Siber saldırı nedir? ve nasıl önlem alınır? Sorularının cevaplarını aşağıda sırasıyla bulabilirsiniz:

Siber Saldırı Nedir?

Siber saldırı, "hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar" şeklinde tanımlanmaktadır. Siber tehditler artık sadece bilgisayar sistemlerine zarar vermekle kalmayıp, bir ülkenin kritik haberleşme sistemlerine, enerji ve ulaşım ağlarına, askeri komuta ve kontrol sistemlerine zarar verecek ölçüde **asimetrik bir harp çeşidi** olarak ortaya çıkmaktadır.

Siber Saldırı Yöntemleri Nelerdir?

Belli başlı siber saldırı yöntemleri şunlardır:

- **Bilgi ve veri aldatmacası (Data Diddling):** Bilgisayara yanlış veri girişi, verilerin özel yöntemlerle değiştirilmesi veya kayıtların silinmesi.
- **Salam tekniği (Salami Techniques):** Bankacılık sektöründe kullanılan, hesaplardaki küsuratların başka bir hesaba aktarılması.
- **Süper darbe (Super Zapping):** Güvenlik kontrollerini aşarak sistemdeki arızaların düzeltilmesi için geliştirilmiş programların kötüye kullanılmasıyla güvenliğin devre dışı bırakılması.
- **Truva atı (Casus Yazılımlar):** Bilgisayar korsanlarının sisteme sızmak için kullandığı zararlı yazılımlar.
- **Bukalemun (Chamelon):** Normal bir program gibi çalışırken arka planda kullanıcı adı ve şifreleri taklit ederek ele geçirme.
- **İstem dışı alınan elektronik postalar (Spam):** Alıcının haberi olmadan gönderilen ticari amaçlı e-postalar.
- **Çöpe dalma (Scavenging):** Silinmiş bilgilerin gelişmiş yöntemlerle tekrar geri getirilmesi.
- **Yerine geçme (Masquerading):** Yetkisiz kullanıcıların yetkili gibi sisteme erişmesi.
- **Web sitesi tahrifatı (Defacement):** Web sitelerinin içeriğinin değiştirilmesi veya kullanılamaz hale getirilmesi.
- **Hizmet aksatma saldırısı (Denial of Service – DoS):** Hedef sistemin kaynaklarını tüketerek hizmet vermesini engelleme.
- **Dağınık hizmet aksatma saldırısı (Distributed Denial of Service – DDoS):** Çok sayıda bilgisayarın eş zamanlı saldırısıyla hedef sistemin hizmet dışı bırakılması.
- **Oltalama (Phishing):** Sahte e-postalar veya web siteleri aracılığıyla kullanıcıların kişisel bilgilerini ele geçirme.
- **Sosyal mühendislik:** Yalan söyleme ve ikna yöntemleriyle bilgi toplama veya sisteme giriş yapma.

Nasıl Önlem Alınır?

Siber saldırılardan korunmak için önlemler:

- **Güvenlik önlemleri almak ve bu alana daha fazla yatırım yapmak** gerekmektedir.
- **Daha etkin savunma sistemleri inşa etmek ve acil durum hazırlıkları oluşturmak** önemlidir.
- **Saldırıların anında tespit edilmesi için sistemler kurmak** gerekmektedir.
- **Sanal ya da fiziksel bariyerler inşa etmek** önemlidir.
- **Bölgesel ve ulusal anlamda siber güvenlik politikaları geliştirmek** zorunlu hale gelmiştir. Türkiye bu bağlamda **Ulusal Siber Güvenlik Stratejisi ve Eylem Planları** hazırlamış ve yürürlüğe koymuştur. Bu planlar yasal düzenlemeler yapılması, ulusal siber olaylara müdahale organizasyonunun oluşturulması, siber güvenlik altyapısının güçlendirilmesi, insan kaynağının yetiştirilmesi, yerli teknolojilerin geliştirilmesi gibi stratejik eylemler içermektedir.
- **Siber güvenlik farkındalığı oluşturmak** ve son kullanıcının da güvenlik tedbirlerinden haberdar olması önemlidir. Çalışanların siber güvenliğe ilişkin konularda eğitilmesi ve bilinçlendirilmesi sosyal mühendislik gibi insan temelli saldırıların riskini azaltacaktır.
- **Siber güvenlik tatbikatları yapmak**, sistemlerin açıklıklarını ortaya çıkarıp gereken tedbirlerin alınmasını sağlamak açısından önemlidir. Türkiye'de yapılan tatbikatların gerçek saldırı ve savunma tekniklerini kullanması bu konuda öne çıkmaktadır.
- **Kritik altyapıların belirlenmesi ve bu altyapılara yönelik risk analizlerinin yapılması** gerekmektedir. Sektörel risk analizi yöntemleri ve acil eylem planları geliştirilmelidir.
- **Ulusal siber olaylara müdahale organizasyonunun oluşturulması** ve **Siber Olaylara Müdahale Ekipleri (SOME)** kurulması önemlidir. USOM (Ulusal Siber Olaylara Müdahale Merkezi) ve SOME'ler aracılığıyla siber olaylara hızlı ve koordineli müdahale edilmesi hedeflenmektedir.
- **Siber güvenlikte yerli teknolojilerin geliştirilmesi** ve milli çözümler üretilmesi önemlidir.
- **Uluslararası işbirliğinin güçlendirilmesi** gerekmektedir.
- **Kurumlar arası işbirliğinin sağlanması** ve bilgi paylaşımının artırılması önemlidir. Kamu ve özel sektör arasında da işbirliği mekanizmalarının kurulması gerekmektedir.
- **Bilişim projelerine güvenlik ayağının eklenmesi** ve kurumların standart çalışma politikaları belirleyip denetlemesi sistemlerin güvenliğini artıracaktır.
- **Kritik sektörlerde kullanılan donanım ve yazılımların test edilmiş ve güvenlik açıkları kapatılmış olması** gerekmektedir.
- **Siber güvenlik alanında nitelikli uzman personelinin yetiştirilmesi ve geliştirilmesi** önemlidir.