GENELGE

Cumhurbaşkanlığından:

Konu: Bilgi ve İletişim Güvenliği Tedbirleri

GENELGE
2019/12

Bilginin dijital ortamlara taşınması, bilgiye erişimin kolaylaşması, altyapıların dijital hale gelmesi ve bilgi yönetim sistemlerinin yaygın olarak kullanılması, ciddi güvenlik risklerini beraberinde getirmektedir. Karşılaşılan güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla aşağıdaki tedbirlerin alınması uygun görülmüştür.

1. Nüfus, sağlık ve iletişim kayıt bilgileri ile genetik ve biyometrik veriler gibi kritik bilgi ve veriler yurtiçinde güvenli bir şekilde depolanacaktır.

2. Kamu kurum ve kuruluşlarında yer alan kritik veriler, internete kapalı ve fiziksel güvenliği sağlanmış bir ortamda bulunan güvenli bir ağda tutulacak, bu ağda kullanılacak cihazlara erişim kontrollü olarak sağlanacak ve log kayıtları değiştirilmeye karşı önlem alınarak saklanacaktır.

3. Kamu kurum ve kuruluşlarına ait veriler, kurumların kendi özel sistemleri veya kurum kontrolündeki yerli hizmet sağlayıcılar hariç bulut depolama hizmetlerinde saklanmayacaktır.

4. Mevzuatta kodlu veya kriptolu haberleşmeye yetkilendirilmiş kurumlar tarafından geliştirilen yerli mobil uygulamalar hariç olmak üzere, mobil uygulamalar üzerinden, gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

5. Sosyal medya üzerinden gizlilik dereceli veri paylaşımı ve haberleşme yapılmayacaktır.

6. Sosyal medya ve haberleşme uygulamalarına ait yerli uygulamaların kullanımı tercih edilecektir.

7. Kamu kurum ve kuruluşlarınca gizlilik dereceli bilgilerin işlendiği yerlerde yayma güvenliği (TEMPEST) veya benzeri güvenlik önlemleri alınacaktır.

8. Kritik veri, doküman ve belgelerin bulunduğu ve/veya görüşmelerin gerçekleştirildiği çalışma odalarında/ortamlarında mobil cihazlar ve veri transferi özelliğine sahip cihazlar bulundurulmayacaktır.

9. Gizlilik dereceli veya kurumsal mahremiyet içeren veri, doküman ve belgeler kurumsal olarak yetkilendirilmemiş veya kişisel olarak kullanılan cihazlarda (dizüstü bilgisayar, mobil cihaz, harici bellek vb.) bulundurulmayacaktır.

10. Kişisel olarak kullanılanlar da dâhil olmak üzere kaynağından emin olunmayan taşınabilir cihazlar (dizüstü bilgisayar, mobil cihazlar, harici bellek/disk, CD/DVD vb.) kurum sistemlerine bağlanmayacaktır. Gizlilik dereceli verilerin saklandığı cihazlar, ancak içerisinde yer alan veriler donanımsal ve/veya yazılımsal olarak kriptolanmak suretiyle kurum dışına çıkarılabilecek; bu amaçla kullanılan cihazlar kayıt altına alınacaktır.

11. Yerli ve milli kripto sistemlerinin geliştirilmesi teşvik edilerek, kurumlara ait gizlilik dereceli haberleşmenin bu sistemler üzerinden gerçekleştirilmesi sağlanacaktır.

12. Kamu kurum ve kuruluşlarınca temin edilecek yazılım veya donanımların kullanım amacına uygun olmayan bir özellik ve arka kapı (kullanıcıların bilgisi/izni olmaksızın sistemlere erişim imkânı sağlayan güvenlik zafiyeti) açıklığı içermediğine dair üretici ve/veya tedarikçilerden imkânlar ölçüsünde taahhütname alınacaktır.

13. Yazılımların güvenli olarak geliştirilmesi ile ilgili tedbirler alınacaktır. Temin edilen veya geliştirilen yazılımlar kullanılmadan önce güvenlik testlerinden geçirilerek kullanılacaktır.

14. Kurum ve kuruluşlar, siber tehdit bildirimleri ile ilgili gerekli tedbirleri alacaktır.

15. Üst düzey yöneticiler de dahil olmak üzere, personelin sistemlere erişim yetkilendirmelerinin, fiilen yürütülen işler ve ihtiyaçlar nazara alınarak yapılması sağlanacaktır.

