BİLİŞİM TEKNOLOJİLERİ HABER BÜLTENİ

TOBB BİLGİ HİZMETLERİ DAİRESİ AYLIK BÜLTENİ ŞUBAT 2008 YIL 3 SAYI 26

TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ
BİLGİ HİZMETLERİ DAİRESİ

İÇİNDEKİLER

2008 INTERNET GÜVENLİĞİ RAPORU

CA tarafından yayınlanan "2008 İnternet Güvenliği Raporu"na göre çevrimiçi oyun oynayanların, sosyal ağların ve ABD Başkanlık seçimi ve Beijing Olimpiyatları gibi yüksek profile sahip etkinliklerin 2008 yılında çevrimiçi tehditler açısından en üst sıradaki hedefler arasında olduğunu tahmin ediliyor. CA'nın gobal güvenlik danışmanları tarafından derlenen verilere dayanan çalışma, 2008 yılı için internet güvenliği konusundaki tahminlerin yanı sıra 2007 yılındaki eğilimleri de raporluyor.

CA İnternet Güvenliği Birimi Başkan Yardımcısı şunları söylüyor: "Siber suçlular, fırsatların bulunduğu ve her çeşit güvenlik zayıflığından yararlanabilecekleri yerlere ulaşıyorlar. Güvenlik koruması, kötü niyetli yazılımları algılama konusunda daha iyi hale geldikçe, çevrimiçi hırsızlar da bilgisayarlara saldırma şekilleri açısından daha akıllı ve daha kolay gizlenebilir hale dönüşüyorlar."

2008 için CA çevrimiçi güvenlik tahminleri arasında şunlar bulunuyor:

1. Bot'lar 2008 yılına hükmedecek: Botnet'lerden etkilenen bilgisayarların sayısı 2008'de önemli ölçüde artacak. Bot'ların saptanmasını zorlaştırmaya yönelik çabalar sonucunda botçobanları taktik değiştirecek ve eşten eşe mimariler yoluyla merkezi olmaktan çıkacaklar.
2. Kötü niyetli yazılımlar daha akıllanacak: Kötü niyetli yazılımlarda yeni gelişim düzeyleri oluşacak. Kötü niyetli yazılımlar, sanallaştırılmış bilgisayarları hedef alacak. Steganografi ve şifreleme gibi açık görüşten saklanmak için uygulanan şaşırtma taktiklerinin daha çok kullanılması, suçluların faaliyetlerini gizlemelerine yardımcı olacak.
3. Oyuncular ateş altında kalacak: Oyun oynayanlar geçmişten beri kişisel bilgisayarlarının sağlam bir güvenlikten çok yüksek performansa sahip olmasıyla daha çok ilgilendikleri için, hesap kimlikleri hırsızlığı için birincil hedefi olmaya devam ediyor. 2008 yılında sanal varlıklar, internet suçluları için gerçek para dünyasına eşit olacak.

4. Sosyal ağ siteleri çapraz hedefler arasında olacak: Sosyal ağ siteleri giderek daha popülerleştiği için daha fazla güvenlik açığına sahip olacaklar. Sosyal ağlarda bulunan fazla sayıdaki potansiyel kurban ve bu kişilerin bilgisayar güvenliğine görece daha az ilgileri, bu siteleri siber hırsızlar için bulunmaz nimet haline getirecek.

5. Önemli tarihler, büyük tehdit altında kalacak: ABD Başkanlık seçimi ve 2008 Beijing Olimpiyatları yıkıcı saldırılar ve tek seferde bilgi hırsızlığı için yüksek profilli fırsatlar sunacak.

6. Web 2.0 hizmetleri ve siteleri saldırılarla karşılaşacak: Web 2.0 hizmetlerinin uygulanması görece kolay olsa da tamamen güvenli olarak yapılandırılması hayli güç olabiliyor. Bu nedenle bu hizmetleri kullanan çoğu internet sitesi, sitenin tehlike altında olduğunun dışarıya görünen çok küçük işaretleriyle birlikte kolay hedefler haline gelecekler.

