

## **Bilgi Güvenliđi Derneđi Yönetim Kurulu Başkanı Taha Yücel İle Söyleşi**

**Bilgi güvenliđi alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak amacı ile Bilgi Güvenliđi Derneđi Yönetim Kurulu Başkanı Taha Yücel ile Türkiye’de bilişim sektörünün durumu ve bilhassa bilgi güvenliđi hususunda ülkemizin dünü, bugünü, geleceđi ve yapılması gerekenleri konuştuk.**

**CyberMag: Öncelikle Bilgi Güvenliđi Derneđi YK Başkanlığı’na seçildiđiniz için tebrik ederiz. Bu konu ile ilgili duygularınızı ve derneđin yüklendiđi misyonu bizimle paylaşır mısınız?**

**Taha Yücel:** CyberMag Dergisi ve Bilgi Güvenliđi Derneđi sektörde çok büyük bir ihtiyacı karşılıyor ve çok önemli bir misyonu var. Başarılarının daim olmasını diliyorum.

Bilgi Güvenliđi Derneđi (BGD), 22.07.2007 tarihinde, bilgi güvenliđi alanında toplumun her kesiminde bilgi ve bilinç düzeyini arttırmak, bu konu ile ilgili teknolojik gelişmeleri izlemek, milli teknolojilerin geliştirilmesine katkı sağlamak; bireysel, kurumsal ve ulusal düzeydeki riskler konusunda farkındalık oluşturmak amacı ile kurulmuştur. BGD’nin vizyonu da “Bilgi güvenliđi alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal sivil toplum kuruluşu olmak” şeklinde belirlenmiştir.

Siber güvenlik tehditlerinin büyük bir kısmının insan zafiyetinden kaynaklandıđı değerlendirildiđinden, bu konuda Derneđimiz yaptıđı çalışmalarla Ülkemiz insan kaynağının eğitilmesi, bilgi düzeyinin yükseltilmesi ve tehditlere karşı farkındalıđının artırılması yönünde çalışmalarını sürdürmektedir.

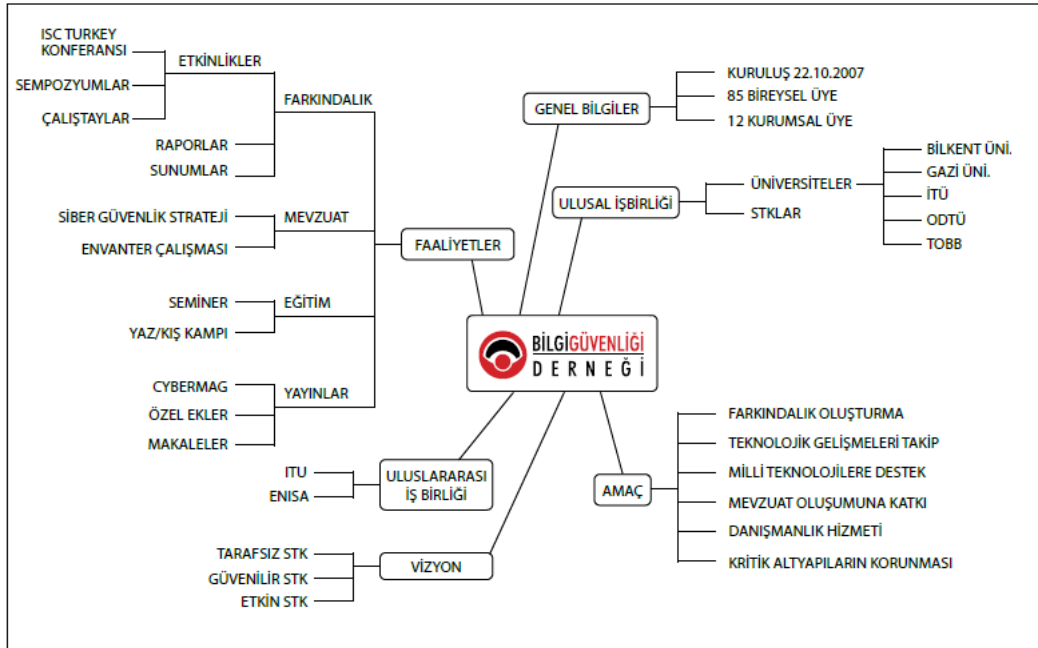
BGD’nin hali hazırda 120 bireysel ve 28 de kurumsal üyesi bulunmaktadır. BGD’nin üye aidatları ve bağışlar dışında bir geliri bulunmamakla birlikte, gerçekleştirdiđi tüm etkinliklerin katılımını ücretsiz ve herkese açık olarak yapmaktadır.

