

I. Bilgi Güvenliğine Giriş

I.IV Güvenliğin Temelleri

Bu konunun sonunda, daha iyi güvenlik kararları alabilmek için bazı yönergeler sunacağız. Aşağıdaki yine kısmi bir listedir:

1. Öncelikle Gereksinimler: Bazılarınız için bu konuyu neredeyse bitiriyor olmamıza rağmen kriptografiye deyinmemiş olmamız şaşırtıcı olabilir. Kriptografi güvenlik amaçlarımıza ulaşmak için kullandığımız bir araçtır (fakat çok önemli bir araçtır). Takip eden konularda da görebileceğimiz gibi, kriptografi her şeyi çözen bir cevap değildir. Bazı saldırılar için kriptografi iyi iken, bazıları için değildir. Bu yüzden bir kripto aleti ne kadar güzel duruyor olsa da, önce bu alete ihtiyaç duyup duymadığınızı kendinize sormalısınız. Güvenlik gereksinimlerinizi doğru ve kesin olarak belirlediğinizde, etkili ve güvenli mimariler tasarlamamız çok daha kolay olacaktır.

2. Güvenlik Bir Zincir Gibidir: Güvenlik bir zincire benzer, bu yüzden sadece ve sadece en zayıf halkası kadar sağlamdır. Bu yüzden güvenlik gereksinimlerinizi belirlerken, en zayıf halkanıza en yüksek önemi vermeniz gerekir. Basit bir konu olarak, kapınız eğer tek yumrukta yere yıkılacak kadar zayıfsa, kapınıza yeni bir kilit almadan önce bu konuyu çözmeniz gereklidir.

3. Güvenlik Eğitimi: Eğitim genel olarak bir gerekliliktir, ve konu güvenlik olunca durum değişmez. Sosyal mühendislik saldırıları olarak tanımlanan (gerçek kullanıcıların manipüle edilerek bilgilerinin ele geçirilmesi) bazı saldırılar vardır, ve bu saldırılardan sadece eğitim ile kurtulabilirsiniz. Eğer birileri çalışanlarınızdan kredi kartı numarası benzeri kişisel gizli bilgilerini isterse, teknik olarak bu konuda yapabileceğiniz bir şey yoktur. Böyle basit saldırılardan korunmak basit görünebilir, fakat temel bazı güvenlik prensipleri olmadan mümkün değildir.

4. Düşmanınızı Tanıyın: Burada üç mevzu vardır. Öncelikler, asla saldırganların yeteneklerini küçük görmeyin. "HoneyNet"ler bilinçli olarak güvenlik açıkları bulundurulmuş deneysel ağlardır. Hedef saldırıları ve saldırganları daha iyi anlamaktır. İlgi çekici bir şekilde, saldırganların bu açık bulduran ağlardaki sorunları bulup güvenlik açıklarını kullanmaya başlamaları bir saatten az vakit almaktadır. İkinci olarak, fiziksel güvenliğin böyle durumlarda çok ön planda olmama sebebi saldırganın elde edebileceği fazla bir şey olmamasıdır. Diğer taraftan, dijital dünyada, saldırılar uzaktan yapılabildiği için (yakalanma riskini minimize edecek şekilde), saldırganlar sisteminize fiziksel olarak saldırmayı düşünmezler bile. Saldırıları bir sonraki günün gazetesine konu etmek onlar için yeterlidir çoğu zaman (bilinirlik saldırıları). Üçüncü nokta, içerideki kimselerin (örn. çalışanlar), hiç kimsenin bilemeyeceği şeyleri bilmeleri, çoğu zaman organizasyon için en büyük risklerden birini teşkil etmektedir. İçerideki kimseler ya iyi kişiler (sosyal mühendislik saldırılarının mağdurları) veya kötü çalışanlar, örn. atılmış-eski çalışanlar olabilir.

Güven bu konuda bahsedilmesi gereken önemli bir husus, ve en uygun zaman da muhtemelen şu an. Güven bir varlığın belirlenen kıstaslar içerisinde güvenilir ve inanılır şekilde faaliyet göstermesi olarak tanımlanabilir. Bir taraftan, güven ve güvenlik ters

