

I. Bilgi Güvenliğine Giriş

I.II Yaygın Bilgi Güvenliği Hedefleri

Bilgi güvenliğinin klasik 3 hedefi şunların korunmasıdır:

1. Gizlilik: Bilginin yetkisiz ellere geçmesinin engellenmesi.
2. Bütünlük: Bilginin izinsiz değiştirilmesinin engellenmesi.
3. Mevcudiyet: Bilgi kaynaklarının izinsiz alı konulmasının engellenmesi.

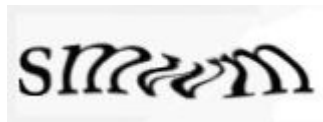
Gizlilik askeri alanda çok derin bir öneme sahiptir ve tarihsel olarak insanlar güvenlik kelimesini duyduklarında ilk akıllarına gelen şeydir. Fakat modern iş yaşamında bütünlük ve mevcudiyet genel olarak gizlilikten çok daha önemlidir.

Bu üç bakış açısı arasında, potansiyel olarak en az anlaşılan "mevcudiyet"dir. İşin aslına bakılırsa, bu problemi çözmeye güvenlik mekanizmalarında bir eksiklik ve yetersizlik vardır. Mevcudiyet için, hizmet reddinin engellenmesini, kaynaklara izinsiz ulaşımın ise engellenmesini isteriz. Daha iyi bir açıklama için, güncel bir gerçek dünya örneğine bakalım.

Pratik

Bazı şirketler (Yahoo, Google, vs.) bedava e-posta hizmeti sunarlar. Bu hizmetler genelde her dakika binlerce e-posta hesabı için başvuru yapan 'bot'lerden zarar görmektedirler, çünkü bu durum normal kullanıcılara hizmet verilmesini engellemektedir. Çözüm bilgisayar ile insan arasındaki farkı ayırt edebilen bir sistem bulmaktır, bu sayede insanlar kayıt olabilmeli, bilgisayarlar olamamalıdır.

Bir captcha ("*completely automated public turing test computers and humans apart*" kısaltması), tam olarak bunu yapar. Yan tarafta bir captcha örneği bulunmakta, bilgisayarlar tarafından okunamayan, fakat insanların anlayabildiği deforme edilmiş bir metin. Tabii ki bu mutlak bir çözüm değildir, yapay zeka bilgisayarların da bu ve benzeri metinleri okumasını sağlayabilir.



Şekil 1. 1 Bu "smwm" captcha'sı bilgisayar ile kullanıcı ayırımı harfleri bozarak, ve arkaplana farklı renkler ekleyerek yapmaktadır..

Kimlik Denetimi ve Yetkilendirme

Bir diğer genel bilgi güvenliği hedefi kimlik denetimidir -bir kişinin gerçekten belirtilen kişi olduğunun anlaşılması süreci. Genel olarak kimlik denetimi yetkilendirme ile takip edilir, bu sayede kişiye bir şeyleri yapma izni verilir.

İki tür kimlik denetimi vardır:

1. Varlık kimlik denetimi
2. Mesaj kimlik denetimi

Varlık kimlik denetimi gerçek zamanlı bir süreçtir ve deklarasyon haricinde başka bir anlamlı mesaj bulundurmaz. Diğer taraftan, mesaj kimlik denetiminin amacı alınan mesajın kaynağını denetlemektir, ve eş zamanlı bir süreç olması gerekmemektedir. Pratikte, mesaj kimlik denetimi aynı zamanda mesaj bütünlüğünü gerektirmektedir, çünkü mesajda bütünlük olmadığı sürece mesaj kaynağının denetiminin bir anlamı yoktur.

Unutmayın ki kontrol bu alanda kullanılan başka bir terimdir. Yetkilendirmeye çok yakın bir anlamı vardır. Kullanıcılar veya süreçler (konular) yetkilendirildiklerinde veya bir şeye (objeye) ulaşmaları olmadığında ortaya çıkar.

Soru: *Yetkilendirmeden önce bir kişinin gerçek kimliğinin doğrulanması kesinlikle gerekli midir?*

Sorumluluk (Denetlenilebilirlik): Kimin neyi yaptığının ve ne zaman yaptığının güvenilir bir şekilde kayıt edilmesidir, bu sayede ileride kişiler yaptıklarından sorumlu tutulabilirler.

Kimlik denetimi ve yetkilendirme engelleme önlemleridir, fakat sorumluluk bir güvenlik açığı farkedildiğinde tepki vermek için gereklidir. "AAA" (Authentication-Authorization-Accountability) bu üç maddeyi kapsayan bir kısaltmadır.

Reddetmeme: Mesajı gönderen/alan üçüncü bir parti önünde iletişimi reddedemez.

