SİBER TUZAK:

API KÖTÜYE KULLANIMIYLA DOLANDIRICILIK

API İSTİSMARI NASIL TUZAĞA DÖNÜŞÜYOR?

Uygulama Programlama Arayüzü ("Application Programming Interface" veya "API"), farklı yazılım sistemlerinin birbiriyle iletişim kurmasını ve veri alışverişi yapmasını sağlayan kurallar, protokoller ve araçlar bütünü olarak özetlenebilir. Dijital altyapının temel taşı olan bu arayüzlerin güvenliği ihmal edildiğinde; API'lerin yetkisiz kullanımıyla veri hırsızlığı yapılması, kullanıcı hesaplarının ele geçirilmesi ve bu yolla finansal çıkar sağlanması mümkün olabilmektedir.

Bu istismar yöntemleri arasında; kısa sürede aşırı sayıda istek gönderilerek sistem kapasitesinin zorlanması, sistemdeki açıklar yoluyla müşteri verilerine ve finansal bilgilere izinsiz erişim, kampanya ve promosyonlardan haksız yararlanma, sahte bilgilerle veya çalıntı verilerle toplu hesap açma ve API parametrelerinin değiştirilerek transfer limitlerinin aşılması ya da indirimlerin kötüye kullanılması gibi işlem manipülasyonları yer almaktadır.

Özellikle yeni nesil fintech uygulamaları, e-ticaret platformları ve dijital üyelik sistemleri bu tür saldırılara karşı en riskli alanlar arasında bulunmaktadır.

HUKUKİ DEĞERLENDİRME:

- ***TCK m.243:*** API aracılığıyla sistemlere izinsiz giriş, "*bilişim sistemine girme*" suçunu oluşturabilir.
- ***TCK m.244:*** API istismarı yoluyla sistemin çalışamaz hâle getirilmesi veya verilerin değiştirilmesi, "*sistemi engelleme, bozma, verileri yok etme veya değiştirme*" suçunu oluşturabilir.
- ***TCK m.136:*** API açıklığı üzerinden kişisel verilere erişilmesi "*verileri hukuka aykırı olarak verme veya ele geçirme*" suçunu oluşturabilir.
- ***TCK m.158/1-f:*** Promosyon istismarı, işlem manipülasyonu gibi yollarla API'ler üzerinden haksız menfaat sağlanması, "*bilişim sistemlerinin araç olarak kullanılması yoluyla nitelikli dolandırıcılık*'' suçunu oluşturabilir.
- ***TCK m.282:*** API suistimaliyle elde edilen kazançların finansal sistemlere aktarılması, "*suçtan kaynaklanan malvarlığı değerlerini aklama*" suçunu oluşturabilir.

VARDAR | ŞANLI

SİBER TUZAK:

API KÖTÜYE KULLANIMIYLA DOLANDIRICILIK

HANGİ ÖNLEMLER ALINMALIDIR?

- API çağrıları için limitler koyularak anormal yoğun istekler engellenmelidir. (*rate limiting*)
- API erişimleri için güçlü kimlik doğrulama mekanizmaları uygulanmalı ve erişim yetkileri düzenli olarak test edilmelidir.
- Hem iletim sırasında hem de depolama sırasında hassas veriler şifrelenmelidir.
- API trafiğini gerçek zamanlı izleyen; şüpheli işlem paternlerini tespit eden uyarı sistemleri kurulmalıdır.
- Teknik ekipler başta olmak üzere API güvenliği ve siber dolandırıcılık yöntemleri hakkında çalışanlara düzenli eğitimler verilmelidir.

VARDAR ŞANLI DEVREDE:

- Kara para aklamanın önlenmesi, kişisel verilerin korunması ve MASAK yükümlülükleri başta olmak üzere, ilgili ulusal ve/veya uluslararası düzenlemeler kapsamında risk değerlendirmesi yaparak kurumsal danışmanlık sunuyor ve şirket içi eğitimler düzenliyoruz.
- API kullanım politikaları, lisans sözleşmeleri, gizlilik hükümleri ile API erişimi, veri paylaşımı ve üçüncü taraf entegrasyonlarına ilişkin sözleşme ve şirket içi prosedürlerin dolandırıcılık riskini minimize edecek şekilde tasarlanmasını sağlıyoruz.
- Anılan dolandırıcılık yönteminin konu edildiği cezai ve hukuki süreçleri bütüncül ve gizlilik odaklı bir yaklaşımla yönetiyor, uluslararası iş ortaklarımızla birlikte sınır ötesi işlemlerde hızlı ve etkin çözümler sunuyoruz.

VARDAR | ŞANLI