BGD, amacı doğrultusunda; tüm paydaşlarla iş birliđi yaparak mevzuatın oluşturulmasında ve geliştirilmesinde aktif rol almakta, gerçekleştirdiđi konferans, sempozyum, çalıştay ve eğitimler ile, yayımladıđı rapor ve yazılar ile farkındalıđın oluşmasına katkı sağlamaktadır.

Bu çerçeve, ülkemiz “Ulusal Siber Güvenlik Stratejisi” hazırlanması görevini üstlenmiş ve hazırladığı taslak metin kabul görmüştür. Bilahare Bakanlar Kurulu Kararı taslağının oluşturulmasında da başrol oynamıştır.

BGD, 2020 yılında 13’üncüsünü düzenlediği “Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı – ISCTURKEY” ile kurulduğu günden bu yana kamu kurumları, özel sektör ve üniversiteleri bir araya getirmeyi başarmıştır. Bu konferansın sonuç bildirgelerinde yer alan hususlar bilgi güvenliği alanında çalışan akademisyenlere, şirketlere ve kamu kurumlarına yol gösterici olmuştur.

BGD, “Ulusal Siber Güvenlik Stratejisi Çalıştayı”, “Veri Merkezleri ve Siber Güvenlik Çalıştayı”, “Siber Güvenlik Hukuku Çalıştayı”, “Mobil Dünyada Çocuk ve Gençlerin Güvenliği Sempozyumu”, “Kritik Enerji Altyapılarının Korunması Sempozyumu”, “Siber Güvenlik Yaz Kampı” gibi etkinlikler düzenleyerek bilgi güvenliğinin dokunduğu her alanda paydaşlar oluşturmuştur. BGD, yayın hayatında da CyberMag Dergisi ile işbirliği yaparak çalışmalarını bu dergide paylaşmaktadır.



**CyberMag: BGD bünyesinde gençlik platformunuz da bulunmakta. Bu platformun amacından ve yapmış oldukları çalışmalardan bahseder misiniz?**

**Taha Yücel:** Alanında ulusal ve uluslararası düzeyde tarafsız, güvenilir ve etkin bir ulusal, sivil toplum kuruluşu olan Bilgi Güvenliği Derneği'nin bünyesinde bir gençlik platformu olarak oluşturulan BGDGenç; Bilgi Güvenliği Derneği'miz ile birlikte; bireysel, kurumsal, ulusal ve evrensel boyutlarda bilgi ve iletişim güvenliği alanında teknik, bilimsel, sosyal ve kültürel faaliyetler yürütmek, orta ve yüksek öğrenim gören genç üyelerimizin mesleki gelişimini artırmak, bilgi güvenliği alanında farkındalık oluşturmak ve bir sinerji yaratmak adına kurulmuştur. Böylece muhtelif kanallardan yapılan bilgilendirmelerle her seviyede siber güvenlik farkındalığının oluşmasına katkı sağlanmaktadır.

BGD, ulusal bazda üniversiteler, kamu ve özel sektör kuruluşları ve STK'lar ile uluslararası bazda da Uluslararası Telekomünikasyon Birliği, ITU ve özellikle Avrupa Birliği Siber Güvenlik Ajansı, ENISA ile işbirliği halinde çalışmalarını sürdürmektedir. Bu bağlamda BGD, ISCTURKEY Konferansı ile ENISA tarafından oluşturulan "Avrupa Siber Güvenlik Ağı" platformuna dâhil olmuştur ve böylece uluslararası arenada da hak ettiği yeri almaktadır.

**CyberMag: Türkiye'nin Dijitalleşmesi sürecinde Bilgi Güvenliği Derneği'nin önemi nedir?**

**Taha Yücel:** Dijital teknolojilerin hızlı geliştiği günümüzde, bu dönüşümün güvenlik boyutu en az ülkelerin fiziki savunması kadar önemli hale gelmiştir. Sınırlarımızın güvenliği ne kadar önemliyse, elektronik sistemlerimizin ve buralarda saklanan verilerin güvenliği de o derece önemlidir. Dijital dünyada, dijital egemenliğimizi koruyabilmek için Siber Güvenliğe gereken önemi vermemiz, kullanılan ürünün milli olmasının, kritik altyapılarımızın ve verilerimizin güvenliği için şart olduğunu düşünüyorum; ancak tek başına yeterli değil. Bu nedenle, bu ürünlerin kullanıldığı sistemlerde siber güvenliğin devamlılığını sağlayacak nitelikli ve yetişmiş insan gücü çok önemli ve insan gücünün yetiştirilmesinde de, STK'lara önemli görevler düşmektedir. Bu konuda çalışan ve Türkiye'de bilişim güvenliği üzerine ilk sivil toplum kuruluşu **Bilgi Güvenliği Derneğimizdir.**

