirmiş olduğumuz Siber Tehdit İstihbarat Ürünümüz Bozok ile bu tarz phishing ve fraud saldırılarını en kısa sürede tespit edip müşterilerimize sunabilmekteyiz. Oltalama ve dolandırıcılık saldırılarında ne kadar hızlı olabiliyorsanız o kadar başarılısınız. Ulusal Siber Güvenliğe de katkı anlamında da mobil ve sabit internet kullanıcılarımız için geliştirdiğimiz Turkcell Dijital Güvenlik Servisi ile bireysel siber güvenlik hizmetini sunmaktayız. Bu hizmete abone olan bireysel kullanıcılarımızı siber saldırılardan ve dolandırıcılık olaylarından en az hasar almasını sağlamayı hedeflemekteyiz." görüşlerini belirtmiştir.

Bilge SGT Genel Müdürü **Sayın Burak ÇİFTER**, "Siber güvenliği ele alırken tehditler ve riskleri bir arada değerlendirerek risk yönetimi çerçevesinde yaklaşmak gerekmektedir. Tehditlere yönelik tedbirlerin alınması ve planlama yapılması için oturmuş risk yönetimi metodolojileri kullanılması gerekmektedir. Siber güvenlik çerçeve çalışmalarının teknik çözümlemelerinden faydalanırken, risk yönetimi üst çerçevesinin kullanılması ve bu teknik çözümlemelerin metodolojik olarak risk yönetim planları içerisinde tehditleri ele alırken kullanılması, ikincil hatalar dahil birçok konunun planlı olarak ele alınmasını sağlayacaktır." olarak görüş belirtmiştir.

Sayın ÇİFTER tarafından, özellikle pandemi dönemi uzaktan çalışma, ortak çalışma, video konferans teknolojileri alanında birçok yerli ar-ge ve ürün geliştirme faaliyeti gerçekleştirildiği, bu faaliyetlerle elde edilen teknolojik birikimin farklı ürünler ve çözümler geliştirmek üzere kullanılması amacıyla kullanılmasının yenilikçi teknoloji üretiminde verimliliği arttıracağı ifade edilmiştir.

Türk Telekom Siber Güvenlik & Şebeke Güvenliği Grup Müdürü **Sayın Selahattin Ahmet TOK**, "Pandemi sürecinin başlaması ile birlikte en önemli kriterleden biri insanların uzaktan erişim ihtiyaçlarının karşılanması dolayısıyla kapasite ihtiyacı sıkıntısının karşılanmasıydı. Çoğu kurumun uzaktan erişim alt yapısı vardı ancak daha çok ihtiyaç durumunda kullanılması yönündeydi. Bu süreçte herkes uzaktan işlerini halledebilsin şekline dönüştü ve sektörde çoğu kurum da bunu çok hızlı bir şekilde çözdü. Fakat bu durumun bize getirdiği bazı sıkıntılar söz konusu oldu; sunulan çözümlerin çok hızlı bir şekilde sunulması anlamında erişim yönetimi çok önemli, yani sadece insanları çok hızlı eriştirelim mantığıyla erişim sağlamak belki peşinde atak düzeni genişletme gibi bir sonuç

doğurabilirdi. Burada yapılar, değerlendirmeler önemli ve bu durum siber güvenlik ekiplerine sonradan binen yüklerden bir tanesi oldu, ihtiyaçları doğru değerlendirmek anlamında. Tabii sadece uzaktan erişim sağlamakla bitmiyor bazı ekiplerin işleri dijitalleşmeye de müsait olmayabiliyor, bu konuda bir ön çalışma başlamıştı ama pandemi bu süreci daha da hızlandırdı. Şunu da söylemekte fayda var aslında birçok uygulama ve çözüm ekibi böyle yeni ihtiyaçlar oluştuğunda siber güvenliğe gelerek çözüm arama noktasında bilinçlenmişler, aslında bu memnuniyet verici bir durum. Siber güvenliğe gelmeleri iyi bir şey ama bu da siber güvenliğe ek iş yükü olarak dönüyor. Bu tip çözümleri de uygulama ekipleri ile gerçekleştirmiş olduk. O dönemde ciddi bir iş yükü binmiş oldu ve bence hala da devam ediyor, çünkü süreç devam ediyor. Yeni normal diyoruz ama bence hala devam ediyoruz, yeni normali daha sonra görebileceğiz. Belirttiğim gibi bu tip hızlı aksiyonlar riskleri de beraberinde getiriyor ve bunları doğru yönetmek lazım. Bu süreçte siber saldırılarda artış var. Oltalama maillerinin arttığını gördük. Ayrıca, uzaktan end pointlerin takibi biraz daha zorlaştı, herkes ofisteyken end pointlerdeki log takiplerini yapmak, onları networkten takip etmek biraz daha kolaydı. Şimdi herkes evlerine gitti ve bu trafikleri takip etmek siber güvenliğin uğraş alanlarından biri oldu, Tabii çözümler de bu anlamda gelişiyor, iyi çözümlerimiz var fakat bunları doğru yönetemediğiniz durumda ciddi risklerle karşı karşıya kalınıyor." şeklinde görüş belirtmiştir.

Sayın TOK, " Önümüzdeki süreçte bizi siber güvenlik anlamında çözmemiz gereken birçok konu bekliyor. Machine learning, yapay zekadan bahsettik. Şu an hali hazırda yaşamakta olduğumuz uzman kaynak sıkıntısının da bir nebze çözümü olacaktır. Türk Telekom olarak ileri dönüşüme önem vermeye başladık. Siber güvenlik alanında yerlileşme gerçekten çok önemli ve değinildiği gibi bunun sadece ülke sınırları içinde kalmayıp küresel seviyede olmasını sağlayacak şekilde yerli siber güvenlik çözümlerine biraz daha eğilmemiz gerekiyor. Türk Telekom olarak öncelik verdiğimiz birkaç çalışma da var bu anlamda. Bir diğer konu kaynakların verimli kullanılması. Yerli siber güvenlik çözümleri konusunda çalışan bir çok Start Up'lar var ülkemizde. Fakat bunların arasında bir koordinasyon ihtiyacı var kaynakların daha verimli kullanılması anlamında. Diğer yandan genel düşüncemiz sadece ürün alıp koymakla siber güvenlik sağlanamıyor, doğru süreçlerin oluşturulması ve doğru insan kaynağı ile yönetilmesi gerçek anlamda bir koruma sağlıyor. Sektörde çok iyi siber güvenlik hizmeti veren firmalar var. Kurumların altyapılarını kuvvetlendirip ya da altyapı yatırımlarını yapıp bunlara doğru süreç ve doğru insan kaynağı ayrılmadığı noktada tavsiyemiz hizmet olarak almaları olacaktır. Gerçek anlamda güvenlik aslında insan, teknoloji ve süreç üçgeninin oluşmasıyla sağlanabilen bir olgu. Bir tanesi bile atlandığında yetersizlik söz konusu oluyor. Bu yüzden hizmet olarak değerlendirme konusuna da dikkat çekmek gerekiyor." ifadelerine yer vermiştir.

Boğazici Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi (BÜSİBER) Yöneticisi **Sayın Doç. Dr. Bilgin METİN**, "BÜSİBER Boğaziçi Üniversitesi Siber Güvenlik Merkezi (www.siber.boun.edu.tr) olarak 4 yıldır yerli milli ekosistemine destek vermeye çalışıyoruz. Bu zamana kadar 10 adet üniversite öğrencileri için ücretsiz yaz ve kış siber kampları düzenledik. Akademik olarak burada yerli milli siber güvenlik çözümlerine farklı açılardan yaklaşılması gerektiğini ortaya koyduk. Konuya yalnızca teknik değil işletme açısından bakarsak ürün geliştirmek kadar mevcut ürünlerin dağıtım ağlarına oluşturmak da son derece önemli. Ek olarak yerli-milli ürünlerin yaygınlaşması için daha okul sıralarında bu ürünler kullanılarak eğitim verilmesi ve öğrencilere zihnindeki olası yerli ürünlere karşı olabilecek bariyerlerin erken dönemde yıkılması gerekiyor. Bu zirvenin son gününde 20 Şubat 2021 tarihinde BÜSİBER TBD ile beraber bir Siber Güvenlik CTF yarışması da düzenledi. Yetenekli gençlerin kendilerini ifade etmesine ve göstermesine olanak tanıdı. Bu faydalı etkinlik ve sektöre sağladığı katkılardan ötürü TBD' ye teşekkür ediyoruz." ifadelerinde bulunmuştur.

Oturum-3: Yapay Zeka Destekli Siber Dayanıklılık

BTK Bilgi Teknolojileri Daire Başkanı Sayın Bülent ARSAL'ın moderatörlüğünü yaptığı "Yapay Zeka Destekli Siber Dayanıklılık" oturumunda; Trend Micro Satış Müdürü Sayın Gökhan ÇÖREKÇİ, TÜRKSAT Kurumsal Bilgi ve Siber Güvenlik Yönetimi Direktörü Sayın Mehmet Ali ERKUL, ODTÜ Siber Güvenlik Bölümü Öğretim Üyesi - INVICTA Ar-Ge Ltd.Şti Yönetici Ortağı Sayın Dr. Attila ÖZGİT ve THY A.O. Kurumsal Gelişim ve Bilgi Teknolojileri Strateji ve Yönetişim Başkanı Sayın Kadir YILDIZ konuşmacı olarak yer almıştır.

Oturum moderatörü BTK Bilgi Teknolojileri Daire Başkanı **Sayın Bülent ARSAL**, "Son yıllarda, veri barındırma kapasitelerinin artması ve internet hızlarının yükselmesi ile işlenmeye hazır çok fazla veri oluşmaya başlamıştır. Bu sayede yapay zeka uygulamaları, bu veri ile beslenerek, insan beyninin ifa etmekte zorlanmadığı fakat sayısal mantık ile idrak edilmesi güç olan görüntü ve ses tanıma, objeleri gruplama ve hatta müzik ve resim yapmak gibi yeteneklere kavuşmuş olup yapay zekanın alt dallarından olan Makine Öğrenmesi son yılların en hızlı gelişen bilimlerinden olmuştur. Yapay Zeka ve Makine Öğrenimi algoritmaları hayatımızın her alanında mevcut bulunmaktadır. Telefonlarımızda kullandığımız sesli komut sistemleri, reklam uygulamalarının kişiye özel tavsiyeleri, finans sektöründe otomatik alım-satım yapan uygulamalar ve hatta trafikte kendi kendine seyredebilen otonom araçlar yapay zeka ürünleridir. Siber güvenlik alanında, siber dayanıklılığın arttırılması amacıyla da yapay zeka kullanılmaktadır. Zararlı yazılım tespiti için klasik yöntemler ile beraber makine öğrenmesi algoritmaları yer almaktadır. Yapay zeka ile ağ trafiğinin dinlenmesi

aracılığıyla siber saldırı tespiti de uygulanabilirliği kanıtlanmış önlemler arasındadır. Spam yani istenmeyen e-postaların engellenmesinde, çok uzun yıllardır makine öğrenmesi algoritmaları kullanılmaktadır. DDOS saldırılarını engelleyen sistemler de yapay zeka uygulamalarına iyi bir örnek teşkil etmektedir. Bununla birlikte davranış analizleriyle anomaliler tespit edilip uyarı/alarm mekanizmaları işletilmesi yapay zeka uygulamaları ile mümkün ve sürekli hale gelmiştir.” şeklinde görüşlerini belirtmiştir.