8. Mobil aygıtlar güvenli olmaya devam edecekler: Mobil aygıtlar bazı kötü niyetli mobil yazılımlara rağmen, güvende olmaya devam edecekler. Akıllı telefonlar ve diğer mobil aygıtlar, 2008 yılında da suçlular için gerçek bir fırsat olmayacak.

CA araştırmacıları, 2007 yılında aşağıdaki eğilimleri izledi:

• Ekim 2007'de, Ocak ayına göre kötü niyetli yazılım hacmi 16 kat büyüdü.

• İlk kez, kötü niyetli casus yazılımlar, kötü niyetli yazılımın en geçerli biçimi olan truva atlarına fark attı. 2007 yılında kötü niyetli yazılımların yüzde 56'sı kötü niyetli casus yazılımlar, yüzde 32'si truva atları, yüzde 9'u solucanlar ve yüzde 2'si virüsler olarak görüldü.

• Reklam yazılımlar, truva atları ve yükleyiciler en yaygın görülen casus yazılım türleri oldu.

• Bu yılın en yaygın solucanları, basit ağ ve çıkarılabilir sürücü solucanlarıydı. Bazı solucanlar ulaştıkları bilgisayarlara hasar verirler. Bazılarıysa başka kötü niyetli yazılımlar bırakır ya da tehlike altındaki bilgisayarların arka kapı denetimini açarlar.

• Aldatıcı – ya da sahte- güvenlik yazılımları da sorun olmaya devam etti. Bu da yanlış yönlendiren uygulamaların giderek arttığının bir göstergesi oldu. Aldatıcı güvenlik yazılımları, 2007 yılında toplam casus yazılımı hacminin yüzde 6'sıydı. Aldatıcı güvenlik yazılımları, genel olarak ücretsiz casus yazılım koruma yazılımları hakkında çevrimiçi reklamlar yoluyla dağıtılıyor.

• Saldırı yöntemleri, şimdi standart olan birçok bileşene sahip tehditleri birleştirdi ve karıştırdı.

• E-postaların yüzde 90'ı istenmeyen e-postalardan oluşuyor. İstenmeyen e-postaların %80'i kötü niyetli sitelere ya da kötü niyetli yazılımlara linkler içeriyor.

• İstenmeyen e-posta kalitesi de iyileşti; artık yazım hataları ile belirgin bir şekilde keşfedilmiyor.

TÜBİDER

TOBB FUAR REHBERİ 2008

TOBB, firmalar ve tüm ilgili kişiler için büyük kolaylıklar sunan Türkiye Fuar Rehberi'ni güncelleyerek ve 2008 yılına ait bilgilerle donatarak Internet ortamında hizmete sunmuştur.

Birliğimizce, ülkemizde düzenlenecek fuarların etkin ve kapsamlı biçiminde tanıtılması ve yıl boyunca kullanabilecek bir bilgi kaynağına duyulan ihtiyaç düşünülerek, 2008 Yılı "Türkiye Fuar Rehberi" hazırlanmıştır. Türkçe ve İngilizce olarak hazırlanan rehberin içeriğinde, 2008 yılında düzenlenecek fuarlar ve bunları düzenleyecek fuar şirketlerine ilişkin temel bilgiler yer almaktadır.

http://www.fuarrehberi.org.tr adresinden ulaşılabilen web sayfasında, konu, şehir, tarih ve düzenleyici firma bilgilerine göre fuarlar listesine erişmek mümkün. Ayrıca fuarlarla ilgili pek çok kritere göre de arama ve sorgulama işlemleri yapılabiliyor.

Hazırlanan sitede Türkiye ve TOBB hakkında yararlı bilgiler bulunuyor. Tamamen dinamik olarak oluşturulan web sayfasının sade ara yüzü de kullanımı oldukça kolaylaşıyor ve böylece sektörle ilgili herkes için önemli bir başvuru kaynağı oluyor.

