TRABZON ÜNİVERSİTESİ

A.3.1.11. TRÜ bilgi yönetim sisteminin güvenliğini sağlaması konusunda yazılım geliştiriciler tarafından yapılan düzenlemelere ilişkin kanıtlar

Kurumumuzun bilgi yönetim sisteminin güvenliğini sağlaması konusunda yazılım geliştiriciler tarafından yapılan düzenlemeler aşağıdaki gibidir:

1-Sorgu sonuçlarının uygulama bileşenleri ve internet tarayıcısı içerisinde açık metin olarak erişiminin engellenmesi, maskeleme işleminin sunucu tarafında yapılması, servisten dönen veri ve/veya verilerin herhangi bir şekilde tarayıcıların geliştirme ortamlarında saklanmaması ve/veya loglanmaması bunun yanı sıra tarayıcıların kalıcı ve/veya geçici saklanma alanlarında (local storage, çerez veya tablo) verilerin kaydedilip işlenmemesi ve işlenmeye açık halde tutulmaması, (alternatif 1)

Madde 1 cevap: Sorgu sonuçlarının uygulama bileşenleri ve internet tarayıcısı üzerinde açık erişimi bulunmamaktadır. Maskeleme işlemi sunucu tarafında yapılmaktadır, servisten dönen veri tarayıcıların geliştirme ortamında tutulmayıp, loglanmamaktadır ve herhangi bir kayıt / işlenme durumu bulunmamaktadır.

2-Sorgulama yapılan sonuçlar herhangi bir şekilde bir servis (api) vasıtasıyla ön yüze servis ediliyorsa ilgili servisin erişimlerinin domain bazlı CSRF ataklarına karşı gerekli önlemlerin alınması

Madde 2 cevap: Uygulamada crosssite scripting ataklarına karşı engelleme vardır. Ayrıca Webapplication Firewall ile her türlü injection ataklarına karşı sistemin savunması bulunmaktadır.

3-Sorgulama yapan son kullanıcılar için rol bazlı yetkilendirme yaparak, tesis edilen işlem ölçüsünde veriye erişebilmesinin sağlanması,

Madde 3 cevap: Sorgulamalar rol bazlı yetki ile kontrol edilerek erişime izin verilmektedir. Ayrıca her kullanıcının sadece kendi verilerine erişim izni vardır.

4-Kimlik Paylaşımı Sisteminden sorgu yapılabilen bilgisayarlarda belirli bir süre işlem yapılmaması halinde oturumlarının sonlandırılması,

Madde 4 cevap: Sistemde maximum oturum süresi varsayılanda 20 dakika olarak belirlenmiştir.

5-KPS'den elde edilen kişisel bilgilerin kendi iş ve işlemlerini gerçekleştirmek üzere kurum sistemlerine kayıt edilmesinin zorunlu olması halinde, buradan yapılan/yapılacak sorgulamaların geri izleme kayıtlarının KPS Yönetmeliğine uygun olarak tutulması ve bu verilere yurt dışı IP lerden erişimin engellenmesi,

Madde 5 cevap: Kurum sisteminde sorgulanan kayıtların geriye dönük izleme kayıtları KPS yönetmeliğe uygun olarak tutulmaktadır. Yapılan bu sorgulamalar üzerinde yerel ve yurtdışı IP kontrolleri yapılmaktadır.

6- KPS'de kullanıcılar sorgu istediğinde bulunduklarında sistem tarafından oluşturulan token I saat süreyle geçerli olup kullanım alışkanlıkları dikkate alındığında her sorgu istediğinde tekrar yetki alma talebi ile birlikte token üretildiği ve bir önceki geçerli token'ın kullanılmadığı görülmüştür. Bu durum sistem üzerinde yük oluşturduğundan, sistemin hızlı ve verimli çalışması açısından sorgu isteklerinde I saat süre ile geçerli olan token'ların kullanılması ve süre bittikten sonra yeni token isteği oluşturulması,

Madde 6 cevap: Sorgularda token ile ilgili bir yavaşlık olmaması için servislere atılan sorgular ve mevcut veriler kontrol edilerek veri yok ise servise gidilir ve veri var ise servise gidilmemesinden dolayı stabillik sağlanmaktadır.

7- Elde edilen verilerin kullanımıyla ilgili tüm personellerin 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında eğitilmesi,

Madde 7 cevap: Personellerin konu hakkında kanun kapsamın eğitimi gerçekleştirilmektedir.