Sayın ARSAL “Ayrıca anonim hesapların yazım analizi aracılığı ile kişisel hesaplarının tespitini sağlayan, olası terör eylemlerini saptayan, sosyal medya aracılığıyla topluluk tespiti yapan ve benzeri diğer açık kaynak istihbaratı uygulamalarında, yapay zeka algoritmalarının başarıyla faaliyete geçirildiği görülmüştür. Video kategorizasyonu ile, yetişkin içerik tespiti başarıyla yapılabilmektedir. Sosyal medya şirketleri, bu yapay zeka algoritmalarını aktif olarak kullanmaktadır. Güncel yapay zeka uygulamalarının faydalı çalışabilmesi için en öncelikli gereksinim verinin çokluğudur. Ne kadar çok veri olursa, algoritma o kadar iyi öğrenecektir. Verilerin bütünlüğüyle tutulması gerekmemekte olup gerekli anonimizasyon ve ayıklama işlemlerinin ardından saklanması da yeterince faydalıdır. Ham veri içerisinden çıkarılacak anlamlı parçaların saklanması, gelecekte yazılabilecek başarılı yapay zeka algoritmaları için zemin oluşturacaktır. “ ifadeleri ile konuşmalarını tamamlamıştır.

Trend Micro Satış Müdürü **Sayın Gökhan ÇÖREKÇİ**, "Yapay zeka finans, sağlık, tarım, eğitim, ulaşım gibi birçok sektörde, bir çok uygulamada kullanılmaktadır. Veriyi ne kadar doğru işlersek tüm sektörlerimizde verimliliğe katkısı o kadar iyi olacaktır. Veriyi yanlı ve taraflı işlersek çıkan sonuçlarda hayatı negatif yönde etkileyecektir. Bu anlamda veriyi işleyen veri analistlerinin çok ciddi sorumlulukları bulunmaktadır. Günümüzde teknolojik gelişmelerin hızlanması ve 5G Teknolojisinin hayata geçmesiyle, internete bağlı cihaz sayısı 18 milyarı bulmakta ve çok fazla veri dünyada dolaşmaktadır. Verilerimizin güvenliğine olan ihtiyaç da gün geçtikçe artmaktadır. Günde 39 saniyede bir siber saldırının olduğu dünyamızda artık siber güvenlik katmanlarının çok iyi tasarlanması, çözümlerin çok iyi performans göstermesini zorunlu kılmaktadır. Trend Micro siber güvenlik çözümlerimizde yapay zeka katkısını oldukça fazla kullanmaktayız. Biz çözümlerimizde çok katmanlı bir güvenlik yaklaşımı ile birlikte tehdit ortamına tam bir bakış sunmaktayız, 360 derece koruma sağlamak, gelen bir atağın tüm sistemden arındırılmasını hedeflemekdir. Bu 360 derece korumayı sadece tesisler de değil bulut yapılarında da çözüm olarak sunuyoruz. Bu tür hibrit çözümlerde, altyapılara uygun şekilde uyum ve entegrasyon sağlamış oluyoruz. Bu çözümler sayesinde özellik farketmeksizin tespit koruma, aksiyon alma imkanı sunuyoruz. Farklı segmentlerdeki ürünlerimiz üzerinden tek bir noktada istihbarat paylaşımı yaparak bağlaşık tehdit koruması (connected threat defense) sağlayabiliriz." ifadelerinde bulunmuştur.

"Sayın ÇÖREKÇİ "Kod aşamasındaki zaafiyetlerin tespit edilmesi çok önemli, daha önce kullanılmış yazılmış kod parçacıklarında zararlı barındırabilen yazılımlar olabilir, açık kaynak kodlarda dışarıdan saldırılara mağruz kalabiliriz. Açık kaynak kodlardaki güvenlik açıklıklarını otomatik olarak bulan uygulamaların bu dijital dönemde çok önemli olduğunu düşünüyorum. Bu kod parçacıklarıyla üretilen her uygulama açıklık oluşturabilir. Smartcheck teknolojisi bu kodlar üzerinde zaafiyat var mı bunu araştırıp raporlamamıza olanak sağlar. Derin Güvenlik Konteyneri koruyabiliriz. Kötü amaçlı yazılımları ayrıntılı olarak inceler ve güvenlik açıklıklarını kapatır. Derin Güvenlik teknolojisi bu kodlar üzerinde zaafiyatleri bulur ve kapatır. Bu teknolojimizle, Konteyner yaratılmadan önce yapılan analiz ve konteyner yaratıldıktan sonra konteyner ve sunucuyu koruyabiliriz. Sunucuların güvenliği çok önemli buralarda yapılan güncellemelerden kaynaklı zaafiyetlerin önüne geçebilmek için sanal yama özelliği kullanılmalıdır. Ağ üzerinde oluşabilecek anomalilerin tespiti için ağ analitik ürünleri konumlandırılmalıdır. İkinci olarak da, birinci maddeyi yakından ilgilendiren, SOC (security operation center); SOC ekipleri, güvenlik olaylarının zamanında tespit edilmesi ve aksiyon alınmasını sağlamak için kritik öneme sahiptir. Bu merkezlerde tehdit analizler için"Makina öğrenme ve siber istihbarat teknolojilerinin" kullanılması önemli, Tehditlerin otomatik olarak kontrol altına alabilmek için SOAR teknolojilerinin kullanımı önemli, bu

çözümlerimiz her birinde yapay zeka teknolojisini doğru kullanarak, koruma anlamında dinamik ve güvenilir bir çözüm sunmaktayız. Siber dayanıklılık için, çözümlerimizde yapay zeka teknolojisini çok doğru kullanmalıyız, insan faktörünü unutmamamız gerekiyor, bu cihazları kullanan insanlarımızı bilinçlendirip geliştirmeliyiz, ayrıca sistemlerimizde ürünler arası entegrasyonun çok iyi olması gerekmekte ve siber güvenlik için kurumsal yapıların oluşturulup geliştirilmesi de çok önemlidir." sözleriyle konuşmalarını tamamlamıştır.

THY A.O. Kurumsal Gelişim ve Bilgi Teknolojileri Strateji ve Yönetişim Başkanı **Sayın Kadir YILDIZ**, oturumda yaptığı konuşmada "Siber Dayanıklılık kavramı sahada yaşanan gerçekliğin kavramsallaşmış hali olarak hayatımıza girdi. Siber saldırıların ve zafiyetlerin hiçbir zaman yok olmayacağı gerçeği artık alınacak önleme tedbirleri yanında toparlanma ve hizmete devam edebilme kabiliyetlerimize de odaklanmamız gerektiğini öğretti. Bu bağlamda Siber Dayanıklılık kavramı tüm resmi ifade etmesiyle anlam bulmuş oldu. Siber güvenlik dünyasında daha yoğun olan ve insan bağımlı analiz, yorum ve karar verme yeteneklerinin yapay zekâ fonksiyonları ile yerine getirilebilmesi önemli bir eşik. Saldırı teknikleri içerisinde de yapay zekâ kullanımının doğal olarak var olacak olması ise mücadelenin boyutlarını artırarak daha asimetrik bir yapıya büründürecektir. Özellikle olay müdahale ve denetim süreçlerinde verimliliği inanılmaz şekilde artıracak olan yapay zeka teknolojisinde doğru adımların atılabilmesi ve ülke olarak öncü olunabilmesi için merkezi bir yönlendirme-denetim mekanizmasının devreye alınması şart. Yapay Zeka konusunda kadim tartışma konusu olan süreçlerde insan ihtiyacının ortadan kalkması ise

en azından kısa vadede gerçekçi görünmüyor. Klasik teknolojilerden çok daha fazla veri ile ancak çok daha doğru sonucu kısa sürelerde servis edebiliyor olsa da Siber Güvenlik gibi disiplinler arası bir dünya da insan kararına her zaman ihtiyaç duyulacaktır. Siber Güvenlik personeli madencilik yapmak yerine ortaya konulan cevheri işleyen sanatçılara dönüşecektir. Ütopik senaryolarda geçen makinaların insanlığı ele geçirmesi ise; kullandıkça aynı kaynaklarla kapasitesini artırabilen insan beyni seviyesinde bir teknoloji icadına kadar mümkün olamayacaktır. 70'lerde sanayileşme için hedef olarak belirlenen "makine yapan makineleri bizzat yapmadıkça makineleşmenin esaret olacağı" fikrinden hareketle "Yapay Zeka" teknolojisi ülkemiz açısından fırsat olarak değerlendirilerek; bu alanda olmayan bir teknolojiyi icat ediyor olmasak da muhakeme ile karar veren sistemler, "kod yazan kod" geliştirmek hedeflenmelidir." ifadelerini kullanmıştır.