INTERNET'TEN E-İMZA İLE DAVA AÇILABİLECEK

Adalet Bakanlığı, yargıyı elektronik imza güvencesiyle sanal aleme taşıma olanağı sunan Ulusal Yargı Ağı Projesi'ni (UYAP) hayata geçiriyor.

Uygulamaya göre elektronik imza sahibi olan herkes, internet üzerinden dava açabilecek, harç ödeyebilecek, duruşma tarihini ve dava seyrini oturduğu yerden öğrenebilecek.

Proje kapsamındaki Avukat Bilgi Sistemi ile de avukatlara, UYAP üzerinden mevcut dosyalarını izleme, davalara evrak gönderebilme, yeni dava açma olanağı tanınacak.

Bunların yanı sıra, davalara ilişkin harç, dosya ücreti ve diğer masraflar için gerekli para transferleri de Internet aracılığıyla yapılabilecek. Avukatlar, vekaletnameleri bulunmayan dosyaları ilgili hakimin bilgisi dahilinde inceleme kolaylığına sahip olurken mahkemeler ve kurumlar arası bürokratik işlemler saniyeler içinde gerçekleştirilebilecek.

Projenin 2008 yılının üçüncü çeyreğinde hayata geçirilmesi hedefleniyor.

CNN TÜRK

TÜBİTAK'TAN DEPREMDE HAYAT KURTARAN BULUŞLAR

TÜBİTAK, depremde arama kurtarma faaliyetlerinde hayat kurtaracak iki farklı buluşunu kamuoyuna duyurdu.

TÜBİTAK Marmara Araştırma Merkezi'nde çalışan uzmanlar, arama kurtarma çalışmalarının seyrini değiştirecek bir buluş elde ettiler. Uzmanların ulaştığı bir elektronik sistem, metrelerce enkaz altındaki canlıyı, kalp atışından tespit ediyor.

17 Ağustos depreminin ardından TÜBİTAK Marmara Araştırma Merkezi can kayıplarını azaltacak teknolojiler üzerine araştırmaya başladı. Birkaç yıl süren çaba, meyvesini verdi ve TÜBİTAK, arama kurtarma çalışmalarının seyrini değiştirecek bir sistem geliştirdi.

Yüzeyaltı tomografi adı verilen sistem mikrodalga teknolojisine dayanıyor. Enkazın üzerine yerleştirilen taşınabilir bir radar sistemiyle enkaz altındakilerin hem hefes alıp verişi hem de kalp atışları izlenebiliyor.

Bir deprem sırasında göçük altındakiler baygın bile olsa arama kurtarma ekipleri dünyada ilk kez geliştirilen bu sistem sayesinde enkaz altındaki kişilere ulaşabiliyor.

TÜBİTAK'ın geliştirdiği diğer bir sistemse, metrelerce duvarın arkasında kalan canlının hem yerini hem de yaptığı hareketleri tam olarak tespit edebiliyor.

Deney için birer metre aralıklarla üç beton duvar arka arkaya yerleştiriliyor. Duvarların arkasında yürüyen kişinin hareketleri eş zamanlı olarak bilgisayar ekranına yansıyor. Bilgisayar ekranından kişinin hareketleri takip edilerek nerede olduğu anlaşılabiliyor. Uzmanlar geliştirdikleri söz konusu buluşun dünyada bir ilk olduğunun altını çiziyorlar.

CNN TÜRK

2009 YILINDA ELEKTRONİK KİMLİK KARTLARI GELİYOR

Hastane önlerinde, devlet dairelerinde çok sık karşılaşılan kuyruklar 2009 yılında sıradan görüntüler olmaktan çıkacak. Elektronik devlete geçiş çalışmaları kapsamında TÜBİTAK'ın hazırladığı kartla, vatandaşlık kartı, yani "elektronik kimlik sistemi"ne geçilecek.

Yeni sistemle her işlem için devlet dairelerine gitme devri de sona erecek. Birçok işlem internet vasıtasıyla yapılabilir şekilde düzenlenecek.

Yüzde yüz güvenli olacağı bildirilen kartın kesinlikle kopyalanamayacağı da ifade ediliyor. 2009 yılında başlayacak uygulama nedeniyle TÜBİTAK'ta yoğun bir çalışma sürdürülüyor.

