**Basın Bülteni Ağustos 2024**

**STM’den Yeni Siber Tehdit Raporu:**

**QR Kodlar Üzerinden Yapılan Siber Saldırılarda Artış Yaşanıyor**

*STM, yeni açıkladığı Siber Tehdit Durum Raporu’nda, gündelik hayatta insanlara kolaylık sağlayan QR kod teknolojisi üzerinden yapılan siber saldırılarda yüzde 587 oranında artış yaşandığına dikkat çekti. Dolandırıcıların sahte QR kodları oluşturarak, bunları kamusal alanlara yerleştirdiği belirtilen raporda, güvenilmez kaynaklardan gelen QR kodların taranmaması ve çeşitli güvenlik yazılımlarının kullanılması gerektiği vurgulandı.*

Türkiye’de siber güvenlik alanında önemli projelere ve yerli ürünlere imza atan STM’nin, Teknolojik Düşünce Merkezi “ThinkTech”, 2024 Nisan-Mayıs-Haziran tarihlerini içeren yeni Siber Tehdit Durum Raporu’nu açıkladı. Siber güvenlik alanında farkındalık yaratmak amacıyla, STM’nin siber güvenlik uzmanları tarafından hazırlanan raporda, 7 ayrı konu başlığı bulunuyor. Raporda, deniz platformlarında siber güvenlik, silah sistemlerinin siber dayanıklılığını artırmak, QR kod tabanlı saldırılar ve güvenlik önlemleri gibi güncel ve ilginç konu başlıkları yer alıyor.

**Gemilerde Siber Güvenlik Tasarım Aşamasında Başlamalı**

Dünya ticaretinin yaklaşık yüzde 90’ını taşımakla küresel ekonominin bel kemiğini oluşturan denizcilik sektörü, dijital dönüşümün getirdiği yenilikler, üzerinde IT (bilgi teknolojileri) ve OT (operasyonel teknoloji) sistemleri barındırıyor. Gemilerde, bu dijitalleşme süreci de, siber güvenlik tehditlerinin artmasına imkân tanıyor.

STM’nin hazırladığı raporda, gemi platformlarına düzenlenen siber saldırıların, büyük finansal kayıplar getirmesinin yanı sıra devletlerin milli güvenliklerini de tehdit eden bir unsura dönüştüğüne dikkat çekiliyor. Buna göre, geminin; otomasyon, navigasyon, iletişim sistemlerine yönelik siber saldırıların yanı sıra liman ve lojistik sistemlerine saldırılar, tedarik zinciri ve lojistik ağlara saldırılar ve veri ihlalleri, casusluk bu alanda ön plana çıkıyor. Siber güvenlik önlemlerinin önemli bir bölümünün geminin henüz tasarım aşamasındayken planlanmaya başlanması gerektiğine değinilen raporda, olası tedbirler belirlenirken üretim, devreye alma ve operasyon sürecinde yapılması gerekenlerin ayrı ayrı ele alınmasının güvenliği bir üst seviyeye çıkartacağına yer verildi.

Bu noktada, varlık yönetimi süreci yürütülerek, platform üzerindeki tüm mobil ve taşınabilir cihazların envanteri alınmalı ve sürekli güncellenmeli. Ağ yönetimi ve güvenliğinde, ağlar arasında etkileşime sadece gerektiği kadar yer verilmeli ve segmente edilmiş ağa sadece yetkili kişiler ve yetkili cihazlar erişebilmeli. Yazılım güvenliğinde, geliştirilebilecek, tedarik edilebilecek ve dışarıdan gelebilecek kötücül yazılımlar için tedbirler alınmalı, yazılımların güvenlik testleri yapılmalı. Erişim güvenliği sağlanırken, uzaktan erişim ile ilgili kontrol ve kısıtlar protokollerinin uygulanması, yaşanabilecek her senaryo için yönergeler hazırlanmalı ve ilgili gemi personellerine siber güvenlik eğitimleri verilmeli. Verilerin yedekleme ve geri döndürme süreçlerinin de yürütülerek, risk yönetim sürecini işletilmesi gerekiyor.

**QR Kodlar Üzerinden Siber Saldırılar**

Restaurantlardan alışverişe, bilet işlemlerinden birçok alana kadar gündelik hayatta insanlara kolaylık sağlayan QR kod teknolojisinin kullanımı özellikle pandemi sonrası önemli derecede yaygınlaştı. QR kod tabanlı saldırılar da bu sebeple son zamanlarda hızla artış gösteriyor. “QR Kod Tabanlı Saldırılar ve Güvenlik Önlemleri” başlığı altında saldırıları ve saldırılara dair alınabilecek önlemler de raporda yer aldı. Yapılan bir araştırmada, Ağustos-Eylül 2023 arasında QR kod kimlik avı saldırılarında yüzde 587 oranında artış olduğu raporlandı. Dolandırıcıların sahte QR kodları oluşturduğu ve bunları meşru görünen yerlere yerleştirerek, cihazlara uygulama indirerek, kötü amaçlı yazılım bulaştırdıkları belirtilen raporda, QR kodların sahte bankacılık, alışveriş sitelerine yönlendirilerek, kullanıcı bilgilerinin çalınabildiğine veya saldırganların, ödeme yapılacak QR kodlarını manipüle ederek paranın kendi hesaplarına yönlendirilmesini sağladığına dikkat çekildi. Raporda, güvenilmez kaynaklardan gelen QR kodlarının taranmaması gerektiği, çeşitli antivirüs yazılımlarının kullanılması ve cihaz yazılımlarının güncel tutulmasının, QR saldırı tehdidinden korunmak için yapılacak temel önlemlerden olduğu belirtildi.

**En çok Siber Saldırıyı Hangi Ülkeler Yaptı?**

STM’nin kendi Honeypot sensörleri tarafından veriler; dünya genelinde en çok siber saldırı toplanan ülkeleri de ortaya koydu. Nisan-Mayıs-Haziran 2024 ayları boyunca STM’nin Honeypot (Bal küpü-tuzak sunucu)’larına toplam 1 milyon 390 bin saldırı yansıdı. En çok saldırıyı yapan ülke, 138 bin saldırı ile Ukrayna olurken, 127 bin saldırı ile ABD ikinci sırada yer aldı. Bu ülkeleri sırasıyla; Rusya, Hindistan, Singapur, Almanya, Mısır, Çin, Estonya ve Vietnam izledi.

Raporun dönem konusunda ise silah sistemlerinin siber dayanıklılığının hangi yöntemlerle artırılacağı mercek altına alındı.

**Rapora Erişim Linki:** <https://thinktech.stm.com.tr/tr/siber-tehdit-durum-raporu-nisan-haziran-2024>

**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)