TÜRKSAT Kurumsal Bilgi ve Siber Güvenlik Yönetimi Direktörü **Sayın Mehmet Ali ERKUL**, "Siber saldırıların yapay zekâ destekli olarak savunma sistemlerini atlatacak şekilde tasarlandığı bir dünyada olay müdahale süreçlerinde de yapay zekâ kullanımının operasyon verimliliğine katkı sunacağını düşünüyoruz. Bu bağlamda güvenlik operasyonlarının daha etkin işletilmesi için yapay zekâ içerikli çözümlerin konumlandırılması ile çalışmalarımız devam ediyor. Yapılan ön değerlendirme çalışmaları kapsamında toplanan tüm telemetri sinyalleri üzerinden anormal davranışları tespit edip doğru olaya hızlı müdahale imkânı sağladığını gördüğümüz teknolojilere gerekli yatırımları yapıyoruz. Bugün kamu kurumlarının sunduğu 1250 hizmetin önünde kimlik doğrulama için e-Devlet Kapısı kimlik doğrulama hizmeti kullanılmaktadır. E-devlet Kapısı'nda kullanıcıların parola dışında kullanabilecekleri 4 farklı kimlik doğrulama mekanizması mevcuttur. Ayrıca haziran ayında 2 faktörlü kimlik doğrulama süreci başlatılacaktır. Kimlik doğrulama hizmetinin davranış analizi kabiliyeti kazandırılması 2021 planlarımız arasındadır. Yapay zekada modeli eğittiğiniz verinin kalitesi ne kadar önemli ise bu verinin kişisel ve kurumsal anlamda gizliliği de bir o kadar önemli. Yazılım geliştirme süreçlerinin Devops'a kaydığı günümüzde test verilerinin güvenliği ve gizliliği ile ilgili de çalışmalar yapmak gerekiyor. Toplanan verilerin hem KVKK vb. regülasyonlara uyumu hem de analitik çalışmaları desteklemesi için kendi geliştirdiğimiz maskeleme çözümleri mevcut. Ayrıca verinin yaşam döngüsünü daha dinamik şekilde yönetme ile ilgili çalışmalarımız devam ediyor." şeklinde görüş bildirmiştir.

ODTÜ Siber Güvenlik Bölümü Öğretim Üyesi ve INVICTA Ar-Ge Ltd.Şti Yönetici Ortağı **Sayın Dr. Attila ÖZGİT**, "Yapay zeka çok büyük bir şemsiye kavram. Çoğu kez terminaloji kargaşasıyla kullanılabiliyor, zaman zaman içi boşaltılsa da yapay zekanın alt bileşenlerinden makine öğrenmesi ve büyük veri kavramları oldukça öne çıkıyor ve aslında birlikte hareket eden kavramlar. Makine öğrenmesi; istatistiki yöntemlerle

öğrenerek iyileşen performansı arttıran algoritmalar oluşturuyor. Bunu yapabilmenin yolu da büyük veriden geçiyor. Büyük veri olmadan makine öğrenmesiyle yapay zeka uygulamaları üretmek pratik olarak çok mümkün değil. Dolayısıyla elinde küçük verileri olan kuruluşların yapay zeka geliştirdiği iddialarını çok hayalci buluyorum. Diğer taraftan büyük veriyi elinde tutan kurumlarımızın kabaca Telekom operatörleri ve bir grup diğer uygulama çalıştıran kurum ya da kuruluşlar olduğunu biliyoruz. Bu verinin güvenilir ellerde temizlenerek yani kişisellikten arındırılmış ama erişim örüntülerini içinde barındıran veriyi ortak bir yerlere yerleştirip bunların üzerinde algoritma yarıştırma noktasına gelmemiz gerekiyor ülke olarak. Çünkü eski deyişle kerameti kendinden menkul algoritmalarla ben çok iyi bir algoritma yazdım diye ortaya çıkanların arkasında hangi veriyle bunu yaptığını bilebilmek lazım. Akademik herhangi bir konuda çalışırken bile yeni algoritmada bir üleştirme yaptık, şu şu nedenlerle şunlardan daha iyi dendiğinde biz hocalar olarak soracağımız ilk soru "peki hangi veri kümesiyle yaptın, o kendini karşılaştırdığın "A" uygulamasıyla aynı veri kümesini kullandın mı ki kendi başarını daha önde görüyorsun" gibi sorulardır. Dolayısıyla güvenilir kaynaklarda sanitize edilmiş, içinde bireysellik taşımayan, ama saldırı patternlarını çok net gösteren veri kümelerini bir yandan oluşturup, bir kenarda barındırıp bunu da uygun yöntemlerle yarışan algoritmalara açan bir yapıyı bence ülke olarak kurmak durumundayız. Bunu kurmadığımız takdirde sürekli içi boş kavramlarla ben daha iyi yapay zeka yapıyorum diyen örneklerle karşılaşacağız. Yapay zeka bu bağlamda kaçınılmaz bir gidiş ve elimizdeki büyük ölçekli veriye de çok büyük ölçekte dayanıyor. Dolayısıyla bu sağlandığı takdirde ancak sağlıklı, verimli ve işe yarar uygulamaları çıkarabileceğiz. Bu işin biraz da akademik yönü. Yani veri olmadan kaliteli algoritma üretmek mümkün değil. Veriyi de bir biçimde herkes elinde barındıramıyor. Sanitization dediğimiz konu akademik dünyada üzerinde çok çalışılan bir konu. Mesela network verisini sanitize etmiş olarak tutan hazır veri setleri var dünyada. Bunları benzer şekillerde saldırılarda da kullanmak mümkün. Yapay zekanın en önemli katkılarından biri anlamlı sonuç çıkartacak algoritmalarımız elimizde olursa yaşanan kriz anlarında da çok daha rahat ederiz. Büyük veriye bakıp ordan anlam çıkartabilmek ve o anlamı kaliteli bir anlam olarak yöneticinin önüne alternatif bir aksiyon planı olarak sunabilmek yapay zeka uygulamalarının çok önemli bir ayağı olacak bu türden saldırılarda dayanıklılığı arttırmak adına. Dayanıklılık dediğimiz zaman o bizi kademeli savunma dediğimiz yere getiriyor. Biz hep savunmanın yüzeyini daraltmaktan bahsediyoruz, ama bazen saldırılar volümetrik olabiliyor ve saldırı yüzeyi çok geniş olabiliyor. Dolayısıyla yapay zekanın karar verme noktasında son derece önemli bir unsur olduğunu düşünüyorum. Ancak içi boş, benim yapay zekam seninkini döver gibi yorumlara karşı da bir bilinç geliştirmemiz gerekiyor diye düşünüyorum." ifadelerini kullanmıştır.

Oturum-4: Kuantum Sonrası Dijital Güvenlik

ODTÜ Öğretim Üyesi Prof. Dr. Melahat Bilge DEMİRKÖZ'ün moderatörlüğünü yaptığı "Kuantum Sonrası Dijital Güvenlik" Oturumunda; 19 Mayıs Üniversitesi Öğretim Üyesi Sayın Doc. Dr. Sedat AKLEYLEK, ODTÜ Öğretim Üyesi Sayın Doc.Dr. Murat CENK, Havelsan Siber Güvenlik Grup Lideri Sayın Dr. Mert ÖZARAR ve ASELSAN HBT- Kripto ve Bilgi Teknolojileri Program Direktörlüğü Lider Mühendisi Sayın Dr. Sinan ŞENOL konuşmacı olarak yer almıştır.

Oturumda kuantum bilgisayarların klasik bilgisayarlara göre farklılıkları ve üstünlüğü, bu bilgisayarların şu andaki genel durumu, klasik bilgisayarlar ile çözümü zor olan hangi tip problemlerin kuantum bilgisayarları ile kolaylıkla çözüldüğü ve bu tip bilgisayarların siber güvenliğe olan etkileri üzerine konuşulmuştur. Ayrıca, kuantum bilgisayarların kriptografi alanına etkileri ve bunların siber güvenlikteki hangi alanları tehdit ettiği konusu detaylandırılarak bu tehditleri ortadan kaldırmak için yapılan çalışmalar üzerine bilgiler verilmiştir.

Oturuma moderatörlük yapan **Sayın Prof. Dr. Bilge DEMİRKÖZ**, Word Wide Web ilk başta savunma sanayiinde kullanılmak amacıyla geliştirilmiş olsada bugün en çok sosyal medyada kullanılmaktadır. Kuantum bilgisayarlarda doğal olarak önce savunma sanayinde kullanılmaya başlayacak ama ekonomik en büyük etkisi ise şüphesiz ki dünya ekonomisin % 60'nı oluşturan malzeme ve kimya alanına olacaktır ifadelerinde bulunmuştur. **Sayın DEMİRKÖZ**, ayrıca bir çok malzemenin önce bilgisayarlarda

hesaplandığını, örneğin uçaklarda kullanılan aleminyum alaşımının önce malzeme bilimcileri ve kimyagerler tarafından benzetimlerinin yapıldığını, gene uçakların uçtuğu zaman arkasında bıraktığı türbülansın benzetiminin yapıldığını, bunun gibi problemlerin çözümünün kuantum bilgisayarlar için çok kolay olacağını, çünkü özellikle kuantum bilgisayarların differansiyel denklemleri çözmede çok iyi olduklarını, özelliklede yapay zeka ağları üzerinde söz konusu işlemleri yapmada çok daha iyi olacaklarını belirtmiştir.

Sayın DEMİRKÖZ, "Kuantum bilgisayarların evimize girip girmeyeceği konusunda da Fizikçi olarak bir katkı sağlamak istiyorum. IBM yaklaşık 1.5 ton ağırlığındaki ilk klasik bilgisayarı piyasaya çıkardığında ve bunları kamyonların arkasında şirketlere göndermeye başladığında bu bilgisayarların evlere kadar ulaşmayacağı söyleniyordu. Şu anda hepimizin cebinde yer alıyor. Hatta nesnelerin internetide (IoT) bu kapsamda sayılabilir. Aynı şekilde bugün kuantum bilgisayarlar olmasa da kuantum işlemcilerin evimize hibrit bilgisayarlarlar aracılığıyla gireceğini düşünüyor. Bu konuda Intel gibi yatırım yapan firmalar var. İntel silikon teknolojisine çok fazla yatırım yapmış bir şirket. Nasıl GPU'lar görüntü işlemeye özel kullanılyorsa Kuantum CPU'ların da hibrit bilgisayarlarda bazı özel işlemler için kullanılabileceği öngörülüyor. Yaklaşık 50-60 yıl içerisinde." İfadeleri ile konuşmasını tamamlamıştır.