Elektronik kart, öncelikle sağlık karnelerinin ve reçetelerin tarihe karışmasını sağlayacak.

Doktorlar hastaya vereceği ilacı "elektronik vatandaşlık kartı"nın üstüne işleyecek. Hasta, kartını alıp eczaneden ilacını alacak, Sigorta kurumu da parayı ödeyecek.

Şu an kullandığımız kimlik kartlarına göre güvenliği son derece artırılmış olan bu kartlar, devletin elektronik hizmet verdiği tüm kurumlarda kullanılabilecek. Vatandaşın yapması gereken tek işlem, kendini devlete elektronik olarak tanıtmak.

Kullanım önceliği sağlık alanına verilen kartın kısa sürede tüm kamu kuruluşlarında uygulamaya geçmesi bekleniyor.

TEKNOPARK

AVRUPA KOMİSYONU MİCROSOFT HAKKINDA İKİ YENİ SORUŞTURMA BAŞLATTI

Avrupa Komisyonu, internet tarayıcısı (Internet Explorer) ve ofis yazılımlarıyla rekabeti ihlal ettiği şikayeti üzerine yazılım şirketi Microsoft hakkında iki yeni soruşturma başlattı.

14 Ocak'ta Avrupa Komisyonu tarafından yapılan açıklamada, Windows işletim sistemine entegrasyon konusunda Microsoft'un, rakip yazılım şirketlerine bilgi verme yükümlülüğünü yerine getirip getirmediğinin soruşturulacağı belirtildi.

Norveç merkezli internet tarayıcısı yazılımı şirketi Opera Aralık 2007 tarihinde, Microsoft'un Internet Explorer yazılımını Windows işletim sisteminden ayırmayarak pazar hakimiyetini kötüye kullandığı ve standartlara uymayarak rakip yazılımların Windows'la uyumlu çalışmasını zorlaştırdığı şikayetiyle Avrupa Komisyonu'na başvurmuştu.

Bilindiği üzere 2004 yılında Avrupa Komisyonu, Microsoft'un piyasadaki hakim konumunu kullanarak rekabeti kısıtladığına karar vermişti. Şirket o zaman 497 milyon Avroluk rekor bir para cezasına çarptırılmış, 2006 yılında ise bu karara uymadığı gerekçesiyle 280,5 milyon Avroluk ilave bir cezaya çarptırılmıştı. 2007'nin Ekim ayında ise Avrupa Toplulukları Adalet Divanı (ATAD) Microsoft'un temyiz başvurusunu reddetmiş; bunun üzerine Microsoft, yazılım sektöründe rekabeti sağlamak amacıyla daha önce alınan kararlara uymayı kabul ettiğini açıklamış ve rakiplerine yazılımlarının kendi ürettiği işletim sistemleri ile uyumlu çalışmasını sağlayacak bilgileri aktaracağını ilan etmişti.

İKV HAFTALIK E– BÜLTEN

TEKNOLOJİDE YEŞİL RÖNESANS BAŞLIYOR

Deloitte'un Teknoloji, Medya ve Telekomünikasyon (TMT) bölümü "2008 Teknoloji Öngörüleri"raporuna göre teknoloji sektörü 2008 yılında veri güvenliği için daha çok para harcayacak. Teknolojide yeşil rönesans başlıyor.

Deloitte'un Teknoloji, Medya ve Telekomünikasyon (TMT) bölümü tarafından hazırlanan ve teknolojideki en son trendlerin araştırıldığı "2008 Teknoloji Öngörüleri" raporu yayımlandı. Her yıl düzenli olarak yayımlanan araştırma sanal ortam güvenliği, e-ticaretteki güvenlik önlemleri, nanoteknolojinin kullanımı ve geleceği ile sayısal bölünmeyle ilgili pek çok önemli bulguyu ortaya koydu.