Kritik sistemlerimizi tehdit eden her türlü siber saldırıyı, ulusal güvenliğimizi tehdit olarak görmek gerekir. Sayısı ve niteliği hızla artan siber tehditlerle mücadele kapsamında ulusal seviyede gerekli önlemlerin alınabilmesi için, strateji ve eylem planlarının geliştirilerek uygulanması büyük önem arz etmektedir. Daha önce de bahsettiğim gibi, Ülkemiz Siber Güvenlik Strateji ve Eylem Planlarının hazırlanmasında Derneğimizin büyük katkıları olmuştur.

Bilindiği üzere, ülkemizdeki siber güvenlik çalışmalarının ivme kazanmasındaki en önemli olay Bakanlar Kurulu'nun 2012 yılında aldığı "Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna ilişkin Kararı" ile olmuştur. Bu karar ile Siber Güvenlik Kurulu oluşturulmuş, kurulun ve o zamanki ismiyle Ulaştırma, Denizcilik ve Haberleşme Bakanlığı'nın (UDHB) yetki ve sorumluluk alanları belirlenmiştir.

Yeni hükümet sistemine geçildikten sonra da, 10.07.2018 tarihli RG'de yayımlanan 2018/1 Sayılı CB Kararnamesi ile farklı kurumlar altında ayrı ayrı sürdürülen dijital dönüşüm (e-Devlet), siber güvenlik, milli teknolojiler, büyük veri ve yapay zekâ ile ilgili çalışmaların tek çatı altında toplanması amacıyla, Cumhurbaşkanlığı Dijital Dönüşüm Ofisi kuruldu. Kurulduğu günden bu yana çok başarılı çalışmalara imza atan Dijital Dönüşüm Ofisi, Ülkemizin Dijitalleşmesi sürecini tamamlaması ve Siber Güvenlik konusunda da gerekli önlemlerin alınması hususunda çalışmalarını hızlı bir şekilde sürdürmektedir.

Bu kapsamda, 06.07.2019 tarihli RG'de 2019/12 sayılı Cumhurbaşkanlığı Genelgesi ile Dijital Dönüşüm Ofisi tarafından hazırlanan, Bilgi ve İletişim Güvenliği Rehberi 10.07.2020 tarihinde yayımlandı. Rehberde; Kamu kurumlarının ve kritik altyapı niteliğinde hizmet veren işletmelerin bilgi ve iletişim güvenliği kapsamında alınması gereken tedbirler ana hatlarıyla açıklanmaktadır. Bilgi ve İletişim Güvenliği Rehberi, yaşayan bir doküman olacak şekilde; ihtiyaçlar, gelişen teknoloji ve değişen şartlar göz önünde bulundurularak sürekli güncellenerek, ülkemizin bu alanda hak ettiği yere gelmesine katkı sağlayacaktır.

***Bu vesileyle, Bilgi Güvenliği Derneği'mize üye olarak bize güç katan ve derneğimizin tüm bu çalışmaları başarıyla gerçekleştirmesi için desteklerini esirgemeyen Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanı Dr. Ali Taha KOÇ'a özellikle şükranlarımı sunuyorum.***

**CyberMag: BGD Gençlik Platformu olarak bizlerden beklemiş olduğunuz çalışmalar nelerdir?**

**Taha YÜCEL:** Türkiye'de genel anlamda mühendislik dalları ile ilgili faaliyet gösteren oluşumların başında elbette gençlik örgütleri gelmektedir. Bu örgütlerimiz çeşitli eğitimler, seminerler, çalıştaylar ve kongreler aracılığıyla mühendislerimizin ve mühendis adaylarımızın mesleki gelişimlerine katkı yapmaktadırlar. Ayrıca, çeşitli bilişim ve bilgi güvenliği derneklerimiz de bu alanda eğitim faaliyetleri düzenlemektedirler.