19 Mayıs Üniversitesi Öğretim Üyesi **Sayın Doc. Dr. Sedat AKLEYLEK**, "Kuantum kriptografi, kuantum mekaniği ile bu yapıya uygun kriptografik teknikleri uygulamaya dayanmaktadır. Özel bir altyapıya ihtiyaç duyan kuantum kriptografi ile anahtar paylaşımı problemine bir çözüm sunulmuştur. Kuantum sonrası kriptografi ise günümüz bilgi ve iletişim teknolojilerinde de kullanılabilecek, matematiksel olarak zor problemlere dayanan ve herhangi bir özel uygulama platformuna ihtiyaç duymayan sistemleri barındırmaktadır. Kuantum sonrası kriptosistemleri ile açık anahtarlı şifreleme, elektronik imzalama, özet alma ve anahtar paylaşımı problemlerine güvenilir çözümler bulunmuştur. Kuantum sonrası kriptografi konusundaki araştırmalar matematik, istatistik, bilgisayar bilimleri, fizik gibi alanları barındıran disiplinlerarası çalışmalar içermektedir. Kuantum bilgisayarlara karşı dirençli algoritma/protokol ve sistem tasarımı zor matematiksel problemlere ve bunların uygulamasına dayandığı için ihtiyaç duyulan en önemli kaynağın araştırmacı olduğu düşünülmektedir. Buna ek olarak, üzerinde çalışılan konuların doğruluğunu ve verimliliğini göstermek için bazı cihazlara ihtiyaç olmaktadır. Ülkemizde, bu kapsamdaki çalışmaların artması ve öncü konumuna gelinebilmesi için hem nitelikli insan gücünün hem de ilgili ürünlerin farklı merkezlere kazandırılması önem arz etmektedir. Kuantum kriptografi ve kuantum sonrası kriptografi konularına yakın gelecekte desteklerin sağlanması gerekliliği değerlendirilmiştir." şeklinde görüşlerini belirtmiştir.

ODTÜ Öğretim Üyesi **Sayın Doc. Dr. Murat CENK**, Kuantum sonrası kriptografi çalışmaları ile ilgili bilgiler vermiştir. **Sayın CENK** "NIST (National Institute of Standard and Technology) tarafından, 2015 yılında kuantum bilgisayarlarındaki gelişmelerden dolayı, şu anda uygulamalarda kullanılan açık anahtarlı sistemlerin yerine kullanılmak üzere, kuantum güvenli yeni algoritmaların standartlaşma sürecine girmiştir. Bu sürecin amacı, 2024 yılına kadar kuantum güvenli olan yeni imzalama ve anahtar kapsülleme algoritmalarını standartlaştırmaktır. Buradaki yaklaşım, tüm dünyadan algoritma başvurularını alarak, yarışma benzeri bir süreçle günlük hayat uygulamalarında kullanılabilecek kuantum güvenli yeni algoritmaların standartlaştırılmasıdır. 2017 yılının kasım ayında başvuru sureci sona ermiş ve toplam 82 başvuru yapılmıştır. Bu algoritmaların 69 tanesi şartlara uygun bulunmuş, daha sonra bunların da 4 tanesi süreçten çekilmesinden dolayı, toplam 64 algoritma birinci tur aday olarak değerlendirmeye alınmıştır." ifadelerinde bulunmuştur.

Sayın CENK, TBD ile birlikte "Kuantum Bilgisayarlar ve Siber Güvenlik" konulu bir rapor hazırladıklarını belirtmiş ve "Açık anahtarlı kriptografi internet güvenliğinden sayısal imzalara, nesnelerin internetinden iletişim güvenliğine kadar birçok uygulamada güvenlik sağlayan yapı taşlarının başında gelmektedir. Bu sistemlerde kullanılan kriptografik algoritmalar; tamsayı çarpanlarına ayırma kriptografisi, sonlu cisim kriptografisi ve eliptik eğri kriptografisidir. Bu algoritmaların güvenlik seviyeleri artık

tartışma konusu olmuştur. NIST tarafından standartların değiştirilmesi amacıyla başlatılan çalışmaların 2024 yılının sonuna doğru tamamlanması ve bu yeni standardın kullanılmaya başlanması beklenmektedir. Bu tarih gelmeden önce kuantum saldıralarına karşı zaafiyeti olan kriptografik algoritmaların kuantum güvenli olanları ile değiştirilmesi üzerine çalışmaların başlatılması önemlidir." Şeklinde görüş belirterek konuşmasını sonlandırmıştır.

Oturum-5: Dijital Oyunlar Siber Güvenlikte Bir Açık Mıdır?

KVKK İkinci Başkanı Sayın Cabir BİLİRGEN'in moderatörlüğünü yaptığı "Sosyal Medya ve Dijital Oyunlar Siber Güvenlikte Bir Açık mıdır?" Oturumunda; Akaydın Hukuk Bürosundan Sayın Av. Ceyda CİMİLLİ AKAYDIN, Vodafone Siber Güvenlik Müdürü Sayın Gökhan BOZDOĞAN, KVKK Veri Güvenliği ve Bilgi Sistemleri Dairesi Başkanı Sayın Ersin CAN, TBD Onur Kurulu Üyesi Sayın İ. İlker TABAK ve Ankara Üniversitesi Tıp Fakültesi Öğretim Görevlisi Sayın Prof. Dr. Betül ULUKOL konuşmacı olarak yer almıştır.

Ankara Üniversitesi Tıp Fakültesi Öğretim Görevlisi **Sayın Prof. Dr. Betül ULUKOL**, "Çocukların elinin altında olan ve siber güvenlik açığı doğurabilecek unsur tabii ki dijital oyunlar öncelikle. Çünkü mesajlaşma programları, sosyal medya etkinlikleri biraz daha ileri yaşların kullandığı alanlar. Ama çocuğun işi aslında oyun oynamak ve oyun dediğimizde de çocuğun içine doğduğu teknolojik dünyanın ürünü olan dijital oyunlar ön planda. Biz Babyboomer adıyla geçen bir nesiliz; dolayısıyla kendi risklerimizi kendi deneyimlerimiz üzerinden değerlendirebiliyoruz. Daha sonra Y kuşağı ve Z kuşağı geldi ve şimdi alfa kuşağı 10' lu yaşlardaki çocuklarımız. Alfa dediğimizde dijital oyunlarla ilk tanışan ve belki de kendilerince bir açılım yapan yaş grubundan bahsediyoruz. Bizim kuşamız da elbette ki bahsi geçen mesajlaşma uygulamalarını, sosyal medyayı kullanıyor ama biz kendi yaşadığımız riskler kadar biliyoruz. Fakat bu çocuklar bu teknolojiye doğdukları için onların risk algısıyla bizim algımız tam olarak aynı değil. İstismar özelinde değerlendirildiğinde; gerçek hayatta, sokakta, okulda, evde istismara uğrayan çocuklarla, dijital oyunlar vasıtasıyla veya dijital ortamda istismara uğrayan çocukların sayısı ve sıklığı noktasında çok bariz bir fark görünmüyor. Aslında dijital ortamda çocukların her şeye daha açık olması sebebiyle bu sayının daha fazla olması gerekir gibi düşünüyoruz ancak bu sayı benim tahmin ettiğimin çok daha altında. Bu durumu çocuklarımızın bu konularda daha bilinçli olması şeklinde yorumlamıyorum ama onlar teknolojiye doğdukları için belki de riskiyle artısıyla daha güçlü değerlendiriyorlar. Bizden daha güçlüler bu konuda; teknolojiyi bizden daha iyi kullanıyorlar, daha iyi biliyorlar, hatta çocuklar teknoloji kullanımını ebeveynlerine öğretiyorlar. Bu noktada çocuklar bize oranla dijital dünya kullanımında daha usta görünüyorlar ancak bizim de ustası olması

gerektiğimiz başka önemli alanlar var; ahlakın ve etiğin ustası olmak. Çünkü ahlak ve etik doğumda edinilmiş kavramlar değiller, öğrenilmiş kavramlar. Bu noktada teknolojiyi, dijital dünyayı nasıl başkalarına zarar vermeden, bir başkasının hakkını yemeden, kendi sorumluluklarımız doğrultusunda kullanabiliriz, program üretirken bu programları yalnızca cebimizi veya gücümüzü düşünerek değil, gerçek anlamda ihtiyacı olana yardım etmek amacıyla nasıl kullanabiliriz bunları düşünerek hareket etmemiz gerekiyor. Bir oyun yaptıysak ve bunu satıyorsak buradaki amacın kendimize milyarlar katmak değil makul bi kazanç çerçevesinde ama insanlığa da yardım olması gerekir ki bu sayede çocuklarımıza da iyi örnek olabilelim. Çünkü en nihayetinde çocuklarımıza teknolojiyi kısıtlamamız mümkün değil. Teknoloji büyük bir hızla ilerliyor, örneğin bugün Whatsapp'ı kapatsanız yerine hızla bir başkası gelecek. Birçoğunun da bizim için nasıl riskler oluşturduğunu bilmiyoruz. Burada yerli ve milli üretimlerin desteklenmesi şart. Ama bunun ötesinde hem bilim ahlakının hem meslek ahlakının günlük yaşamda çocuklarımıza da aktarabileceğimiz boyutlara gelmesi çok önemli. Bizim yapabileceğimiz en büyük katkı, dünyanın da geleceği için, ahlak ve etiğin öğretilebilmesi." görüşlerini belirtmiştir.

Sayın ULUKOL, daha sonra "İşin aslı örneğin Mavi Balina ve benzeri oyunlar evinde anne babasıyla keyif içinde vakit geçirebilen çocuklara zarar veren uygulamalar değiller. Bu uygulamalar anne baba ilgisi, sevgisi göremeyen, kendi başına kalan çocukların oynadığı oyunlar oldular belki de. Eğer bizler erişkin olarak bu anlamda çocuklarımızı koruyabilseydik oyunlar da çocuklarımızı bu noktaya sürükleyemezdi. Bu noktada gayret içinde olmalıyız. Başka bir noktadan, yerli ve milli uygulamaların bizim çocuklarımıza rol

model olduğunu ve motive ettiğini unutmamak gerekir. Örneğin; ASELSAN' ın geliştirdiği bir programın Türkiye' de kullanılıyor olması çocuğumuza da bu yönde üretimler yapması noktasında motivasyon kaynağı olacaktır. Bu noktada çalışmalar da sürdürülmelidir. Sonuç olarak tüm bu konularda kendimize, kendi çocuklarımıza ve ülkemize yatırım yapmamız gerektiğini düşünüyorum." ifadelerinde bulunmuştur.

