

I. Bilgi Güvenliğine Giriş

I.III Güvenlik Yönetimi ve Politikalar

Güvenlik hakkında konuşmak organizasyonel bir içerik içinde anlamlıdır. Ekstrem bir durum olarak, küçük bir ofisi ve bir askeri üssü düşünün. Ofisinizde kapıdaki sağlam bir kilidin yeterince güvenlik sağladığını düşünebilirsiniz, fakat askeri bir üste kapıdaki kilit diğer yüzlerce güvenlik önleminde sadece bir tanesidir. Bu yüzden her şeyden önce, organizasyonumuzda sahip olduklarımızı ve değerlerini belirlememiz gerekir. Bizim için daha değerli şeyler için, güvenlik daha kritik olacaktır.

İkinci olarak, sahip olduğumuz ile ilgili saldırıya açıklıkları, tehditleri ve riskleri belirlememiz gereklidir. Bu önemli bir konudur zira mevcut olabilecek her saldırıya karşı koruyan bir güvenlik sistemi yoktur. Eğer ofisiniz ilk katta ise, kapıdaki bir kilit yeterli değildir. Pencerelerden gelebilecek bir saldırıyı göz önünde bulundurup, camlarınıza demir parmaklıklar yaptırmayı düşünebilirsiniz.

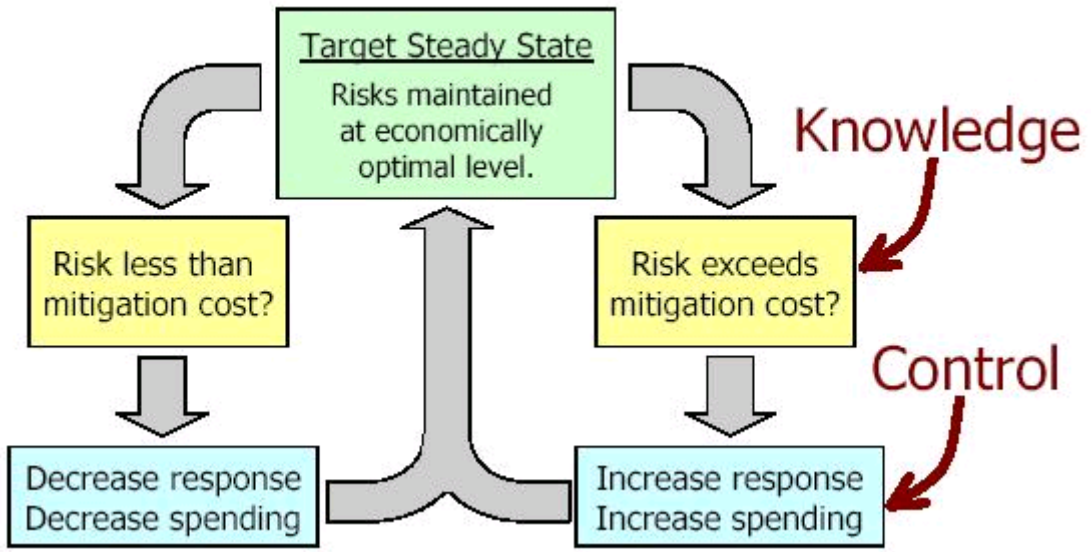
Askeri üs için bile, ne kadar para harcasanız da ne kadar önlem alsanız da, “mutlak güvenlik” diye bir şeye ulaşamazsınız. Güvenlik masrafları hafifleteceği risklere göre yapılmalıdır. Bu tek seferlik bir olay değildir, yanda gösterildiği gibi devam eden bir süreçtir.

Üçüncüsü, legal ve kontrata bağlı gereklilikleri de belirlemelisiniz. Mesela, eğer sigortanız varsa, bir kilit veya alarm almadan önce hırsızlık durumunda sigorta şirketinin yapacağı geri ödemeler ve bunların şartları ilgili politikalarını okuyabilirsiniz.

Yukarıdaki üç soruyu cevaplandırmanız sizin organizasyonunuz için güvenliğin ne demek olduğunu tanımlayan bir güvenlik politikası dokümanı yaratacaktır. Güvenlik politikası organizasyondaki yetkilendirilmiş ve engellenmiş etkinlikleri anlattığı gibi, çalışanların genel ve özel sorumluluklarına da değinir.

Bunların yanı sıra, güvenlik politikası saldırılara karşı kullanılan (uygulanan) güvenlik ölçütlerini (engelleme, tespit etme veya tepki verme türleri) de açıklar. Ayrıca çalışanların güvenlik konularında eğitilmesi de bir plana bağlanmalıdır, zira bazı güvenlik problemlerini teknik önlemlerle engellemek neredeyse imkansızdır.

Güvenlik politikasından sorumlu, politikayı uygulayan, devam ettiren, gözden geçiren ve etkililiğini belirleyen bir tek yönetici olması tercih sebebidir. Güvenlik politikalarının daha kesin bir tanımı için, organizasyonda otomatik olarak uygulanabilecek formal güvenlik politikası modelleri de bulunmaktadır



Şekil I.III-I : Temel güvenlik yönetimini anlatan bir figür