Sahte Diplomalar Konusunda Bulgu ve Önerilerimiz

TMMOB
Bilgisayar Mühendisleri Odası
26 Eylül 2025
ANKARA

ÖNSÖZ

Türkiye'de elektronik imza kullanımı hızla yaygınlaştırılırken ve dijitalleşme projeleri büyük bir hevesle hayata geçirilirken, farklı toplumsal kesimler için oluşabilecek risklerin yönetimi konusunda aynı hassasiyetin gösterilmediği endişeyle izlenmekte, büyük ölçekli projeler yürütülürken, şeffaflık ve hesap verilebilirliğin yeterince önemsenmediği görülmektedir.

Bu yaklaşımın sonuçları, ne yazık ki son yıllarda iki önemli olayla somutlaşmıştır. İlk olarak, 2023 yılında milyonlarca vatandaşımızın kimlik numarası, cep telefonu, adresi ve diğer kişisel bilgilerini içeren kamu kayıtları çalınarak satışa sunulmuş, Ağustos 2025'te ise sahte elektronik imzaların üretilerek sahte diplomaların oluşturulması gibi birçok yasadışı işlemde kullanıldığı ortaya çıkmıştır. Aynı dönemlerde BMO sorumluların tespit edilmesine ve bağımsız denetimlerin yapılmasına ilişkin taleplerini kamuoyuyla paylaşmıştır.

Bu doküman, dijital altyapımızdaki güvenlik zafiyetleri ve veri mahremiyeti konusundaki ihmallerin açık bir göstergesi olan olaylara ilişkin araştırma bulguları ve politika önerilerini bir araya getirerek kamuoyuyla paylaşmaktadır.

Kamuoyunun bilgilerine sunarız.
Saygılarımızla,
TMMOB Bilgisayar Mühendisleri Odası
7. Dönem Yönetim Kurulu

TEKNİK BULGULAR

1. Kimlik verilerinin geçmişte birkaç defa çalındığı, hatta kamuya açık paneller üzerinde servis edildiği biliniyor iken, bunun olası sonuçları üzerinde bir etki analizi yapılmadığı, etkilenebilecek sistemler ve iş süreçleri üzerinde gerekli değişikliklerin yapılmadığı anlaşılmaktadır.
2. Elektronik imza edinme süreçlerinde kimlik bilgileri üzerinde kontrol yapılmış, en basit ticari uygulamalarda bile karşılaşılabilecek iki aşamalı doğrulama yöntemi kullanılmamıştır. Özellikle kamusal işlemler yürütülürken kullanılan ve TUBİTAK'a bağlı Kamu Sertifikasyon Merkezi tarafından sağlanan elektronik imzaların çıkarılmasında ve yenilemesinde kolaylıkla yürütülebilecek kontrol mekanizmaları sistem akışında yer almamaktadır ya da işletilmemiştir.
3. E-İmza kullanımı ile yapılan işlemlerin genellikle kurumsal uygulamalara paralel ya da bütünleşik olarak çalışan Elektronik Belge Yönetim Sistemi (EBYS) uygulamaları üzerinden yürütüldüğü bilinmektedir. EBYS uygulamalarında kurumdaki imza hiyerarşisi ve yetki devirleri çerçevesinde gerçekleştirilen (tamamlanmayan, iptal edilen, düzeltme işlemine tabi tutulanlar da dahil) tüm işlemlerin güncesinin ("log") tutulması zorunludur. Söz konusu günceler üzerinden yapılan iş ve işlemlerin geriye dönük olarak elde edilmesi, paraf, imza ve onayların hangi kayıtlar üzerinde, hangi tarihte, hangi kullanıcılar tarafından yapıldığının ortaya çıkarılması mümkün olmalıdır. Buna rağmen bu konuda somut açıklamaların yapılmaması; bazı sistemlerin hatalı tasarlandığına, bazı durumlarda eksik kullanıldığına ya da bu bilgilerin bir şekilde yok edildiğine ilişkin şüpheler oluşturmaktadır.
4. Yukarıda belirtilen günce tutma süreci; hayatın olağan akışı dışındaki istisnai iş ve işlemler yürütülürken (not ortalaması değiştirme, diplomanın sahibini değiştirme, daha önce açıklanmış bir sınav sonucunu değiştirme vb.) daha da hassas tutulmalıdır. Sadece işlemlerin gerçekleştirildiği kullanıcı, tarih ve bilgisayar bilgilerini değil, kayıtların eski ve yeni durumlarının da kurumsal uygulama tarafında tutulması önem arz etmektedir. Buna paralel olarak söz konusu süreçlerin herhangi bir bilgi olmadan ve bir iş akış/onay mekanizması yaşanmadan gerçekleşemeyeceği düşünüldüğünde EBYS tarafında da güncelerin bulunması, iş ve işlemin gerçekleşmesinde yaşanan dolandırıcılıkların yakalanması bakımından kritik önem arz etmektedir.