7. Son olarak: Gollmann'ın bilgisayar güvenliği ile ilgili prensiplerini tekrarlıyoruz:

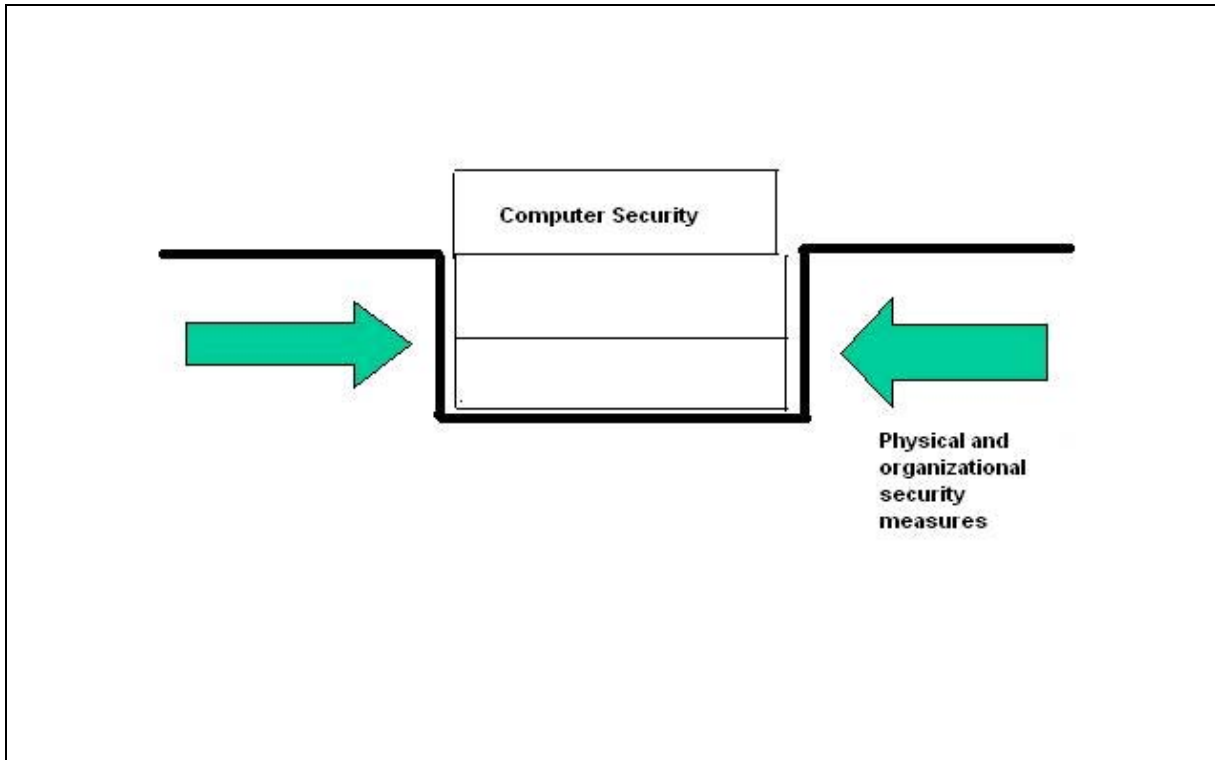
1. “Bir uygulamada, koruma mekanizmaları veriye mi, işlemlere mi yoksa kullanıcılara mı odaklanmalıdır?”
2. “Güvenlik mekanizması bilgisayar sisteminin hangi katmanında bulunmalıdır?”

Uygulamalar Hizmetler İşletim Sistemi İşletim Sistemi Çekirdeği Donanım

3. “Basitlik ve daha fazla güvenceyi, özellik açısından daha zengin ve güvenli bir ortama tercih ediyor musunuz?”
4. “Güvenliği tanımlayan ve uygulayan görevler merkezi bir varlığa mı sunulmalı yoksa sistemin bileşenlerine mi bırakılmalı?”
5. Bir saldırganın güvenlik mekanizmasının bir alt katmanına ulaşmasını nasıl önleyeceksiniz?”

Bu son prensip üzerinde biraz daha detaylı konuşmamız gerekir. Bizim sunduğumuzun aksine, Gollman'ın listesi bu noktaya kadar daha teknik bir listedir, fakat son prensip fiziksel ve organizasyonel güvenlik ölçütlerinin teknik ölçütlere birleştirilmesini gerektirmektedir (yandaki figürü inceleyin).

Bir örnek olarak, bilgisayarınızın fiziksel olarak güvende olmadığını düşünün. O zaman, ne kadar sofistike yetkilendirme mekanizmalarınız olursa olsun, bir saldırgan basitçe bilgisayarınızın diskinin yerini öğrenip, diskinizdeki verilere fiziksel olarak ulaşabilir, verilerinizi okuyabilir ve kendisi için saklayabilir.



Şekil I.IV-II : Figür fiziksel ve organizasyonel güvenliğin teknik güvenlikte birleştirilmesini göstermektedir

Sorular: *Koruma mekanizmaları veriye mi, işlemlere mi yoksa kullanıcılara mı odaklanmalıdır? Sizce hangisi daha kullanıcı dostudur?*

Başka sistemler için benzer katmanlandırma yapıları var mıdır?

Nedern basitlik daha yüksek güvence demektir? (Sistemler üzerindeki tartışmamızı hatırlayın)