Araştırmaya göre, internet ortamında kullanılan sanal kimlik uygulaması 2008 yılında e-ticaretin yaygınlaşması ile birlikte yerini gerçek kimliklere bırakmaya hazırlanırken, hizmet satışından ve özellikle veri güvenliğinden elde edilen gelirlerde bir artış olacak. Geçen yılki araştırmada dikkat çeken çevre dostu teknolojiler, 2008 yılında da cazibesini koruyor.

İşte 2008 için 10 teknoloji öngörüsü

1.Sayısal güvenliğin değeri artacak
2.Mahremiyet ön plana çıkacak
3.Anonim sanal ortamlardan gerçek kimliklerin kullanılacağı orijinal yapılara geçilecek
4.Sayısal bölünme önemli sorunlar yaratacak
5.Nanoteknolojide yeşil rönesans yaşanacak.
6.LED ampulün yerini alacak
7.Gerçeklikten değer yaratılacak
8.Ana bilgisayar ve bakım konusunda yetkin eleman sıkıntısı yaşanacak
9.Bir milyardan fazla kişi temiz suya ulaşmakta zorluk yaşayacak
10.Ticari raporlamada iş dünyası artık aynı dili konuşacak

TÜBİDER

KISA MESAJLARDA TÜRKÇE KARAKTER SORUNU BİTİYOR

Uzunca bir süredir kamuoyunda tartışılan, Türkçe karakter içeren kısa mesajların 2 ya da 3 parçaya bölünerek ücretlendirilmesi sorunu 24 Ocak tarihinde GSMA'nın yönetim Kurulu Üyesi, GSMA'da görevli uzmanlar, Telekomünikasyon Kurumu temsilcileri, işletmeciler, STK'lar ve GSM el terminali üreten firmaların Türkiye temsilcilerinin hazır bulunduğu bir toplantıda tartışıldı.

Türk cep telefonu kullanıcılarının gönderdikleri Kurul, Türkçe karakterlerden kaynaklanan sorunu çözmeleri için, işletmecilere ücretlendirme altyapılarını yeniden düzenlemesi ve gerekli tedbirlerin alınması yolunda 31 Mart 2008 tarihine kadar, üretici/ithalatçı/ yetkili temsilcilere de 1 Temmuz 2008 tarihine kadar süre verdi. TK kararında, bu tarihten sonra aynı sorunu devam eden cihazların ülkeye sokulmayacağı da belirtiliyordu.

Yapılan çalışmalarda sorunun nedeni, GSM alfabesinde yer alan karakterlerin 7 bit olarak kodlanması ve kısa mesaj kapasitesinin 160 karakterden oluşması olarak belirlendi. Kullanılan cihaz ve sistemler, GSM alfabesi dışında kalan harfleri Unicode (UC) olarak algılıyor, 16 bit olarak kodluyor ve bu nedenle de mesaj kapasitesi otomatik olarak 70 karaktere düşüyor. Özetle, bir kısa mesaj içerisinde bir tane bile alfabe dışı karakter kullanılırsa, kodlama tekniğinin farklılaşması nedeniyle kısa mesaj kapasitesi 70 karaktere düşüyordu.

Bu arada Türkiye içinden de, Telekomünikasyon Kurumu ve uzmanlar birlikte, sorununun çözümüne yönelik bir öneri oluşturdular. Türkçe karakterlerin GSM alfabesi genişleme tablosuna standart olarak yerleştirilmesi şeklindeki çözüm önerisinde kullanılan her bir Türkçe harf için 2*7=14 bit kullanılarak, mesaj uzunluğunun 70 karaktere düşmemesi sağlanıyordu. Ortalama mesaj uzunluğu kısa mesaj içerisinde kullanılan Türkçe karaktere bağlı olarak değişiyor ama 140-160 karakter aralığında oluyor. 24 ocak tarihinde Telekomünikasyon Kurumu temsilcileri, GSMA uzmanları, işletmeciler, üretici temsilcileri ve STK'ların hazır bulunduğu, bir toplantıda işte bu konu ve çözüm önerisi tartışıldı. Toplantı boyunca, önerilen çözüm üzerinde tartışmalar yapıldı. GSMA uzmanları da kendi önerilerinin aynı olduğunu belirtince, katılanlar ittifak ile bu önerinin en mükemmel çözüm olduğu ve en yakın tarihteki 3GPP'ye götürülmesinin uygun olacağı kararını aldılar.

