ağ güvenliği- giriş

Bilgisayar Güvenliği Problemlerinin Nedenleri

1-Buglar

Hata barındırmayan yazılım yok diyebiliriz. Bunun sebepleri şunlar olabilir:

-Programın yanlış yazılması

-APIların yanlış kullanılması olabilir

-Algoritmanın uç noktaları değerlendirmemesi olabilir.

Bu hataların bazıları zararsız(beklendiği gibi çalışmaz) bazıları zararlı olabilir.

2-Sosyal mühendislik

Kişileri normalde istemeyecekleri faaliyetlere sevk ederek zarar vermek.

3- Para kazanma motivasyonu

Her saldırının parasal bir karşılığı bulunuyor.

a- Saldırıyla elde eden verilerin(exploits) satıldığı marketplaceler bulunuyor

b- Insanlara ait bilgisayarlar(Owned machines) için para ödeyip bir saldırı yapılacağı zaman bu bilgisayarları kullanılması(PayPerInstall) için bir marketplace.

c- Değerli hassas bilgilerin elde edilmesi

Bu Kadar Bug Olmasının Nedenleri

1- Kriptografiyle ilgili problemler

Kriptografi için kullanılan APIlar veya farklı yöntemler eksik veya yetersiz olabilir.

2- Kullanıcının bilgilerinin olabildiğince az toplanıp paylaşılması gerekir

Örnek: Browser'dan linke tıklayıp zoom uygulamasının açılmasına izin veriyoruz. Bunun sonucu olarak tüm web siteleri zoom uygulamasını açabilir ve bizi istemediğimiz toplantılara sokabilir.

3- Adaptasyon problemleri

Yeni bir işletim sistemi kontrol mekanizması eklendi diyelim. Yeni işletim sistemine uyumlu olmayan uygulamamız burada problemler yaşanmasına sebep olabilir.

What Motivates Attackers?

1-) IP adreslerin kullanılması ve bant genişliğinin çalınmasının sebebi saldırganların kimliklerini gizlemek için bunları kullanmasıdır. Bu IP adresleri Spam veya DoS veya Click Fraud için kullanılabilir.

2-) Kullanıcı bilgilerinin çalınması

Man in the middle. Mobilde de benzer saldırılar olabiliyor.

3-) Ransomeware

Şifrelenmiş bilgilerini kurtarmak için para ödemen gerekebilir.

Server-side attacks

4-) Data hırsızlığı

5-) Politik motivasyon

6-) Ziyaret eden kullanıcıları enfekte etmek

Zerodium: Siber güvenlik araştırması, açıkları bulup bildirenlere ödül veriyorlar.

Source kodu incelesek okeylesek bile güvenemeyiz çünkü compiler sorunlu olabilir. Compileri inceleyip derlesek ona da güvenemeyiz o da C'de yazılmıştır en iyi ihtimalle onu da derleyeceğiz. Sonuç olarak hiçbir şeye güvenemeyiz. Çözüm:

Trusted Computing Base(TCB): Bir noktayı güvenli kabul edeceğiz ve onun üzerine kodlamaya devam edeceğiz.