Vodafone Siber Güvenlik Müdürü **Sayın Gökhan BOZDOĞAN**, "Güvenlik günümüzde geleneksel yaklaşımın dışına çıkmış ve çok katmanlı bir mimariye evrilmiştir. İçinde barındırdığı Ağ, Mobil, Veri, Uygulama, Bulut ve kullanıcı adımları beraberinde birçok risk alanını da yanında getirmektedir. Geleneksel güvenlik yaklaşımları yerini hedef odaklı, son kullanıcının yaşamına hitap eden, şirketlerin zayıf noktalarını bulup hedef alan süreçlere evirilmiştir. Mekan bağımlılığının ortadan kalkması, yüksek bant genişlikleri, bilgiye erişim kaynaklarının çeşitlenmesi ve bilgiye her yerden erişim hayatımızı kolaylaştıran unsurlar olsa da, siber zafiyetler anlamında ciddi riskleri de beraberinde getirmiştir. Son yılların parlayan ve hızla büyüyen sektörlerinden olan Sosyal Medya ve Dijital oyun sektörü bu büyümeden en büyük payı alan alanlar olmuştur. İnternet penetrasyonun 2020 yılında %74 olduğu Türkiye'de sosyal medya kullanıcıları bir önceki yıla oranla 2.2 milyon artış göstermiştir. Bu artış insanların dijital dünyanı ne derece benimsediklerini ve aynı hızla nasıl tüketici konumuna geldiğini çok net şekilde göstermektedir. Sosyal Medya ve oyunları bu kadar hızlı şekilde kabullenip benimsemek siber riskleri de beraberinde getirmiş ve bu alandaki yükselişi hızlandırmıştır. Bu durumun sonucu "bağlantılı" insan kavramını ön plana çıkarmıştır. Her an erişim sağlayan, her saniye veri aktarıp alan, birbirine dijital dünyada sıkı sıkı bağlı sistemler ve insanlar topluluğu. Siber riskler bu kullanım alışkanlıkları ile 2 aşamada değerlendirilmelidir. İlk aşama bireysel olarak kullandığımız uygulamalar kendi kişisel siber güvenliğimiz. Diğer aşama ise aslında kurduğumuz uygulamalar ile dahil olduğumuz teknolojik ekosistem ve bu ekosistemin kötü amaçlı kişilerce internet servis sağlayıcılarına ve ülke güvenliğine karşı birer siber tehdit oluşturması." olarak görüş bildirmiştir.

Sayın BOZDOĞAN, "Kurulan uygulamalardaki güvenlik zafiyetleri, uygulamaların topladığı bilgiler, eriştiği kaynaklar hackerlar ve internet korsanları için kullanıcıları birer "köle" haline getirebilmekte ve istenilen anda uzaktan yönetilen birer saldırgan durumuna getirmektedir. Bu durumda altyapı yöneticilerine özellikle tehditler oluşturmaktadır. Sosyal medyada var olmak hayatımızın kaçınılmaz bir parçasıdır ve böyle devam edecektir. Bireysel olarak alacağımız basit önlemler ile hem kendi güvenliğimizi hem de servis sağlayıcılarımızın güvenliğini ciddi anlamda azaltabileceğimizi unutmayalım." ifadelerine yer vermiştir.

Akaydın Hukuk Bürosundan **Sayın Av. Ceyda CİMİLLİ AKAYDIN**, "İnternet ortamında ve sosyal medyada hukuki düzenlemeler yapılması konusu uzun yıllardır gündemimizdedir. Bu konuda iki temel görüş olup, birincisi yeni kullanılmaya başlayan tüm teknolojiler ve ortamlara ilişkin düzenlemeler yapılması için mevzuatta değişiklik yapılması gerektiğini savunurken bir diğeri temel hukuk kurallarının yorumlanarak ve uyarlanarak yeni teknolojinin getirdiği değişikliklerin uygulanabileceğini, sürekli olarak mevzuatta düzenleme yapmanın hukuk güvenliğini sarsacak ağını savunmaktadır. Benim de bu konudaki görüşüm iki görüşten yanadır çünkü teknoloji gerçekten çok hızlı ilerlemektedir. Mevzuatın benzer ve hızlı değişmesi yurttaşların mevzuatı takip etme ve yasalara uygun davranma imkânlarını zorlaştıracak, vatandaşların sürekli olarak yeni mevzuatı takip edememe nedeniyle yasaya aykırı hareketler yapmaları riskini doğuracaktır. Bu nedenle sosyal medya ve dijital ortamlarda ve oyun platformlarında düzenlemeler yapılması için yeni mevzuat çıkartılmasına gerek yoktur. Var olan mevzuat yeterlidir. Burada var olan mevzuattan suç ve ceza'yı tanımlayabilmek açısından en temel iki yasa Türk Ceza Kanunu ve 5651 sayılı internet ortamındaki yayınların düzenlenmesi ve bu ortamda işlenen suçlarla mücadele kanunudur. Türk Ceza Kanunu klasik ortamlarda da, dijital ortamlarda da işlenebilen suçları tanımlar, verilmesi gereken cezaları düzenler. Bu suçlara örnek olarak dolandırıcılık, hakaret, iftira, özel hayatın ve haberleşmenin gizliliğinin ihlali gibi suçlar gösterilebilir. Ceza kanunu ve ilgili mevzuat bu suçları ve cezalarını tanımlayarak suçun işlendiği ortama bakılmaksızın düzenlemeyi yapmaktadır. Birçok suç açısından suçun sanal ortamlarda işlenmiş olması ağırlaştırıcı neden olarak görülmektedir. Bunun dışında örneğin hakaret suçunun sosyal medyada

dijital oyunlarda veya fiziksel ortamlarda işlenmesinin bir farkı olmayacaktır. Aradaki tek fark suçun tespiti, suçlunun tespiti açısından kullanılacak yöntemlerdir. Bunlar da hukukun değil daha çok kolluk kuvvetlerinin konusudur. 5651 sayılı yasa öncelikle internet ortamındaki yer sağlayıcı, servis sağlayıcı, içerik sağlayıcı gibi aktörleri belirler bunların yükümlülük ve sorumluluklarını tanımlar. Ayrıca yasanın en temel fonksiyonlarından birisi de internet ortamında konusu suç oluşturan içeriğin kaldırılması veya erişimin engellenmesidir. Yasa öncelikle erişimin engellenmesini gerektirecek katalog suçları saymış ayrıca erişimin engellenmesi kararının nasıl uygulanacağı, istisnai durumlarda neler yapılabileceği ve bu karara karşı başvurulabilecek yolları belirlemiştir. Belirtilen bu 2 mevzuat ve diğer ilgili mevzuatla sosyal medyada ve dijital oyunlardan çocukların mı erişkinlerin haklarının korunması ve bu ortamlarda faaliyet gösterenlerin sorumluluklarının belirlenmesi konusunda yeterli düzenleme sağlanmıştır. Bu aşamadan sonra yapılması gereken şey hem mevzuat ve haklar konusunda bireyleri bilgilendirmek hem de yasanın uygulanabilmesi ve suçun oluşması durumunda suçlunun bulunup cezalandırılabilmesi için kolluk kuvvetlerinin bu alandaki çalışmalarının arttırılmasıdır." olarak görüşlerini belirtmiştir.

TBD Onur Kurulu Üyesi **Sayın İ. İlker TABAK**, oturum konuşmasında "Anlık İleti Hizmetleri" konusunda TBD İcra Kurulu tarafından gerçekleştirilen çalışmalara ve hazırlanan raporda yer alan değerlendirmelere ilişkin olarak özet bilgiler aktarmıştır.

Sayın TABAK, WhatsApp'ın 4 Ocak 2021 tarihinde "kullanıcılar ile yeni sözleşme imzalanacağını, bu sözleşmeyi imzalamayan kullanıcıların 8 Şubat 2021 tarihinden itibaren WhatsApp'ı kullanamayacağını" açıklaması ile hem Türkiye'de hem de dünyanın

çeşitli ülkelerinde kullanıcılar arasında ciddi bir kaos yaşandığını; bunun sonucunda WhatsApp kullanıcılarının çok irdelemeden, panik halinde benzer uygulamalara geçmeye başlamaları üzerine, TBD tarafından anlık ileti hizmetleri hakkında toplumu bilgilendirmek, birey olarak kullanıcılara, düzenleyici otoritelere ve STK'lara düşen görev ve sorumlulukları tartışmak amacıyla 3 aşamadan oluşan bir dizi çalışma başlatıldığını belirmiştir.

Sayın TABAK, "TBD bu konuda hızlı tepki verebilmek için bu çalışmanın ilk adımında kamuoyunun bilgilendirilmesi ve farkındalığının artırılmasına yönelik bu konuların tartışıldığı bir çalıştay düzenleyerek 13 Ocak 2021 tarihinde ilgili kurumlar, STK'lar ve basın ile paylaşılan "WhatsApp tarafından kullanıcılarına gönderilen yeni sözleşme değişikliğine ilişkin Türkiye Bilişim Derneği'nin Değerlendirmeleri" başlıklı kamuoyu duyurusunu yayımlamıştır. Çalışmanın ikinci aşamasında anlık ileti hizmetlerinin teknik, idari ve hukuki açılardan ele alındığı kapsamlı bir rapor hazırlanması hedefiyle 21 Ocak 2021 tarihinde yeni bir çalıştay gerçekleştirilmiştir." ifadelerine yer vermiştir.

Günümüzde kullandığımız Anlık İleti Sistemleri'nin kısa bir tarihçesini verdikten sonra, kişisel verilerin önemi de vurgulanmış, bu uygulamaların topladığı kişisel verilerden örnekler paylaşılmıştır. En önemli örneğin "Cambridge Analytica" skandalı olduğunu belirten **Sayın TABAK**, arka kapı olayları ile sanal profillemelere de dikkat çekmiştir.

Sayın TABAK tarafından Facebook tarafından satın alınan Whatsapp ve Instagram uygulamalarınca toplanmakta olan verilerin diğer uygulamalar tarafından da toplandığı

belirtilmiş, özellikle yerli olarak tanımlanan uygulamaların da benzer açık kaynaklı altyapılardan yararlanarak geliştirildiği ve birçok kişisel veriyi topladığı anımsatılmıştır. Ayrıca son kullanıcıların bu uygulamaları seçiminde dikkat edeceği ölçütler de aktarılmış; kişilerin, STK'ların ve düzenleyici otoritelerin görev ve sorumluluklarına değinilmiştir. KVKK tarafından "Güvenli Ülkeler" listesinin açıklanmasının kısmen zorlukların aşılmasını sağlayacağı belirtilmiştir.

Siber Güvenlik Farkındalık Eğitimleri

Zirve'de sosyal sorumluluk projesi kapsamında ücretsiz olarak beş (5) değişik konuda siber güvenlik farkındalık eğitimi verilmiştir. Söz konusu farkındalık eğitimleri; Siber Güvenilir Kullanıcı, Bilgi Güvenliği Yönetim Sistemi (27001) Bilgi Güvenliği Farkındalığı, Bulut Bilişim ve Güvenliği, Kişisel Verileri Koruma (KVKK ve GDPR) ve İşletim Sistemi Güvenliği ve Sıkılaştırma eğitimlerini kapsamaktadır.