Söz etmeye değer bir oluşum da ABD merkezli olup dünya genelinde faaliyet gösteren Institute of Electrical and Electronics Engineering (IEEE)'dir. Bu kuruluşun gerek Türkiye şubesi gerek birçok üniversitemizde kurulmuş olan öğrenci kolları oldukça aktiftir. Bu öğrenci kolları, mühendislik öğrencilerimizin profesyonellerle iletişimini sağlayarak onları iş hayatına hazırlamaktadırlar. Ayrıca çeşitli eğitimler ve yarışmalar aracılığıyla teknik gelişimlerine de katkıda bulunmaktadırlar. Bizim gençlik platformumuz da bu dernekler ile kamu-özel sektör iş birliğini oluşturmada köprü olmalı, geliştirilecek projelerde katalizör rol üstlenmeli ve Akademik hayata doğru hazırlanarak uluslararası çalışmalara imza atmalıdır.

**CyberMag: BGD YK Başkanlığı görevinin yanı sıra, uzun yıllardır RTÜK Üst Kurul Üyesi olarak da görev yapmaktasınız. Edinmiş olduğunuz tecrübeleri göz önünde bulundurarak, dünyada ve Türkiye'de bilişim sektörünün bugünü ve geleceği hakkında neler söylemek istersiniz?**

**Taha YÜCEL:** Dünyada ve ülkemizde bilişim sektörü her geçen gün daha da gelişmekte ve büyümektedir. Gün geçtikçe bu pazar, siber güvenlik sektörünün doğuşu ile birlikte sağlık, enerji, inşaat, finans alanlarındaki bilişim güvenliği kısmındaki harcamaların artmasına neden olmuştur. Türkiye'nin dünya genelinde yüzde 1 ortalama pay aldığını düşünürsek, birçok sektörde dünya geneli ortalamalarla Türkiye arasındaki boşluğu ülke olarak 3-5 sene içinde kapatacağımız gibi görünüyor.

Dolayısıyla, siber güvenlik algısının getirdiği önlemler, tüm sektörlerde ki sağlık, finans, enerji, inşaat vb. getirdiği yeni yaklaşımlarla birlikte, Türkiye'de bu rakam gün geçtikçe tüm sektörlerde daha da artacak. Bu hepimizin geleceği ve güvenliği için zaruret arz eden bir konu. Dolayısıyla bilişim ve Telekom tarafı olarak baktığımız zaman bu pazar durmadan artacak. Pazarın yeni nesil servisler olarak adlandırılan; nesnelerin interneti, IoT ve bulut servisler olarak vatandaşın ihtiyacını en iyi karşılayacak gelir getirici yönlere gideceklerini düşünüyorum.

**CyberMag: Son yıllarda internetin kullanımının artmasıyla birlikte ortaya çıkan IoT (nesnelerin interneti) kavramı ve internete bağlı cihaz sayısının artışı; bir başka hayati husus olarak bilgi güvenliği konusunun önemini, yerli ve milli çözümlerin ülkemiz adına geliştirilmesi gerektiğini gösteriyor. Bu bilgiler ışığında, Türkiye'deki siber güvenlik sektörünün durumu hakkında ne düşünüyorsunuz?**

**Taha YÜCEL:** Malumunuz, insanlık tarihi esas itibariyle deęişimlerin ve dönüşümlerin tarihidir. Bu deęişim ve dönüşüm sürecinde sanayi toplumu olma şansını yakalayamayan millet olarak, bilgi çağının bilgi toplumu olma şansını yakalayıarak bu tarihi süreçte yerimizi alma mücadelesi içerisindeyiz. Günümüzde ülkelerin gelişmişliklerinin ve zenginliklerinin tek ölçüsünün “sahip oldukları bilgili insan sayısı ve bilgi miktarı ile ölçüldüğü” düşünöldüğünde, bilgi toplumunun gelecekteki e-bireylerini ve bilgili insan kaynakları yetiştirmek, devletimiz ve milletimiz adına büyük bir kıymet ve anlam ifade ettięi tarihi bir gerçektir.

Toplum olarak bilgi toplumunun e-bireyleri olabilmek için fiziksel dönüşümden kültürel dönüşüme geçiş sürecini başarılı bir şekilde tamamlamamız ve bilgi ve iletişim teknolojilerini etkin ve güvenilir bir şekilde kullanıyor olmamız elzemdir.

Bu teknolojileri kullanırken, birçok farklı saldırılara maruz kalmamız kaçınılmazdır. Soyut bir ortam düşünün, saldırının nereden ve nasıl geldiğini kestirmek zor. Dolayısıyla sorunun kaynağına inerek, imalattan tutun seri üretime kadar, tüm örnekleriyle yerli ve milli ürünlerimizi ortaya çıkarmamız gerekmektedir. Kaynak kod kullanarak sonuca gitmeye çalışmak fayda vermeyecektir. Tamamen her şeyiyle yerli ve milli güvenlik yazılımlarımızı ve ürünlerimizi hayata geçirmemiz lazım. Aksi takdirde %90 oranında yabancı menşeli yazılım kullanılan ülkemizde siber güvenlik alanında rahat olmayı beklemek biraz zor olacaktır.

