Siber Güvenlik Temel Kavramları

Siber güvenlik, en genel anlamıyla, **siber alanda alınan güvenlik tedbirlerini ifade eder**. **Siber**, bilgisayar ve ağlarını içeren kavram ya da varlıkları tanımlamak için kullanılır. **Siber alan (cyber space)** ise birbiriyle bağlantılı sistem, yazılım, donanım ve insanların iletişim ve/veya etkileşimde bulundukları soyut veya somut alanı tarif etmek için kullanılmaktadır.

Siber güvenlik kavramı, **bilgi güvenliği (information security)** ve **bilgisayar güvenliği (computer security)** kavramlarıyla benzer anlamlarda kullanılmaktadır. Bilgi güvenliği çoğunlukla kişisel ve kurumsal verilerin güvenliğiyle ilgili bir kavram olarak anlaşılırken, bilgisayar güvenliği bilişim sistemlerinin güvenliği olarak değerlendirilmektedir. Ancak her iki kavram da ortak öğeler içermektedir. Hatta hangi aktivitelerin siber suç olduğunun anlaşılabilmesi için öncelikle siber güvenlik kavramının tanımlanmasının daha doğru olacağı belirtilmektedir. İlk olarak 1990'lı yıllarda bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarlarla ilgili güvenlik sorunlarını ifade etmek için siber güvenlik terimi kullanılmıştır.

Siber Güvenliğin Temel Amaçları

Siber güvenliğin temel amaçlarından bazıları şunlardır:

- **Gizlilik (Confidentiality):** Saklanan bilginin yetkisiz kişiler tarafından erişilememesi demektir. Bilişim sistemlerinde işlenen bilginin gizliliğinin güvence altına alınması hedeflenir.
- **Bütünlük (Integrity):** Bilginin yetkisiz kişilerce değiştirilmemiş, kısmen ya da tamamının silinmemiş olmasıdır. Bilişim sistemlerinde işlenen bilginin bütünlüğünün güvence altına alınması hedeflenir.
- **Erişilebilirlik (Availability):** Saklanan bilginin gerektiğinde yetkisi olan kişiler tarafından erişilebilir olmasıdır. Bilişim sistemlerinin saldırılardan korunması ve bu ortamda işlenen bilginin erişilebilirliğinin güvence altına alınması amaçlanır.

Siber Güvenliğin Önemi

Günümüzde siber güvenlik giderek daha önemli hale gelmektedir. Bilişim teknolojilerine olan bağımlılığın artması, bireylerin siber suç mağduru olma riskini artırmanın yanı sıra siber alanı ulusal güvenliğin önemli bir parçası konumuna getirmiştir. Hatta siber tehditlerin önümüzdeki yıllarda da önemli tehditlerden biri olacağı düşünülmektedir. Ülke olarak bilişim altyapılarına ve internete olan bağımlılığın artmasıyla siber alanda taşınan riskler de büyümektedir. Türk şirketleri ve hükümet yetkililerinin sürekli olarak siber suçların ve siber casusluğun hedefinde olmaları bu alandaki probleme dikkat çekmekte ve daha fazla yatırım yapılmasının gerektiğini göstermektedir.

Siber Tehditler

Siber tehditler artık sadece bilgisayar sistemlerine verilen zararlarla sınırlı kalmamakta, ülkelerin kritik altyapılarına da zarar verebilecek **asimetrik bir harp çeşidi** olarak ortaya çıkmaktadır. Bir ülkenin varlıklarına yöneltilen siber saldırılar, ülkenin kendi sınırları içinden doğmak zorunda değildirler. Siber uzayın nispeten kontrolsüz yapısı, saldırganların kimliğini belirlemeyi zorlaştırmaktadır. Devletler siber uzayın belirsizliğini kendi çıkarları için kullanmaktadırlar. Sanıldığının tersine siber güvenlik dünyasında açıkça ilan edilen saldırılardan ziyade sessizlikle icra edilenler daha etkin ve korkutucudur.

Siber Güvenlik

Siber güvenlik alanında donanım ve yazılımın önemi vurgulanırken, bu altyapıyı kullanacak olan **insanların en önemli halka** olduğu unutulmamalıdır. Özellikle son kullanıcının siber güvenlik tedbirlerinden haberdar olması ve bu konuda farkındalığının sağlanması giderek önem kazanmaktadır.

Siber Saldırı

Siber saldırı ise “hedef seçilen şahıs, şirket, kurum, örgüt ve devlet gibi yapıların bilgi ve iletim sistemlerine ve kritik altyapılarına yapılan planlı ve koordineli saldırılar” şeklinde tanımlanmıştır. Günümüzde çok çeşitli siber saldırı yöntemleri bulunmaktadır.

Sonuç olarak, **siber güvenlik**, siber alandaki varlıkların gizliliğini, bütünlüğünü ve erişilebilirliğini korumayı amaçlayan, giderek artan öneme sahip **çok boyutlu bir kavramdır** ve insan faktörünü de içeren geniş bir alanı kapsamaktadır. Siber güvensizliğin yaratacağı maliyetin siber uzayın getirdiği yararlardan daha ağır olabileceği belirtilmektedir. Bu nedenle siber savunmaya daha fazla yatırım yapılması gerekmektedir.