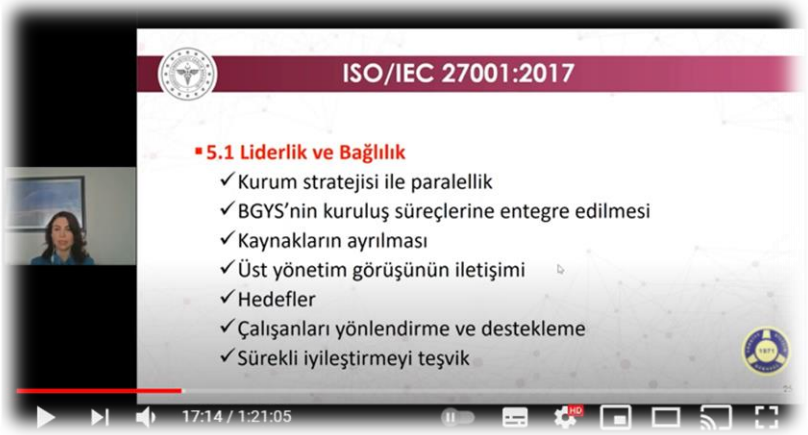
- **Siber Güvenilir Kullanıcı Eğitimi**

  Eğitmen **Sayın İ. İlker Tabak** tarafından verilen, Siber Güvenilir Kullanıcı eğitimi, internet ve sosyal medyanın güvenli olarak kullanılmasına ve siber uzaydan gelebilecek saldırılara karşı bireylerin kendilerini koruyabilmelerine yönelik önemli ve pratik bilgileri kapsamaktadır. Çevrimiçi olarak verilen bir (1) saatlik eğitime kırkyedi (47) kişi katılmış ve yirmiiki (22) kişi sertifika almaya hak kazanmıştır.

- **Bilgi Güvenliği Yönetim Sistemi (27001) Bilgi Güvenliği Farkındalığı Eğitimi**

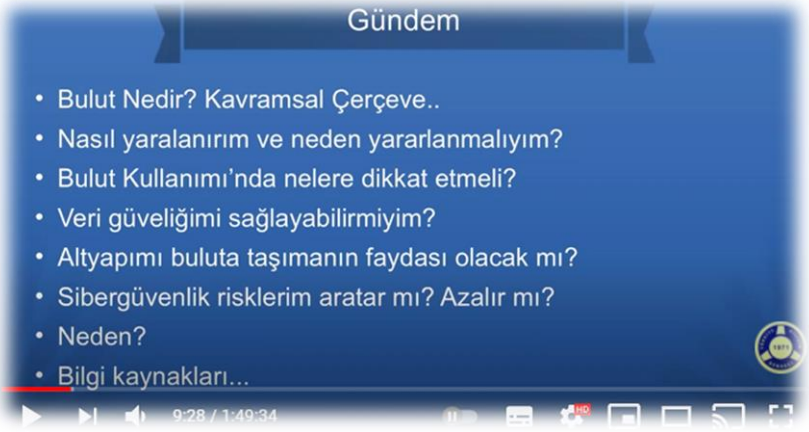
  Eğitmen **Sayın Dilek Şen KARAKAYA** tarafından verilen, Bilgi Güvenliği Yönetim Sistemi (27001) Bilgi Güvenliği Farkındalığı eğitimi, ISO 27001 Bilgi Güvenliği Yönetim Sisteminin ne olduğunu ve standardın gerekliliklerinin nelerden oluştuğunu açıklayan, bilgi ve bilgi güvenliği ile ilgili temel kavramları ve standart

hakkında farkındalık yaratmaya yönelik önemli bilgileri kapsamaktadır. Çevrimiçi olarak verilen birbuçuk (1.5) saatlik eğitime altmışdört (24) kişi katılmış ve yirmi (20) kişi sertifika almaya hak kazanmıştır.



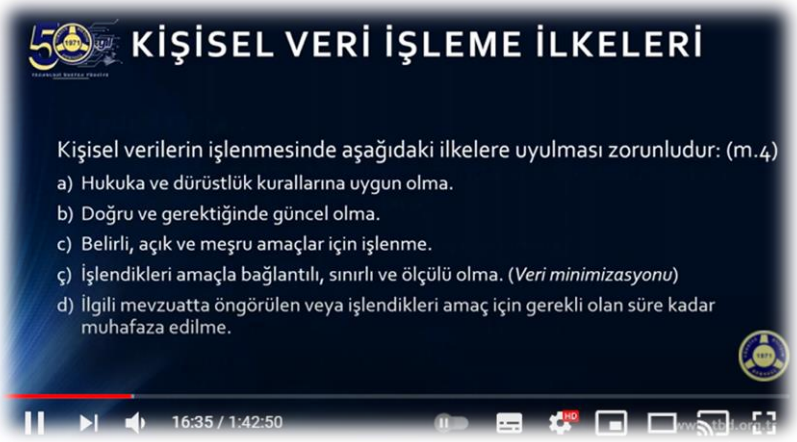
- **Bulut Bilişim ve Güvenliği Eğitimi**

  Eğitmen **Sayın Dr. Ziya KARAKAYA** tarafından verilen, Bulut Bilişim ve Güvenliği eğitimi, dijital dönüşüm teknolojilerinin başında yer alan ve özellikle de COVID-19 Pandemisi sürecinde uzaktan eğitim ve/veya evde çalışma gibi uygulamalarda kurumlara önemli avantajlar sunması nedeniyle kullanımı hızla yaygınlaşan Bulut Bilişim ve Güvenliği hakkında temel bilgileri ve uygulamada dikkat edilmesi gereken hususlara yönelik önemli bilgileri kapsamaktadır. Çevrimiçi olarak verilen birbuçuk (1.5) saatlik eğitime kırkyedi (47) kişi katılmış ve yirmiiki (22) kişi sertifika almaya hak kazanmıştır.



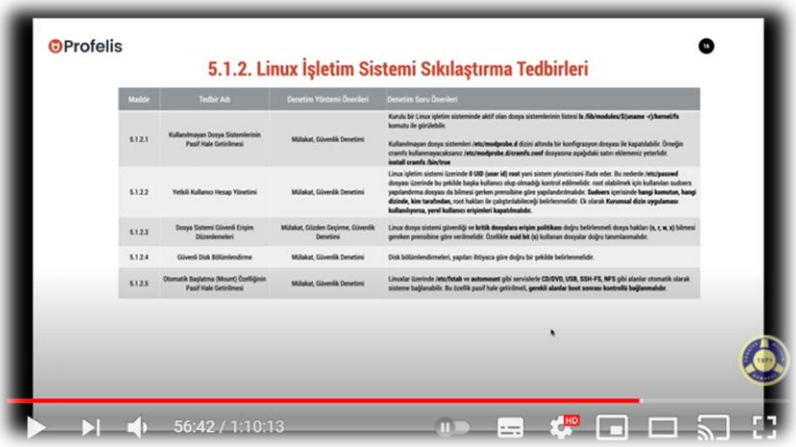
- **Kişisel Verileri Koruma (KVKK ve GDPR) Eğitimi**

  Eğitmen **Sayın Mehmet Ali İNCEEFE** tarafından verilen, Kişisel Verileri Koruma (KVKK ve GDPR) eğitimi, her geçen gün artan veri ihlalleri ve saldırılar karşısında kurum ve kuruluşların bu süreci nasıl yönetmeleri gerektiğine, kişilerin temel hak ve özgürlükleri ile mahremiyetlerinin en kritik unsurlardan birisi olan kişisel verilerinin korunması ve güvenliğinin sağlanmasına yönelik olarak çıkartılan KVKK ve GDPR düzenlemelerinin temel ilkelerine ve KVKK ve GDPR düzenlemelerinin uygulama alanları ile getirdiği yükümlülükler hakkında farkındalık yaratılmasına yönelik önemli bilgileri kapsamaktadır. Çevrimiçi olarak verilen birbuçuk (1.5) saatlik eğitime kırk (40) kişi katılmış ve ondört (14) kişi sertifika almaya hak kazanmıştır.



- **İşletim Sistemi Güvenliği ve Sıkılaştırma Eğitimi**

  Eğitmen **Sayın Çağlar ÜLKÜDERNER** tarafından verilen, İşletim Sistemi Güvenliği ve Sıkılaştırma eğitimi, hem sistem yöneticilerinde hem de sistem kullanıcılarında güvenlik bilincinin geliştirilmesine yönelik olarak işletim sistemlerinin açıklıkları ve uygulanması gereken güvenlik önlemleri, sıkılaştırmalar, yönetim ve denetim mekanizmaları hakkında temel bilgileri vermek ve uygulamada dikkat edilmesi gereken hususlar konusunda farkındalık yaratılmasına yönelik önemli bilgileri kapsamaktadır. Çevrimiçi olarak verilen birbuçuk (1.5) saatlik eğitime yirmiüç (23) kişi katılmış ve onbir (11) kişi sertifika almaya hak kazanmıştır.



Siber Güvenlik Bayrağı Yakala (CTF) Yarışması

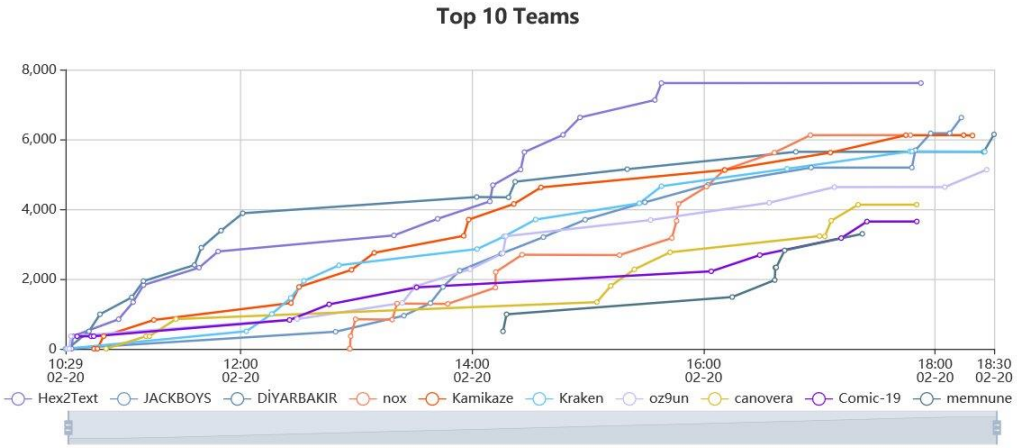
Zirvenin son günü sosyal sorumluluk projesi kapsamında "Siber Güvenlik Bayrağı Yakala (CTF)" Yarışması çevrimiçi olarak düzenlenmiştir.