Ben önceden beri bunu söylüyorum. IoT hizmetleri insanların hayatını kolaylaştırmasının yanında riskleri de beraberinde getiriyor. Bu çözümlerin insan hayatına tedbirleriyle beraber sokulması gerekiyor. Aksi takdirde evinizde kullandığınız yeni nesil televizyonunuz sizi izleyebilecek bir cihaz konumuna gelebilir. Akıllı arabalar örneğine bakarsak, birisi sistemi ele geçirdiğinde sizi şeritten çıkarabilecektir. Dolayısıyla heyecan verici olduęu kadar endişe yaratıcı bir durum bu.

**CyberMag: Siber güvenlik pazarının ve tehditlerin bugünkü durumu nedir? Bir siber savaşta neler tehdit altında?**

**Taha YÜCEL:** Koronavirüs salgını sebebiyle günlük hayatımızın çevrim içi dünyaya taşındığı 2020 yılı, siber saldırılar açısından da oldukça aktif bir yıl oldu ve dijitale kayan dünya ile dijital ortamdaki tehditlerin boyutu ve sayısı arttı.

Siber uzmanlar tarafından, 2020 yılında siyah çapkalı hackerların verdięi Küresel zararın 6 Trilyon Dolar, siber güvenlik pazarının ise; 184 milyar Dolar olacağı, 2025 yılında ise verilecek

Küresel zararın 10,5 Trilyon Dolar ve siber güvenlik pazarının da 290 milyar Dolar olması öngörülmektedir.

Ülkemizde ise 2019 da Türkiye siber güvenlik pazarının 120 milyon Dolar olduğu ve 2025 de 260 milyon Dolar olacağı öngörülmektedir. Ancak, ülkemiz ekonomisinin Dünya ekonomisinin % 1'i dolayında olduğunu düşündüğümüzde, siber güvenlik sektöründe dünyaya kıyasla daha az pay aldığımız (bu oran % 0.1 gibi) görülmektedir.

Küresel bazda en hızlı büyüyen siber suç türünün fidye yazılımı saldırıları olduğu ve bu saldırıların 2016'da her 40 saniyede bir iken, 2021 yılında ise her 11 saniyede bir kez olacağı ve fidye yazılımı kaynaklı zararların maliyetinin 2021 yılına kadar 20 milyar dolar olacağı tahmin edilmektedir. Bu oran 2015'tekinden 57 kat daha büyüktür.

Bu açıdan, her türlü kritik alt yapı tehdit altında, bireyler tehdit altında. Konuştuğumuz gibi IoT(internet of things)'yi düşündüğünüz zaman "ağa bağlı" herkes tehdit altında; bu tehdit cebinde internete bağlı cep telefonu taşıyan herkes için geçerli. Kişinin, kişiye özel bilgilerinin olduğu bir kutudan bahsediyoruz.

Büyük boyutta bakarsak haberleşme sistemleri, ulaşım, sağlık sistemi, bankalar, enerji ve gaz şebekeleri siber savaşta hedef olabilir. Bir ülkeyi bir savaşta mağlup etmek için, örneğin elektrik ve haberleşme şebekelerini yok etmek veya çalışamaz hale getirmek, belki de binlerce askerini öldürmekten daha etkili olacaktır. Geçtiğimiz yıllarda 74 ülkeyi hedef alan "WannaCry" fidye yazılımı saldırısı da dünya çapında meydana gelen ve yüz binlerce insanı etkileyen bir yazılımın gücünü gösterir nitelikte. Bu hadise, ABD başta olmak üzere birçok ülkenin güvenliğini mercek altına almaya sevk etmiştir. Bizim de yapmamız gereken budur.

Basında birçok batı ülkesinin savunma sistemlerinin defalarca kırıldığı ve içeri sızmaların meydana geldiği yer aldı. Ayrıca, Amerikan Deniz Kuvvetleri'nin bilgisayarlarına sızıldığı, bir başka habere göre ise İran'ın 16 ülkede 50 hedefe koordineli bir saldırı yaptığı yer almıştı. Bütün bu durumu göz önünde bulundurarak dünyanın büyük bir siber savaşın eşiğinde olduğunu açıkça söyleyebiliriz. Böyle bir savaşta ise, ülkenin bütün sosyal ve ekonomik kaynakları (elektrik, su, sağlık, eğitim sistemleri ve bu sistemlerdeki kişilere özgü bütün bilgiler) tehdit altındadır.