GSMA uzmanları, GSM alfabesi genişletilmiş tablosunda değişiklik önerisini ve toplantıya katılanların bu metni desteklediği şeklindeki kararı kaleme aldılar.

Karar bu şekliyle, Meksika'da 28 Ocak-1 Şubat 2008 tarihleri arasında yapılacak olan 3GPP toplantı gündemine sokuldu.

Toplantıya katılan uzmanlardan birisi, toplantı sırasında, 3GPP'deki temsilcileri ile görüştüklerini ve çözüm önerisinin 3GPP'de kabulünü desteklemesi istediklerini aktardı. Uzman, "alınan cevaplardan bu önerinin büyük bir ittifak ile kabul edileceği kanaati oluşmuştur" dedi.

Öneri kabul edildiği takdirde, kısa mesajlarda Türkçe karakterler rahatlıkla kullanılabilecek ve 140-160 harften oluşan kısa mesajda Türkçe harf kullanılsa bile tek bir kısa mesaj ücretlendirilmesi olacak.

Türkçe karakterlerin standart hale gelmesi durumunda, ayrıca Türk bilişimciler kendi dillerinde mobil program yazma imkanına da sahip olacaklar.

TURK.INTERNET

TOBB BİLGİ HİZMETLERİ DAİRESİ AYLIK BÜLTENİ

TÜRKİYE ODALAR VE BORSALAR BİRLİĞİ
BİLGİ HİZMETLERİ DAİRESİ

Aylık Bilişim Teknolojileri
Haber Bülteni
Yıl: 3 Sayı: 26
Şubat 2008

Her ayın ilk iş günü elektronik olarak yayınlanır ve dağıtılır.

Atatürk Bulvarı No : 149
Bakanlıklar ANKARA
Tel : 312-413 80 00
Faks : 312-425 48 54
E-posta : sinan@tobb.org.tr

BİLİŞİM TEKNOLOJİLERİ HABER BÜLTENİ

BİLİNÇLİ KULLANIM RİSKİ AZALTIR

Her geçen gün bilgisayarların güvenliği ve kişisel bilgilerin gizliliği daha fazla tehdit edilir hale geliyor. Söz konusu risklerin artmasında bilgisayar korsanları kadar bilinçsiz kullanımın da payı olduğu yadsınamaz bir gerçek...

Bilinçsiz kullanım olgusunu iki farklı açıdan ele almak mümkün. Bunlardan ilki "crack" siteleri gibi güvenli olmayan kaynaklardan edindikleri dosyaları virüs testinden geçirmeden kullanmakta bir sakınca görmeyen ya da kendilerine ödül ya da armağan vaat eden her bağlantıya tıklamaktan çekinmeyen kullanıcıların davranışlarıyla açıklanabilir.

İkinci bakış açısı ise kullanıcıların dikkatsizlik ya da üşengeçliklerinden dolayı ortaya çıkmaktadır.

Genelde ücretsiz yazılımlarda karşılaşılan ancak bazı durumlarda bedeli ödenerek edinilmiş programlarda da kendini gösteren bir takım eklentiler yüklenebilmeleri için kullanıcıdan izin isterler. Kullanıcıların büyük bir kısmı da maalesef bu tür mesajları okumadan onay verirler. Bu şekilde istenmeyecek sonuçlar doğurabilecek eklentiler bilgisayara kurulmuş olur.

Yazılımlar aracılığıyla gelen bu tür eklentiler, sponsor olarak kullanıcıların ücretsiz bir şekilde söz konusu yazılımı kullanmalarını sağlarlar. Bunun karşılığında da kullanıcı alışkanlıklarını kaydederek web sitelerinde uygun reklamlar göstermeye çalışırlar.