CTF (Capture The Flag), ''Bayrağı Yakala'' adıyla bilinen siber güvenlik alanında düzenlenen uygulamalı öğretici yarışmalarıdır. Bayrağı yakala yarışmalarının (CTF) asıl amacı, hack konusunda öğrenilen bilgiye sahip olan insanların bu bilgileri pratiğe dökerek

kendilerini test etmelerini sağlamaktır. Bayrağı yakala yarışmalarına (CTF) katılanlar; siber korsanlardan, güvenlik uzmanlarından, bilgi güvenliği araştırma gruplarından veya öğrencilerden oluşabilmektedir. Bu alanda kendini yetiştirmek isteyen gençlere yeteneklerini ölçme ve sergileme olanağı sağlamaktadır.

Türkiye Bilişim Derneği ve BÜSİBER Boğaziçi Üniversitesi YBS Siber Güvenlik Merkezi tarafından düzenlenen Çevrimiçi Siber Güvenlik Bayrağı Yakala (CTF) Yarışmasına 140 katılımcı 67 takım halinde kayıt yaptırmıştır.

4. Siber Güvenlik Ekosistemi Geliştirme Zirvesi kapsamında yer alan bu yarışmada gençler yeteneklerini sınama fırsatı bulmuşlardır. Takımlar arasında an be an heyecanlı geçen mücadele aşağıdaki grafiğe yansımıştır. Yine aynı grafikte ilk 5 dereceye giren takımlar görülmektedir.



Place	Team	Score
1	Hex2Text	7614
2	JACKBOYS	6624
3	DİYARBAKIR	6143
4	nox	6122
5	Kamikaze	6110

TBD Siber Güvenlik Ekosistemi Ödülleri

TBD tarafından siber güvenlik ekosistemine katkı verenlere 2018 yılından beri her yıl verilmekte olan "SİBER GÜVENLİK EKOSİSTEMİ ÖDÜLLERİ" kamu, özel sektör, akademi, medya dalında olmak üzere toplam dört (4) kategoriden oluşmaktadır. 2021 yılı TBD Siber Güvenlik Ekosistemi Ödüllerinde;

- Siber Güvenlik Ekosistemine Katkı Veren Kamu Kurumu Kategorisinde; “Ulusal Siber Olaylara Müdahale Merkezi (USOM)” Projesi ile Bilgi Teknolojileri ve İletişim Kurumu ve “Siber İstihbarat ve Kaynak Kod Analiz yazılım testleri ve bu yazılımların geliştirilmesine ilişkin gerçekleştirilen kavram kanıtlama çalışmaları" ile T.C. Adalet Bakanlığı ödüle layık görülmüştür.

- Siber Güvenlik Ekosistemine Katkı Veren Kamu Görevlisi Kategorisinde; "Enerji sektörü kapsamında oluşturulan Siber Olaylara Müdahale Ekibi (SOME) çalışmaları ve yakın zamanda başlatılan enerji sektöründe Siber Güvenlik Olgunluk Modeli Projesi çalışmalarına öncülük etmesi" ile Enerji Piyasası ve Düzenleme Kurumu Bilgi İşlem Dairesi Başkanı Sayın Mehmet YILMAZER ödüle layık görülmüştür.

- Siber Güvenlik Ekosistemine Katkı Veren Akademisyen Kategorisinde; Siber güvenlik alanında yapmış olduğu akademik araştırma çalışmaları ve nitelikli insan kaynağı yetiştirilmesine yönelik ekosisteme verdiği katkılar ile ODTÜ Siber Güvenlik Bölümü Öğretim Üyesi Sayın Dr. Attila ÖZGİT ödüle layık görülmüştür.

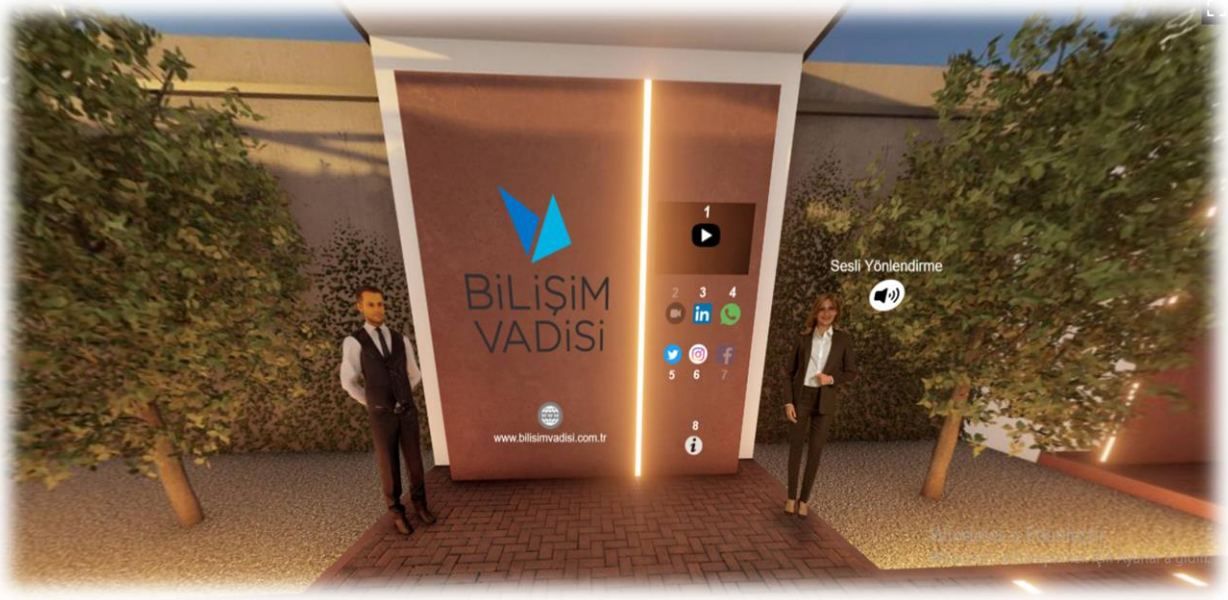
- Yerli ve Milli Teknoloji Geliştirme Kategorisinde;"DataFlowX Ürünü" ile BilgeSGT Firması ödüle layık görülmüştür.

Ödüller T.C Ulaştırma ve Altyapı Bakan Yardımcısı Sayın Dr. Ömer Fatih SAYAN, BTK Başkanı Sayın Ömer Abdullah KARAGÖZOĞLU ve TBD Genel Başkanı Sayın Rahmi AKTEPE tarafından verilmiştir.

Sanal Stantların Ziyareti

4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'ne 1200 kişi çevrimiçi olarak katılım sağlamıştır. Milli kabiliyetlerle özgün olarak geliştirilen 360 derece tur özelliğine sahip **SanalFuar360.com** dijital platformu üzerinden gerçekleştirilen etkinliğimizdeki akıllı stantları 750 kişi ziyaret etmiştir.

1000 kişi ise **SanalFuar360.com** dijital platformunda yer alan sanal konferans salonlarından canlı olarak gerçekleştirilen oturumları izlemiştir.



4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi'ne sponsor olan firmalardan onikisi (12) sanal stant açmıştır.

Açılış konuşmalarını müteakip, oniki (12) firmanın yer aldığı sanal stant alanları BTK Başkanı **Sayın Ömer Abdullah KARAGÖZOĞLU** ve TBD Genel Başkanı **Sayın Rahmi AKTEPE** tarafından ziyaret edilmiştir.

Zirveden Çıkan Sonuçlar

1. Cumhurbaşkanlığı sistemine ve hızla gelişen dijital dönüşüm teknolojilerine uyumlu ve tüm paydaşları kapsayacak şekilde sürdürülebilir "Siber Güvenlik Ekosistemi"nin yeniden yapılandırılması,
2. Avrupa Birliği'nde de olduğu gibi insan odaklı Siber Güvenlik Stratejilerinin ülkemizde de oluşturulması,
3. Yerli siber güvenlik ürün ve hizmetlerinin kamu kurumlarında ve kritik altyapılarda kullanımının yaygınlaştırılmasına yönelik strateji ve eylem planlarının hazırlanması,
4. Gelişen teknolojilerin ışığında siber suçlarla etkin mücadele edebilmek, ulusal seviyede siber dayanıklılığın arttırılmasına ve siber vatanın azami oranda korunmasına yönelik, siber güvenlik sertifikası temelli olarak çevrimiçi hizmetlerin ve tüketici cihazlarının siber güvenliğini arttıracak, siber uzayla ilgili teknik, idari ve yasal düzenlemeleri kapsayan bir çerçevenin oluşturulması amacıyla Siber Güvenlik Yasasının hazırlanması,
5. Siber güvenlik tedbirlerinin ürün ve teknoloji bağımsız olarak uygulanabilir olmasının sağlanması,

6. Milli Uzay Programı 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 önemlidir. Yapay zeka, derin öğrenme, otonom araçlar, nesnelerin interneti, eklemeli imalat ve siber güvenlik başta olmak üzere dijital teknolojilerin yoğun olarak kullanıldığı uzay teknolojilerindeki kazanımların bilişim ve siber güvenlik ekosisteminin sürdürülebilirliğine önemli katkılar sağlayacağı,

