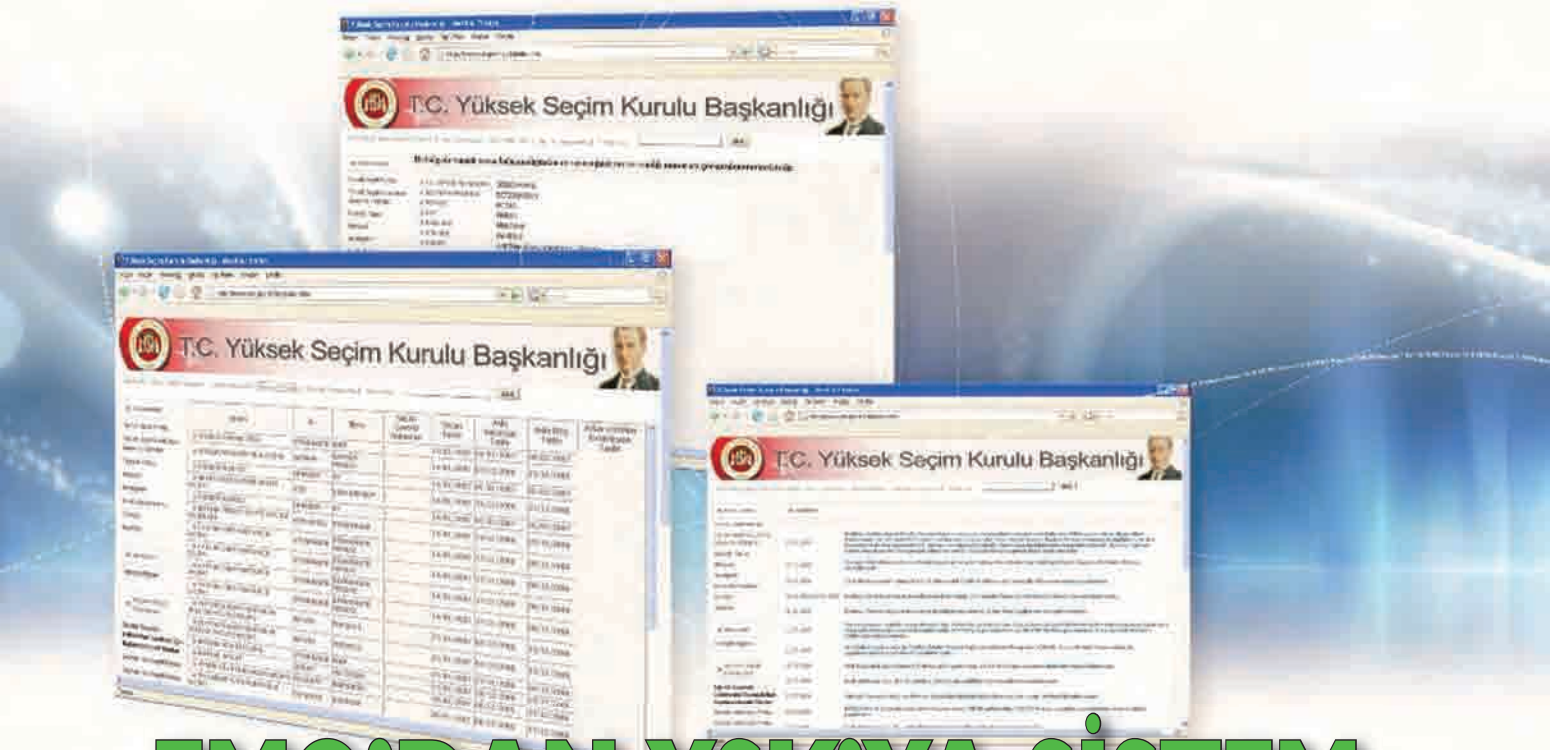

EMO'DAN YSK'YA SİSTEM GÜVENLİĞİ UYARISI

Elektrik Mühendisleri Odası (EMO) 42. Dönem Yönetim Kurulu, 12 Haziran 2011 tarihinde yapılan genel seçimler öncesinde 1 Haziran 2011 tarihinde yazılı bir basın açıklaması yaparak, seçim sisteminin güvenilirliğine ilişkin uyarılarda bulundu. Seçim güvenliğinin sağlanması için Yüksek Seçim Kurulu'nun (YSK) kullandığı SEÇSİS adlı sistemin sahip olması gereken özelliklere yer verilen basın açıklamasında, şöyle denildi:

"Bilgi-işlem ve bilgi-iletişim teknolojileri, dünyanın ulusal amaçlarını belirlemiş ülkelerinde oldukça hızlı bir biçimde gelişmektedir. Bilginin üretilmesi, iletilmesi, paylaşılması ve kendi gereksinimlerimize göre yorumlanması bu yüzyılın en önemli konusu olmuştur.

İnternet sayesinde bilgi temelli gelişmeler; sanayiden ticarete, eğitimden yönetime kadar birçok alanda günlük yaşamımızı etkilemektedir.

Ülkemiz bilgi teknolojilerinin kamusal alanda kullanımında sıkıntı yaşamaktadır. Bilgisizlik, deneyimsizlik ve amaç dışı kullanım gibi değişik nedenlerle çıkan bu olumsuzlukların faturası ise EMO üyesi olan bilişim sektöründe çeşitli görevlere sahip meslektaşlarımıza kesilmektedir. Bunun sonucunda halkımız çağdaş yaşam biçimlerinin doğal gerekliliği olan bilişime şüphe ile bakar duruma gelmiştir."

YSK'nın kullandığı sitemde 29 Mart 2009 tarihinde yapılan yerel yönetim seçim sonuçları sisteme girildiği sırada saat 22:00 sıralarında kesintiler yaşandığının hatırlatıldığı açıklamada, "bu kesintinin seçim sonuçlarının doğruluğunu şüpheye düşürecek etkilerinin olabileceğine dair iddialar ortaya atıldığı" belirtildi. 2011 yılında ise Yükseköğretime Geçiş Sınavı kitapçıklarının hazırlanması ve sınav sonuçlarının değerlendirilmesi ve açıklanması aşamalarında kamuoyunda, kullanılan yazılımların güvenilirliğine ve tarafsızlığına dair endişe oluştuğun yer verilen açıklamada, şöyle denildi:

"Sınava giren gençlerde gelecek kaygısı yaratan, en az yargı kadar güvenilir olması beklenen ÖSYM'ye olan güveni sarsan bu olayda fatura belki de tek hatası bulabildiği işte çalışmak/çalışmayı devam ettirebilmek olan bilgisayar mühendisi meslektaşımıza kesilmiştir."

12 Haziran 2011 Genel Seçimi'nde benzer bir durum yaşanmaması, kamu vicdanını rahatsız edecek bu tür şüphelerin doğmaması, güven ortamının sağlanması için EMO bünyesinde çalışmalarını sürdüren Bilgisayar Mühendisliği Meslek Dalı Ana Komisyonu'nun üzerine düşen her türlü görevi yerine getirmeye hazır olduğunun belirtildiği açıklamada, "Oda bünyesinde bulunan bilgili, birikimli ve değerli uzmanlarımızın; bütün kaynak kodla-

rın incelenmesi, seçim sonuçları girilmesi ve işlenmesi sırasında tarafsız gözlem yapılması, yukarıda sıralanan teknik konularda yapılabilecek iyileştirmelerin belirlenmesi ve gerçekleştirilmesi konularında her türlü göreve hazır olduğunu belirtiriz" denildi.

EMO'dan YSK'ya Öneriler

YSK'nın sistemlerinin sahip olması gereken özellikler açıklamada şöyle sıralandı:

"• Sistem kurulumu, bilgi girişleri ve seçim sonuçlarının değerlendirilmesi sürecinde ilgili hiçbir donanım ve yazılımlarda değişiklik yapılmamalıdır. Sistem kurulumu yapıldıktan sonra gerek komut, gerek ilk değişkenler, gerekse ilk kurulum bilgileri değişmemeli, kendi üzerinde değişiklik yapan herhangi bir komuta izin verilmemelidir.

