STRATEJİK İLKELER

1. Mevcut siber güvenlik riskleri, siber güvenlik kapsamında stratejik amaçların en doğru şekilde tanımlanabilmesi için siber güvenlik riskleri değerlendirilecek.

2. Kritik altyapıların kullandığı bilişim sistemlerine yapılacak saldırılar karşısına alınacak önlemler, bunlara ek olarak kişisel bilgilerin çalınmaması ve ifşa olmaması için alınabilecek önlemler belirlenecek.

3. Toplumun internet ve sosyal ağlara olan bağımlılığının artması ve siber güvenlik alanında yeterli düzeyde bilgi ve bilinç seviyesine sahip olmaması hususlarında toplumu bilinçlendirme adına yapılacak eylemler kararlaştırılacak.

4. Özellikle online bankacılık trojanlerinin müşteri bilgilerini çalmak için kullandıkları yöntemleri ortaya çıkarmak için popüler bankacılık trojanlerinin dinamik ve statik analizlerinin merkezde görevli öğrenciler tarafından gerçekleştirilecek.

5. Tehdit unsurlarının saldırı yapmadan önce bertaraf edilmesi için proaktif siber savunma adına yapılacak eylemler kararlaştırılacak.

6. Siber suçlarla müdahelede birikimli ve donanımlı bireylerin yetiştirilmesi adına birimin yapacağı eğitim faaliyetleri gerçekleştirilecek.

7. Nesnelerin Interneti Botnet (IoT BOTNET) saldırılarının tespiti ve vermiş olduğu zararların ortaya çıkarılması noktasında, bu tür zararlı yazılımların dinamik ve statik analizleri yapılacak.

8. Siber Güvenlik Uygulama ve Araştırma Merkezi'nin öğrenci merkezli olarak faaliyetlerine devam edilecek.