Siber güvenlik anlamında baktığımız zaman, biz bu verileri korurken sadece internetin görünen yüzünü takip etmekle kalmamamız gerekiyor. İnternetin bir de karanlık yüzü var, dolayısıyla orda biraz da istihbarat anlamında elemanlar yetiştirip, analistlerin eğitimine önem vermemiz

gerekiyor. İşin bir de analiz boyutu var. Bu insanların da işin içine girmesi gerekiyor. Topyekûn bir seferberlik yapılması gerekiyor. Türkiye'nin konumu gereği, etrafındaki ülkeler gereği, etrafındaki doğalgaz, petrol gibi bütün kaynakların olduğu jeopolitik konumu açısından bizim çok dikkatli davranmamız gerekiyor. Daha fazla çalışmaya ihtiyacımız var.

**CyberMag: İnternet kullanım oranlarındaki artışı neye bağlıyorsunuz? İnsanlar açık bilgi ortamlarına neden bu kadar istekli? Endüstri 4.0 trenini kaçırmamak adına özel sektörün ve devletimizin alması gereken sorumluluklar nelerdir?**

**Taha Yücel:** İnternetin, gerçek dünyada ulaşılamamış isteklerin ve hayallerin, sanal bir evrende de olsa gerçekleştirilebileceğini iddia etmesi, insanların üzerinde büyü etkisi yapmış olabileceğini de göz önünde bulundurmamız gerekiyor. Elbette, bilginin “güç” olmasının keşfedilmesi ile birlikte bilgiye olan aşırı büyük ilginin de bu başarıda büyük katkısı olmuştur

Bizim ülkemizde ise zeki, kapasiteli ve dinamik bir genç nüfusumuz var. Bu genç nüfusumuzun doğru eğitilerek, yönlendirilerek ve hedef verilerek sayısal ortama adapte edilmesi lazım. Sayısal ortamdan kastım bilgi, iletişim, medya ve bütün hepsini de içeren ortamdır. Bu ortam ile ilgili büyük fabrikalar, büyük sanayi altyapıları kurmamız, büyük yatırım yapmamız gerekmiyor. Bu bizim için büyük bir fırsat. Biz doğru eğitimle doğru beyin gücümüzle yazılım sektöründe dünyada sayılı ülkeler arasına girebiliriz çünkü bu potansiyelimiz var. Bunun için ilkokuldan itibaren hem internet okuryazarlığını ders olarak vermemiz hem de çocuklarımıza kod yazmayı öğretmemiz lazım.

Biz yazılımda güçlü olursak, eğitimde, savunmada, sağlıkta, otomotivde, tarımda ve aklımıza gelebilecek her sektörde iddialı, başarılı ve vazgeçilmez oluruz. İnsanların faydasına da bunu kullanırız. Türkiye bir teknoloji geliştirirse insanların faydasına kullanır. Bizim insanımızın, genç nüfusumuzun birlik ve beraberlik içinde Türkiye'nin faydasına çalışması lazım.

**CyberMag: Son dönemde siber güvenlik kurulunun oluşturulması veya USOM ve SOME birimlerinin hayata geçirilmesi gibi birçok adım atıldı. Siz bu adımları yeterli buluyor musunuz? Rusya veya ABD gibi bu alanda sözü geçen bir ülke konumunda olmak için neler yapmamız gerekiyor?**

**Taha Yücel:** Türkiye'nin bu konuda topyekûn seferber olması gerekiyor. Her şeyi devletten beklememek gerekir. Üniversitelerimizin bu konuya daha fazla odaklanması lazım. Sivil toplum örgütlerimizin de aktif olması lazım. Bilgi Güvenliği Derneği'mizin ve dergimizin misyonu da zaten budur. Yani bilgi güvenliği konusunda, siber güvenlik konusunda şuur



oluşturmak, unutturmamak, farkındalık oluşturmak, eksiklikleri tespit etmek, bunlarla mücadele etmek, sinerji oluşturmak gerekir. Üniversitelerimiz, sivil toplum örgütlerimiz, özel sektörümüz ve devletimiz hep birlikte bilgi güvenliği konusunu önemsememiz lazım. Bilgi güvenliği farkındalık eğitimlerinin de yaygınlaştırılması gerekiyor. Bilgi Güvenliği Derneği'mize de bu hususta önemli bir sorumluluk düşüyor.

