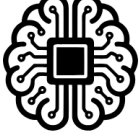




Eskişehir Osmangazi Üniversitesi
Bilgi İşlem Daire Başkanlığı
Siber Olaylara Müdahale Ekibi (SOME)



HIZLI OLSUN" DERKEN KURUMSAL BİLGİLERİ SİBER UZAYA SIZDIRMAYIN!

"Nasıl olsa işimi hızlandırıyor" diyerek Kurumsal bilgileri dış kaynaklı yapay zeka araçlarına (ChatGPT, Gemini vb.) kopyalıyor musunuz?

Saldırganlar doğrudan Kurumun sunucularını hacklemekle uğraşmak yerine, personellerin yapay zeka araçlarına duyduğu güvenden faydalanır.

Girdiğiniz hassas veriler yapay zekanın genel veritabanına kaydedilir. Bugün yazdığınız gizli bir bilgi, yarın başka bir kullanıcının sorusuna cevap olarak sızabilir!

- **Kurumsal Verileri Dış Kaynaklı AI Araçlarına Asla Girmeyin!**
- **"Sıfır Güven" (Zero Trust) Kültürünü Benimseyin!**
- **Sosyal Medyada Aşırı Paylaşım (Oversharing) Yapmayın!**

Saldırganların Kullandığı Yöntemler:

- Hackerlar, popüler açık kaynaklı yapay zeka modellerinin veya bulut tabanlı LLM sistemlerinin veri işleme mekanizmalarını inceleyebilir ya da bu sistemlere sızarak daha önce yüklenen gizli bilgileri toplayabilir.
- Sizlerin masumca AI modeline yapıştırdığı bir veritabanı parolası, kişi listesi veya gizli bir kurumsal bilgi yapay zekanın arka plandaki eğitim veya önbellek mekanizmalarına takılır ve veritabanına kaydedilebilir. Hackerlar doğru komutları (prompt) vererek, yapay zekanın sizden öğrendiği bu gizli bilgileri ifşa etmesini sağlayabilir.
- Dolaylı Komut Enjeksiyonu: Hackerlar yapay zekaya doğrudan saldırmak yerine, yapay zeka ajanlarının okuyacağı internet sitelerine, dökümanlara veya e-postalara gizli komutlar yerleştirirler ve yapay zeka gizli komutu kendi talimatı sanarak çalıştırır ve Kurumun hassas verilerinin sızdırılmasına sebep olabilir.
- LinkedIn, Instagram veya diğer platformlarda çalıştığınız projeler, kullandığınız teknolojiler, seyahat planlarınız ve iş arkadaşı detaylarınız hakkında fazla bilgi vermeyin. Saldırganlar bu verileri yapay zeka ile işleyerek size özel iltalama tuzakları kurabilir.



Hackerlar için LLM zehirlenmesi; çalışanların kendi elleriyle Kurumsal bilgileri açığa çıkardığı bir "istihbarat toplama" ve yapay zekayı bir "köstebeğe" dönüştürme yöntemidir.

