



7/16360 GK 14

GÜNLÜDÜR
02/12/2024

İSTANBUL MİLLETVEKİLİ SAYIN İSA MESİH ŞAHİN'İN
7/16360 ESAS SAYILI YAZILI SORU ÖNERGESİNE İLİŞKİN CEVAPLAR

Lübnan'da, İsrail'in "pager" isimli çağrı cihazlarına sızarak patlatması sonucu 8 kişinin hayatını kaybettiği ve yaklaşık 2800 kişinin yaralandığı olay, elektronik iletişim sistemlerine yönelik siber saldırıların ne denli büyük tehdit oluşturabileceğini bir kez daha gözler önüne sermiştir. Türkiye'nin coğrafi konumu, stratejik önemi ve bölgesel gerilimler göz önünde bulundurulduğunda, benzer saldırılara karşı ülkemizin güvenliği ve vatandaşlarımızın korunması son derece önem arz etmektedir.

Lübnan'da yaşanan bu olay, çağdaş savaş yöntemlerinin ve siber saldırıların, sadece dijital dünyada değil, fiziksel dünyada da büyük yıkımlara yol açabileceğini göstermektedir. Türkiye'nin güvenliği açısından, benzer saldırılara karşı önceden önlem almak ve gerekli düzenlemeleri hayata geçirmek elzemdir. Özellikle vatandaşlarımızın hayatını tehlikeye atabilecek bu tür riskler karşısında güçlü bir siber güvenlik altyapısının oluşturulması büyük önem taşımaktadır.

Bu bağlamda;

Soru 1- Türkiye, elektronik iletişim cihazlarına yönelik olası siber saldırılara karşı ne tür güvenlik önlemleri almaktadır? Özellikle kritik altyapılar ve kamuya ait sistemler bu tür saldırılara karşı yeterli korumaya sahip midir?

Soru 2- Cep telefonu, çağrı cihazı, telsiz gibi iletişim araçlarına yönelik siber saldırılar veya uzaktan manipülasyon girişimlerine karşı Türkiye'deki güvenlik birimlerinin bir risk değerlendirmesi yapılmış mıdır? Eğer yapıldıysa, bu değerlendirmelerin sonuçları nelerdir?

Soru 3- Lübnan'daki olaya benzer şekilde Türkiye'de elektronik cihazların patlaması veya infilak etmesi riskine karşı özel bir denetim mekanizması kurulması düşünülmekte midir?

Soru 4- İletişim alanında ne tür millî teknoloji çalışmalarımız mevcuttur? Varsa çalışmalar hangi aşamada?

CEVAPLAR:

Cevap 1-2-3-4- Ülkemizde siber güvenlik faaliyetleri, bireysel yetkinlik ve toplumsal farkındalık kazanımı, özel sektörde dijital dönüşüm, yerli ve milli ürün geliştirme, kamu kurumları ve kritik altyapılarda güvenlik tedbirleri, siber olaylarla mücadele gibi geniş bir yelpazede yürütülmektedir. Bu yelpazenin farklı kısımlarında, farklı kurumların sorumluluğu söz konusudur.

Ülkemizde kritik altyapılar, kamu kurumları, elektronik haberleşme sistemleri gibi kritik unsurların siber güvenliğinin sağlanması Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, Bilgi ve İletişim Kurumu ve diğer güvenlik birimlerinin sorumluluğunda yer almaktadır. Bu çerçevede, ilgili kurumlarımız etkin çalışmalarını yürütürken ülkemizin siber güvenlikteki kurumsal yapısı ve performansı sürekli iyileştirilmektedir.

Sanayi ve Teknoloji Bakanlığı ise, bir yandan kamuda siber güvenliğin sağlanmasına katkıda bulunurken diğer yandan ise ülkemizde siber güvenlik ekosisteminin geliştirilmesi, toplumda siber güvenlik farkındalığının oluşturulması, teknoloji uzmanlarının yetiştirilmesi, siber

güvenlik girişimlerinin desteklenmesi, bu alanda kullanılacak kritik teknolojilerin ve altyapıların geliştirilmesi, siber güvenlik alanına ilişkin teknik kriterler hazırlanması ve mevzuat düzenlemeleri gibi birçok boyutta faaliyet yürütmektedir.