7. Covid-19 ve/veya benzeri küresel salgın dönemlerinde ivmelenen siber saldırılara karşı ülkemizin siber dayanıklılığının arttırılabilmesi amacıyla, yapay zekâ destekli Siber Güvenlik Kalkanının oluşturulması,
8. Siber Güvenlik alanında yerli ve milli olmanın yanı sıra uluslararası rekabet gücü yüksek ürünlerin geliştirilmesi ve mevcut durumda siber güvenlik çözümlerindeki yüzde 5-10 seviyesinde olan yerlilik oranının gelecek 5 yıl içerisinde en az yüzde 50 seviyesine getirilmesi,
9. Siber güvenlik teknolojilerinde dışa bağımlılığın asgari seviyelere indirilebilmesi ve siber güvenlik alanında teknolojik egemenliğin arttırılmasına yönelik olarak ihtiyaç duyulan teşvik ve destek mekanizmalarının oluşturulması ve etkin olarak uygulanması,
10. Siber güvenlik ürünlerinin ticarileştirilmesine yönelik olarak sektöre danışmanlık hizmeti verilmesi ve dikeyde ihtisaslaşan KOBİ'lerin oluşturduğu teknoloji ve ürünlerin büyük ve/veya mega projelerde kullanılmasına olanak sağlayacak yapıların oluşturulması,
11. Siber güvenlik eylem planlarının etkin ve tarafsız olarak uygulandığının ölçüm ve izlenmesi amacıyla STK, Akademi ve özel sektörün de yer aldığı izleme komisyonlarının oluşturulması,
12. Kamu kurum ve kuruşları ile kritik altyapılarda kullanılacak olan siber güvenlik ürün, sistem ve hizmetlerine yönelik asgari güvenlik isterlerinin tanımlanması, standartların ve ürün sertifikasyon süreçlerinin belirlenmesi ve Siber Güvenlik Sertifikasyon Programının oluşturulması,
13. Siber Güvenlik ekosisteminde yer alan tüm paydaşların iş birliği ve katılımıyla kapsamlı bir "Siber Güvenlik Uzmanlar Yetenek Havuzu" nun oluşturulması ve bu yapının sürdürülebilirliği için "Ulusal Siber Güvenlik Akademisi"nin kurulması,
14. Siber güvenlik alanında ihtiyaç duyulan; gelişen dijital dönüşüm teknolojilerine uyum sağlayabilecek, dijital becerileri gelişmiş "Nitelikli İnsan Kaynağı"nın yetiştirilmesine ve/veya mevcut sayının arttırılmasına yönelik ulusal bir programın oluşturulması,

15. Siber güvenlik alanında farklı kurumlar tarafından oluşturulan kümelenmelerin etkinliğinin arttırılabilmesi amacıyla iş birliği yapmalarının sağlanması ve bilgi paylaşımının gerçekleştirilmesi, bu kapsamda Siber Güvenlik Bilgi Paylaşım Platformunun oluşturulması,
16. Kuantum bilgisayarların gelişimine parelel olarak çıkan Kuantum saldıralarına karşı zaafiyeti olan kriptografik algoritmaların kuantum güvenli olanları ile değiştirilmesi üzerine çalışmaların başlatılması,
17. Kişisel Verilerin azami oranda korunabilmesi ve WhatsApp benzeri olarak anlık ileti ve/veya sosyal medya uygulamalarında yaşanabilecek sorunların ve/veya maduriyetlerin giderilmesi amacıyla Kişisel Verileri Koruma Kanunu'nda, özellikle denetim ve yaptırımlardaki GDPR ile olan farklılıklar giderilerek ivedilikle uygulamaya alınması,

sonuçlarına varılmıştır.

Sonuç ve Değerlendirme

Türkiye Bilişim Derneği tarafından Bilgi Teknolojileri ve İletişim Kurumu (BTK), T.C. Ulaştırma ve Altyapı Bakanlığı ve T.C. Cumhurbaşkanlığı Savunma Sanayi Başkanlığı iş birliği ile düzenlenen ve 4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi 18 – 20 Şubat 2021 tarihleri arasında Bilgi Teknolojileri ve İletişim Kurumu Merkez Binası'nda hibrit (Yüzyüze ve çevrimiçi) olarak başarıyla gerçekleştirilmiştir.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı **Sayın Dr. Ali Taha KOÇ**, T.C. Ulaştırma ve Altyapı Bakan Yardımcısı **Sayın Dr. Ömer Fatih SAYAN**, BTK Başkanı **Sayın Ömer Abdullah KARAGÖZOĞLU** ve **KVKK Başkanı Sayın Prof. Dr. Faruk BİLİR** , Kamu, Özel Sektör ve Üniversitelerin yöneticileri, öğretim üyeleri, Sivil Toplum Örgütlerinin temsilcileri, Siber Güvenlik Uzmanları ve öğrencilerin katılımı ile gerçekleşen zirvede; siber güvenlik alanında söz sahibi olan otuzüç (33) konuşmacı yer almış ve 1200 kişiden fazla çevrimiçi katılım olmuştur. Zirveye sponsor olan firmalardan onikisi (12) sanal stant açmıştır. Stant alanları TBD YK üyeleri ve tüm katılımcılar tarafından ziyaret edilmiş, firmaların ürün ve çözümleri hakkında bilgi alınmıştır.

360 derece tur özelliğine sahip dijital platform üzerinden çevrimiçi kısmı gerçekleştirilen etkinliğimizdeki stantları 750 kişi ziyaret etmiş, bin (1000) kişi ise sanal konferans salonlarından canlı olarak gerçekleştirilen oturumları izlemiş ve ikiyüzonbir (211) kişi çevrimiçi olarak gerçekleştirilen eğitimlere katılım sağlamıştır. Ayrıca etkinlik boyunca

gerçekleştirilen tüm oturumlar TÜRKSAT tarafından bir (1) milyar kişinin izleyebileceği şekilde uydu üzerinden canlı olarak yayınlanmıştır.

4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesinden ülkemizin güvenliğine ve kalkınmasına doğrudan etki edecek sonuçların çıktığını görmekteyiz. Ortaya konan sonuçlar siber güvenlik ekosisteminin geliştirilmesine, milli imkan ve kabiliyetler ile yürütülen yerli ürün ve/veya hizmet geliştirme faaliyetlerinin sürdürülebilirliğine ve yaygınlaştırılmasına, ulusal kapasitenin arttırılmasını, ekosistem içerisinde yer alan firmaların rekabetçilik endeksinin yükseltilmesine ve siber güvenlik ekonomisinin büyütülmesine yönelik olarak uygulanması gereken temel politika ve stratejilerinin belirlenmesi açısından yol gösterici olmaktadır.


4. SİBER GÜVENLİK
Zirvesi
Hibrit Etkinlik
İOnline ve BTK Konferans Salonu
18-19-20 Şubat 2021
TÜRKİYE BİLİŞİM DERNEĞİ
Danışma
SANAL FUAR 360
Yeni Normal Etkinlikler
SANAL FUAR 360


4. SİBER GÜVENLİK ZİRVESİ
18-19-20 Şubat 2021

MEDYADAN YANSIMALAR

'4. Siber Güvenlik Zirvesi'nin ardından..

Hilmi DEVELİ
EKONOMİDE SATIR ARASI
hilmideveli@gmail.com

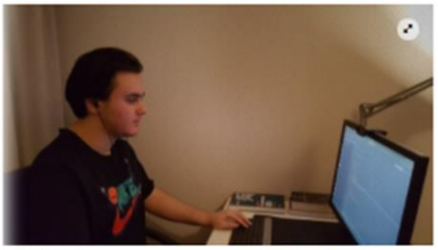
04 Mart 2021 Perşembe

Bu yıl 50. Kuruluş yılını kutlayan Türkiye Bilişim Derneği (TBD) bu bağlamda yıl boyunca bir dizi etkinlikleri bir bir gerçekleştiriyor.

Son etkinlik, "4. Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi", Cumhurbaşkanlığı, bağlı kuruluşlar, bakanlıklar, yerel yönetimler, üniversite, özel sektör, STK temsilcileri, bilim insanları, bilişim profesyonelleri ve uzmanlarının katılımı ile 18-19 Şubat 2021 tarihlerinde BTK ana konferans salonu'nda hibrit (Fiziksel ve Sanal Katılım) olarak gerçekleştirildi.

Ted Kocaeli Koleji öğrencisinin büyük başarısı

Siber güvenlik uzmanlarının yetiştirilmesine ve güvenlik farkındalığının artırılmasına katkı sağlamak amacıyla BÜSİBER (Boğaziçi Üniversitesi Yönetim...



Siber güvenlik uzmanlarının yetiştirilmesine ve güvenlik farkındalığının artırılmasına katkı sağlamak amacıyla BÜSİBER (Boğaziçi Üniversitesi Yönetim Bilişim Sistemleri Siber Güvenlik Merkezi) ve TBD (Türkiye Bilişim Derneği) işbirliği ile düzenlenen Capture the Flag yarışmasında TED Kocaeli Koleji Özel Anadolu Lisesi 10. sınıf öğrencisi Cem EKE 2. oldu. TBD (Türkiye Bilişim Derneği) tarafından düzenlenen 4. Siber Güvenlik Zirvesi kapsamında TBD ve BÜSİBER tarafından 20 Şubat 2021 Cumartesi günü organize edilen "Capture the Flag (Siber Güvenlik)" yarışmasına 67 takım ve 140 kişi katıldı.

Cem EKE, "TBD-BÜSİBER CTF Siber Güvenlik Yarışması"na "JACKBOYS" takma adı ile bireysel olarak katıldı. Siber Güvenlik alanında uygulamalı 15 görevden 12 tanesini tamamlayarak çoğunluğu üniversite öğrencilerinden oluşan rakiplerini geride bırakıp yarışmayı ikincilikle tamamladı.

ZİRVEDEN FOTOĞRAFLAR


ULAK
SOITRON
AKGÜN
Efor


4. SİBER GÜVENLİK
18-19 Şubat 2021
Zirvesi
BTK
www.tbd.org.tr | www.siberguvenlikzirvesi.org.tr

4. SİBER GÜVENLİK EKOSİSTEMİNİN GELİŞTİRİLMESİ Zirvesi

18-19-20 Şubat 2021

ANA SPONSOR

BİLİŞİM VADİSİ Technology Development Zone.

PLATİN SPONSORLAR

Türk Telekom Değerli Hissettirir

ALTIN SPONSORLAR

artı&artı teknoloji hizmetleri

FORTINET

MITSUBISHI ELECTRIC Changes for the Better

TREND MICRO

ULAK HABERLEŞME A.Ş.

GÜMÜŞ SPONSORLAR

AKGÜN

BG-TEK

Bilge Siber Güvenlik Teknolojileri

EXCLUSIVE NETWORKS

invicta

SOITRON SİBER GÜVENLİK SERVİSLERİ

İLETİŞİM SPONSORU

TÜRKSAT

MARKA-DESTEK SPONSORU

Profelis

BULUT BİLİŞİM SPONSORU

veriyum

ÜRÜN & HİZMET SPONSORLARI

BITES

XDECE

GLOBALNET INTERNET TECHNOLOGIES

Probilişim

BASIN & MEDYA SPONSORLARI

AKILLI GÜNDEM

BThaber 1995'ten beri

dg

faselis

ICT media

KobiEfor AYLIK SANAYİ EKONOMİ DERGİSİ

Maramiro Security? Reliability?