**Basın Bülteni Ağustos 2023**

**STM’den Dikkat Çeken Siber Tehdit Raporu:**

**ChatGPT’te Kullanıcıların Bilgileri Sızdırıldı**

*STM yeni açıkladığı Siber Tehdit Durum Raporunda, yapay zeka aracı ChatGPT’de yaşanan bir kesinti sonucu bazı kullanıcıların; kişisel bilgileri ve kredi kartı bilgilerinin sızdırıldığına dikkat çekti. STM raporda, kritik enerji tesislerindeki siber güvenlik yetkinlik modelini ve siber-fiziksel sistemlerde alınması gereken önlemleri de mercek altına aldı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, Nisan-Haziran 2023 tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 8 ayrı konu başlığı bulunuyor. Raporda, yapay zeka aracı ChatGPT’te yaşanan kesinti ve zafiyetler, enerji sektöründe siber güvenlik yetkinlik modeli, siber-fiziksel sistemlerin güvenliği, en çok siber saldırı gerçekleştiren ülkeler gibi birçok güncel ve ilginç konu başlıkları yer alıyor.

**ChatGPT’te Bazı Kullanıcıların Bilgileri Sızdırıldı**

Son zamanların en popüler yapay zeka uygulamalarının başında gelen ve çıkış yaptığı ilk aylarda 100 milyon kullanıcı barajını aşan ChatGPT’nin ücretli abonelik sürümü olan “ChatGPT Plus” Şubat ayında kullanıma sunulurken, ChatGPT’de Mart ayının son haftasında birkaç saatlik kesinti meydana geldi. STM’nin raporuna göre, ChatGPT’nin kullandığı bir açık kaynak kütüphanesi bu kesintiye sebep oldu ve bu kütüphanede kullanıcıların birbirlerinin sohbet geçmişlerini görmesine olanak sağlayan zafiyetler oluştu. OpenAI yaptığı açıklamada, ChatGPT Plus üyeliği olan kullanıcıların yüzde 1,2’sinin belli bir saat diliminde aktif bir şekilde platformu kullandılarsa, ödeme bilgilerinde veri ifşasının gündeme geldiğine dikkat çekti. Raporda, o zaman dilimindeki aktif kullanıcıların; isim, soy isim, e-posta adresi, fatura adresi, kredi kartı tipi, kredi kartının son dört hanesi ve kredi kartının son kullanma tarihi gibi verilerinin görüntülendiği tespiti yer aldı.

Bir diğer araştırmada ise CHATGPT’ye yerleştirilen bir dosya sayesinde, kullanıcıların bu bağlantıya tıklamasıyla, hesaplarının ele geçirildiği ortaya çıktı. Saldırganların, bu yolla kullanıcıların hesap bilgilerini, sohbet geçmişlerini, fatura bilgilerine erişebildiği belirtilirken, OpenAI’in bu zafiyeti kısa sürede kapattığı kaydedildi.

**“Siber-Fiziksel Sistemlerde Önlem Alınmazsa Veri Kaybı Yaşanabilir”**

STM’nin raporunda ele alınan bir diğer konu ise CPS (Cyber-Physical System) yani Siber-Fiziksel Sistemler oldu. Fiziksel ve dijital bileşenlerin birlikte çalıştığı gerçek zamanlı gömülü sistemler olan CPS’nin günlük hayatta kullanımı giderek yaygınlaşıyor. Bir fabrikada otomatik makinelerin ve robotların birlikte çalışması, sağlık sektöründe tıbbi cihazların veri paylaşımı veya sivil-askeri birçok alandaki sistemlerde gerçek zamanlı veri paylaşımı CPS örnekleri olarak karşımıza çıkıyor. Ancak bu dijitalleşme beraberinde bazı risklerinde beraberinde getiriyor. Raporda, CPS’lerin kötü niyetli kişilerin siber saldırılarına maruz kalabileceği, bu saldırılar sonucunda sistemlerin kapalı kalma süresine, veri kaybına, hatalı çalışmasına ve hatta kullanıcıların fiziksel olarak zarar görmesine neden olabileceğine dikkat çekildi. Bu tehditlerden korumak için; veri güvenliği, ağ güvenliği ve yazılım güvenliğinde gerekli önlemlerin alınması gerektiği belirtilerek, “Güvenlik uzmanları, CPS sistemlerini sürekli olarak değerlendirmeli, güncellemeler yapmalı ve güvenlik açıklarını tespit etmelidir” uyarılarına yer verildi.

**Kritik Enerji Tesislerinin Siber Güvenliği**

STM raporda, Türkiye’de 6 Haziran 2023 tarihinde yürürlüğe giren ve enerji sektöründe kullanılan endüstriyel kontrol sistemlerinin siber güvenliğini iyileştirmeyi amaçlayan “Enerji Sektöründe Siber Güvenlik Yetkinlik Modeli Yönetmeliği”ni de detaylı şekilde ele aldı. Elektirik dağıtım şirketlerinden doğalgaz dağıtım sektörüne kadar kritik enerji tesislerinde siber güvenlik uygulamalarının sınıflandırması, yetkinlik modeli ve atılacak adımlar raporda yer aldı.

**En Çok Siber Saldırı ABD’den**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. 2023’in Nisan, Mayıs ve Haziran ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu)’larına toplam 3 milyon 304 bin saldırı yansıdı. En çok saldırıyı yapan ülke 194 bin ile Amerika Birleşik Devletleri (ABD) olurken, 185 bin saldırı ile Rusya ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Hindistan, Fransa, Hollanda, Almanya, Çin, Vietnam, Polonya ve Türkiye izledi.

**Rapora Erişim Linki:** <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2023>

**STM ThinkTech Hakkında**

STM ThinkTech, savunma–güvenlik ve mühendislik-teknoloji alanlarında var olan bilgi birikimi ve insan kaynağıyla bölgesel ve küresel stratejiler, teknolojik öngörüler, olası senaryolar ve karar destek sistemleri geliştiriyor. Türkiye’nin gelecek vizyonuna uygulanabilir, düşünsel ve pratik katkılar sunan STM ThinkTech, başta savunma olmak üzere havacılık, enerji, ulaştırma, eğitim ve sağlık alanlarında objektif bir yaklaşımla teknoloji odaklı analizler ile özgün çözümler geliştiriyor ve veri işleme yeteceğiyle raporlar yayımlıyor. STM ThinkTech, geliştirmekte olduğu öngörüler ve stratejik çözümler için akademisyenler, diğer düşünce kuruluşları, üniversiteler, yüksek teknoloji üreten firmalar, kamu kurumları ve karar vericilerle iş birliği gerçekleştiriyor.

<https://thinktech.stm.com.tr>

**STM Hakkında**

Savunma sanayiine mühendislik, teknoloji ve danışmanlık alanlarında çeyrek asırdan uzun bir süredir hizmet veren STM, bugün sahip olduğu temel kabiliyet ve teknolojilerini askeri deniz platformlarından taktik mini İHA sistemlerine, uydu çalışmalarından siber güvenliğe, büyük veri analitiğinden yapay zekâ uygulamalarına varan stratejik alanlarda kullanarak Türkiye'nin ve dost ülkelerin ihtiyacı olan kritik alanlarda çalışmalar yürütmektedir.

[www.stm.com.tr](http://www.stm.com.tr)