16. Endüstriyel kontrol sistemlerinin internete kapalı konumda tutulması sağlanacak, söz konusu sistemlerin internete açık olmasının zorunlu olduğu durumlarda ise gerekli güvenlik önlemleri (güvenlik duvarı, uçtan uca tünelleme yöntemleri, yetkilendirme ve kimliklendirme mekanizmaları vb.) alınacaktır.

17. Milli güvenliği doğrudan etkileyen stratejik önemi haiz kurum ve kuruluşların üst yöneticileri ile kritik altyapı, tesis ve projelerde görev alacak kritik önemi haiz personel hakkında ilgili mevzuat çerçevesinde güvenlik soruşturması veya arşiv araştırması yaptırılacaktır.

18. Kamu e-posta sistemlerinin ayarları güvenli olacak biçimde yapılandırılacak, e-posta sunucuları, ülkemizde ve kurumun kontrolünde bulundurulacak ve sunucular arasındaki iletişimin şifreli olarak yapılması sağlanacaktır.

19. Kurumsal olmayan şahsi e-posta adreslerinden kurumsal iletişim yapılmayacak, kurumsal e-postalar şahsi amaçlarla (özel iletişim, kişisel sosyal medya hesapları vb.) kullanılmayacaktır.

20. Haberleşme hizmeti sağlamak üzere yetkilendirilmiş işletmeciler Türkiye'de internet değişim noktası kurmakla yükümlüdür. Yurtiçinde değiştirilmesi gereken yurtiçi iletişim trafiğinin yurtdışına çıkarılmamasına yönelik tedbirler alınacaktır.

21. İşletmeciler tarafından, kritik kurumların bulunduğu bölgelerdeki veriler, radyolink ve benzeri yöntemlerle taşınmayacak, fiber optik kablolar üzerinden taşınacaktır. Kritik veri iletişiminde, radyolink haberleşmesi kullanılmayacak; ancak kullanımın zorunlu olduğu durumlarda veriler milli kripto sistemlerine sahip cihazlar kullanılarak kriptolanacaktır.

Güvenlik risklerinin azaltılması, etkisiz kılınması ve özellikle gizliliği, bütünlüğü veya erişilebilirliği bozulduğunda milli güvenliği tehdit edebilecek veya kamu düzeninin bozulmasına yol açabilecek kritik türdeki verilerin güvenliğinin sağlanması amacıyla ulusal ve uluslararası standartlar ve bilgi güvenliği kriterleri çerçevesinde, kamu kurum ve kuruluşları ile kritik altyapı niteliğinde hizmet veren işletmelerde uygulanmak üzere farklı güvenlik seviyeleri içeren "Bilgi ve İletişim Güvenliği Rehberi" Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı koordinasyonunda, ilgili kamu kurum ve kuruluşları tarafından gereken katkı sağlanarak hazırlanacak ve *www.cbddo.gov.tr* adresinde yayımlanacaktır. Rehber ihtiyaçlar, gelişen teknoloji, değişen şartlar ile Ulusal Siber Güvenlik Stratejisi ve eylem planlarında yapılacak değişiklikler göz önünde bulundurularak güncellenecektir.

Tüm kamu kurum ve kuruluşları ile kritik altyapı hizmeti veren işletmelerde yeni kurulacak bilgi sistemlerinde, Rehberde yer verilen usul ve esaslara uyulması zorunludur. Mevcut bilgi teknolojisi altyapıları, güvenlik seviyesi öncelikleri dikkate alınarak yayımlanmasını müteakip Rehberde yer alacak plan çerçevesinde kademeli olarak bu esaslara uyumlu hale getirilecektir. Uyum çalışmalarında ve yeni kurulacak bilgi sistemlerinde, belirtilen adreste yayımlanan güncel sürüm dikkate alınacaktır.

Milli güvenliğin sağlanması ve gizliliğin korunması kapsamında yürütülen görev ve faaliyetler hariç olmak üzere kurum ve kuruluşlar, Rehberin uygulanmasına ilişkin denetim mekanizmalarını oluşturacak ve yılda en az bir defa uygulamayı denetleyecektir. Denetim sonuçları ile yapılan düzeltici ve önleyici faaliyetler, Rehberde belirtilen usul ve esaslara göre bir rapor halinde Dijital Dönüşüm Ofisine iletilecektir.

Bilgilerini ve gereğini rica ederim.

5 Temmuz 2019

Recep Tayyip ERDOĞAN
CUMHURBAŞKANI