Türkiye siber saldırıya uğrayan ve/veya siber saldırı yapan ülkeler arasında her zaman ilk onda yer almaktadır. Ülkemizden başlatılan siber saldırıların temelinde lisanssız yazılımlar ve bilinçsiz BT kullanımı yer almaktadır. Lisanssız yazılım ve bilinçsiz BT kullanımı nedeniyle köle (Zombi) haline gelen bilgisayarların uzaktan kötü niyetli kişiler ve/veya örgütler tarafından kullanılmasıyla söz konusu saldırılar gerçekleştirilmektedir. Ülkemize yapılan siber saldırıların büyük çoğunluğu ise kamu kurumlarının web sayfalarına ve/veya kritik altyapılara yapılan hizmet dışı bırakma ve/veya bilgi elde etmeye yönelik olarak gerçekleştirilmektedir. 15 Temmuz sonrasında ise kamu kurumlarına ve kritik altyapılara yapılan siber saldırıların sayısında büyük artışlar olduğu resmi makamlarca ifade edilmektedir. BGD Yönetim Kurulu Başkanı olarak sürdürülebilir bir siber güvenliğin sağlanması amacıyla, kamu BT altyapısı ile kritik altyapılarda milli olarak geliştirilen özgün bilişim ve siber güvenlik ürünlerinin kullanılmasının, siber güvenlik alanında nitelikli insan kaynağı yetiştirilmesinin ve kamuda farkındalık eğitimlerinin düzenli olarak yapılmasının önemli olduğuna bir kez daha dikkat çekmek istiyorum.

**CyberMag: Bu bilgiler ışığında sizce Türkiye'de siber güvenlik adına yapılması gerekenler nelerdir? Ulusal güvenlik açısından siber güvenliğin önemi nedir?**

**Taha YÜCEL:** Teknoloji geliştikçe bilgi artışı gerçekleşmekte, bilgi artışı geliştikçe de teknoloji gelişmektedir. Teknolojinin gelişmesi; bilgi güvenliği kavramı adına da bir tehdit unsuru oluşturmaktadır. Bir devlete ait teknik, askeri ve mali bilgiler, bir şirkete ait yatırım, borç ve alacak bilgileri, bir üniversiteye ait ar-ge proje bilgileri, bir kişiye ait özel iletişim, harcama bilgileri, üst düzey kişilere ait sağlık bilgileri çok kritik ve önemlidir. Dolayısıyla, sanal dünyanın en önemli ögesi olan insanımızı yetiştirilmeli ve bireysel küreselleşmeyi sağlayarak bilgi ve iletişim teknolojilerini amacına uygun ve bilinçli bir şekilde kullanmamız gerekmektedir.

Bugün genç bir çocuk 9 yaşında hacker'lığa başlamış olabiliyor. Bu bir anlamda fırsat aslında. Biz eğer bunu iyi yönde bir fırsata çevirebilirsek, yani kıvrak zekâ boyutunu eğer güvenlik tarafına yönlendirebilirsek başarı kaçınılmaz olacaktır.

Bir diğerk boyutu da devlet yönetiminde önemli kararlar alınması. Şöyle düşünün: İnternete fiziksel olarak bağılı ne kadar cihaz varsa, hepsinin teknik olarak siber saldırıya uğraması mümkündür. Tek kişiyle de bir ülkeyi çok rahatlıkla alt edebilecek bilgiye sahip olabilirsiniz. Konu siber güvenlik olduğu zaman bir tek kişi de dev bir ordu görevi görebilir. Herhangi bir sistemin internet üzerinden siber saldırı karşısında risk altında olması için o sistemi internete bağlayan tek bir bilgisayar veya cihaz yeterlidir. Bu durumda, bilgisayarlara yüksek oranda bağımlı olarak işleyen aklınıza gelebilecek her sistem tehdit altında olabilir demektir. Bu da internet erişimi dahil olmak üzere mobil ve konvansiyonel haberleşme şebekelerini, TV-radyo yayınlarını, tren, tramvay ve metro gibi ulaşım sistemlerini, hava ulaşımını, enerji üretim ve nakil ve dağıtım sistemlerini, hastaneleri, bankaları ve daha birçok sistemi kapsayan bir güvenlik ihtiyacının ortaya çıkması demektir. Bu şekilde düşünüldüğünde siber güvenliğin ulusal güvenlik açısından önemi anlaşılır. Mesela Merkez Bankası'ndaki bir güvenlik duvarı cihazı, adeta sınır karakolunda nöbet tutan bir asker gibi görülebilir.