5. Kamuoyuna yansıyan bilgilerden; genellikle bürokraside üst düzey görev alan yöneticilerin e-imzalarının kopyalanarak veri değişikliği yapıldığından bahsedilmektedir. Bu işlemler eğer uygulama üzerinden doğrudan, herhangi bir paraf, imza, onay vb. süreci yürütülmeden yapılabiliyorsa, bu ciddi bir tasarım ve/veya yetkilendirme hatasına işaret etmektedir. Kurumsal yapının gereği olarak tüm iş ve işlemlerde yürütülmesi gereken belli bir iş süreci söz konusudur, buna paralel olarak o işleme özgü hiyerarşi içinde her bir kullanıcının yapacağı yetkiler sınırlıdır. Üst yönetim yetkisinde bir kullanıcının; sisteme giriş yaparak doğrudan veri girişi, güncellemesi ya da silme işlemi yapması gerçek e-imza ile dahi mümkün olmamalı, bu tip kritik veri güncellemeleri de ayrı olarak tasarlanmış bir iş akışı çerçevesinde gerçekleştirilmelidir. Skandalda sözü geçen ve kamusal işlem yürüten kurumlarda geliştirilen uygulamalarda bu prensiplerin uygulanmadığı, gerçek e-imza ile dahi yapılmaması gereken işlemlerin sahte e-imzayla yapılarak işlemlerin sonuçlandırıldığı görülmektedir.
6. İşlemler uygulama üzerinden değil, e-imza kullanımı ile veri tabanına erişim sağlanarak gerçekleştirilmişse bu çok daha kötü bir duruma karşılık gelmektedir. Veri tabanına üstelik sadece sorgulama da değil, güncelleme hakkına erişen doğrudan erişim yetkisinin e-imza ile ilişkilendirilmesi üst düzey bir güvenlik açığı olarak düşünülmelidir.

POLİTİKA ÖNERİLERİ

1. **E-İmza Edinme Süreçlerinin Güncellenmesi:** E-İmza oluşturma ve edinme süreçlerinin yeniden ele alınması, kontrollerin farklı mekanizmalarla güçlendirilmesi, birden fazla e-imzanın edinilmesinin (varsa istisnai durumlar haricinde) engellenmesi gerekmelidir.
2. **Bağımsız Mesleki İnceleme:** Yaşanan dolandırıcılıkların, tüm yönleriyle aydınlatılabilmesi için, ilgili kurum çalışanlarının ve meslek odamızın temsilcilerinin de içinde yer alacağı, bağımsız ve teknik uzmanlardan oluşan bir çalışma grubunun ivedilikle oluşturulması talep edilmeli, süreç sadece adli vaka olmaktan ve atanacak bilirkişilerin raporlarından ibaret kılınmamalıdır.
3. **Uygulamaların Gözden Geçirilmesi:** Yapılacak araştırmaların bulgularından hareketle, ilgili tüm uygulamalar gözden geçirilmeli, ortaya çıkan hatalı iş akışları giderilmeli ve güvenlik açıkları ivedilikle kapatılmalıdır.
4. **Sistem Bağımlılıkları Raporlaması:** İlerde oluşabilecek veri çalınmalarının olası sonuçlarının hızla analiz edilmesi ve müdahalelerin yapılması için e-devlet kapsamında hizmeti verilen, ancak farklı kurum ve kuruluşlarda çalışan uygulamaların birbirlerine olan bağımlılıkları rapor haline getirilmeli ve düzenli güncellenmesi sağlanmalıdır.
5. **Güncelerin ("Log") Saklanması:** Kamu kurum ve kuruluşlarında yürütülen iş ve işlemlere ilişkin güncelerin oluşturulması, kurum ve genel devlet yapısı içinde arşivlenmesi için yasal mevzuat oluşturulmalı ve uygulamaya geçirilmelidir.
6. **Dokümantasyon Hazırlanması ve Güncellenmesi:** Uygulamaların hazırlanmasına esas olan Sistem Gereksinimleri Belirtimi, Sistem Analiz Raporu ve buna benzer dokümanların mesleki standartlara uygun olarak hazırlanması, özellikle değişen gereksinimler doğrultusunda uygulamada yapılan değişikliklerin söz konusu dokümanlara yansıtılması ve bu sürecin meslek odaları tarafından denetlenmesi için gerekli yasal altyapı hazırlanmalıdır.
7. **Kamu adına Mesleki Denetim Gereksinimi:** Büyük ölçekli bilişim projelerinin başta meslek odaları olmak üzere sivil toplum kuruluşlarının ve bağımsız uzmanlarca denetlemensinin gerekliliği vurgulanmalı, bu konuda usul ve esasların belirlenmesi için çalışmaların acilen başlatılması konusunda inisiyatif alınmalıdır. Kamusal denetim ile hem olası hataların oluşması engellenecek, hem de sistemlerin daha hayata geçmeden şeffaflaşması sağlanacaktır.

8. **Yurttaş Odaklı Koruma:** Mağdur durumda olan veya veri güvenliği riski altında bulunan vatandaşlarımıza yönelik, somut adımlardan oluşan bir önlem planı derhal açıklanmalıdır.
9. **Veri mahremiyeti ve bilgi güvenliği konusunda farkındalık ve duyarlılık:** Türkiye'de elektronik imza kullanımı hızla yaygınlaştırılırken ve dijitalleşme projeleri hayata geçirilirken, riskler ve bunların yönetimi konusunda duyarlılık yaratacak, her yaştan ve her eğitim düzeyindeki insanın farkındalığını arttıracak çalışmalar başta eğitim olmak üzere her alanda yaygınlaştırılmalıdır.
10. **E-seçim Uyarıları:** Yaşanan bu güvenlik krizleri göz önünde bulundurularak, demokratik meşruiyetin en temel kaynağı olan seçimlerle ilgili olarak hükümetin e-seçim sistemi geliştirilmesi ve kullanılmasına yönelik girişimlerinin son derece sakıncalı olacağı kamuoyu gündemine taşınmalı, yurttaşlar, bu hayati konuda duyarlı olmaya ve mücadeleye davet edilmelidir.