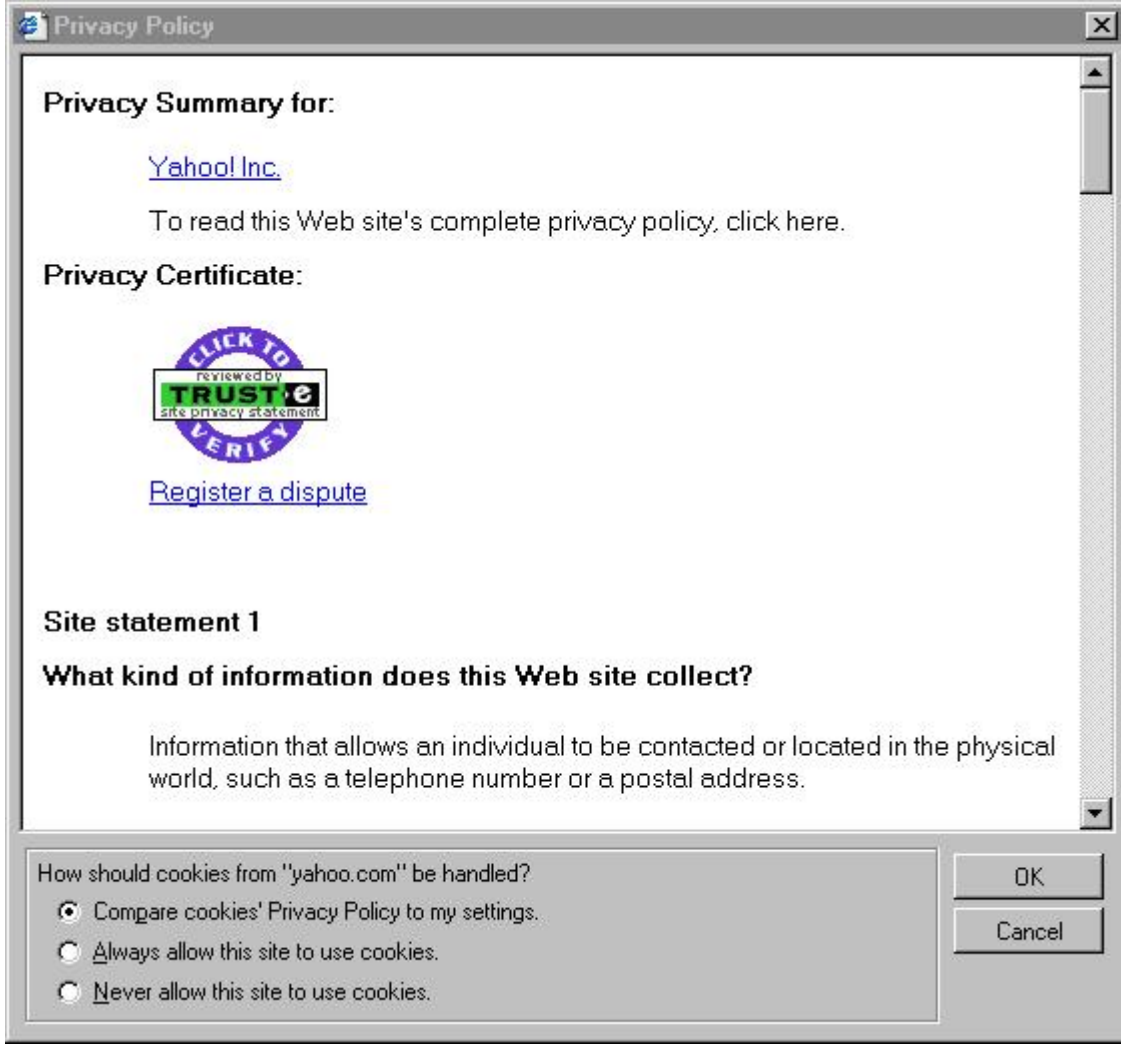
Soru: *"Sorumluluk" ve "Reddetmeme" arasındaki ilişki nedir?*

Gizlilik ve Mahremiyet

Gizlilik: Kişisel bilgilerin açığa vurulmasının ve kullanılmasının kontrol edilmesidir.

Gizlilik ve kesin gizlilik aynı şeylerdir. Örnek olarak bedava bir e-posta hizmetine kayıt olduğunuzu düşünün. E-posta hizmeti sizden bazı kişisel bilgiler isteyecektir (neden?) veya bazılarını sormadan alacaktır (örn. IP adresiniz). Kesin gizlilik gönderdiğiniz bilgilerin karşınızdaki siteye giderken başkaları tarafından okunmamasını istemeniz ile ortaya çıkan bir durumdur. Diğer taraftan, istenilen alıcı (e-posta şirketi) için sizin kişisel bilgileriniz kesin bir şekilde gizli değildir, fakat yine de gizlilik haklarınız bulunmaktadır (mesela e-posta şirketlerinin e-posta adresinizi spam yapanlara satmasını istemezsiniz). Bu şartlar sitelerin güvenlik poliçelerinde açıklanmaktadır.

Unutmayın ki kişisel bilgilerinizi şirkete gönderdiğinizde, üçüncü kişilerin bu bilgilere ulaşmasını engellemenin bir çok teknik yönü vardır. Fakat yine de şirketin gizlilik politikalarında bir eksiklik gördüğünüzde tepki verebilirsiniz.



Şekil 1. 2 Yahoo.com'un gizlilik politikası (Internet Explorer ile görüntülenmiştir).

Diğer Güvenlik Hedefleri

Geri getirilebilirlik: Ne olursa olsun, sistemimizi önceki iyi bir durumuna geri getirebileceğimizden emin olmamız gereklidir.

Saldırı Tespit Etme: Sistemdeki normal olmayan durumları otomatik olarak farketmemiz gereklidir.

Steganografi: İletişim etkinliğini başkaları farketmeden gerçekleştirebilmemiz gereklidir.

Steganografinin gizlilikten çok daha güçlü bir gereklilik olduğunu unutmayın, çünkü sadece iletişim verilerini gizli tutmak değil, iletişimde bulunduğunuzu da gizli tutmanız gerekmektedir.

Uyarı: Bu liste de dahil olmak üzere, hiçbir liste tam olarak tamamlanamaz.