• Merkezi seçim değerlendirme yazılımı ve dağınık operatör veri girişi yazılımlarının yerli ve açık kaynak kodlu olması, birer örneğinin siyasi partilerin genel merkezlerinde de kullanılabiliyor olması, dosya yapıları ve dosya kimlik doğrulama bilgilerinin açık, değişmez ve denetlenebilir olması gerekmektedir.

• Veri bütünlüğünü sağlayabilmek için seçim sonuçlarının girilmesi, iletilmesi, kaydedilmesi ve değerlendirilmesi sırasında gerekli önlemler, güvenlik bilgileri eklenerek sağlanmalıdır.

• Seçim sistemi, seçmenler ve siyasi partilerin kolaylıkla ulaşabileceği, seçim bölgesi ve sandık numarası temelli sorgulama alanlarına sahip olmalıdır. Sandık görevlilerinin adları, görevli oldukları sandıklardaki verileri inceleyip, tutanaklarla karşılaştırabilmesi amacı ile veri tabanına işlenmelidir.

• Verilerin gizliliğini sağlamak için, seçim sonuçlarının değerlendirilmesi sırasında dışarıdan herhangi bir erişime izin verilmemelidir. Seçmen bilgileri ve seçim sonuçları arasında herhangi bir ilişki kurulmasına neden olacak yapılanmalar bulunmamalıdır.

• Sistem güvenilirliğini sağlamak için seçmen sonuçlarına dokunulmaksızın bütün iç işlemler gözlemlenebilir olmalıdır. Bu gözlemlere, işlenmiş ve işlenmemiş seçim sonuçları, programlama ve yönetsel eylemler de dahildir. Gözleme işlemleri hiçbir biçimde kapatılamaz olmalı ve bütün operatör kimlik doğrulamaları, giriş/çıkışlar ve eylemler, tarih ve saat bilgisi ile birlikte kayıt altına alınmalıdır.

• Sistem şeffaflığını sağlamak üzere sistemde bulunan bütün donanım, yazılım ve özel birimler dokümantasyonu da dahil olmak üzere incelemeye açık olmalıdır

• Seçimde kullanılacak olan tüm donanım, yazılım ve çevre birimlerinin kurulumu, işletimi ve bakımının, bu konuda ilgili ve yeterli mesleki eğitimi almış, gerekli mesleki deneyime sahip, mesleğin etik değerlerine bağlı kişi ve kurumlarca yapılması gerekir.

• Veri tabanındaki değişikliklerinin izlenebilmesi için gerekli kimlik doğrulama önlemleri alınmış olmalıdır.

• Yetkisiz erişim, kişisel verilerin açıklanması, veri ya da komutlara zarar verilmesi, yetkili erişimin kesintiye uğraması, saldırılar ya da bilgisayar virüslerine karşı önlem alınmış olmalıdır.

• Aşırı yükleme ve kapasite yetersizliğinden doğabilecek veritabanı erişim sorunlarına karşı önlemler geliştirilmiş olmalıdır.

• Veri tabanı ve ilgili yardımcı programlarda oluşabilecek yasadışı yetki yükseltmesi, veri kaybı ya da bozulması gibi yazılım hatalarına karşı önlemler alınmış olmalıdır.

• Kullanıcıların veri tabanına bağlanabileceği terminallerin ağ adreslerinin tanımlı olup olmadığı, bu kullanıcıyla veri girişi yapılacak terminaller dışında bir bilgisayardan veri tabanına kaçak olarak bağlanılıp bağlanılamayacağı araştırılmalıdır.

• Seçim sonuçlarının tutulacağı tabloların SEÇSİS uygulaması dışında güncellenmemesi gerekmektedir.

• Haberleşme ve kimlik tanımlama protokollerinde açıklara karşı önlem alınmış olmalı, istemciler ve sunucu arasında iletilen bütün bilgiler kriptolanmalıdır."