Kamuda hizmet alınacak bilişim firmalarının teknik ve bilgi güvenliği kapasitesi yükseltmek amacıyla Kamu Bilişim Alımları Yetkilendirme Sistemi kapsamında tüm firmaların TS 27001 Bilgi Güvenliği Standardına, sızma testi hizmeti sunacak firmaların ise TSE Sızma Testi Firma Belgesine sahip olmaları zorunlu hale getirilmiştir.

Sanayi ve teknoloji ekosistemimizin ihracatını yakından ilgilendiren, Avrupa Birliği tarafından 2027 yılında zorunlu uygulamaya girecek olan Siber Dayanıklılık Yasası Bakanlığımızca yakından takip edilmektedir. Yazılım ve donanım dâhil, dijital ürünlerin tasarımı, geliştirilmesi, üretimi ve piyasaya arz edilebilmesinde gerekli siber güvenlik standartlarının çerçevesini çizen bu düzenleme, uyumlaştırılmak suretiyle iç mevzuatımıza kazandırılacaktır. Bu doğrultuda, Bakanlığımızca mevzuatın uyumlaştırılması, etki analizi, onaylanmış kuruluşlar ve test laboratuvarları kapsamında çalışmalar yürütülmektedir.

TÜBİTAK burs ve destek programları kapsamında siber güvenlik alanında/sektöründe 2002-Günümüz döneminde 775 proje ve 211 kişiye (2024 sabit fiyatlarıyla) toplam 4,76 Milyar TL destek verilmiştir:

- Sanayiye yönelik destek programları kapsamında 637 projeye 3,75 Milyar TL (2024 sabit fiyatlarıyla) destek verilmiştir.
- Akademiye ve kamuya yönelik destek programları kapsamında 138 projeye 337,82 Milyon TL (2024 sabit fiyatlarıyla) destek verilmiştir.
- Bilim insanlarına yönelik burs ve destek programları kapsamında 211 kişiye 673,5 Milyon TL (2024 sabit fiyatlarıyla) destek verilmiştir.

TÜBİTAK BİLGEM Siber Güvenlik Enstitüsü, ulusal siber güvenlik kapasitesinin artırılmasına yönelik çalışmalar gerçekleştirmekte olup ulusal çapta, ülkemizin teknolojik bağımsızlığına katkı sağlayacak projeleri hayata geçirmek amacıyla çeşitli alanlarda araştırma ve geliştirme faaliyetleri yürütmektedir.

Türkiye’de ilk kez, IoT (Internet of Things) (Nesnelerin Güvenliği) Cihazlarını Araştırma / Geliştirme çalışmalarında kullanabilmek ve test/ danışmanlık proje taleplerini karşılayabilmek amacıyla, Siber Güvenlik Enstitüsü bünyesinde, 2022 yılında, “**IoT Güvenliği Laboratuvarı**” kurulmuştur. **IoT Güvenliği Laboratuvarı**, “Donanım Güvenliği”, “Firmware Analizleri”, “Uygulama Güvenliği” ve “Radyo Frekans Güvenliği” alanlarında hizmet vermektedir.

USOM ve SOME sistemlerinin temelini oluşturulan TR-BOME (Türkiye Bilgisayar Olaylarına Müdahale Ekibi) TÜBİTAK tarafından kurulmuştur.

Milli Savunma Bakanlığı (MSB) ile imzalanan protokol ile Siber Güvenlik Enstitüsü, Türk Silahlı Kuvvetleri’nin siber olgunluğunu arttıracak test ve danışmanlık hizmetlerini sağlamaktadır. Bu kapsamda MSB ve bağlı kuvvetler için sızma testi, risk analizi, statik kod güvenlik analizi ve eğitim hizmetleri verilmektedir. Ayrıca bu yapılarda kullanılacak yerli ürünler için de gerekli denetimler sağlanmaktadır.

TSK Bulut Bilişim Danışmanlığı projesinin güvenlik danışmanlığı alanında AYYILDIZ projesi danışmanlığı Siber Güvenlik Enstitüsü tarafından gerçekleştirilmiştir.