Bazı yazılımlar bilgisayara kurulmak için mutlaka söz konusu eklentinin kurulmasını şart koşarken bazıları da kullanıcıya serbestlik tanımayı tercih ederler.

Yükleme ekranında bulunan lisans sözleşmeleri kullanıcıları söz konusu eklentiler ve pek çok şey hakkında bilgilendirseler de genelde çok uzun oldukları için çoğu kullanıcı tarafından okumadan kabul edilir.

Literatürde "EULA" adıyla anılan ve "Son Kullanıcı Lisans Sözleşmesi" olarak Türkçeye çevrilen kurulum ekranlarında karşılaşılan bu tür uzun metinlere onay verilmesinin günlük yaşamda resmi bir sözleşmeyi imzalamaktan bir farkı yok gibidir. Bu nedenle lisans sözleşmelerinin dikkatli bir şekilde okunması kullanıcılara büyük fayda sağlayacaktır.

Lisans sözleşmeleri, kullanıcılara sahip olunan programla birlikte ne tür bileşenlerin ve eklentilerin yükleneceği gibi konuların yanında; programın kaç tane bilgisayara kurulabileceği, programla üretilen projelerin hangi koşullar altında dağıtılabileceği ve bu projelerin para karşılığında satılıp satılamayacağı gibi teknik hususlarda da bilgi verirler. Ayrıca kullanıcının yazılımın sahibi ya da kullanım hakkını elinde bulunduran birisi mi olduğu noktasını açıklığa kavuşturur. Bu nedenle tıpkı gerçek dünyada olduğu gibi sanal ortamlarda da bir sözleşmenin okunmadan imzalanmaması gerekir.

Geçtiğimiz aylarda bir firmanın lisans sözleşmelerinin okunma oranlarını tespit etmek için yaptığı bir deneme kullanıcıların bu konuyu ne kadar dikkate aldığını da gösterir niteliktedir. Firma, deneyde lisans metnine "Bu satırları okuyup bize dönüş yapan kişiye bin dolar ödeyeceğiz." gibi bir ibare yerleştirmişti. Sadece bir kullanıcının yazılımın piyasaya sürülmesinden birkaç ay sonra firmayla bağlantıya geçmesi durumun ciddiyetini gözler önüne sermektedir.

Bazı yazılımlar kullanıcılara kolaylık sağlamak için eklentileri yüklemeden önce lisans metinleri yerine uyarı mesajlarını kullanmayı tercih etseler de kurulum işlemini olabildiğince kısa tutmak isteyen kullanıcılar karşılarına çıkan her uyarı ya da mesaja evet demekte bir sakınca görmüyorlar.

Şimdiye kadar bu tip eklentilerin kimsenin bilgisayarına zarar verip kullanılamaz hale getirmemesi, insanların bu durumu önemsememelerindeki en büyük etken olabilir. Söz konusu eklentilerin arka planda kullanıcı alışkanlıklarını takip etmeleri neticesinde pek çok kullanıcı bu durumdan rahatsız olmuyor ancak eklentilerin topladıkları bilgileri gönderirken kendi internet bağlantılarını yavaşlattıklarının farkına varamıyorlar.

Ücretsiz yazılım kullanabilmek kulağa çok hoş gelse de bir takım yazılımların varlıklarını söz konusu eklentilerin sponsorluğu altında sürdürebildikleri de bir gerçek. Bu nedenle kullanıcıların yükleme ekranları ve özellikle de lisans sözleşmelerini dikkatli bir şekilde okumaları gerekmektedir.

Zararlı eklentilerden arınmış ve ücretsiz yazılımlar için açık kaynaklı yazılımların tercih edilmesi yerinde bir karar olacaktır çünkü bu yazılımların kodları herkese açık olduğu için eklenti barındırmazlar ve ilerde risk oluşturabilecek bir durum olduğunda gönüllü programcılar tarafından müdahale edilebilirler ancak ilerde bu yazılımlar için yazılmış eklentiler kurulumdan sonra ayrı olarak yüklenebilir.

(sinan@tobb.org.tr)