**CyberMag: RTÜK olarak, bilgi güvenliğı konusunda çalışma yürüten sivil toplum kuruluşlarına, derneklere destek veriyorsunuz. Aynı zamanda sektörün ek köklü STK'sı olan Bilgi Güvenliğı Derneğı Yönetim Kurulu Başkanı olarak göreve başladınız. Bu durum göz önünde bulundurulduğunda, sektör üzerinde bir sinerji oluşturmak ve farkındalık yaratmak adına yola çıkan ve yayın hayatına beş seneyi aşkın bir süredir devam eden CyberMag Dergisi hakkında düşünceleriniz nelerdir?**

**Taha Yücel:** Çıktığı ilk günden itibaren CyberMag Dergisi'ni takip ediyorum, zevkle okuyorum, istifade ediyorum ve çok da önemsiyorum. Öncelikle, bir şeyin az da olsa sürekli olması faydalıdır. Bir şeyin hepsi ele geçmezse bir kısmını da elden kaçırmamak gerekir. Tabi ki daha yapılması ve geliştirilmesi gereken şeyler var. Mesela dergideki bazı makalelerin İngilizcelelerini de eklemek iyi olur, belki yurt dışına da açılmak gerekir. Sizleri de gençlik platformu olarak yurt dışına taşımakta fayda var. Yurt dışında bu alanda ve benzeri alanlarda yazılım sektörü ile ilgili, bilgi güvenliğı ile ilgili, blok zincir teknolojisi ile ilgili, ITU'da, Amerika'da, Avrupa'da nerede kritik etkinlik varsa mutlaka birkaç arkadaşımızın desteklenerek oralarda Türkiye'mizi temsil etmesi gerekir. Şöyle güzel bir söz var; "Kovandan çıkmayan arı bal yapamaz". Kovan Türkiye, Türkiye'den dışarı çıkacaksınız ki Türkiye'ye daha çok bal yapacaksınız. Göreceksiniz ki dünyada konuşulan konular ile sizin konuştuğunuz konular çok farklı değil, dünyada yapılanlar ile sizin yaptıklarınız çok farklı değil. Ama sadece internet ortamından veya Türkiye'den elde ettiğimiz bilgilerle değil, yüz yüze dostluklar geliştirerek, insan tanıyarak, konunun uzmanlarını tanıyarak iletişim kurmalıyız.

**CyberMag: Son olarak BGD'nin gelecek çizmiş olduđu vizyon nedir?**

BGD, sosyal sorumluluğunun farkında olan bir sivil toplum kuruluşu olarak bundan böyle katılımcı, paylaşımcı ve iş birliğine açık bir çalışma yöntemiyle ve bütüncül bakış açısıyla sürdürülebilir ve milli çözümlerden yana olarak mevzuatın geliştirilmesi, ulusal kapasitenin artırılması, bilgi ve bilinç düzeyinin yaygınlaştırılması yönünde çalışmalarına daha verimli ve etkili bir şekilde çalışmaya devam edecektir.

**CyberMag: Eklemek istediğiniz başka bir konu var mı?**

**Taha Yücel:** Genel hatlarıyla, Türkiye'ye baktığımızda siber güvenlik pazarında, farkındalığın arttığını söyleyebilirim. Ama benim kişisel görüşüm odur ki biz güç birliği yapmadığımız sürece bu farkındalık istediği kadar artsın Türkiye'yi yeterli düzeye çıkaramayız. Türkiye'deki bütün unsurları ortak akıl çerçevesinde kamu, özel sektör, devlet ve üretici iş birliğiyle masaya yatırarak ortak çözüm oluşturulabilir. Aksi takdirde çok mümkün görünmüyor. Bu nedenle Bilgi Güvenliği Derneği'ne her konuda destek vererek ortak çalışma yapacak kurum ve kuruluşlardan memnuniyet duyuyoruz.

Bizim Türk insanı doğası gereği paylaşmayı sevmez. Hele konu siber güvenlik konu olunca asla paylaşmaz. Ama bunu yapmak zorundayız. BGD olarak bizim misyonumuz çalışmalarımızı sürdürdüğümüz her alanda ortak paydada buluşarak, tüm sektörlerde temkinli ve bilinçli hareket etmektir. Devam eden tüm projelerimizde, bu ülkedeki ihtiyaç olan ortak akıl oluşturup, önümüzdeki dönemde ülke genelinde söz sahibi olmak için adımlarımızı atıyoruz.

Bu alanda durum tehlikeli olsa da tehlikeyi fırsata çevirip, dünyada söz sahibi olup beklenen ve aranan Türkiye konumuna geleceğimizi düşünüyorum. Genç girişimciler olarak çalışarak sonuca gideceğiz ve ülkemizi layık olduđu konuma getireceğiz. Saygılarımla...